معوقات إثبات الجرائم المتعلقة بتقنية المعلومات

الباحث/ منصور فهيد سعيد الحارثي

باحث بكلية الحقوق- جامعة الزقازيق

إشراف

أ.د. عبد التواب معوض الشربجي

أستاذ القانون الجنائي- كلية الحقوق- جامعة الزقازيق

(ISSN: 2537 - 0758)

معوقات إثبات الجرائم المتعلقة بتقنية المعلومات

الباحث/ منصور فهيد سعيد الحارثي

ملخص

تثير الجريمة المعلوماتية نظرا لخصوصيتها، مشكلة عدم كفاية إجراءات التحري والتحقيق التقليدية في الحصول على الدليل الرقمي الناتج عن ارتكابها، مما أدى إلى ضرورة التطوير في هذه الإجراءات من خلال التطوير في الأحكام العامة للإجراءات التقليدية، وعن طريق خلق إجراءات حديثة مختلفة عن تلك المتبعة في سبيل مكافحة الجرائم العادية.

على الرغم من الجهود المبذولة في مكافحة الجريمة المعلوماتية، إلا أن هناك بعض المعوقات في إثبات الجريمة المعلوماتية. وقد يكون مصدر صعوبة الدليل في أن أجهزة الحاسب الآلي، وحسب نظمها، لا يمكن فيها أن تتبع الطريق العكسي لما يخرج منها، يمكن القول بأن الدليل المتحصل من الوسائل المعلوماتية يستمد طبيعته من ذات العمليات المعلوماتية التي نتج منها في حالة الاعتداء عليها بالأفعال غير المشروعة، ولذلك فهو يتخذ أيضا طبيعة الكترونية بحيث تصعب على المحقق الا بأتباع إجراءات معينه يكون الغالب منها ذو طبيعة فنية.

كثيرا ما يكون ضحايا الجرائم المعلوماتية هم السبب في تصعيب اكتشاف هذه الجرائم لعدة أسباب منها نقص الخبرة الفنية التقنية، وعدم اتخاذ الحيطة والحذر، والامتناع عن الإبلاغ عن الجريمة المعلوماتية، وعدم إدراك خطورة هذا النوع من الجرائم، كما أن الجرائم المعلوماتية لاتصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، ولا تترك خلفها اثأرا مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة، وجثة المجني عليه في القتل.

كما ان هناك صعوبات تتعلق بجهة التحقيق، منها نقص المعرفة الفنية لدى سلطات التحقيق، ولدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة المعلوماتية عن طريق الحاسب الآلي وكيفية التعامل معها، وضعف التعاون الدولى فى مواجهة جرائم تقنية المعلومات.

ولمواجهة أي معوقات تتعلق بالجرائم المعلوماتية فإنه يجب ابتداء تفعيل عدة أمور لمكافحة الجرائم المعلوماتية وإمكانية ضبط الأدلة الجنائية مثل تفعيل دور الضبط

الإداري، التدريب التخصصي لجهات التحقيق، والاستعانة بالخبرة في هذا المجال والتنسيق بين الخبير المعلوماتي والمحقق الجنائي قبل محاكمة الجاني في الجريمة المعلوماتية.

كما يجب تفعيل وزيادة التعاون الدولي في مكافحة الجريمة المعلوماتية ضرورة رسم سياسة جنائية متناسقة من اجل الأجرام المعلوماتي عن طريق التدخل بالتقويم للأنشطة الإجرامية المعلوماتية، مع الأخذ في الاعتبار أهمية الاتفاق على ماهية الأنشطة التي يضفي عليها التجريم المعلوماتي حتى يؤدي هذا التجريم ثماره وتسد الثغرات في وجه المجرمين المعلوماتيين.

المقدمة

على الرغم من المزايا الهائلة التي تحققها تقنية المعلومات في شتى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل ظهور الجرائم المعلوماتية، التي تمتاز بسمات متميزة عن الجرائم التقليدية، الأمر الذي أثار مشكلة عدم إمكانية تطبيق النصوص الموضوعية التقليدية لقانون العقوبات، فتبلورت لدى الدول فكرة وضع نصوص قانونية خاصة إلا أنها اختلفت في أسلوب المعالجة التشريعية لذلك، فبالنظر إلى الطبيعة الخاصة للجرائم المتعلقة بشبكة الانترنت والقدرة على ارتكابها عبر الحدود وتميزها بالعالمية، فيتعين أن تواكب القواعد القانونية الموضوعية هذا التغيير فى نمط الجريمة لتحقيق العدالة الجنائية فى الملاحقة والمساءلة[1].

كما تثير الجريمة المعلوماتية من جهة أخرى نظرا لخصوصيتها، مشكلة عدم كفاية إجراءات التحري والتحقيق التقليدية في الحصول على الدليل الرقمي الناتج عن ارتكابها، مما أدى إلى ضرورة التطوير في هذه الإجراءات من خلال التطوير في الأحكام العامة للإجراءات التقليدية، وعن طريق خلق إجراءات حديثة مختلفة عن تلك المتبعة في سبيل مكافحة الجرائم العادية.

على الرغم من الجهود المبذولة في مكافحة الجريمة المعلوماتية، إلا أن هناك بعض المعوقات في إثبات الجريمة المعلوماتية. لذلك سوف نتناول هذا البحث من خلال المباحث التالية:

المبحث الأول: الصعوبات المتعلقة بالدليل ذاته.

---

[1] د. حسين بن سعيد الغافرى، السياسة الجنائية فى مواجهة جرائم الانترنت "دراسة مقارنة"، دار النهضة العربية، ٢٠٠٩، ص٧٥.

(ISSN: 2537 - 0758)

المبحث الثانى: الصعوبات المتعلقة بجهات التحقيق.
المبحث الثالث: معوقات الحصول على الأدلة وضخامة البيانات المتعلقة بالجريمة.

المبحث الأول
الصعوبات المتعلقة بالدليل ذاته

تمهيد وتقسيم:

في الجريمة التقليدية، فإن دليل الإثبات فيها يكون مرئية من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب، وكذلك المادة السامة التي استعملت في القتل، أو المحرر ذاته الذي تم تزويره، أو النقود التي زينت وأدوات تزييفها، وفي كل هذه الأمثلة يستطيع رجل الضبط أو التحقيق الجنائي رؤية الدليل المادي وملامسته بإحدى حواسه. ولكن في الجريمة المعلوماتية عن طريق الحاسب الآلي، فإن الوسيلة المستخدمة عبارة عن نبضات إلكترونية غير مرئية تتم عبر أجزاء الحاسب الآلي والشبكة، كما تنساب الكهرباء عبر الأسلاك، فهي غير مرئية، ولا يقف الأمر عند حد عدم الرؤية، لكنها غالباً مشفرة بحيث لا يمكن للإنسان قراءتها، بل تقرأها الآلة وتظهر على شاشة الحاسب الآلي، ولذلك يمكن للمجرم أن يطمس دليل جريمته طمسة كام ولا يترك وراءه أي أثر، ومن ثم يتعذر إن لم يسكن مستحي" ملاحقته أو كشف شخصيته.

والدليل هو أداة الإثبات عموماً، ويقصد بهذا الإثبات القواعد المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء وتقديرها من جانبه للوصول إلى حكم بشأن الواقعة محل الإثبات، ويقتصر الإثبات على إثبات الوقائع لا بيان وجهة نظر المشرع وحقيقة قصده، فالبحث في هذا يتعلق بتطبيق القانون وتفسيره وهو من عمل المحكمة، وينقسم الإثبات إلى نوعين، الإثبات بالأدلة المباشرة والتي هي الاعتراف والشهادة والخبرة والمعاينة لمسرح الواقعة، والإثبات بالأدلة غير المباشرة والتي يصل القاضي إلى الحقيقة منها عن طريق الاستقراء والاستنتاج، وهذا الإثبات في نوعية يخضع لمبدأ الإثبات الحر والذي يعتمد على حرية القاضي الجنائي في الإقناع، فالدليل الجنائي معنى يدرك من مضمون واقعه تؤدي إلى ثبوت الإدانة أو ثبوت البراءة، ويم ذلك باستخدام الأسلوب العقلي وأعمال المنطق في وزن وتقدير تلك الواقعة، ليصبح المعنى المستمد منها أكثر دقه في الدلالة على الإدانة أو البراءة[٢].

[٢] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، مصر، ٢٠٠٧، ص ٥٨.

فأهمية الدليل في المواد الجنائية أهمية عظيمة لأنه هو الذي يناصر الحقيقة ويبين مرتكبها، وهو الذي يحول الشك إلى يقين، فالحقيقة في معناها العام تعني معرفة حقيقة الشيء بأن يكون أو لا يكون، وهذا لا يتحقق إلا بالدليل بحسبان أنه المعبر عن هذه الحقيقة، وان إجراءات جمع الأدلة لم ترد في القانون على سبيل الحصر، ولذلك يجوز للمحقق أن يباشر أي إجراء أخر يرى فيه فائدة للإثبات طالما انه لا يترتب على اتخاذه تقييد الحريات الأفراد أو مساس بحرمة مساكنهم(٣).

وقد يكون مصدر صعوبة الدليل في أن أجهزة الحاسب الآلي، وحسب نظمها، لا يمكن فيها أن تتبع الطريق العكسي لما يخرج منها، بمعنى لو طبعت ورقة تحتوى على بيانات مخزنة من جهاز الحاسب الآلي، فلا يمكن معرفة من قام بطباعتها وغرض الطباعة إلى خلافه، وحتى لو جدت هذه الخاصية فإنه يتعين على من يقوم بالتحليل أن يكون متخصصاً وعلى مستوى عال من التدريب والتقنية في علوم الحاسب الآلي وهو ما لم يتوافر لدى رجل الأمن العادي أو المحقق العادي. ولذلك يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسئولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم، وهذا يقتضي توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم المعلوماتية، وبمعنى آخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال، للاستعانة بها في التحقيق في هذه الجرائم ويتعين عدم التذرع بالميزانيات المالية كسبب يحول دون قيام الدول بواجباتها نحو تحقيق العدالة الجنائية، وحتي يتم ذلك يرى هذا الجانب ضرورة الاستعانة بالنخبة المتخصصة في الحاسب الآلي حال تحقيق الجريمة المعلوماتية عن طريق الحاسب الآلي وذلك لضبط هذه الجرائم واكتشافها، وتقديم أدلة الإدانة فيها، وشرح هذه الأدلة وأبعادها أمام المحاكم. ونرى ذلك شرط أن يتم في إطار القانون الجنائي وخصوصا قواعد الخبرة أمام المحاكم والتي ينظمها قانون الإجراءات الجنائية(٤).

وعلى ضوء ذلك يمكن القول بأن الدليل المتحصل من الوسائل المعلوماتية يستمد طبيعته من ذات العمليات المعلوماتية التي نتج منها في حالة الاعتداء عليها بالأفعال

---

(٣) د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، ص٣٦٩.

(٤) د. محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات، ٢٠٠٠، ص٥٢.

(ISSN: 2537 - 0758)

غير المشروعة، ولذلك فهو يتخذ أيضا طبيعة الكترونية بحيث تصعب على المحقق الا بأتباع إجراءات معينه يكون الغالب منها ذو طبيعة فنية، وليس أدل على ذلك من أن التلاعب في المستندات المعلوماتية لا يمكن كشفه بالطرق التقليدية وإنما قد يحتاج ذلك إلى أدلة الكترونية قد تتحصل من الوسائل المعلوماتية ذاتها أو باستخدام التقنية العلمية المتقدمة التي يتعين إتباعها للوصول إليه[٥].

وعليه سوف نقسم هذا المبحث إلى ثلاثة مطالب على ضوء الصعوبات التي تواجه سلطة الاستدلال والتحقيق الجنائي في استخلاص الدليل، وهي عدم ظهور الدليل المادي وطبيعة المجني علية بالجرائم المعلوماتية وفقدان أثار الجريمة.

المطلب الأول: عدم ظهور الدليل المادى.

المطلب الثانى: طبيعة المجنى علية فى هذه الجرائم.

المطلب الثالث: فقدان آثار الجريمة.

المطلب الأول
عدم ظهور الدليل المادي

إن من أبرز خصائص الجريمة المعلوماتية هو وقوعها في بيئة الكترونية وهذه الخاصية تترتب عليها جمله نتائج تصعب من مهمة اكتشاف هذه الجرائم لا بل وحتى التحقيق فيها.

وهذا عكس الجرائم التقليدية، فرجل الشرطة الذي يقوم بجمع التحريات في واقعة سرقة حتى يصل المتهم، ويستصدر امرأ بالقبض عليه وتتولى جهات التحقيق استجوابه وأحالتها إلى محكمة الموضوع، فكل هذه وقائع خاضعة السيطرة أجهزة العدالة، والدليل فيها مرئي ومقروء، عكس الجريمة المعلوماتية التي تتم دون رؤية لدليل الإدانة، وحتى في حالة وجود الدليل يمكن للجاني طمس الدليل او محوه وفي حضور أجهزة العدالة غير المتخصصة، ولذلك فغالبية الجرائم المعلوماتية تكتشف مصادفة وليس بطريق الإبلاغ عنها[٦].

---

[٥] د. خالد ممدوح إبراهيم، التقاضي الالكتروني، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٧ ص٣٢٣ وما بعدها.

[٦] د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٢، ص٢٤

لأنها لا تخلف في الغالب أية أثار مادية كتلك التي تخلفها الجرائم التقليدية، حيث أنها لا تخلف لا سكينة ولا سلاحا ولا ظروفا فارغة لطلقات نارية ولا بقعة دموية أو غير ذلك من الآثار المادية[٧].

كما أن أغلب الآثار المتخلفة عن هذه الجرائم هي أثار الكترونية وهذه الآثار بدورها أنما هي عبارة عن نبضات الكترونية غير مرئية بالعين المجردة[٨]، فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة بحيث انه لا يمكن رؤيتها ألا من خلال الاستعانة بأجهزة ووسائل تقنية تظهرها للعيان. إن ضخامة حجم وكم البيانات والملفات المعلوماتية التي تتواجد في البيئة المعلوماتية تصعب من أمكانية تحديد الملفات والبيانات المعلوماتية المجرمة، من بين ذلك الكم الهائل لفصلها عن تلك البريئة منها، وتؤدي في الغالب إلى اصطدام مهمة الاكتشاف بحق الأفراد في الخصوصية الشخصية.

أن البيئة المعلوماتية غالبا ما تكون مؤلفة من شبكات منتشرة في كافة أرجاء المعمورة ومرتبطة ببعضها البعض عن طريق شبكة الانترنيت، بحيث تتيح الفرصة أمام مجرمي المعلوماتية للولوج عن بعد إلى البيانات المعلوماتية المخزونة في أية بقعة من بقاع العالم[٩]، وعلى العكس من ذلك فأن سلطات الضبط القضائي والسلطات التحقيقيه لا يكون بإمكانها الولوج إلى تلك البيانات كونها تقع في الغالب خارج حدود اختصاص دولها، بحيث تصطدم بسيادة الدول الأخرى[١٠].

ولصعوبة استخلاص الدليل في مثل هذه الجريمة يرى المختصين في جرائم الحاسب الآلي، أن هذا الجهاز ومايقع علية من جرائم معلوماتية يعد تحديا هائلا لرجال الأمن،

---

[٧] د. عائشة بن قاره مصطفى، حجية الدليل الالكتروني في مجال الإثبات، دار الجامعة الجديدة، ٢٠١٠ ، ص ٦٢

[٨] د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنلوجيا الحديثة، دار النهضة العربية، ٢٠٠٢، ص١١٥

[٩] د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنلوجيا الحديثة، مرجع سابق، ص١٥

[١٠] تجدر الإشارة إلى أن الأدلة المتحصلة من الوسائل الالكترونية قد تنتمي إلى أدلة الإثبات التقليدية وذلك إذا كانت نتاج شهادة أو اعتراف أو خبره، فقد يمكن أثبات جرائم الاحتيال والسرقة والاختلاس في الجرائم الالكترونية عن طريق الوثائق الأصلية المحفوظة في الميكروفلم أو بالشريط الممغنط او بحافظات الأكواد أو بمخرجات الحاسب وسجلات التشغيل.

(ISSN: 2537 - 0758)

ذلك أن رجل الأمن غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادرة على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية عالية[١١].

ويعد انتحال الشخصية، وكذلك التسلل الإلكتروني من أبرز أمثلة السلوك الإجرامي في الجرائم المعلوماتية، وذلك كدليل على عدم رؤية دليل الجريمة، فكلاهما يستخدم أساليب عالية التقنية في الدخول إلى المناطق المؤمنة والمحمية إلكترونية أو الوصول إلى مراكز الحاسب الآلي والدخول إلى قواعد المعلومات، ويكون الدخول شخصية أو إلكترونية، فالدخول أو التسلل الإلكتروني، يتم عن طريق قيام الجاني بتوصيل جهازه إلى جهاز آخر له حق الدخول وذلك عن طريق خط هاتفي، وعندما يفتح الجهاز المتصل بمركز المعلومات والمسموح له بذلك، نجد أن جهاز الجاني يمارس نشاطه ويحصل على ذات المعلومات دون أن يراه أحد إلى أن يغلق الجهاز الأصلي صاحب الحق في الدخول، وهذه الجريمة وإن أمكن السيطرة عليها بوسائل متطورة وحراسة شخصية ومراقبة إلكترونية، فإن محاولات القراصنة والمحتالين في الجرائم المعلوماتية تتجاوز هذه الحراسات، ويتضح من خلال ما سبق، أنه عند كشف وتجميع الأدلة في الجرائم المعلوماتية عن طريق الحاسب الآلي تواجهه صعوبة بالغة سببها عدم رؤية الدليل أو عدم القدرة على استظهاره[١٢].

بينما في الجرائم المعلوماتية تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي مما تجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة[١٣].

لذلك يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم، وهذا يقتضي توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم المعلوماتية، وبمعنى أخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال،

---

[١١] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنه، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤، ص٢٣.

[١٢] د. عبد الناصر محمد فرغلى، محمد عبيد المسمارى، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، ٢٠٠٧، ص ٢٦

[١٣] د. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط١، ٢٠٠٨، ص ٥٦

للاستعانة بها في تحقيق هذه الجرائم، ويتعين عدم التذرع بالميزانيات المالية كسبب يحول دون قيام الدولة بواجباتها نحو تحقيق العدالة الجنائية، وحتي يتم ذلك يرى هذا الجانب ضرورة الاستعانة بالنبضة المتخصصة في الحاسب الآلي حال تحقيق الجرائم المعلوماتية وذلك لضبط هذه الجرائم واكتشافها، وتقديم أدلة الادانه فيها وشرح هذه الادله وإبعادها أمام المحاكم، ويجب أن يتم ذلك في أطار القانون الجنائي وخصوصا قواعد الخبرة أمام المحاكم الجنائية والتي ينظمها قانون الإجراءات الجنائية[١٤].

المطلب الثاني
طبيعة المجني عليه فى جرائم تقنية المعلومات عبر الانترنت

تتطلب الجرائم المعلوماتية على غرار الجرائم التقليدية حرفية عالية سواء عند ارتكابها أو عند العمل على اكتشافها من الشخص الذي يرتكبها، أي يجب ان يكون ذلك الشخص خبيرة بالقدر اللازم والكافي بأمور الحوسبة والانترنت ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي، وأن الشرطة تبحث أول ما تبحث عن خبراء الكومبيوتر عند ارتكاب هذا النوع من الجرائم[١٥].

لذلك يعمد الجاني إلى تشفير الملفات أو البيانات المعلوماتية التي تتضمن محتوى غير مشروع بغية منع الغير من الاطلاع عليها واكتشافها، كما هو الحال في حالة نقل البيانات المتعلقة بجرائم غسيل الأموال عبر الانترنت بعد تشفيرها[١٦].

ويحرص الجاني بعد ارتكابه لجريمته على محو أثارها التي تدل على وقوعها، وذلك من خلال التوسل بتقنيات معدة لهذا الغرض مع الأخذ بنظر الاعتبار سهولة وسرعة إمكانية محو وتعديل البيانات المعلوماتية التي يمكن القيام بها في أزمان قياسية متناهية القصر تقاس باللحظات والثوانى[١٧].

---

[١٤] د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات، ٢٠٠٠، ص ٥٢

[١٥] د. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت– دار الفكر الجامعي– الإسكندرية، ط ١، ٢٠٠٧، ص ٣٧ وما بعدها.

[١٦] د. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية) دار الجامعة الجديدة، الإسكندرية، ٢٠٠٩، ص ٥٨٦.

[١٧] د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع الشبكة الانترنت، طلا، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٤٢

(ISSN: 2537 - 0758)

بناء على ذلك كثيرا ما يكون ضحايا الجرائم المعلوماتية هم السبب في تصعيب اكتشاف هذه الجرائم لعدة أسباب وهي:

١- نقص الخبرة الفنية التقنية:

ان البيئة المعلوماتية عموما وعلى وجه الخصوص على شبكة الانترنيت توفر مناخا مثالية لاجتماع الفرائس بصياديها في بودقه واحدة، خصوصا وان اغلب مستخدمي هذه الشبكة لا تتوفر لديهم المعرفة التقنية اللازمة للتعرف على هذه الجرائم وأساليب ارتكابها، مما يجعلهم عرضة للاقتناص من قبل مجرمي المعلوماتية من دون أن يشعروا بذلك، فمثلا قد يرسل الجاني رسالة متضمنة الفيروس أو ملف تجسس خفي إلى الضحية

والتي تظهر في الغالب كرسالة، بحيث انه بمجرد قيام الأخير بفتح الرسالة، فأنه يتم إدخال الفيروس أو الملف ألتجسسي تلقائية إلى كمبيوتر الضحية ومن دون أن يشعر الأخير بذلك، كونه لا يعرف معنى الرسائل تلك ليقوم الفيروس في النهاية بإتلاف نظام الكومبيوتر أو أن يقوم الجاني بالولوج إلى كومبيوتر الضحية من خلال ملف التجسس، ومن دون أن يتمكن المجني عليه من اكتشاف ذلك، وحتى ولو اكتشفه فأن ذلك غالبا بعد مرور زمن طويل من وقوع الجريمة وبالتالي بعد فوات الأوان وبعد زوال أغلب أثارها[١٨].

٢- عدم اتخاذ الحيطة والحذر:

الكثير من ضحايا الجرائم المعلوماتية لا يتخذون الحيطة والحذر اللازمين لاكتشاف مثل هذه الجرائم في حال وقوعها فأغلب الإفراد من مستخدمي شبكة الانترنت لا يستخدمون برامج وتقنيات الحماية ضد الاختراق والتجسس والوقاية من الفيروسات، ما يترتب على ذلك عدم أمكان اكتشافهم للجريمة الواقعة لحظة ارتكابها وقد يكتشفونها بعد مرور مدة طويلة وقد لا يكتشفونها أبدا أن هذا الأمر يشمل حتى المؤسسات والشركات المالية والتجارية[١٩]، فهي لا تقوم بمراجعة حساباتها المالية والتجارية يومية ولا حتى شهريا لتكتشف مثل هذه الجرائم قبل فوات الأوان، وحتى ولو قامت بمثل هذه المراجعة فأنها غالبا ما تعتبر المفارقات الحاصلة في حساباتها مجرد مفارقات عادية ناجمة عن خسائرها الاعتيادية أو عن عمليات دفع أجله.

---

[١٨] د. محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، المحله الكبرى، ٢٠٠٨، ص ١٠٨

[١٩] د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٦، ص ٩٦.

كما وان هذه المؤسسات غالبا ما تتسابق مع بعضها البعض في توفير خدماتها للعملاء بأكبر قدر ممكن من التسهيلات بحيث توجه اهتمامها إلى تحسين وتسهيل الحصول على خدماتها على حساب نظامها الأمني، مما ينجم عنه بالتالي سهولة اختراق نظامها الأمني وفي الغالب من دون أن يكتشف أمر الاختراق[٢٠].

٣- الامتناع عن الإخبار:

تظل الجريمة المعلوماتية مستترة ما لم يتم الإبلاغ عنها، ومن ثم عمل الاستدلالات أو تحريك الدعوى الجنائية حسب النظام السائد، والصعوبة التي تواجهه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة العادية كما هو الحال في الجريمة التقليدية، وذلك لصعوبة اكتشافها من قبل الأشخاص العاديين أو حتى الشركات والمؤسسات التي وقعت مجني عليها في هذه الجرائم، أو لأن هذه الجهات تحاول إخفاء الأثر السلبي للإبلاغ عما وقع لها وحرصا على ثقة العملاء فلا تبلغ عن تلك الجرائم التي ارتكبت ضدها[٢١].

وتنطبق نفس الأحكام في الجرائم المعلوماتية، لكن المجني عليه في كثير من الأحيان يفضل عدم التبليغ عن الإصابة بفيروس وخاصة إذا كان المجني عليه مؤسسة مالية كبيرة كالبنوك، وذلك حتى لا تهتز ثقة المتعاملين معها ويترتب على ذلك سحب ودائعهم واستثماراتهم فيها[٢٢]، وكذلك تدخل هذه المؤسسات في اعتباراتها أن الإبلاغ عن الجرائم المعلوماتية التي وقعت ضدها ربما يؤدي إلى إحاطة المجرمين علما بنقاط الضعف في أنظمتها.

ولذلك يبدو لنا من الملائم لدى سلطات الأمن في الجرائم المعلوماتية واكتشافها أن ترصد ميدانية حركة المعاملات التجارية داخل المؤسسات المالية وحولها، وذلك عن طريق جمع المعلومات السرية عن حركة السوق وتداول الأموال والممتلكات والتغيرات الاجتماعية والسلوكية للموظفين وصغار رجال الأعمال الذين يرتبطون بمؤسسات الجريمة المنظمة، سيما وأن جرائم الحاسب الآلي هي من أدوات وأسلحة هذه الجريمة،

---

[٢٠] د. حسين بن سعيد الغافري، السياسية الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة،٢٠٠٩، ص ٥٢٣

[٢١] د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص٤٢

[٢٢] محمد أمين الرومي، جرائم الكومبيوتر والانترنت، دار المطبوعات الجامعية الاسكندرية، ٢٠٠٤، ص ٣١.

(ISSN: 2537 - 0758)

حيث يجري استقطاب صغار الموظفين وذوي القدرات الفنية والذين هم على مقربة من أسرار برامج الحاسب الآلي للمؤسسات المالية والشركات التجارية ويرتبط ذلك بضرورة تطوير ثقافة الحاسب الآلي في وسط رجال الأمن، وربط تلك الثقافة بالثقافة الأمنية في صورها التقليدية، وهو ما يضمن نجاحة للأجهزة الأمنية في مواكبة ظاهرة الجرائم المعلوماتية[٢٣].

٤- عدم أدراك خطورة الجرائم المعلوماتية[٢٤]:

إن كثيرا من ضحايا الجرائم المعلوماتية لا يدركون خطورة هذه الجرائم، لا بل وان بعضهم لا يتصور أمكانية وقوع مثل هذه الجرائم.

ويبدو أن معالجة هذه الأمور تتوقف عموماً على قيام الدولة ممثلة بمؤسساتها التعليمية والقانونية والإعلامية بنشر الثقافة القانونية بين مواطنيها ومؤسسات المجتمع المختلفة، وتحذيرهم بخصوص خطورة الجرائم عموما والجرائم المعلوماتية خصوصاً وكذلك أرشادهم إلى ضرورة اتخاذ كافة الاحتياطات اللازمة والكفيلة بضمان عدم وقوعهم ضحايا لمثل هذه الجرائم.

ومثل هذا الأمر يعد في الحقيقة من الواجبات المفروضة على الدولة تجاه الإفراد في المجتمع في سبيل حماية أموالهم و أنفسهم وأعرافهم من مخاطر الجرائم عموما ولها في سبيل ذلك أن تستعين بكافة الوسائل المتاحة والمشروعة، على أن واجب الدولة هنا لا يقتصر على مجرد التوعية، بل ينبغي عليها أن تقوم بتجريم الأفعال التي يقتضي واقع الحال تجريمها[٢٥].

---

[٢٣] د. عبد الفتاح بيومي حجازي، المبادئ الإجرائية الجنائية، في جرائم الكومبيوتر والانترنت، المصدر السابق، ص١١٠

[٢٤] للتوضيح الجرائم المعلوماتية هي الجرائم المتعلقة بالحاسوب والانترنيت، فاصطلاح الجرائم المعلوماتية عام ويشمل التقنيات الحالية والمستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الانترنت مع ملاحظة أن جريمة الحاسب الالي هي الجريمة التي تقع بواسطة الحاسب الألي أو على مكوناته المادية والمعنوية، اما جرائم الانترنت فهي الجرائم العابرة للحدود والتي ترتكب بواسطة الانترنيت أو عليه من شخص ذا دراية فائقة بها.

[٢٥] د. أحمد عبد اللطيف الفقي الدولة وحقوق ضحايا الجريمة، دار الفجر، القاهرة، ط١ ٢٠٠٣، ص٢١ وما بعدها.

وتدخل هذه المؤسسات في اعتباراتها أن الإبلاغ عن الجريمة المعلوماتية عن طريق الحاسب الآلي التي وقعت ضدها ربما يؤدي إلى إحاطة المجرمين علماً بنقاط الضعف في أنظمة الجهات المجني عليها، والجريمة في صورتها التقليدية تصل إلى علم سلطات الضبط عن طريق الشكوى أو الإبلاغ والتي يجب على المحقق قبولها متى وردت في شأن جريمة ويحرر بها محضرا يرسله فورا إلى الجهة المختصة، حتى يتسنى لها مراقبة مشروعية أعمال الاستدلال، والشكوى كالبلاغ، إلا أنها توجه ضد شخص معين، وتقدم من المجني عليه أو المضرور من الجريمة، بينما البلاغ يقدم من غيرهما أو يخلو من تعيين اسم من تنسب إليه الجريمة[٢٦].

ومن أجل تفعيل عملية الإبلاغ عن الجريمة المعلوماتية عن طريق الحاسب الآلي، ومن ثم المساهمة بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، طالب البعض في الولايات المتحدة الأمريكية بأن تتضمن القوانين المتعلقة بالجريمة المعلوماتية، نصوصا تلزم موظفي الجهة المجني عليها أيا كانت بضرورة الإبلاغ عما يصل إلى علمهم من جرائم تتعلق بهذا المجال، وتقرير خبراء على الإخلال بذلك الالتزام. إلا أنه ولدى عرض هذا الاقتراح على الجنة خبراء مجلس أوربا "قوبل بالرفض لسبب قانوني وهو أن المجني عليه وهو الشركة التي ارتكب في حقها جريمة الاعتداء الإلكتروني، سوف تصبح متهمة أو جانية بعد أن كانت مجنية عليها ولذلك وردت اقتراحات بديلة قد تكون مقبولة منها الالتزام بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات، وكذلك إصدار شهادة "أمن خاصة "تمنع بعد عمل مراجعة وتدقيق من قبل هيئة خاصة من المراجعين، ويتعين على هذه الهيئة إبلاغ الشرطة بما تكتشفه من جرائم[٢٧].

ولذلك فإن من صعوبات الإبلاغ عن هذه الجرائم على نطاق دولي، عدم وجود شبكة دولية لتبادل المعلومات الأمنية. ولذلك فإن الشرطة الدولية (الانتربول) بدأت تهتم بمكافحة جرائم الكومبيوتر وأنشأت لديها فرقة خاصة لهذا الغرض. وتثير مسألة الإبلاغ

---

[٢٦] د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية، المجلد الأول، ١٩٩٠، ص ٢٨٠.

[٢٧] د. عمر الفاروق الحسيني، تأملات في بعض صور الحماية الجنائية لنظام الحاسب الآلي. تقرير مقدم إلى الدورة التدريبية التي ينظمها اتحاد المصارف العربية في الفترة من ٧- ٩ مايو، في الجوانب القانونية النجمة عن استخدام الحاسب الآلي في أعمال البنوك، ١٩٩١، ص ٣٢

(ISSN: 2537 - 0758)

عن الجريمة المعلوماتية عن طريق الحاسب الآلي مسائل تتعلق بمدى ما هو متاح من نصوص في الأنظمة الجزائية التي توجب الإبلاغ وترتب عقوبة على ذلك[٢٨].

المطلب الثالث

فقدان آثار الجريمة

المشكلة التي تواجه أجهزة العدالة الجنائية أن الجرائم المعلوماتية لاتصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، لا تخلق اثأرا مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة، وجثة المجني عليه في القتل، واختلاس المال من المجني عليه في السرقة وغيرها، ويرجع السبب في فقدان الآثار التقليدية للجريمة المعلوماتية إلى 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 معدة ومخزنة على جهاز الحاسب، ويتوافر أمام المتعامل عدة اختيارات، وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد فتكتمل حلقة الأمر المطلوب تنفيذه، كما في المعاملات المالية في البنوك أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى حيث يتم ترصيد الأشياء المخزونة أو حسابات العملاء، أو نقلها من مكان لأخر بطريقة إليه وحسب الأوامر المعطاة لجهاز الحاسب الآلى[٢٩].

ويمكن في الفروض السابقة ارتكاب بعض أنواع الجرائم كالاختلاس أو التزوير وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب أو تعديل البرنامج المخزن في جهاز الكومبيوتر، وتكون النتيجة مخرجات على هوى مستعمل الجهاز الذي ادخل البيانات أو عدل البرنامج دون استخدام وثائق أو مستندات ورقية، وبالتالي تفقد الجريمة أثارها التقليدية[٣٠].

---

[٢٨] د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية، المجلد الأول، ١٩٩٠، ص ٢٨٢.

[٢٩] د. عبد الفتاح بيومي حجازي، المبادئ الإجرائية الجنائية، في جرائم الكومبيوتر والانترنت، المصدر السابق ص٨٤

[٣٠] فمثلا في جريمة التزوير نفترض وجود محرر مزور تم تزويره بغرض الاستعمال، هذا المحرر من الاثار التقليدية لجريمة التزوير، لوجود مضاهاة بأصل المحرر مع المحرر المزور، وكذلك الحال في جريمة الاختلاس في صورتها العادية نجد مستندات تشير الى ارقام وخصائص قد تكون مبالغ مالية في

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل المعلوماتية انه يمكن محو الدليل في زمن قصير، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جدًا.

بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها فأنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات أقامة الدليل ضده[٣١]، لذلك يجد أعضاء الضبط القضائي، أحيانا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم فضلا عن صعوبة أجراء التحريات السرية وتتبع مسار العمليات المعلوماتية العابرة للحدود[٣٢].

ومن المسائل التي أثيرت كذلك بمناسبة تعذر الحصول على الدليل في الجريمة المعلوماتية بطرق تقليدية نظرا لخصوصية هذا النوع من الجرائم، هو مدى سريان الحماية المعول بها للاطلاع غير المصرح به على الأوراق المختومة أو المغلقة، لتمتد إلى نظام المعالجة الآلية للبيانات والمحمي فنية ضد الاختراق، حيث يجب عدم المساس بمبدأ المشروعية[٣٣].

إن السبب في حظر الاطلاع على الأوراق المغلقة، والمغلقة والمختومة هو رغبة صاحبها في عدم اطلاع الغير عليها، بدليل انه اتخذ سبل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها، بدليل إغلاق هذه الأوراق أو تغليفها بأي طريقة وذات العلة تتوافر في البيانات المعالجة أليا، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو الكود أو كلمة المرور الدخول إلى نظام هذه البيانات، وبذلك يكون صاحب ذلك النظام قد رفض مسبقا عمليات الاطلاع غير المصرح به ما لم يكن الراغب في الاطلاع مصرح له عن طريق أعطائه مفتاح المرور إلى هذه البيانات وذلك لا يتوافر في حالة عضو الضبط القضائي القائم بالتفتيش موضوع الحديث، إن هذا التوجه يهدف أولا

الحسابات او بضاعة في المخزن اختلسها صاحب العهدة لنفسه، لكن عند ارتكاب هذه الجريمة بطريقة الحاسب الالي لا يظهر للمشاهد سوى ارقام وبيانات لا يعلمها سوى صاحب الشأن نفسه ولا تعطي دلالة سوى لشخص تخصص.

[٣١] د. هشام محمد فريد رستم، بحث مقدم الى مؤتمر القانون والكومبيوتر والانترنيت والذي عقد بدولة الامارات العربية المتحدة سنة ٢٠٠٠

[٣٢] د. خالد ممدوح ابراهيم، التقاضي الالكتروني، مصدر سابق، ص٣٢٤

[٣٣] د. محمد زكي أبو عامر، الاثبات في المواد الجنائية، الفنية للطباعة والنشر، الاسكندرية ص ١١٩

(ISSN: 2537 - 0758)

وأخيرا إلى إيجاد مظلة حماية قانونية لنظام البيانات المعالجة ألياً والتي لا يصرح للغير بالاطلاع عليها[٣٤].

ولا يفوتنا أن نتطرق إلى المعاينة في الجريمة المعلوماتية كوسيلة للحصول على الدليل، فالمعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة حيث يقوم عضو الضبط القضائي بمعاينة الأثار المادية للجريمة ويعمل في المحافظة عليها[٣٥].

وعلى أي حال فإنه عند معاينة مسرح الجريمة المعلوماتية يجب مراعاة عدة ضوابط وهى[٣٦]:

١- تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملف، وذلك لتعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها، ويراعى تصوير الأجهزة الموجودة، خاصة الأجزاء الخلفية منها.

٢- وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة بل ورصد الاتصالات الهاتفية من والى مكان مسرح الجريمة.

٣- ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها، ومعرفة السجلات المعلوماتية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار.

٤- عدم نقل المواد المعلوماتية خارج مسرح الجريمة ألا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات الممرات المغناطيسية التي قد تتسبب في محو البيانات.

٥- التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقه وشرائط وأقراص ممغنطة وغير سليمة أو محطمة ورفع البصمات التي قد تكون عليها.

---

[٣٤] د. خالد ممدوح ابراهيم، التقاضي الالكتروني، مرجع سابق، ص٣٢٥

[٣٥] د. سليم ابراهيم حربة وعبد الامير العكيلي، شرح قانون اصول المحاكات الجزائية، بغداد، ١٩٨٨، ص ١٠٠

[٣٦] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية، في جرائم الكومبيوتر والانترنت، المصدر السابق ص ١٠٣ وما بعدها.

٦- قصر المعاينة على الباحثين والمحققين الذين لديهم كفاءة علمية وخبرة فنية في مجال الحاسبات والشبكات واسترجاع المعلومات وان يكونوا قد تلقوا تدريبا جيدة على ذلك.

وبالتالى تظل الجريمة المعلوماتية عن طريق الحاسب الآلي مجهولة ما لم يبلغ عنها اللجهات الخاصة بالاستدلالات أو التحقيق الجنائي، والمشكلة التي تواجه أجهزة العدالة الجنائية أن هذه الجرائم لا تصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، لا تخلف آثارة مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة، وجثة المجني عليه في القتل، واختلاس المال من المجني عليه في السرقة إلى آخره، ويرجع ذلك إلى صعوبة اكتشاف الجريمة المعلوماتية عن طريق الحاسب الآلي، ذلك أن الجهات التي تتعامل بالحاسب الآلي في معاملاتها اليومية كالشركات التجارية أو المؤسسات لا تراجع أعمالها يوميا، وحتى تلك التي تقوم بالمراجعة اليومية أو الأسبوعية أو الشهرية، قد لا تكتشف الجريمة وتبدو لها وكأنها خسائر عادية على أثر ممارسة نشاطها، وحتى في حال اكتشافها فإن بعض الجهات المجني عليها لا تقدم على الإبلاغ خوفا من الأثر السلبي الذي ينعكس عليها من جراء هذا البلاغ[٣٧].

وقد يرجع السبب في افتقاد الآثار التقليدية للجريمة المعلوماتية عن طريق الحاسب الآلي ما يلاحظ 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 معدة ومخزنة على جهاز الحاسب، ويتوافر أمام المتعامل عدة اختيارات، وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد فتكتمل حلقة الأمر المطلوب تنفيذه، كما في المعاملات المالية في البنوك، أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى حيث يتم ترصيد الأشياء المخزنة أو حسابات العملاء، أو نقلها من مكان لآخر بطريقة آلية وحسب الأوامر المعطاة لجهاز الحاسب الآلي، ويمكن ارتكاب بعض أنواع الجرائم المعلوماتية كالاختلاس أو التزوير، وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب أو تعديل البرنامج المخزن في جهاز الكمبيوتر، وتكون النتيجة مخرجات على حسب متطلبات مستخدم الجهاز الذي أدخل

[٣٧] د. محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي. مرجع سابق، ص ٢٠.

(ISSN: 2537 - 0758)

البيانات أو عدل البرنامج دون استخدام وثائق أو مستندات ورقية، وبالتالي تفقد الجريمة آثارها التقليدية[٣٨].

ولذلك يتعين عند البحث عن آثار الجريمة المعلوماتية عن طريق الحاسب الآلي وأدلتها بمعرفة سلطات الاستدلال والتحقيق، أن توجه تحرياتها إلى دائرة المتعاملين في نطاق المؤسسة أو الجهة التي وقعت بها الجريمة سواء كانوا موظفين بتلك الجهة أو من المتعاملين معها، وذلك برصد حركة المعاملات المعلوماتية ومراقبة المشبوهين داخل المؤسسات وحولها[٣٩].

ويتضح من خلال ذلك ضرورة حصر البحث الجنائي عن آثار الجريمة المعلوماتية عن طريق الحاسب الآلي في دائرة المهتمين والمتعاملين بجهاز الحاسب الآلي، حيث إنه يتعين تطوير ثقافة الحاسب الآلي وسط رجال الأمن، وربط تلك الثقافة بالثقافة الأمنية التقليدية بحيث يكفل للأجهزة الأمنية نجاحا في مواكبة الظاهرة للتعامل مع الجريمة المعلوماتية وذلك من حيث القدرة على الملاحظة، ومراعاة تصرفات الأشخاص العاملين في مجال الحاسب بدقة أو المهتمين ببرامجه أو هواة صناعة الأنظمة المعلوماتية وتقليدها، فدراسة تصرفات هؤلاء ومراقبتها، تعد مدخلا جيدة للسيطرة الأمنية على نشاط مرتكبي الجريمة المعلوماتية عن طريق الحاسب الآلي ووسيلة لضبطها، ذلك أن الفئات التي يجب وضعها تحت المراقبة والملاحظة الدائمة هم في الغالب من المتعلمين والذين تدل مظاهرهم على الوقار والمكانة الاجتماعية المرموقة، وللتعامل مع هؤلاء يتعين الانتقال بالحس الأمني الرجل البحث الجنائي من اهتمامه بالعاطلين والمتشردين والطبقات الفقيرة إلى مراقبة طبقات اجتماعية حديثة تتسلح بالعلم والخبرة والذكاء والثقافات المتنوعة، ولن يأتي ذلك إلا إذا كان قادرا على فهم عبارات ومفردات لغة الحاسب الآلي، التي تمكنه من جمع المعلومات المناسبة ومتابعتها[٤٠].

---

[٣٨] د. علي محمود حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي. بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية مركز البحوث والدراسات أكاديمية شرطة دبي – محور القانون الجنائي في الفترة من ٢٤– ٢٨ أبريل ٢٠٠٣، ص٢٨١.

[٣٩] د. جودة حسين محمد. جهاد، المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، دراسة مقارنة، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١–٢ مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون، ٢٠٠٠، ص ٤

[٤٠] د. محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي. مرجع سابق، ص ٢١.

وفضلا عن رفع المستوى الثقافي لرجال الضبط في الجريمة المعلوماتية عن طريق الحاسب الآلي وأجهزة التحقيق، وربطهم بثقافة الحاسب الآلي، وذلك كوسيلة للسيطرة على آثار الجريمة المعلوماتية عن طريق الحاسب الآلي وضبط أدلتها، لأنها في النهاية ستؤول إلى الجناة بوصفها ثمرة الجريمة، وحينئذ يمكن ضبط مرتكبي الجريمة. ومن الأسباب التي تساعد في تعذر الحصول على آثار تقليدية تخلف الجريمة المعلوماتية عن طريق الحاسب الآلي أن الجاني نفسه يملك محو الأدلة التي تدينه أو تدميرها في زمن قصير جدا وحتى لوتم ضبطه فقد يرجع هذه الجريمة إلى خطأ في نظام الحاسب أو الشبكة أو الأجهزة[٤١].

المبحث الثاني
الصعوبات المتعلقة بجهات التحقيق

تمهيد وتقسيم:

إن اكتشاف الجرائم عموماً ومن ضمنها الجرائم المعلوماتية بعد وقوعها يدخل ضمن المفهوم العام للتحريات التي بدورها من إجراءات الاستدلال، التي تدخل ضمن مهام أعضاء الضبط القضائي المكلفون قانوناً بعدة واجبات من ضمنها التحري عن الجرائم والكشف عنها[٤٢]، بكافة الوسائل المتاحة والمشروعة وهذا الواجب يشمل أيضا محاولة اكتشاف أية جريمة يمكن أن تكون قد وقعت[٤٣].

فهم عين العدالة وإذنها في التنقيب عن الجرائم عموما، ووضع مرتكبها تحت تصرف القضاء، ألا أن مهمتهم هذه ليست بالسهلة، وإنما تكتنفها صعوبات عدة كنقص المعرفة الفنية لدى سلطات التحقيق، والخبرة في الجرائم المعلوماتية، وضعف التعاون الدولي في مواجهة الجريمة المعلوماتية، **وهو ما سنتناوله فى المطالب التالية:**

المطلب الأول: نقص المعرفة الفنية لدى سلطات التحقيق.

المطلب الثانى: الخبرة فى جرائم تقنية المعلومات.

المطلب الثالث: ضعف التعاون الدولى فى مواجهة جرائم تقنية المعلومات.

---

[٤١] د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص ٣٥.

[٤٢] د. قدري عبد الفتاح الشهاوي، ضوابط الاستدلالات والإيضاحات والتحريات في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، ٢٠٠٢، ص١٦٢.

[٤٣] د. محمد قادر، شرح قانون أصول المحاكمات الجزائية، ط١، اربيل، ٢٠٠٣، ص ١٣٢.

(ISSN: 2537 - 0758)

المطلب الأول
نقص المعرفة الفنية لدى سلطات التحقيق

من الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة المعلوماتية نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي وكيفية التعامل معها، وذلك على الأقل في البلدان العربية، نظرا لان تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخرة عن أوربا والولايات المتحدة، فقد اثبت الوقائع بان بعض من أعضاء الضبط القضائي قد أعانوا مجرمي المعلوماتية على ارتكاب جرائمهم عن جهل ومن دون قصد، بدلا من ضبطهم وذلك بالنظر لعدم امتلاكهم المعرفة اللازمة للتعرف على مثل هذه الجرائم ووسائل ارتكابها[٤٤].

وبالتالى فإن الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة المعلوماتية تتمثل فى نقص الخبرة لدى المحقق، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة المعلوماتية عن طريق الحاسب الآلي وكيفية التعامل معها، وذلك على الأقل في البلدان العربية، نظرا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخرة عن أوربا وكندا والولايات المتحدة، وأن أجهزة العدالة المقاومة الجرائم المرتبطة بهذه التقنية تبدأ في التكوين والتشكيل عقب ظهور هذه الجرائم، وهو أمر يستغرق وقتا أبطأ من وقت انتشار الجريمة لان هذه الجريمة تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن فإن الحركة التشريعية، أو الثقافية الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلبا على فنية إجراء الاستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة المعلوماتية عن طريق الحاسب الآلي، ومن هنا تأتي الدعوة إلى وجوب تأهيل المختصين في جهات التحقيق والادعاء تأهيلاً مناسباً في شأن هذه الجرائم[٤٥].

---

[٤٤] د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط١، الرياض، ٢٠٠٤، ص١٠٧.

[٤٥] د. ممدوح عبد الحميدعبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية. الشارقة، دار الحقوق، ٢٠٠١، ص١٧.

إن جهات الضبط القضائي التقليدية تعاني عموماً من ضعف الثقافة القانونية اللازمة للتعرف على الجرائم المعلوماتية وتقدير خطورتها، ومثل هذه الإشكالية تتضاعف أضعافا مضاعفة في الدول التي لا تملك قانون خاص بمكافحة الجرائم المعلوماتية، فوجود الأخير ضرورة لا غنى عنها لتعريف المجتمع عموماً وجهات الضبط القضائي خصوصا بخطورة هذه الجرائم، وكذا لتحديد الأفعال التي تشكل هذه الجرائم من عدمها[٤٦].

وهذا ما لاحظه جانب كبير من الفقه الجنائي، ذلك أن البحث والتحقيق في الجريمة المعلوماتية هي مسألة في غاية الأهمية والصعوبة، ولاسيما بالنظر لاعتبارات التكوين العلمي والتدريبي، والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي، ذلك أن حداثة هذه الجرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق إلمام كاف بها، فلا يكفي أن يكون لديهم الخلفية القانونية أو أركان العمل الشرطي فقط، ولكن لا بد من الإلمام بخبرة فنية في مجال الجريمة المعلوماتية عن طريق الحاسب الآلي[٤٧].

ويزيد من التحدي الذي تواجهه أجهزة العدالة الجنائية في جرائم الحاسب الآلي وجرائم الانترنت، أن الجناة في هذه الجرائم لهم المفردات والمصطلحات الخاصة بهم، لدرجة أنهم يطلقون على أنفسهم اسم (النخبة) بدعوى أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاته المتميزة، ويطلق على رجال الشرطة والنيابة والقضاء صفة الضعفاء[٤٨].

يبدو لنا أن هذا القصور الفني والمعرفي لدى سلطات التحقيق يتطلب ابتداء تفعيل عدة أمور لمكافحة الجرائم المعلوماتية وإمكانية ضبط الأدلة الجنائية أن وجدت ويمكن أن نورد أهمها:

١ – تفعيل دور الضبط الإداري:

يعد الضبط الإداري أو البوليس الإداري من أهم وظائف الإدارة، ويهدف إلى المحافظة على النظام العام في الأماكن العامة عن طريق إصدار القرارات اللائحية

---

[٤٦] قانون مكافحة جرائم تقنية المعلومات الاتحادية رقم (٢) لسنة ٢٠٠٦، وقانون الإجراءات الجزائية الإماراتي رقم ٣٥ لسنة ١٩٩٢.

[٤٧] د. ممدوح عبد الحميدعبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية. الشارقة، دار الحقوق، ٢٠٠١، ص٢٠.

[٤٨] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، مرجع سابق، ص١٢٤

(ISSN: 2537 - 0758)

والفردية واستخدام القوة المادية، مع ما يتبع ذلك من فرض قيود على الحريات الفردية، يستلزمها انتظام أمر الحياة في المجتمع[٤٩].

إن بعض العاملين في بيئة الانترنت يتمتعون بصفة الضبطية الإدارية، كمزودي الدخول وخدمات الانترنت، إذ تبعا لاعمالهم ووفقا للقانون فهم يمنحون الصلاحية في الرقابة عبر المزود عن سير حركة العمل ومدى الخضوع للنظام والقانون من قبل العاملين والمتعاملين مع الانترنت، حيث إذ حدث ووجدت الجريمة باكتشافها بهذا الأسلوب، فانه ليس الرجل الضبط الإداري سوى التحفظ على أدلة الجريمة إلى حين حضور رجال الضبط القضائى[٥٠].

والى جانب الإجراءات التي يتخذها رجال الضبط الإداري لمواجهة جرائم الانترنت مبكرة، وبالتالي منع وقوعها، هناك إجراءات يقوم بها العاملون بالمنشآت الحيوية، يطلق عليها، امن المعلومات، وهي عبارة عن احتياطات وإجراءات تتخذها الإدارات الحديثة لمنع وقوع الجريمة، وذلك من خلال تحديد المعلومات الهامة، ثم تحليل المخاطر والتهديدات والقابلية للعدوان، ثم تطبق الإجراءات المضادة لتصل إلى مرحلة التقييم[٥١].

٢- التدريب التخصصي لجهات التحقيق:

ان التحقيق في الجرائم المعلوماتية في حاجة إلى خبرة ومهارات خاصة لا تتأتى دون تدريب تخصصي يراعى فيه عدة عناصر تتعلق بشخص المتدرب ومنهج التدريب، وصفته ما أن كان رسمية ام غير رسمي وكذلك أسلوب التدريب وجهة التدريب فبخصوص المتدرب، لابد أن يكون الشخص مؤهلا لذلك سواء من رجال الشرطة أو سلطات التحقيق الجنائي، وهذا يتطلب قدرات ذهنية ونفسية خاصة لتلقي هذا التدريب، ألا أن تدريب المتخصصين في معالجة البيانات ونظم التشغيل يؤتي ثماره وبسرعة عن أولئك المنتمين لأجهزة العدالة كما في الشرطة والتحقيق الجنائي، ويتعين توافر الخبرة لدى متلقي برنامج التدريب[٥٢].

---

[٤٩] د. ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، ١٩٩٤، ص٤٧١

[٥٠] د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة،٢٠٠٤،ص٨٠٩

[٥١] د. ايمن عبد الحفيظ عبد الحميد، إستراتيجية مكافحة جرائم الحاسب الألي، دراسة مقارنه، رسالة دكتوراه، أكاديمية الشرطة، بدون سنة طبع، ص٣٧٤ وما بعدها.

[٥٢] د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، مرجع سابق، ص٥٢

والتدرب قد يكون بصفة رسمية أو غير ذلك، والتدريب غير الرسمي يكون بتكليف المتدرب بالعمل مع شخص لديه خبرة في تحقيق الجرائم المعلوماتية، أما التدريب الرسمي فيكون من خلال حلقات دراسية أو حلقات نقاش وهو ما يسمى (بورش العمل)، وذلك حول جرائم الحاسب الآلي وشبكات المعلومات وإساءة استخدامها[٥٣].

المطلب الثاني
الخبرة في جرائم تقنية المعلومات

أن الفلسفة العامة التي تسود الإثبات الجنائي انه يعتمد على القناعة الوجدانية، وذلك أن الإثبات ينصب على واقعه طواها الزمن ويتعين أعادة تركيب صورتها كما وقعت حتى تنطبق الحقيقة القانونية مع الحقيقة الواقعية، وصعوبة ذلك تبرر اعتماد كل وسائل الإثبات المتاحة دون تقيد، خصوصا وان محل الإثبات يتسع ليشمل كل العناصر التكوينية للجريمة وما يلابسها من ظروف نفسية ويواكبها من أسباب الإعفاء أو الإباحة وما إلى ذلك. ومن ثم كان على القاضي أن يقوم بدور ايجابي فليس دوره فقط الموازنة بين الأدلة المقدمة من هذا الفريق أو ذاك بالإدانة أو البرائة، وإنما عليه اتخاذ كل الإجراءات الضرورية والتحقق من صدق أية وسيلة تثار في سبيل الكشف عن الحقيقة وتكوين قناعته.

لقد كان اللجوء إلى الخبرة في الماضي استثنائية غير أن أمرها تعاظم نتيجة الطفرة التي عرفتها مختلف العلوم واطراد توسع دائرة التقنية خلال القرن الحالي، الأمر الذي نتج عنه تزايد الأفعال الممنوعة قانوناً بكيفية لم تكن متوقعه كما بينا.

تعرف الخبرة بأنها إجراء يتعلق بموضوع يتطلب الماما بمعلومات فنية لا مكان استخلاص الدليل منه، أو أنها الاستشارات الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقرير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوفر لدي القضاة بحكم العمل أو الثقافة.

كما عرفها الفقه الجنائي[٥٤] بأنها "تقدير مادي أو ذهني يبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها بمعلوماته

---

[٥٣] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، مرجع سابق، ص ١٣٠

[٥٤] د. سليم ابراهيم حربة وعبد الامير العكيلي، شرح قانون أصول المحاكمات الجزائية مصدر سابق، ص ١٢٥.

(ISSN: 2537 - 0758)

الخاصة سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أو بجسم الجريمة أو المواد المستعملة في ارتكابها أو أثارها".

أن انتداب الخبراء أجراء من إجراءات التحقيق تختص به سلطة التحقيق (القاضي أو المحقق)، غير أن هذا لا يمنع عضو الضبط القضائي من استدعاء أهل الخبرة بشأن الجريمة التي يباشر فيها التحقيق سواء تعلقت الخبرة بجسم الجريمة أو موادها وأثارها، على أن المشرع لم ينص صراحة على حق سلطة الضبط القضائي باستدعاء الخبراء كما فعل المشرع المصري[٥٥]، إلا أنه ذكر بأن لعضو الضبط القضائي عند تحقيقه في الجريمة المشهودة أن يحضر في الحال كل شخص يمكن الحصول منه على إيضاحات.

من بين خبراء الدولة ومؤسساتها الرسمية وشبه الرسمية أو من بين مؤسسات القطاع الاشتراكي أو المنظمات المهنية، كما أنها أن احتاجت إلى خبير من غير هؤلاء والذين اشرنا إليهم فأنها تستطيع استدعائه وتكليفه بالمهمة، علما بأن الخبراء المسجلين في الجدول لا يمارسون أعمالهم لأول مرة ألا بعد حلفهم اليمين بأن يؤدوا خبرتهم بأمانة وإخلاص، أما الخبير الذي يستعين به القائم بالتحقيق من غير المسجلين في الجدول فأنه يحلف اليمين في كل مرة يكلف بها في قضية، ويستطيع القائم بالتحقيق استبدال الخبيرمتى ما وجد ان الامر يستدعي ذلك كما يستطيع القائم بالتحقيق مناقشته وتوجيه الأسئلة إليه بحضور ذوي العلاقة، كما أن رأي الخبير غير ملزم على ما يبدو طالما يستطيع القائم بالتحقيق استبداله[٥٦]. ومشروعية الدليل العلمي المستمد من أعمال الخبرة متفق على وجوب مشروعيته في كافة النظم القانونية ومنها الأدلة المستمدة من عمليات سحب وتحليل عينات الدم وعينات البول وعينات الكتابة والصوت[٥٧].

---

[٥٥] نصت المادة (٢٩) من قانون الإجراءات الجنائية المصري على انه "المأموري الضبط القضائي اثناء جمع الاستدلالات ايسمعوا اقوال من تكون لديهم معلومات عن الوقائع الجنائية وان يسألوا المتهم عن ذلك، ولهم أن يستعينوا بالاطباء وغيرهم من اهل الخبرة ويطلبوا رايهم شفهية أو بالكتابة".

[٥٦] د. سليم ابراهيم حربة وعبد الأمير العكيلي، شرح قانون أصول المحاكمات الجزائية مصدر سابق، ص ١٢٧، وانظر دكتور سامي النصراوي، دراسة في أصول المحاكمات الجزائية، الجزء الأول، مطبعة دار السلام، بغداد، ١٩٧٨، ص ٣٦٥

[٥٧] د. مأمون محمد سلامة، قانون الإجراءات الجنائية معلق عليه بالفقه وأحكام القضاء دار الفكر العربي، ١٩٨٠، ط١، ص٣٣٧، وانظر كذلك د. محمد زكي ابو عامر الاثبات في المواد الجنائية، مصدر سابق، ص١٨٦

والخبرة في مجال الحاسب الآلي والانترنت أنواع عديدة[٥٨]، منها الخبرة الخاصة وهذه تعد اقوي أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنظمات الخاصة، والى جوار الإفراد توجد المنظمات الخاصة في كافة المجالات والتي يكون لها السبق في مجال الخبرة، وتختلف المنظمات الخاصة مابين منظمات أهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق المعلوماتية وبين نوعيه من المنظمات تسعى إلى فك طلاسم العالم الافتراضي على أسس تجارية.

ان الخبير الجنائي يواجه معوقات متعددة في سبيل جمع الأدلة الرقمية من أجهزة الحاسب الآلي أو الشبكات الرقمية، وعليه يجب أخذ الحذر في كل إجراء أو ملاحظة النقاط الآتية خلال أداء عمله[٥٩]:

١) فقد جزء كبير من المعلومات والأوامر، التي تشكل الأدلة الرقمية حال إغلاق جهاز الحاسب الآلي بطريقة غير صحيحة، أو في حالة القطع المفاجئ للتيار الكهربائي عن الجهاز. فعند غلق أو قطع التيار الكهربائي عن جهاز الكمبيوتر فإن مثل هذا الفعل قد يؤدي إلي محو المعلومات من ذاكرة الجهاز أو العمل علي تحريف بيانات هامه وحدوث ضرر في أجهزة الكمبيوتر، أو منع نظام التشغيل من إعادة التحميل وبالتالي فقدان للأدلة الجوهرية.
٢) قيام الجاني بتهيئة جهاز الكمبيوتر للتفجير أو التدمير بمجرد تشغيله بالضغط على زر توصيل الطاقة.
٣) طبيعة مسرح الجريمة، فالشبكات المنتشرة على مستوي العالم، لذا فقد لا يكون ممكن الحصول علي دليل في حالة توزيع مسرح الجريمة بين أكثر من دولة بسبب تعقيد الإجراءات أو وجود مشاكل عملية وتشريعية في بعض الدول مما يحول دون الحصول على دليل رقمي، كما أن سرعة مرور البيانات الرقمية عبر الشبكات الأقل من جزء من الثانية مع مهارة المجرمون في تدمير الأدلة أو تحريف أو تعديل

---

[٥٨] د. حسين بن سعيد الغافري، الخبرة ودورها في كشف الجرائم المتعلقة في الانترنت، تقرير منشور في الانترنت.

[٥٩] د. عبد الناصر محمد فرغلى، محمد عبيد المسمارى، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مرجع سابق، ٢٠٠٧، ص ٣٢

(ISSN: 2537 - 0758)

البيانات لحماية أنفسهم، وكذلك حجم البيانات الضخمة التي تمر بالشيكات مما يكون لها التأثير العكسي عند البحث عن دليل إدانة أو البراءة.

٤) إخفاء الهوية، فعند تعمد المستخدم إخفاء هويته حال استخدام الإنترنت سواء القيام ببعض الإجراءات أو استخدام بعض البرامج والتطبيقات التي تؤدي لطمس الهوية مما يشكل عائقا أمام المحقق الجنائي أو الخبير الفني.

٥) وجود بعض البرامج خاصة بإخفاء المعلومات أو البيانات المخفية وذلك لخلق ما يعرف بنظام غير آمن عبر استخدام الشبكة العالمية الإنترنت مما تجعل عملية استعادة الأدلة أو إعادة تركيبها في غاية الصعوبة أمام المحقق الجنائي أو الخبير، ويتضح مما تقدم فإن الحصول على الأدلة الجنائية الرقمية أمر صعب الوصول إليه لما تتطلبه من خبرة ومهارة كبيرة في مجال الكمبيوتر.

وبعد ذلك يتعين على المحقق أن يحدد للخبير المعلوماتي دوره في المسألة المنتدب فيها على وجه الدقه، وهذا يعود بنا إلى ضرورة تأهيل رجال الضبط وسلطات التحقيق في الجرائم المعلوماتية لنجاح تحقيق مثل هذه الجرائم، ودرءا لما ينأى به البعض من انه يمكن الخبير نفسه أن يحدد أطار مهمته، إذ أن ذلك سوف يقوض دور المحقق والقاضي في الدعوى الجزائية في مثل هذه الجرائم المعلوماتية[٦٠].

وعلى ضوء ذلك هناك أسلوبان لعمل الخبير في الجرائم المعلوماتية هما:

١- القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كما هو الشأن في التهديد أو النصب أو السب أو جرائم النسخ وبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق ودعارة الأطفال وغيرها، ثم القيام بعملية تحليل رقمي لها المعرفة كيفية إعدادها البرمجي ونسبتها الى مسارها الذي أعدت فيه، وتحديد عناصر حركتها، وكيف تم التوصل الى معرفتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت الذي ينسب الى جهاز الحاسوب الذي صدر عنه هذا الموقع.

٢- القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته، وإنما تؤدي حال تتبع موضوعاتها إلى قيام الإفراد بارتكاب جرائم كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية

[٦٠] د. هشام محمد فريد رستم، المصدر السابق، ص٣٨

التي تناسب وزن الإنسان بادعاء انه إذا تتبع التعليمات الواردة فيها فلن يصاب الشخص بحالة إدمان، وأيضا كيفية زراعة المخدرات بعيدة عن أعين الغير، وكيفية أعداد القنابل وتخزينها، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها، وكذلك القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بالدخول من مكان ثابت، ومثل هذا الأمر جائز الحدوث كما لو كان مرتكبي الجريمة مشتركة لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها ويقوم بالولوج إلى الانترنت من محل أقامته.

وحيث أن أسلوب عمل الخبير يكون بهذه الصورة لذلك يتعين التنسيق مابين الخبير المعلوماتي والمحقق الجنائي قبل محاكمة الجاني في الجريمة المعلوماتية، على أن يشمل اللقاء كافة الخبراء الذين ساهموا من سلطات الضبط أو التحقيق في تلقي البلاغ أو إجراءات الضبط أو التفتيش أو فحص البرامج وجمع الأدلة الجنائية، على أن يتم في هذا اللقاء حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بينة أو قرينة، كما يجب على المحقق الجنائي أن يشرح لهؤلاء الخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة المقام عنها الدعوى الجزائية ضد المتهم[٦١]،

المطلب الثالث
ضعف التعاون الدولي
في مواجهة جرائم الاعتداء على الحياة الخاصة عبر الانترنت

غالبا ما تكون المعلومة ذاتها مملوكة لبعض الأفراد أو الشركات أو المؤسسات والدول في بعض الأحيان الأخرى، وتتأتى صعوبة مكافحة الجريمة المعلوماتية من أن مالكي المعلومات أو حائزيها يحاولون اتخاذ إجراءات الحماية اللازمة بصفة مستقلة ومنفردة، فالأفراد من ناحية والمؤسسات والدول أيضا من ناحية أخرى يحاولون تسخير إمكانياتهم من اجل حماية الأنظمة المعلوماتية الخاصة بهم دون تكاتف أو تعاون مشترك بهدف حماية المعلومات بشكل عام، فغياب التعاون والتنسيق بين الأفراد والشركات والدول يلعب دورا رئيسا ومؤثرا في عدم انحسار مد الجريمة المعلوماتية وبالتالي صعوبة إثباتها[٦٢].

---

[٦١] د. محمد الأمين البشري، المصدر السابق، ص ٥٩

[٦٢] د. عمر ابو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة الكترونية، دار النهضة العربية، القاهرة، ٢٠١٠، ص٤٣٨

(ISSN: 2537 - 0758)

ومن ناحية أخرى فان غياب سياسة التعاون الدولي والتنسيق بين الدول في مقاومة الجريمة المعلوماتية يقابله في ذات الوقت تعاون واضح بين محترفي الإجرام المعلوماتي، ففضلا عن البرامج التي يستعين بها القراصنة في أنشطتهم الإجرامية، فأنهم يتعاونون فيما بينهم ويتبادلون النصائح والخبرات فيما يتعلق بأنشطتهم مما يزيد من فاعلية وخطورة هجومهم وخصوصا في ظل قصور وعدم فاعلية سياسة الدفاع الخاصة والمنفردة ضد الجريمة المعلوماتية[٦٣].

ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية، ألا أن هناك عوائق تحول دون ذلك، وتجعل هذا التعاون صعبة وأهمها:

١) عدم وجود نموذج موحد للنشاط الإجرامي:

فالأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية لا يوجد فيها اتفاق عام مشترك حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها، فما يكون مباحاً في أحد الأنظمة قد يكون مجرمة وغير مباح في نظام أخر، ويمكن إرجاع ذلك إلى عدة أسباب و عوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لأخر، وبالتالي اختلاف السياسة التشريعية من مجتمع لأخر[٦٤].

اختلاف النظم القانونية الإجرائية:

بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحري والتحقيق والمحاكمة التي ثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دوله أخرى أو قد لا يسمح بأجرائها، كما هو الحال بالنسبة للمراقبة المعلوماتية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة قد تكون ذات الطريقة غير مشروعه في دولة أخرى، وبالتالي فان الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنقاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي انه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعه، حتى وان كان هذا الدليل تم الحصول علية في اختصاص قضائي وبشكل مشروع[٦٥].

---

[٦٣] د. حاتم عبد الرحمن منصور، الإجرام المعلوماتي، دار النهضة العربية، ط١، ٢٠٠٢، ص١٥٣

[٦٤] د. جميل عبد الباقي الصغير، الجوانب الإجرائية، المصدر السابق، ص٧٢

[٦٥] د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المصدر السابق، ص٦٩٢

٢) عدم وجود معاهدات ثنائية أو جماعية بين الدول[٦٦]:

وحتى في حال وجود هذه المعاهدات فأنها قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الانترنت، ومن ثم تطور الجريمة المعلوماتية بذات السرعة على نحو يؤدي إلى إرباك المشرع وسلطات الأمن في الدول، وبعدها يظهر الأثر السلبي في التعاون الدولى.

٣) مشكلة الاختصاص في جرائم الانترنت:

الجرائم المتعلقة بالانترنت من اكبر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي أو الدولي وعند وجود أي مشكله بالنسبة للاختصاص على المستوى الوطني أو المحلي يتم الرجوع إلى القواعد الإجرائية المحددة قانونا لذلك[٦٧].

ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية والتي ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالانترنت التي تتميز بكونها عابرة للحدود، وكذلك اعتبرت من الجرائم الدولية[٦٨].

عدم وجود قنوات اتصال:

أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لازما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العلمية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون[٦٩].

بناء على ما تقدم أصبح أمر التعاون الدولي في مكافحة الجريمة المعلوماتية أمرا حتمية، ويجب اتخاذ خطوات جادة في هذا الصدد أو استكمال ما بدأ، أو تعزيز فاعليته،

---

[٦٦] د. نائله عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي القومية، ٢٠٠٠، ص٥٥

[٦٧] هذه القواعد هي مكان القبض على المتهم، مكان وقوع الجريمة، أو محل إقامة المتهم

[٦٨] د. محمود صالح العادلي، الجريمة الدولية، دراسة مقارنه، دار الفكر الجامعي، الإسكندرية، ٢٠٠٣، ص ٦١ وما بعدها وانظر: نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٨، ص١٣٣

[٦٩] د. حسين بن سعيد الغافري، السياسة الجنائية، مصدر سابق، ص٦٩٢

(ISSN: 2537 - 0758)

وان نقطة البداية التي يجب أن يفطن إليها المجتمع الدولي في سبيل مكافحته للجريمة المعلوماتية، هي ضرورة رسم سياسة جنائية متناسقة من اجل الأجرام المعلوماتي عن طريق التدخل بالتقويم للأنشطة الإجرامية المعلوماتية، مع الأخذ في الاعتبار أهمية الاتفاق على ماهية الأنشطة التي يضفي عليها التجريم المعلوماتي حتى يؤدي هذا التجريم ثماره وتسد الثغرات في وجه المجرمين المعلوماتيين، وعلى ذلك ينبغي القضاء على التناقضات الموجودة في سياسة التجريم، فإذا لم يتم التنسيق الدولي في هذا الإطار فسينتهي الأمر إلى جعل المعلوماتية بمثابة مكان ترفيهي للقراصنة على غرار ما يحدث في مجال غسيل الأموال والتهرب الضريبي، حيث سيجد القراصنة مأوى يلجأون إلية في سبيل تحقيق ما يريدون دون الوقوع تحت طائلة القانون، ولا شك أن محور الارتكاز بالنسبة للتعاون الدولي هنا يستند إلى ضرورة الموازنة بين واجب حماية الحق في الإعلام والاتصال من ناحية وأهمية مقاومة الأجرام المعلوماتي والقضاء علية من ناحية أخرى.

وقد لقي هذا الموضوع الأخير اهتماما من العديد من الدول والمنظمات والهيئات الدولية، ومنها المؤتمر الدولي لمكافحة استغلال الأطفال في الجنس على الانترنت[٧٠].

وعمل الاتحاد الأوربي على وضع مشروع اتفاقية دولية لمواجهة هذه النوعية المستحدثة من الجرائم، ويقضي مشروع هذه الاتفاقية بمعاقبة أي وصول غير مشروع الى معطيات المعلوماتية[٧١].

وعلى المستوى الإقليمي فقد اهتمت منظمة التعاون والتنمية الاقتصادية الأوربية بموضوع الجريمة المعلوماتية، فبعد أن عرفتها بأنها سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به، يرتبط بالمعالجة الإلية للبيانات أو نقلها، حاولت وضع الحلول والمقترحات في هذا المجال، بعد رصد هذه الظاهرة وتحليلها بواسطة مجموعة من الخبراء المتخصصين[٧٢].

---

[٧٠] عقد المؤتمر الدولي لمكافحة استغلال الأطفال في الجنس في فيينا في شهر سبتمبر ١٩٩٩، بالنمسا، انظر: د. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، ٢٠٠٠، ص ١٢٨

[٧١] د. هلالي عبد اللاه احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست ٢٠٠١، دار النهضة العربية، ط١، ٢٠٠٣، ص ٣٣

[٧٢] د. أحمد خليفة الملط، الجريمة المعلوماتية، ٢٠٠٠، ص ٦٧٦

ومن جهود الأمم المتحدة في ذلك أن مؤتمرها الثامن لمنع الجريمة والمجرمين والذي عقد في هافانا ١٩٩٠، قد حث في قراره المتعلق بالجرائم ذات العلاقة بالحاسب الآلي، الدول الأعضاء أن تكثف جهودها لمكافحة إساءة استعمال الحاسب بفاعلية، وذلك بتجريم هذه الأفعال جنائية واتخاذ تدابير تضمن وحدة الإجراءات والقوانين الراهنة بشأن سلطات التحقيق والأدلة، وادخل تغييرات مناسبة عليها آذ دعت الضرورة لذلك، وحث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من اجل مكافحة الجرائم المتصلة بالحاسبات وتبادل المساعدة في المسائل الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب، فضلا عن توصيات أخرى هدفها مواجهة هذه النوعية من الجرائم بفعالية أكثر[٧٣].

المبحث الثالث

معوقات الحصول على الأدلة وضخامة البيانات المتعلقة بالجريمة

اولاً: معوقات الحصول على الأدلة:

إن الجريمة المعلوماتية عبارة عن حرب ما بين المجني عليه وهو ربما يكون فرد أو مؤسسة أو شركة وتكون هدفا للاعتداء على نظامها المعلوماتي ومن ثم الإضرار بها، وما بين المجرم المعلوماتي أو الجناة في حال تعددهم، لذلك فإن الهيئات والجهات التي تتبنى في نشاطها نظام معلوماتية لتسيير حركتها سواء كانت جهات خدمية أو أمنية أو مؤسسات اقتصادية تحاول دائما الحفاظ على معلوماتها وبياناتها عن طريق تخزين هذه البيانات والمعلومات بعيدة عن أيدي محترفي الجريمة المعلوماتية عن طريق الحاسب الآلي، ويظهر ذلك واضحا في مجال التجارة المعلوماتية، ومنها التعاقد بطريقة الإنترنت. ولذلك تحاول الجهات المعنية بالتجارة المعلوماتية المحافظة على عمليات الدفع الإليكتروني- أي السداد بطريقة آلية- فضلا عن تواصل المعلومات والبيانات بينها وبين الأطراف الأخرى، وكذلك حماية عملية التحويلات المالية، ويتبع في ذلك طريقتين هما استخدام أسلوب التشفير والتحقيق عن شخصية المتعاقدين. وفيما يتعلق بالشفرة فهي متفق عليها بين الطرفين، ويعرف كلاهما مفتاح هذه الشفرة لضمان عدم قراءة الرسالة إلا لمن هو مصرح له بذلك[٧٤].

---

[٧٣] د. عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكومبيوتر والانترنت، مرجع سابق، هامش ص ١٤٥

[٧٤] د. سميرحجازى، التهديدات الإجرامية للتجارة الالكترونية. دبي، مركز البحوث والدراسات بإدارة شرطة دبي، ١٩٩٩، ص٣

(ISSN: 2537 - 0758)

أما التحقق من شخصية المتعاقدين فيتم عن طريق استخدام "شفرة المفتاح العام" حيث يمكن للطرفين المتعاقدين أن يوقعا على المستندات بطريقة رقمية، ويتأكد كل طرف من توقيع الطرف الأخر باستخدام المفتاح العام للشفرة[٧٥].

وعلى الرغم من قيام الجهات ذات الأنظمة المعلوماتية بحماية نظمها عن طريق الترميز والتشفير وغيرها من طرق الحماية المعلوماتية، فإن قراصنة الحاسب الآلي والعاملين في ذات المؤسسات يستطيعون اختراق هذه الأنظمة ومن ثم يجعلون حمايتها عديمة الجدوى، لا سيما لو كانوا من العاملين داخل المؤسسة، وذلك بالدخول إلى المعلومات السرية أو الأسرار التجارية بغرض بيعها أو استخدامها في مؤسسات جديدة يسعون إلى إنشائها أو يكون هدفهم فقط تغيير الأرقام والبيانات أي تخريب المعلومات، كما أن الأمور لا تقف عند هذا الحد، بل إن هؤلاء يقومون بفرض تدابير أمنية لمنع التفتيش المتوقع بحثا عن أدلة إدانة ضدهم، وذلك كاستخدام كلمات سر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة الإطلاع على أي دليل يخلفه نشاطهم الإجرامي، الأمر الذي يعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة، حيث إنه بعد تقدم شبكة الإنترنت الدولية، لم تعد الحدود الجغرافية عائقا في الاختراق، بل أكثر من هذا يلجأ الجاني إلى أسلوب حماية لمنع ضبطه أو الإيقاع به، الأمر الذي يشكل تهديدا لحرمة البيانات الشخصية المخزنة، وكذلك أسرار التجارة المعلوماتية وكذلك تدابير الدفاع والأمن[٧٦].

والحقيقة فإن مسألة استخلاص الدليل في الجريمة المعلوماتية، وبغير الطرق التقليدية، يثير ما يسمى "بالدليل العلمي" في مسألة الإثبات الجنائي، والدليل العلمي يقصد به النتيجة التي تسفر عنها التجارب العلمية والمعملية لتعزيز دليل سبق تقديمه سواء لإثبات أو لنفي الواقعة التي يثار الشك بشأنها، وبطبيعة الحال فإن إجراء هذه التجارب والوسائل لا تكون سوى من مختص فنية وهو بهذه المثابة لا يعدو إلا إن يكون رأيا فنيًا. وهذا الدليل العلمي، يعد شكلا استثنائية للأدلة المقدمة في الدعوى الجنائية، ويكون طلبه بناء على طلب القاضي أو أحد الخصوم في الدعوى، وطلب القاضي للدليل العلمي، هو من المسائل الفنية التي لا يجوز للمحكمة أن تحل نفسها فيها محل

---

[٧٥] المرجع السابق، ص٤

[٧٦] د. جودة حسين محمد. جهاد، المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، مرجع سابق، ٢٠٠٠، ص٦

الخبير، لأنها مسألة فنية في حاجة إلى خبير فني، ومع ذلك لو كان طلب ندب الخبير من جانب الخصوم فإن المحكمة غير ملزمة بإجابة طلبهم طالما أن الواقعة قد وضحت لديها، وفي مقدورها أن تشق طريقها في المسألة المطروحة عليها(٧٧).

والقاعدة العامة أن الدليل العلمي والمستفاد من الخبرة الفنية لا بد وأن يكون مشروعة. ومع ذلك ورغم مشروعية الدليل العلمي والحاجة إليه، فإن ذلك لا يعني سلب المحكمة حقها في أن تأخذ أو لا تأخذ بتقرير الخبير الذي نديته، إن هي رأت لأي سبب من الأسباب ألا تأخذ بتقرير الخبير فلا يصح رميها بالتناقض، وتفسير ذلك أن الدليل العلمي يخضع لوزن وتقدير القاضي في ضوء الأدلة التي قدمت في الدعوى من خلال بحث مشروعية الأساليب التي يمكن من خلالها الحصول على هذا الدليل وإن كان هذا الدليل هو الوحيد في الدعوى فلا يمكن عده قاطعة في الإثبات أو النفي، ومن ثم يفسر الشك لمصلحة المتهم. وهناك جانبا من الفقه القانوني يرى أن الوسائل العلمية في أغلب حالاتها ليست دليلا مستقلا في ذاته وإنما هي قرائن يتم دراستها واستخلاص دلالتها، وهي غير مستقلة عن القرائن، ويرجع ذلك إلى أنها لا تصلح في ذاتها كدليل وحيد في الإثبات الجنائى(٧٨).

ولو تم التسليم بالقواعد التقليدية في الإثبات في شأن وزن الدليل العلمي في الجريمة المعلوماتية عن طريق الحاسب الآلي وعدم اعتماده وحده كدليل في الإثبات بوصفه قرينة ما لم تؤازره أدلة أخرى فسوف يؤدي ذلك إلى إفلات الجناة في هذه القضايا، كما أن عدم وجود كوادر فنية مدربة من رجال أجهزة العدالة في شأن ضبط هذه الجرائم، فيؤدي ذلك إلى أن تقوم هذه الأجهزة بندب الفنيين والخبراء في مجال الحاسب الآلي لضبط هذه الجرائم، وهؤلاء الفنيين والخبراء يقومون بالمعاينة، والمشاركة في الضبط وفحص الأدوات وتحليل الأجهزة والتوصل للمعلومات ووضعها تحت يد أجهزة العدالة وتحت إشرافهم، والقول بأن عمل هؤلاء الخبراء ليس سوى قرينة يتعين أن تؤازر بأدلة أخرى(٧٩).

---

(٧٧) د. علي محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مرجع سابق، ص ٢٨٢

(٧٨) د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت. مصر، دار الكتب القانونية،٢٠٠١، ص٨٩

(٧٩) د. محمود عبد الله حسين، سرقة المعلومات المخزنة في الحاسب الآلي. القاهرة، دار النهضة العربية، ٢٠٠٢، ص ٣١

(ISSN: 2537 - 0758)

ومن المسائل التي أثيرت كذلك بمناسبة تعذر الحصول على الدليل في الجريمة المعلوماتية عن طريق الحاسب الآلي بطرق تقليدية نظرا لخصوصية هذا النوع من الجرائم، وذلك من خلال مدي سريان الحماية المعمول بها بمنع الإطلاع غير المصرح به على الأوراق المختومة أو المغلقة، لتمتد إلى نظام المعالجة الآلية للبيانات، والمحمى فنية ضد الاختراق. ويتضح من خلال ذلك أنه يحظر على المحقق الإطلاع على الأوراق المختومة أو المغلفة في الجرائم التقليدية، وبالتالي فإنه يحظر على المحقق من الإطلاع على نظام الحماية الآلية البيانات المخزنة والمحمي كليا أو جزئية ضد الإطلاع كما قدمنا، إما عن طريق التشفير أو الترميز أو بأي وسيلة فنية أخرى ضد الاختراق، ويرى الجانب الذي أثار هذه المسألة الرد بالإيجاب وأنه يمنع المحقق من الإطلاع وذلك لسببين[٨٠]:

١) أن السبب في حظر الإطلاع على الأوراق المغلفة والمغلقة، هو رغبة صاحبها في عدم إطلاع الغير المصرح بها، بدليل أنه اتخذ سبل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها، بدليل إغلاقه هذه الأوراق أو تغليفها بأي طريقة، وذات العلة تتوافر في البيانات المعالجة آلية، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو الكود أو كلمة المرور الدخول إلى نظام هذه البيانات، وبذلك يكون صاحب ذلك النظام قد رفض مسبقا عمليات الاطلاع غير المصرح به ما لم يكن الراغب في الاطلاع مصرح له عن طريق إعطائه مفتاح المرور إلى هذه البيانات وذلك لا يتوافر في حالة المحقق القائم بالتفتيش موضوع الحديث.

٢) هناك قاعدة عامة بالنسبة للاطلاع على الأسرار التي حصنها صاحبها ضد الاطلاع غير المصرح به أيا كان وعاء هذه الأسرار أو البيانات والمعلومات، يستوي في ذلك أن يكون وعاءها تقليدية كالأوراق أو الصور الضوئية أو الفوتوغرافية أو غير تقليدي عن طريق استعمال الشرائط الممغنطة والأقراص المرنة، وحتى الذاكرات الداخلية للحاسبات، وشبكات المعلومات المحلية والدولية، وعليه يحظر على المحقق الإطلاع على هذه البيانات والمعلومات المخزنة سواء من تلقاء نفسه متى توافرت لديه المقدرة الفنية على ذلك، أو عن طريق آخرين من أهل الخبرة الفنية في مجال الحاسب الآلي لمساعدته في إزالة واختراق الحماية الفنية المقامة حول النظام المعلوماتي المذكور.

---

[٨٠] د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص٣٦ وما بعدها.

ثانيًا: المعوقات المتعلقة بضخامة البيانات المتعلقة بالجريمة:

لعل من الصعوبات الكبيرة التي تواجه رجال الضبط وسلطات التحقيق الجنائي في الجرائم المعلوماتية عن طريق الحاسب الآلي كمية المعلومات والبيانات الضخمة والتي هي في حاجة إلى فحص ودراسة كي يستخلص منها دليل هذه الجريمة، ففضلا عن ضرورة توافر الخبرة الفنية في مجال الحاسب الآلي والمعلوماتية لدى رجل الضبط أو المحقق، يتعين كذلك أن يتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة على الحاسب الآلي أو على ديسكات أو اسطوانات منفصلة[٨١].

ولذلك يمكن القول أن ضخامة هذه البيانات والمعلومات، تعد عائقا في تحقيق الجرائم المعلوماتية عن طريق الحاسب الآلي، ذلك أن طباعة كل ما هو موجود على الدعامات الممغنطة لحاسب متوسط العمر، يتطلب مئات الآلاف من الصفحات، في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئا مفيدة للتحقيق. وهذا عكس ضخامة أو وفرة المعلومات في الجرائم التقليدية كالقتل أو السرقة، ذلك أن وفرة المعلومات في مثل هذه الجرائم هو أمر يساعد العدالة ويساعد رجل الضبط أو المحقق على السواء –في استخلاص الدليل الجنائي في هذه الجريمة[٨٢].

ومن خلال ما سبق، وفي ظل تواضع المستوى الفني لرجل الضبط والمحقق الجنائي فيما يتعلق بفنون الحاسب الآلي واستخداماته، فإنه يكون الملائم وجوب ندب خبراء فنيين في مثل هذه الجرائم حتى يمكن فرز المعلومات التي يحتاجها التحقيق عن تلك التي لا حاجة لها، وإلا دخل رجل الضبط والمحقق في دائرة مغلقة من المعلومات لن يخرج منها، وهذا يتطلب أن يكون ندب هؤلاء الخبراء وجوبية، ومن ثم تعديل التشريعات الجنائية القائمة التي تجعل ندب خبير في الدعوى أمر جوازي للمحقق إن شاء أمر به أو رفضه؛ وذلك لأن طبيعة الجريمة تستلزم التعامل معها بطريقة حرفية أو فنية تفوق قدرات رجل الضبط أو المحقق؛ إلا إذا كان مؤهلا لذلك، فيمكنه الاعتماد على قدراته الشخصية في ضبط وتحقيق هذه الجرائم، بشرط ألا يخرج عمله عن الأصول الفنية المتعارف عليها[٨٣].

---

[٨١] د. نبيل على على العرب وعصر المعلومات، الكويت، عالم المعرفة، ١٩٩٤، ص٩١

[٨٢] د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص٣٦

[٨٣] المرجع السابق، ص٣٧

(ISSN: 2537 - 0758)

الخاتمة

في ختام البحث نعرض للنتائج التي توصلنا إليها ونعقب ذلك ببعض التوصيات على النحو التالي:

النتائج:

- فأهمية الدليل في المواد الجنائية أهمية عظيمة لأنه هو الذي يناصر الحقيقة ويبين مرتكبها، وهو الذي يحول الشك إلى يقين.
- الدليل المتحصل من الوسائل المعلوماتية يستمد طبيعته من ذات العمليات المعلوماتية التي نتج منها في حالة الاعتداء عليها بالأفعال غير المشروعة، ولذلك فهو يتخذ أيضا طبيعة الكترونية بحيث تصعب على المحقق الا بأتباع إجراءات معينه يكون الغالب منها ذو طبيعة فنية.
- ويعد انتحال الشخصية، وكذلك التسلل الإلكتروني من أبرز أمثلة السلوك الإجرامي في الجرائم المعلوماتية، وذلك كدليل على عدم رؤية دليل الجريمة، فكلاهما يستخدم أساليب عالية التقنية في الدخول إلى المناطق المؤمنة والمحمية إلكترونية أو الوصول إلى مراكز الحاسب الآلي والدخول إلى قواعد المعلومات، ويكون الدخول شخصيا أو إلكترونية.
- إن السبب في حظر الاطلاع على الأوراق المغلقة، والمغلقة والمختومة هو رغبة صاحبها في عدم اطلاع الغير عليها، بدليل انه اتخذ سبل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها، بدليل إغلاق هذه الأوراق أو تغليفها بأي طريقة وذات العلة تتوافر في البيانات المعالجة ألياً، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو الكود أو كلمة المرور الدخول إلى نظام هذه البيانات.

التوصيات:

نقترح الأخذ ببعض المقترحات حتى يتسنى الوصول إلى مكافحة أكثر فعالية لهذا النوع المستحدث والمتطور من الإجرام، ويمكن لنا تلخيص هذه التوصيات في النقاط التالية:

- مناشدة المشرعين المصري والاماراتى لإعادة النظر في قانون مكافحة جرائم تقنية المعلومات، والمرسوم بقانون فى شأن مكافحة الشائعات والجرائم الالكترونية، والنص صراحة على بعض الجرائم التقليدية التي تطورت وأصبحت ترتكب بواسطة وسائل

التقنية الحديثة كالارهاب الإلكترونى والتجسس والنصب، والتزوير وإدراجها في نصوص عقابية رادعة تتناسب وخطورتها، مع ضرورة وضع نصوص إجرائية تنظيمية تتعلق بإجراءات تحريك الدعوي القضائية ومباشرة الخصومة أمام الجهات القضائية والطعن في الأحكام.

- الدعوة إلى ضرورة إصدار قانون ينظم إجراءات الضبط والتفتيش للكيانات المعنوية للحاسب الآلي، ونظم تقنية المعلومات، مع ضرورة الأخذ في الاعتبار خصائص جرائم تقنية المعلومات من حيث سرعة إخفاء الدليل وتدميره وعدم ترك آثار مادية.
- ضرورة أن يتضمن قانون الإجراءات الجزائية الاتحادي بدولة الإمارات، وكذلك قانون الإجراءات الجنائية المصرى قواعد لتنظيم إجراءات الضبط في جرائم تقنية المعلومات، يعطي مأموري الضبط القضائي سلطة استخدام كافة الوسائل الممكنة للضبط المشروع عن طريق الشبكة الإلكترونية.
- نظيم واجب التعاون بين رجال الضبط القضائي والجهات العامة والجهات الخاصة التي تمتلك أجهزة معالجة المعلومات والتي يمكن أن تحوز معلومات تفيد في كشف الحقيقة عن وقوع جريمة معينة أو نسبتها إلى فاعلها، وذلك من ناحية شروطه وأحواله، مع التحفظ الخاص بالملتزمين بسر المهنة.
- ضرورة الإهتمام بكفالة عقد دورات تدريبية مكثفة في مراكز فنية متخصصة لتدريب رجال ومأموري الضبط القضائي وإعداد وتنمية الكوادر الفنية المتخصصة للاستعانة بهم في معاونة رجال الأمن والقضاء في كشف الجريمة والتحقيق فيها، وعقد تلك الدورات أيضًا لأعضاء النيابة العامة والقضاة لتثقيفهم فنياً والإلمام بالأمور الفنية التي تعينهم على كشف الجرائم المعلوماتية التقنية والتحقيق فيها ومعرفة عناصرها وأسرارها.
- الاهتمام بدور الخبرة الفنية المتخصصة في مجال تقنية المعلومات وتفعيل الاستعانة بخبراء التقنية وجعل التقارير الفنية الصادرة عنهم إلزامية أي الخروج بها من مرحلة الاستشارية إلى الإلزامية لأهميتها في كشف ملابسات وطلاسم الجريمة.

(ISSN: 2537 - 0758)

المراجع

- د. أحمد عبد اللطيف الفقي الدولة وحقوق ضحايا الجريمة، دار الفجر، القاهرة، ط١ ٢٠٠٣.
- د. ايمن عبد الحفيظ عبد الحميد، إستراتيجية مكافحة جرائم الحاسب الألي، دراسة مقارنه، رسالة دكتوراه، أكاديمية الشرطة، بدون سنة طبع.
- د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، ٢٠٠٢.
- د. جودة حسين محمد. جهاد، المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، دراسة مقارنة، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١-٢ مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون،٢٠٠٠.
- د. حاتم عبد الرحمن منصور، الإجرام المعلوماتي، دار النهضة العربية، ط١، ٢٠٠٢.
- د. حسين بن سعيد الغافرى، السياسة الجنائية فى مواجهة جرائم الانترنت "دراسة مقارنة"، دار النهضة العربية، ٢٠٠٩.
- د. حسين بن سعيد الغافري، الخبرة ودورها في كشف الجرائم المتعلقة في الانترنت، تقرير منشور في الانترنت.
- د. خالد ممدوح إبراهيم، التقاضي الالكتروني، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٧ .
- د. سامي النصراوي، دراسة في أصول المحاكمات الجزائية، الجزء الأول، مطبعة دار السلام، بغداد، ١٩٧٨.
- د. سليم ابراهيم حربة وعبد الامير العكيلي، شرح قانون اصول المحاكات الجزائية، بغداد، ١٩٨٨.
- د. سمير حجازى، التهديدات الإجرامية للتجارة الالكترونية. دبي، مركز البحوث والدراسات بإدارة شرطة دبي، ١٩٩٩.
- د. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية) دار الجامعة الجديدة، الإسكندرية، ٢٠٠٩.
- د. عائشة بن قاره مصطفى، حجية الدليل الالكتروني في مجال الإثبات، دار الجامعة الجديدة، ٢٠١٠.
- د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٢.
- د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، مصر، ٢٠٠٧.

- د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٦.
- د. عبد الناصر محمد فرغلى، محمد عبيد المسمارى، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، ٢٠٠٧.
- د. علي محمودحمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي. بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية مركز البحوث والدراسات أكاديمية شرطة دبي – محور القانون الجنائي في الفترة من ٢٤– ٢٨ أبريل ٢٠٠٣.
- د. عمر ابو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة الكترونية، دار النهضة العربية، القاهرة، ٢٠١٠.
- د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية، المجلد الأول، ١٩٩٠.
- د. عمر الفاروق الحسينى، تأملات في بعض صور الحماية الجنائية لنظام الحاسب الآلي. تقرير مقدم إلى الدورة التدريبية التي ينظمها اتحاد المصارف العربية في الفترة من ٧– ٩ مايو، في الجوانب القانونية النجمة عن استخدام الحاسب الآلي في أعمال البنوك، ١٩٩١
- د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٤.
- د. قدري عبد الفتاح الشهاوي، ضوابط الاستدلالات والإيضاحات والتحريات في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، ٢٠٠٢.
- د. ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، ١٩٩٤.
- د. مأمون محمد سلامة، قانون الإجراءات الجنائية معلق عليه بالفقه وأحكام القضاء دار الفكر العربي، ١٩٨٠.
- د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط١، الرياض، ٢٠٠٤.
- د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات، ٢٠٠٠.
- د. محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، المحله الكبرى، ٢٠٠٨.
- د. محمد زكي ابو عامر، الإثبات في المواد الجزائية، دار الجامعة الجديدة، الإسكندرية، طبعة ٢٠١١.
- د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع الشبكة الانترنت، طلا، دار النهضة العربية، القاهرة، ٢٠٠٩.
- د. محمد قادر، شرح قانون أصول المحاكمات الجزائية، ط١، اربيل، ٢٠٠٣.

(ISSN: 2537 - 0758)

- د. محمود صالح العادلي، الجريمة الدولية، دراسة مقارنه، دار الفكر الجامعي، الإسكندرية، ٢٠٠٣.
- د. محمود عبد الله حسين، سرقة المعلومات المخزنة في الحاسب الآلي. القاهرة، دار النهضة العربية، ٢٠٠٢.
- د. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، ٢٠٠٠.
- د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت. مصر، دار الكتب القانونية، ٢٠٠١.
- د. ممدوح عبد الحميدعبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية. الشارقة، دار الحقوق، ٢٠٠١.
- د. نائله عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي القومية، ٢٠٠٠.
- د. نبيل على على العرب وعصر المعلومات، الكويت، عالم المعرفة، ١٩٩٤
- د. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت– دار الفكر الجامعي– الإسكندرية، ط ١، ٢٠٠٧.
- د. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط١، ٢٠٠٨.
- د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ط ١٩٩٢.
- د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنه، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤.
- د. هشام محمد فريد رستم، بحث مقدم الى مؤتمر القانون والكومبيوتر والانترنيت والذي عقد بدولة الامارات العربية المتحدة سنة ٢٠٠٠.
- د. هلالي عبد اللاه احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست ٢٠٠١، دار النهضة العربية، ط١، ٢٠٠٣.
- محمد أمين الرومي، جرائم الكومبيوتر والانترنت، دار المطبوعات الجامعية الاسكندرية، ٢٠٠٤.
- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٨.