المعهد القومى للملكية الفكرية
The National Institute of Intellectual Property
Helwan University, Egypt

المجلة العلمية للملكية الفكرية وإدارة الابتكار

دورية نصف سنوية محكمة يصدرها

المعهد القومي للملكية الفكرية

جامعة حلوان

العدد الثالث

يناير ٢٠٢٠

الهدف من المجلة:

تهدف المجلة العلمية للملكية الفكرية وإدارة الابتكار إلى نشر البحوث والدراسات النظرية والتطبيقية فى مجال الملكية الفكرية بشقيها الصناعي والأدبي والفني وعلاقتها بإدارة الابتكار والتنمية المستدامة من كافة النواحي القانونية والاقتصادية والادارية والعلمية والأدبية والفنية.

ضوابط عامة:

- تعبر كافة الدراسات والبحوث والمقالات عن رأى مؤلفيها ويأتي ترتيبها بالمجلة وفقا لإعتبارات فنية لا علاقة لها بالقيمة العلمية لأى منها.
- تنشر المقالات غير المحكمة (أوراق العمل) فى زاوية خاصة في المجلة.
- تنشر المجلة مراجعات وعروض الكتب الجديدة والدوريات.
- تنشر المجلة التقارير والبحوث والدراسات الملقاه في مؤتمرات ومنتديات علمية والنشاطات الأكاديمية في مجال تخصصها دونما تحكيم في أعداد خاصة من المجلة.
- يمكن الاقتباس من بعض مواد المجلة بشرط الاشارة إلى المصدر.
- تنشر المجلة الأوراق البحثية للطلاب المسجلين لدرجتى الماجستير والدكتوراه.
- تصدر المجلة محكمة ودورية نصف سنوية.

ألية النشر فى المجلة:

- تقبل المجلة كافة البحوث والدراسات التطبيقية والأكاديمية في مجال حقوق الملكية الفكرية بكافة جوانبها القانونية والتقنية والاقتصادية والادارية والاجتماعية والثقافية والفنية.
- تقبل البحوث باللغات (العربية والانجليزية والفرنسية).
- تنشر المجلة ملخصات الرسائل العلمية الجديدة، وتعامل معاملة أوراق العمل.
- يجب أن يلتزم الباحث بعدم إرسال بحثه إلى جهة أخرى حتى يأتيه رد المجلة.
- يجب أن يلتزم الباحث بإتباع الأسس العلمية السليمة في بحثه.
- يجب أن يرسل الباحث بحثه إلى المجلة من ثلاثة نسخ مطبوعة، وملخص باللغة العربية أو الانجليزية أو الفرنسية، فى حدود ٨ ـ ١٢ سطر، ويجب أن تكون الرسوم البيانية والإيضاحية مطبوعة وواضحة، بالإضافة إلى نسخة إلكترونية Soft Copy، ونوع الخط Romanes Times New ١٤ للعربى، و١٢ للانجليزي على B5 (ورق نصف ثمانيات) على البريد الالكتروني: ymgad@niip.edi.eg
- ترسل البحوث إلى محكمين متخصصين وتحكم بسرية تامة.
- في حالة قبول البحث للنشر، يلتزم الباحث بتعديله ليتناسب مع مقترحات المحكمين، وأسلوب النشر بالمجلة.

مجلس إدارة تحرير المجلة	
أ.د. ياسر محمد جاد الله محمود	أستاذ الاقتصاد والملكية الفكرية وعميد المعهد القومي للملكية الفكرية (بالتكليف) - رئيس تحرير المجلة
أ.د. أحمد عبد الكريم سلامة	أستاذ القانون الدولي الخاص بكلية الحقوق بجامعة حلوان والمستشار العلمي للمعهد سلطان عضو مجلس إدارة تحرير المجلة
أ.د. وكيل المعهد للدراسات العليا والبحوث	سكرتير تحرير المجلة
أ.د. جلال عبد الحميد عبد اللاه	أستاذ الهندسة الانشائية بكلية الهندسة بالمطرية بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. هناء محمد الحسيني	أستاذ علوم الأطعمة بكلية الاقتصاد المنزلي بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. وزير مفوض/ مها بخيت محمد زكي	مدير إدارة الملكية الفكرية والتنافسية بجامعة الدول العربية - عضو مجلس إدارة تحرير المجلة
اللواء أ.د. عبد القدوس عبد الرزاق العبيدلي	رئيس مجلس إدارة جمعية الامارات للملكية الفكرية - عضو مجلس إدارة تحرير المجلة
Prof Dr. Alexander Peukert	أستاذ القانون المدنى بجامعة جوته فرانكفورت أم ماين – ألمانيا - عضو مجلس إدارة تحرير المجلة
Prof Dr. Andrew Griffiths	أستاذ القانون التجارى بجامعة نيو كاسل - بريطانيا - عضو مجلس إدارة تحرير المجلة

المراسلات

ترسل البحوث إلى رئيس تحرير المجلة العلمية للملكية الفكرية وإدارة الابتكار بجامعة حلوان
جامعة حلوان - ٤ شارع كمال الدين صلاح - أمام السفارة الأمريكية بالقاهرة -جاردن سيتى
ص.ب: ١١٤٦١ جاردن سيتي
ت: ٠٢٥٤٨١٠٥٠ ٢٠٢ + محمول: ٢٠١٠٠٠٣٠٠٥٤٨ + ف: ٠٢٧٩٤٩٢٣٠ ٢٠٢ +
http://www.helwan.edu.eg/niip/
ymgad@niip.edu.eg

"الدور العملي لوزارة الداخلية في مكافحة الجريمة المعلوماتية"

محمد سامي السيد احمد

"الدور العملي لوزارة الداخلية في مكافحة الجريمة المعلوماتية"

محمد سامي السيد احمد

مقدمة :

إن أهم ما يميز العصر الحالي عن غيره من العصور هو ما نشهده اليوم من تطور مثير في المجالات التكنولوجية الأمر الذى انعكس على مجمل مجالات الحياة بحيث القول بثقة بأنه لم يعد هناك شأن بالحياة الانسانية إلا ناله نصيب من هذا التطور التكنولوجي المثير الذي احدث ثورة ادخلت البشرية في عصر جديد وعلى الرغم من الايجابيات العديدة التى احدثتها تقنية الانترنت في تسهيل نقل وتبادل المعلومات ألا أن هناك خشية متزايدة من تنامى الخروق والسلبيات لهذه الشبكة واستغلالها من قبل بعض العصابات والافراد لارتكاب وتعميم اعمال وافعال تتنافي مع القوانين ومع الأعراف والأخلاق والأداب.

أهمية البحث :

تبدو مشكلة الدراسة فى أن معظم جرائم التطور التكنولوجى تعد من الجرائم الخفية حيث يقع العديد منها دون اكتشافه ، وذلك لطبيعة هذه الجرائم التى تنطوى على قدر كبير من الخداع والاحتيال الذى يبدو فى قدرة مرتكبيها على إقناع ضحاياهم بأن أهدافهم عادية ومشروعة، كما تتسم هذه الجرائم بالتعقيد المتزايد الأمر الذى يعوق عملية الكشف عنها أو حتى ملاحقة مرتكبيها وعقابهم لقدرتهم الفائقة على إخفائها ، فضلا عن أنهم من ذوى الياقات البيضاء. هذا بالإضافة إلى عدم وجود أجهزة متخصصة لكشفها والتحقق منها ، وللقصور التشريعى فى مواجهتها، وموقف الضحايا السلبى إما لعدم علمهم بارتكاب جرائم ضدهم ، أو لعدم وجود دليل مادى على مرتكبى الجرائم ضدهم، أو للتسجيل المغلوط لجرائم التطورالتكنولوجى.

هدف الدراسة وتساؤلاتها:

تسعى الدراسة الحالية إلى محاولة الكشف عن العلاقة التى تربط بين التطور التكنولوجى والجريمة ، ويهدف ايضاً إلي التركيز علي آليات وجهود مكافحة هذه الجرائم امنياً ولتحقيق هذا الهدف ستحاول الدراسة الإجابة عن التساؤلات الآتية:

ما هي الجريمة المعلوماتية وما هي خصائصها ومن هو المجرم المعلوماتي وما هي سماته وما دور وزارة الداخلية فى مواجهة جرائم التطور التكنولوجي وتحديد حجمها؟

منهج البحث :

استخدم الباحث المنهج التحليلي االذي يسعي الي وصف وتحليل وتشخيص موضوع البحث من مختلف جوانبه وأبعاده بهدف الوصول الي نظرة واضحة عن الإليات الملائمة لمكافحة هذه الظاهرة الإجرامية المستحدثة

خطة البحث :

تتضمن خطة البحث موضوع المواجهة الأمنية للجرائم المعلوماتية وسوف نتناول الموضوع كالتالي :

مبحث تمهيدي :

تعريف الجريمة المعلوماتية وخصائصها وسمات المجرم الالكتروني

المبحث الاول
الدور العملي لوزارة الداخلية في مكافحة الجريمة المعلوماتية والمتمثل في دور مامور الضبط القضائي بصفته المنوط به ضبط الجريمة ومكافحتها

مبحث تمهيدي

لقد صاحب التطور التكنولوجي الهائل الذى احدثته تقنية المعلومات ظهور بعض الفئات التي سعت الي تحويل هذة التقنية الي وسيلة لارتكاب الجرائم الالكترونية سنحاول في هذا المبحث التعرف علي ماهية هذة الجرائم من خلال توضيح مفهومها وخصائصها (مطلب اول) وسمات المجرم الالكتروني (مطلب ثاني).

المطلب الاول

تعريف الجريمة المعلوماتية

اولا : التعريف الفقهي للجرائم المعلوماتية :

تعدد تعريفات الفقه للجرائم المعلوماتية (١) :

نتناول فيما يلى بعض التعريفات الفقهية التى قيلت فى تعريف الجريمة المعلوماتية بالنظر إلى إعتبار المعلوماتية كموضوع للجريمة أو كوسيلة لإرتكاب الجريمة، وذلك على النحو التالى:

الإتجاه الأول: المعلوماتية كموضوع الجريمة:

إرتكز جانب كبير من الفقه الجنائى فى تعريف الجريمة المعلوماتية على التقنية المعلوماتية كموضوع أو كوسيلة إعتداء، فقد ذهب البعض على تعريفها بأنها: "الإعتداء القانونى الذى يرتكب بواسطة المعلوماتية بغرض تحقيق ربح".

وذهب الفقيه روزبلات إلى تعريفها بأنها: "كل فعل أو إمتناع عمدى ينشأ عن نشاط غير مشروع لنسخ أو تغييرات أو حذف أو الوصول إلى المعلومات المخزنة فى الحاسب، أو تلك التى تحول عن طريقه".

وقد عرفها جانب ثالث بأنها: "كل أستخدام فى صور فعل أو إمتناع غير مشروع للتقنية المعلوماتية ويهدف إلى الإعتداء على أية مصلحة مشروعية سواء كانت مادية أو معنوية.

وأخيراً عرفتها منظمة التعاون الإقتصادى والتنمية على أنها: "كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة عن تدخل التقنية المعلوماتية".

---

(١) انظر في تعدد تعريفات الجرائم المعلوماتية د. هشام محمد فريد رستم: الجرائم المعلوماتية – اصول التحقيق الجنائي الفني ، ورقة عمل مقدمة الي مؤتمر القانون والكمبيوتر والانترنت ، كلية الشريعة والقانون ، جامعة الامارات العربية المتحدة مجلد ٢ ، ص ٤٠٥ وما بعدها.

ويتضح من التعريفات السابقة أن الإتجاه السابق يرى الجريمة المعلوماتية بإعتبارها كل سلوك إيجابى أو سلبى يقع بإستخدام التقنية المعلوماتية على مصلحة مشروعة بالإعتداء.

الإتجاه الثانى :المعلوماتية كوسيلة لإرتكاب الجريمة :

وهناك جانب آخر من الفقه الجنائى من ذهب إلى تعريف الجرائم المعلوماتية بالنظر إلى إعتبار الحاسب الآلى كوسيلة لإرتكاب الجريمة، إذ عرفها الفقيه الألمانى تاديمان بأنها كل "أشكال السلوك غير المشروع (أو الضار بالمجتمع) الذى يرتكب بإستخدام الحاسب".

وقد عرفها مكتب تقييم التقنية فى الولايات المتحدة الأمريكية، من خلال تعريف جريمة الحاسب بأنها "الجرائم التى تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دوراً رئيسياً"، كما عرفتها الأستاذة **Eslie D. Ball** بأنها: "فعل إجرامى يستخدم الكمبيوتر فى إرتكابه كأداة رئيسية".

الإتجاه الثالث: التعريف الشامل للجرائم المعلوماتية:

وإلى جانب هذا التعريف، فهناك من ذهب إلى وضع تعريفاً شاملاً للجريمة المعلوماتية، يتمثل فى تعريفها بأنها تتضمن كافة أشكال السلوك غير المشروع الذى يرتكب بإستخدام الحاسب، أو الجرائم التى تلعب فيها البيانات التكنولوجية والبرامج المعلومات دوراً رئيسياً.

أو أى فعل إجرامى يستخدم الحاسب الآلى فى إرتكابه كأداة رئيسية، أو أى نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التى تحول عن طريقه، أو أية جريمة يكون متطلباً لإختراقها توافر لدى فاعلها معرفة تقنية الحاسب.

أو هى كل فعل أو إمتناع من شأنه الإعتداء على الأحوال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، أو كل سلوك غير مشروع أو غير أخلاقى أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها.

ثانيا :سمات الجرائم المعلوماتية والمجرم المعلوماتي

تُعد الجرائم المعلوماتية من الجرائم التى تتسم بسمات خاصة عن غيرها من الجرائم، فهى تستهدف معنويات وليست ماديات محسوسة، فضلاً عما يتسم به مرتكبو هذه الجرائم من سمات خاصة عن المجرمين التقليدين، وفيما يلى نتناول سمات الجرائم المعلومتية على النحو الاتي:

الفرع الاول

سمات الجرائم المعلوماتي

تمثل الجرائم المعلوماتية إفرازاً طبيعاً لتقنية المعلومات وإتساع نطاق تطبيقها فى المجتمع، مما يضفى عليها طابعاً قانونياً خاصاً، وفيما يلى نتناول الطابع التقنى والمتنوع للجرائم المعلوماتية فضلاً عن الطابع العابر للحدود على النحو التالى:

أولاً : طابع التقنية :

تتسم الجرائم المعلوماتية بسمة خاصة، تتمثل فى إرتكاب هذه الجريمة بواسطة أجهزة الحاسب الآلى، بل أن بعض هذه الجرائم قد ترتكب عبر شبكة الإنترنت، وهو ما يتطلب طبيعة خاصة فى مرتكبى هذه الجرائم، وأن يكونوا على دراية فائقة فى إستخدام الحاسب الآلى. ويترتب على الطابع التقنى للجريمة المعلوماتية، خصائص مشتركة قد لا تتوافر فى الجرائم التقليدية ، ويمكن إيجازها فى إتسامها بكثير من التعقيد والغموض، وكذا عدم إتسامها بالعنف(١)، فضلاً عن صعوبة إكتشاف وضبط مرتكبيها ومحاكمتهم، وضخامة الخسائر الناجمة عنها، وأخيراً إمكانية تدمير المعلومات التى يمكن أن تستخدم كدليل فى الإثبات فى مدة لا تقل عن الثانية الواحدة(٢).

---

[١] () سليمان أحمد فضل: البعد الدولى للجرائم المعلوماتية وطرق مواجهتها، ورقة عمل مقدمة لندوة الواقع الأمنى مسئوليات– إنجازات، مركز بحوث الشرطة بأكديمية الشرطة، القاهرة، ص٥.

[٢] () هشام محمد فريد رستم: قانون العقوبات، ومخاطر تقنية المعلومات، الطبعة الاولي ، مكتبة الالات الحديثة ، اسيوط ، ١٩٩٢ ، ص٤٢.

ثانياً : الطابع العابر للحدود :

تتسم الجرائم المعلوماتية بسمة أخرى هى الطابع غير الوطنى؛ فهى جريمة تتخطى الحدود الجغرافية للدول، فهى جريمة لا تعرف حدوداً وطنية(١)، وهو ما يسبغها الطابع الدولى، فغالبية الجرائم المعلوماتية يتم إرتكابها عبر شبكة الإنترنت، والتى يُمكن لمستخدميها إرتكاب أية جريمة فى دولهم أو أى دولة أخرى فى العالم، هذا بالإضافة إلى سرعة نقل البيانات والمعلومات، والأموال فى مثل هذه الجرائم(٢)، وهو ما يترتب عليه صعوبات إجرائية فى ملاحظة هؤلاء الجناة، تحتاج إلى تضافر الجهود الدولية فى تنظيم أطر المواجهة والتعاون الدولى لمكافحة هذه الطائفة من الجرائم.

فملاحقة مرتكبى الجرائم المعلوماتية، تتطلب القيام بأعمال إجرائية خارج حدود الدولة، حيث إرتكبت الجريمة أو جزء منها كمعاينة وتفتيش المواقع الإلكترونية، وضبط البيانات والمعلومات، والوسائل المادية التى تحتوى على مثل هذه البيانات والمعلومات، وهو ما لا يتحقق بدون مُساعد الدول الأخرى(٣).

ثالثاً: طابع التنوع :

من السمات الخاصة التى تتسم بها الجرائم المعلوماتية طابع التنوع، فالجريمة المعلوماتية ذات وجه مُتغير، فهى تبدأ من جريمة فردية كما هو الحال فى جرائم قرصنة المعلومات الفردية إلى الإجرام المعلوماتى المُنظم عبر عصابات الجريمة المنظمة والجماعات الإرهابية المتطرفة التى تستخدم شبكة الإنترنت فى أنشطتها الإجرامى، وما تقوم به هذه العصابات من حيل للدخول على شبكة الإنترنت وتنفيذ مخططاتهم الإجرامية.

---

(١) كريستوفر بينتر، التهديد الذي تفرضه الجريمة المعلوماتية والحاجة الي التعاون الدولي ، ورقة عمل مقدمة للمؤتمر الدولي السادس للجرائم المعلوماتية الذي نظمته المنظمة الدولية للشرطة الجنائية " الانتربول " ، القاهرة ، ترجمة بحوث الشرطة ، ص٦٦.

(٢) نائلة عادل محمد فريد قورة: جرائم الحاسب الإقتصادية– دراسة نظرية وتطبيقة، دار النهضة العربية، القاهرة، ٢٠٠٤، ص٤٧.

(٣) سليمان أحمد فاضل، مرجع سابق، ص١٨.

المطلب الثانى
سمات وأنماط المجرم المعلوماتى

إن فكرة المجرم المعلوماتى فكرة جديدة على الفقه الجنائى، ففى الجرائم المتعلقة بالحاسب الإلكترونى نحن لسنا بصدد سارق أو محتال عادى ولكن مجرم ذو مهارات تقنية وذو دراية بالتكنيك المستخدم فى نظام الحاسب الإلكترونى، قادر على إستخدام هذا التكنيك لإختراق الكود السرى لتغيير المعلومات أو لتقليد البرنامج أو التحويل من الحسابات عن طريق إستخدام الحاسب نفسه.

وهذا شيء منطقى حيث ترك عالم الجريمة البؤساء ليدخل إلى عالم مجرمى المهارات المعلوماتية فشخصية المجرم وميكانيكية إرتكابه للجريمة له سمات خاصة بهذا النوع الجديد من الإجرام(١).

أولاً: سمات المجرم المعلوماتى: يمكن إجمال أهم سمات المجرم المعلوماتى فيما يلى (٢):

(١) **مجرم متخصص:** فقد ثبت من عديد من القضايا أن عدداً من المجرمين لا يرتكبون إلا جرائم الحاسب الالي أى أنهم يتخصصون فى هذا النوع من الجرائم.

(٢) **مجرم عائد إلى الإجرام:** يعود كثير من مُجرمى المعلومات إلى إرتكاب جرائم أخرى فى مجال الحاسب الالي إنطلاقاً من الرغبة فى سد الثغرات التى أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة فى المرة السابقة. ويؤدى ذلك إلى العود إلى الإجرام وقد ينتهى بهم الأمر مع ذلك فى المرة التالية إلى تقديمهم المحاكمة.

(٣) **مجرم محترف:** لا يسهل على الشخص الهاوى، إلا فى حالات قليلة، أن يرتكب جرائم بطريق الحاسب. فالأمر

---

[١]() هدى حامد قشقوش، جرائم الحاسب الالكتروني والتشريع المقارن ، دار النهضة العربية ، ١٩٩٢ ، ص٢٧.

[٢]() غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر ، مؤتمر القانون والكمبيوتر والانترنت ، كلية الشريعة والقانون ، جامعة الامارات العربية المتحدة ، ٢٠٠٠، ص٣٥.

يقتضى كثيراً من الدقة والتخصص فى أنظمة الحاسب كما يحدث فى البنوك مثلاً.

(٤) **مجرم ذكي:** لا يمكن أن ينتمى المجرم المعلوماتى إلى طائفة المجرمين الأغبياء، فالمجرم المعلوماتى دائماً ما يتسم بالذكاء، ويتمتع بمهارة وقدرة فائقة على التعامل مع الحاسب الآلى وشبكات المعلومات، ولديه قدرة على إختراقها، والوصول إلى البيانات والمعلومات المطلوبة، فمن يسرق من منزل أو من سيارة غالباً ما يكون منخفض الذكاء بالمقارنة بمن يستعين بالحاسب فى السرقة من أموال بنك أو شركة، نظراً لما يتميز به من مستوى ذكاء مرتفع، حتى يتستطيع أن يتغلب على كثير من العقبات التى تواجهه فى إرتكاب جريمته، فهو أقرب إلى مرتكبى جريمة النصب منه إلى مُرتكبى جريمة السرقة.

علاقة السن بالجريمة المعلوماتية: تجدر الإشارة إلى عدم تقيد المجرم المعلوماتى بسن معين؛ إذ فى العديد من الحالات وُجد أن الجانى كان حدثاً؛ أى أقل من ثمانية عشر عاماً، وهو ما يشير إلى الخصوصية التى تتمتع بها الجريمة المعلوماتية، والتى قد تستهوى العديد من الشباب بدافع إثبات الذات والمغامرة لإرتكاب جرائم ذات آثار وتداعيات خطيرة، وهو أمر فى غاية الخطورة، ومن ضمن الحالات التى تناولت الجرائم المعلوماتية لجناة أحداث، ما قام به صبى كندى يبلغ من العمر (١٤) عاماً فى فبراير عام ٢٠٠٠ بتعطيل بعض المواقع الإلكترونية للعديد من الشركات التجارية **I-TRAFE, I-Bay**، وبعض المواقع الكبرى **CNN, Yahoo**، وهو ما أسفر عن تضررها وخروجها من الخدمة مؤقتاً وتعطيل أعمالها[١]، وأيضاً قيام مجموعة من الشباب الصغار فى هولندا عام ٢٠٠٤ بإختراق بعض المواقع الحكومية[٢].

---

[١] () كريستوفر بينتر، مرجع سابق، ص٦٣.

[٢] () أنظر: ياب فإن أوس: التهديدات الموجهة للبنية التحتية للمعلومات، ورقة عمل مقدمة للمؤتمر السادس للجرائم المعلوماتية، القاهرة ، ترجمة مركز بحوث الشرطة، ص٧٥.

(٥) **مجرم غير عنيف:** ينتمى الإجرام المعلوماتى إلى إجرام الحيلة، فلا يلجأ المجرم المعلوماتى إلى العنف فى إرتكاب جرائمه، هذا النوع من الجرائم لا يستلزم مقداراً من العنف للقيام به.

(٦) **مجرم مُتكيف إجتماعياً:** لا يضع المجرم المعلوماتى نفسه فى حالة عداء سافر مع المجتمع الذى يحيط به بل انه إنسان مُتكيف معه، ذلك أنه أصلاً إنسان مُرتفع الذكاء ويساعد ذلك على عملية التكيف، وما الذكاء فى رأى كثيرين سوى القدرة على التكيف. ولا يعنى ذلك التقليل من شأن المجرم المعلوماتى، بل إن خطورته الإجرامية قد تزيد إذا زاد تكيفه الإجتماعى مع توافر الشخصية الإجرامية لديه.

ثانياً: أنماط المجرم المعلوماتى[١] :

يمكن تصنيف هؤلاء المجرمون إلى الفئات التالية :

(١) **القراصنة:** هناك قسمين من القراصنة: **(الأول):** الهواة وهم من الشباب الفضوليين الذين يسعون للتسلية ولا يشكلون خطورة على أنظمة المعلومات، **(والثانى):** المحترفون وهم أكثر خطورة من الصنف الأول وقد يحدثون أضراراً كبيرة ، وقد يؤلفون أندية لتبادل المعلومات فيما بينهم، ويفضل القراصنة العمل عادة فى جماعات عن العمل الفردى وغالباً ما يكون دافعهم لإرتكاب الجريمة إما الحصول على المال أو بغرض الشهرة أو إثبات تفوقهم العلمى ومدى ما يتمتعون به من ذكاء[٢].

---

[١] () جمال توفيق وآخرون: الجرائم المعلوماتية، دراسة مركز بحوث الشرطة حول الجرائم المعلوماتية وطرق مواجهتها ، مركز بحوث الشرطة ، اكاديمية الشرطة ، الاصدار الثالث ، ص٣٤-٣٦.

- وليد عالكوم: مفهوم وظاهرة الإجرام المعلوماتى، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠، ص٢٧.

[٢] () أيمن عبدالحفيظ: إستراتيجية مُكافحة الجرائم الناشئة عن إستخدام الحاسب الآلى، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، ص٢١٦.

(٢) **المُخادعون:** وهولاء يتمتعون بقدرات فنية عالية بإعتبارهم عادة من الأخصائيين فى المعلوماتية ومن أصحاب الكفاءات، وتنصب معظم جرائمهم على شبكات تحويل الأموال ويمكنهم التلاعب بحسابات البنوك أو فواتير الكهرباء والهاتف أو تزوير بطاقات الإعتماد أو ما شابه[١].

(٣) **الجواسيس:** يهدف هؤلاء إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التى تتنافس فيها بينها.

المبحث الأول

الدور العملي لمأمور الضبط القضائي في مكافحة الجرائم المعلوماتية

المطلب الاول

تلقى البلاغات والشكاوى فى جرائم المعلومات

تبقى الجريمة المعلوماتية كغيرها من الجرائم مستترة عادة إلى أن يتم الإبلاغ عنها للجهات المختصة، وتكمن المشكلة التى تواجه مأمورى الضبط القضائى فى أن تلك الجرائم لا تصل إلى علمهم لصعوبة إكتشافها بواسطة الأشخاص العاديين، أو حتى من قبل المؤسسات الكبرى فى الغالب، وفى حالة إكتشافها من قبل تلك المؤسسات يتم التردد فى الإبلاغ عنها خوفاً على سمعتها، وتظهر أهمية الإبلاغ عن تلك الجرائم فى رصد مرتكبيها ومراقبة المشبوهين.

الفرع الأول

الإبلاغ عن الجرائم المعلوماتية

إن تحريك إجراءات التحقيق فى الجرائم المعلوماتية يختلف عن الجريمة التقليدية التى يدرك عناصرها الرجل العادى كجرائم القتل والسرقة، فالجريمة المعلوماتية تحتاج لمن يدرك عناصرها وطرق إرتكابها والمراحل

---

[١]() باسم منصور: الآليات الأمنية لمواجهة جرائم الحاسب والإنترنت، مجلة مركز بحوث الشرطة، عدد (٣٥)، يناير ٢٠٠٩، ص٢٧١.

التى مرت بها، لذا فتلقى الجهات الأمنية للبلاغات بخصوص تلك الجرائم له آثر وقائى فعال فى مكافحتها، كما أن سرعة التبليغ تجعل الأمور أكثر يسراً فى ضبط مرتكبيها.

ولا يوجد إختلاف حول تلقى البلاغ بالجريمة المعلوماتية عما هو الحال عليه بالجريمة التقليدية، إلا أن به شيئاً من الخصوصية، فهناك تباين فى المعلومات التى ينبغى أن يسجلها مأمور الضبط القضائى عند تلقى البلاغ بتباين فئات الجرائم والطبيعة الفنية، كالمعلومات ذات العلاقة بالأنظمة المعلوماتية وطبيعة البرامج المستخدمة وطريقة الإتصال، لذا كان الأفضل أن يكون لدى متلقى البلاغ نماذج معدة مسبقاً يخصص كل فئة بنوع معين من الجرائم توفيراً للوقت وضماناً للدقة وتسهيلاً لمهمة لإستدلال، لذا يجب أن يكون مصدر البلاغ على درجة كبيرة من الوعى والقدرة والمعرفة بتفاصيل ما يدلى به من معلومات، ويقدم وصفاً علمياً محدداً للنشاط الإجرامى(١).

وتختلف الجريمة المعلوماتية عن الجريمة التقليدية فى أن الأولى لا يمكن إكتشافها غالباً من قبل الأفراد العاديين لصعوبة ذلك، وخصوصاً حينما تركب في على المؤسسات المالية الكبيرة كالبنوك، إذ قد تتردد تلك الجهات فى لإفصاح عن الجريمة لعدة إعتبارات كالسمعة وردة فعل المنافسين المساهمين والمودعين(٢)، مما يؤثر سلباً على سياسة مواجهة تلك الجرائم ، حيث تحرص أكثر الجهات التى تتعرض أنظمتها المعلوماتية للإنتهاك أو تمنا بخسائر فادحة على عدم الكشف عن تلك الإنتهاكات، بل تكتفى بإجراء إحتياطات داخلية دون إبلاغ السلطات المختصة، فالجانب الأكبر من الجرائم لمعلوماتية لا يتم الكشف أو الإبلاغ عنه، فإحاطة جهات الإستدلال بحجم هذه النوعية من الجرائم لا تكون إلا جزئية(٣).

---

(١) محمد الأمين البشرى: التحقيق فى جرائم الحاسب الآلى ، جامعة الامارات ، كلية الشريعة والقانون ، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت .

(٢) محمد الأمين البشرى: مرجع سابق ذكره .

(٣) وتشير بعض الدراسات المسحية الأمريكية إلى أن ٦٪ فقط من الجرائم المعلوماتية يتم الإبلاغ عنها إلى السلطات المختصة بتنفيذ القانون. للمزيد أ.د. هشام فريد رستم: الجرائم المعلوماتية، مرجع سابق، ص ٤٣٦.

وتنص بعض التشريعات على وجوبيه الإبلاغ عن مثل تلك الجرائم من قبل موظفى أمن المعلومات بتلك الشركات متى تم العلم بها بينما قوبل ذلك بالرفض ببعض الدول على أساس إعتبار أن المجنى عليه لا يجوز تحويله إلى مرتكب جريمة(١).

ويعتقد بعض الفقه أنه يمكن التخفيف من ذلك بإلزام تلك الجهات بإبلاغ جهات خاصة أو سلطات إشرافية[٢]، إلا أن الباحث يرى أن ذلك الإجراء يعيق دور مأمورى الضبط القضائى فى مواجهة الجريمة المعلوماتية ، حيث أن الهدف من كشف الجرائم هو ضبط مرتكبيها لتوقيع العقاب عليهم لتحقيق الردع العام والخاص.

أما فيما يتعلق بالشكوى فى الجريمة المعلوماتية فليس هناك أى إختلاف عما هو الحال عليه فى أحكام الشكوى بالجريمة التقليدية، فلا يجوز تحريك الدعوى إلا من صاحب الحق فيها أو من ينوب عنه ، وبما أن الجريمة المعلوماتية يصعب تحديد الجانى فيها أو من ينوب عنه، وبما أن الجريمة المعلوماتية يصعب تحديد الجانى فيها فقد حدا ذلك ببعض الفقه إلى المناداة بتحميل مزود تقديم الخدمة المسئولية طبقاً لمبدأ إفتراض مسئولية الغير(٣)، وبالتالى فإن الشكوى ستنصب على مسئولية مقدمى تلك الخدمة من دون الحاجة إلى البحث عن المجرم الحقيقى، ويرى الباحث أن ذلك سيؤدى إلى عرقلة العدالة.

---

[١]() نبيلة هبة هروال: الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلال دراسة مقارنة ، الاسكندرية ، دار الفكر الجامعي ، ٢٠٠٧ ، ص١٨٥.

[٢]() هشام محمد فريد رستم: الجرائم المعلوماتية، مرجع سابق، ص ١٦-١٧.

[٣]() نبيلة هبة هروال: مرجع سابق ذكره، ص١٩٢.

الفرع الثانى

البلاغ الرقمى

فى الوقت الحاضر أصبح من اليسير الولوج إلى موقع خاص بالبلاغات الرقمية وكتابة البلاغ حول الجريمة ثم إرسالها إلى الجهات المختصة وذلك تمشياً مع التقدم التكنولوجى، فقد تم وضع مواقع مخصصة للتبليغ عن الجرائم التقليدية والمعلوماتية من خلال إرسالها للجهة المختصة، كما هو الحال فى بعض المواقع الأمريكية، كموقع المباحث الفيدرالية (**F B I**) ومركز معالجة الشكاوى فى الولايات المتحدة الأمريكية (**IC3**) [١]، وموقع وزارة الداخلية بجمهورية مصرالعربية ، ومواقع الشرطة المحلية بدولة الإمارات[٢].

فالبلاغ الرقمى هو ما يتم من خلال إرسال رسالة إلكترونية إلى عنوان البريد الإلكترونى للجهات المختصة بتلقى البلاغات والتحرى عن تلك الجرائم، أو من خلال ملء إستمارة رقمية بالموقع نفسه، كأن يقوم أحد الأشخاص بإبلاغ إدارة مكافحة جرائم الحاسبات وشبكات المعلومات المخصص لتلقى البلاغات والشكاوى بجمهورية مصر العربية[٣] عن صفحات إلكترونية على مواقع الويب تقوم بعرض مواد مخلة بالآداب كصورة جنسية، فلم يشترط القانون شكلاً معيناً للبلاغات، كما أنه لم يشترط أن يكون مصدر البلاغ معلوم الهوية، فللمبلغ الحرية فى الإفصاح عن هويته أو إبقائها مجهولة.

ولا يقتصر البلاغ الإلكترونى على الجريمة المعلوماتية فيمكن من خلاله الإبلاغ والشكوى عن الجريمة التقليدية.

وبعد تلقى البلاغ يقوم مأمور الضبط القضائى بمراجعته وتحليله من الناحية التقنية والقانونية للتأكد من صحة المعلومات وجسامة الجريمة ، كما يتم التحقيق من الإختصاص كموقع الخادم أو موقع المضرور حسب

---

[١] () الموقع الإلكترونى: www.ifvvfbi.gov

[٢] () وقد قامت القيادة العامة لشرطة دبى بإنشاء أول مركز شرطة إلكترونى بالشرق الأوسط يعنى بتلقى البلاغات والشكاوى وتعقب المجرمين إلكترونيا من خلال تقديم الخدمات الإلكترونية.

– للمزيد يرجى زيارة الموقع الإلكترونى لشرطة دبى www.dubaipolice.gov.ae

[٣] () من خلال الموقع: www.ccd.gov.eg

القوانين الإجرائية المتبعة ، وبعد إنعقاد الإختصاص يتم تسجيل البلاغ حسب الإجراء المتبع ، ومن ثم إبلاغ الجهة المختصة[١] لتبدأ بعد ذلك عملية الإستدلال عن الجريمة ، وإمداد كل من له علاقة مهنية بالجريمة بكافة البيانات للازمة لسير الإستدلالات، وتتم تلك المعالجة من متخصصين فى مجال تقنية المعلومات والإجراءات الجنائية[٢].

وخلاصة القول أنه على رجال الضبط القضائى قبول البلاغات والشكاوى (العادية والرقمية) عن جميع الجرائم، خاصة وأن أغلب النظم الإجرائية لا تتطلب شكلاً معيناً لتقديم البلاغ أو الشكوى.

المطلب الثاني

البحث والتحرى فى الجريمة المعلوماتية

لعل من أكثر الأمور صعوبة فى البحث والتحرى التوافق بين مقتضيات كشف الحقيقة عند وقوع الجريمة وبين حرية المتهم التى تصونها النظم القانونية بإعتباره بريئاً حتى تثبت إدانته، مع الأخذ فى الإعتبار ضرورة التحرك العاجل لجمع الأدلة خوفاً من طمسها وضياع ملامحها[٣].

ويقوم دور مأمور الضبط القضائى من خلال البحث والتحرى عن الجريمة المعلوماتية بوضع خطة البحث والتحرى عن طريق تحديد خطواتها وإتجاهاتها بتعيين الأشخاص المشتبه بهم والعمليات والإجراءات الواجب إتباعها.

ويؤثر حجم الجهة المجنى عليها وطبيعة أعمالها والسلوك الإجرامى المرتكب فى تحديد نطاق خطة البحث[٤]، فيتم فحص طبيعة تقنية المعلومات محل الجريمة، وفحص الإحتمالات المختلفة، وبحث الإستعانة ببعض المعاونين لإستخدامهم فى الدعم الفنى كالمسئولين عن الإتصالات بغية تحديد الرقم الذى تم عن طريقة الإتصال بمواقع على الشبكة

---

[١] () نبيلة هبة هروال: مرجع سابق، ص ١٨٦.

[٢] () حسن بن سعيد بن سيف الغافرى: السياسة الجنائية فى مواجهة جرائم الإنترنت، رسالة دكتوراة ، جامعة عين شمس ، ص٣٥٢.

[٣] () ممدوح عبدالحميد عبد المطلب: جرائم إستخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت)، دار الفتح، الطبعة الأولى، ٢٠٠٠، الشارقة، ص١١١.

[٤] () للمزيد حول أسلوب فريق التحقيق راجع المرجع السابق، ص ٤٨٧.

المعلوماتية، أو العنوان الذى أرسلت إليه المعلومات، وإعداد قائمة بالمشتبه فيهم، وتحديد من له سجل إجرامى بهذا النوع من الجرائم، كما يمكن إستخدام وسيلة تقنية المعلومات المعتدى عليها للمساعدة على التعرف على هوية مرتكب الجريمة.

ومن وسائل البحث والتحرى عن الجريمة المعلوماتية ما يلى :

أولاً: التحرى الإلكترونى :

مجموعة من الإجراءات التى يقوم بها مأمور الضبط القضائى بواسطة تقنية المعلومات للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء حسب طبيعتها، للحد من الجريمة المعلوماتية أو ضبطها لتحقيق الأمن المعلوماتى"[١] . فلمأمور الضبط القضائى سلطات تقديرية واسعة لإختيار وسائل التحرى التى يراها مناسبة لإتمام عمله بصورة إيجابية من خلال جمع المعلومات المفيدة فى كشف الجريمة وضبط مرتكبيها، وتتضمن برامج التقنية التى ترشد إلى المشتبه فيهم كإستخدام رقم الـ **(IP)** لتحديد هوية الحاسب الذى تم من خلاله الولوج الي حاسوب المبلغ، والبروكسي" **(PROXY)** بإعتباره وسيطاً بين المستخدم وشبكة المعلومات لإتاحة الفرصة بالرقابة والتحكم فى البيانات الداخلة والخارجة، فإستخدام تلك الوسائل الفنية والبرامج املعلوماتية المتخصصة يهدف إلى كشف غموض الجريمة من خلال التعرف على الأسلوب الإجرامى المرتكب وإماطة اللثام عن شخصية مرتكبة[٢].

حيث يساعد إستخدام أجهزة تقنية المعلومات رجال الضبط القضائى فى الحصول على خلاصة المعلومات المنتقاة، وتسهيل عملية البحث والتحرى عن الأدلة، فتسمح التقنية الحديثة بإرسال وإستقبال صور البصمات والمجرمين لمقارنتها والإحتفاظ بأصحاب السوابق[٣].

---

[١] () مصطفى محمود موسى: دليل التحرى عبر شبكة الإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٥، ص٢٢.

[٢] () هشام رستم: الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م، ص١٩٥.

[٣] () حسين إبراهيم: الإستدلال ،كلية الشرطة ، القاهرة ، ٢٠٠٤ ، ص١١٣.

كما يهدف التحرى عن الجريمة المعلوماتية إلى الحصول على أكبر قدر ممكن من المعلومات عن السلوك المكون للجريمة المعلوماتية وأسلوب وظروف إرتكابها فى غضون وقت قصير نسبياً، من خلال المقابلات الإستطلاعية التى تجرى مع ممثلى الجهة المجنى عليها إذا كانت إحدى المؤسسات أو من الأفراد المجنى عليهم . وبناءً على طبيعة السلوك الإجرامى المرتكب يتحدد نطاق وتوقيت هذا التحرى والوقت الذى يستلزمه كون الدليل المستند إلى المعالجات الآلية للبيانات يمكن أن يكون متاحاً لفترة قصيرة من الزمن، بالإضافة إلى إمكانية أن تكون تلك الجرائم من النوع المستمر من حيث نتائجها أو تنفيذها، كما هو الحال فى جرائم نشر الفيروسات على شبكات التقنية المعلوماتية.

فيهدف مأمور الضبط القضائى من خلال أعمال البحث والتحرى عن الجريمة المعلوماتية إلى التثبت من وقوع الجريمة، والتعرف على نمط وطبيعة الجريمة المرتكبة، بالإضافة إلى التعرف على التقنيات المستخدمة فى إرتكابها للتعرف على الجانى أو الجناة المحتملين أو المشتبه فيهم، والأسباب والدوافع المحتملة لإرتكاب الجريمة.

كما يجب عند القيام بأعمال البحث والتحرى عن الجريمة المعلوماتية تحديد نوع النظام المعلوماتى، وأخذ كشف بأسماء العاملين التقنيين والمسئولين عن أمن المعلومات بالمنشأة، وحصر التلفيات الموجودة، وتحديد طبيعة الروابط لمعرفة طريقة نقل المعلومات[1].

ثانياً: المراقبة الإلكترونية للإتصالات عبر شبكة المعلومات[2]:

تعتبر المراقبة من أهم مصادر التحرى التى تتم بإستخدام تقنية المعلومات، لجمع البيانات عن المشتبه فيهم ، وذلك حسب نوع الجريمة التى يتعامل معها إلا أن المراقبة– لكونها من الإجراءات التى تعتدى على حق الخصوصية (كمراقبة البريد الإلكترونى الخاص بالمشتبه فيهم) والذى كفله الدستور والقانون بالحماية– تتطلب قبل البدء بها قيام مأمور الضبط

[1] () جميل عبد الباقى الصغير: أدلة الإثبات الجنائى والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، ٢٠٠٢، ص١١٩–١٢٠.

[2] () نبيلة هبة هروال: مرجع سابق، ص١٩٧.

القضائى بالحصول على الإذن بها إلا فى حالات إستثنائية، ولم تتطرق القوانين العربية الإجرائية لهذا النوع من المراقبة.

ويسمح القانون الفيدرالى الأمريكى بمراقبة الإتصالات السلكية والإلكترونية بناءً على أمر المحكمة ، وذلك بناءً على طلب فيدرالى بواسطة وزارة العدل لمدة ثلاثين يوماً اعتماداً على أسباب معقولة ترجح أن المراقبة سوف تكشف عن دليل الجريمة كالعدوان الجنائى المتوقع، ويشترط لمنح ذلك التصريح أن يتبين أن التحريات التقليدية غير مجدية، والقانون يجيز مراقبة الإتصالات السلكية والإلكترونية إذا وافق أحد أطراف الإتصال[١]، كأن يقوم أحد الأشخاص بستجيل مكالماته الهاتفية، فلا ضرر من ذلك سواء كانت الموافقة معلنة أو ضمنية (يستدل عليها من الظروف).

كما تجوز المراقبة فى حالة إعلام الشخص بالمراقبة، وتتم هذه الطريقة فى الغالب بأن يوضع إعلان تحذيرى لمن أراد دخول موقع معين بأنه عرضه للمراقبة فى حالة الدخول ، كما أن إستخدام الشعار الذى يعلم مستخدمى الإنترنت بأن هذه الصفحة مراقبة، وتجاوزها بالدخول يعتبر موافقة ضمنية على المراقبة[٢].

وتكمن صعوبة المراقبة فى الجريمة المعلوماتية من كون المجرم المعلوماتى قد يهاجم جهاز المجنى عليه أو أحد المشتركين بالشبكة أو الخادم[٣] فهم يستخدمون سلسلة مركبة من البرامج والأجهزة الفنية المعقدة لكى لا ينكشف أمرهم. وجدير بالذكر أن هناك أنواعاً وطرقاً للمراقبة الإلكترونية تكون مشروعة بحسب طبيعتها، فعندما يقوم الموظفون لدى مقدمى خدمة الإتصال بمراقبة الإتصالات لحماية حقوق مزودى الخدمة فيكتشفون الإختراقات التى قد تحدث ويكشفونها فلا يوجد بذلك إنتهاك

---

[١] () مشار إليها لدى د. يونس عرب: الإجراءات الجنائية عبر الإنترنت فى القانون الأمريكى (دار النهضة، القاهرة، الطبعة الثانية، ٢٠٠٦، ص٣٧٤.

[٢] () المرجع السابق ذكره ، ص٣٣٧

[٣] () الخادم أو الـ (Server) هو حاسب آلى فى شبكة يقوم بخدمة مجموعة من الحاسبات والنهايات الطرفية لتسهيل المشاركة فى إستخدام الأجهزة المختلفة المتصلة بالشبكة.

للقانون، وكذا مراقبة شركة الإتصالات لإتصال غير مشروع من مكان معين[١].

فمزودو الخدمة الذين يحققون فى الإستخدامات غير المشروعة لنظم المعلومات لديهم سلطة موسعة للمراقبة، ولديهم الحق فى الكشف عن دليل الإستخدام غير المشروع، ولكن ليس لهم الكشف عن الإتصالات الخاصة، فيجب أن يكون الشيء المراقب من الأشياء الماسة جوهرياً بحق مقدم الخدمة.

ثالثاً: الإرشاد الجنائى عبر شبكة المعلومات[٢]:

يجوز لمأمور الضبط القضائى الإستعانة بالمرشدين بالتعامل معهم للقيام بإمداده بالمعلومات عن الجريمة ومرتكبيها سواء كانوا مرشدين مرتبطين باحد أطراف الجريمة. ويعد الإرشاد من أهم المصادر التى يعتمد عليها مأمور الضبط القضائى فى تحرياته وجمع المعلومات لدوره الكبير فى كشف الجريمة.

ويتمثل الإرشاد الجنائى عبر الإنترنت من خلال الولوج فى غرف الدردشة ومنتديات الحوار الإلكترونية ، والتنكر بهيئات مختلفة ، والإستعانة بأسماء وصفات مستعارة للظهور بالمظهر الطبيعى سعياً وراء التعرف على مرتكبى الجريمة ، كسؤال مخربى ومخترقى مواقع الإنترنت عن كيفية قيامهم بالجريمة ، فالبعض من المجرمين يقومون بالتفاخر بإرتكاب مثل ذلك الجرائم(٣)، كما يمكن لمأمور الضبط القضائى القيام بهذا الدور .وقد ساهم الإرشاد عبر الإنترنت فى التعرف على العديد من الجرائم المرتكبة وضبط مرتكبيها(٤) ، كما إتجهت بعض النظم الإجرائية فى ظل التطور التكنولوجى الذى نعيشه إلى توسيع قاعدة الإرشاد الجنائى لتشمل أحقية سلطات التحقيق فى الإتصال بمزود الخدمة لكى يتولى التحفظ على السجلات المخزنة فى الخادم العام، وما يتعلق بالإتصال وكافة الأدلة

---

[١] () يونس عرب: الإجراءات الجنائية عبر الإنترنت فى القانون الأمريكى، الطبعة الثانية ، دار النهضة العربية ٢٠٠٧ ، ص٣٨١.

[٢] () نبيلة هبه هروال: مرجع سابق، ص١٩٥.

[٣] () سليمان أحمد محمد فضل: مرجع سابق، ص٢٧٣ وما بعدها.

[٤] () للمزيد راجع نبيلة هبة هروال: مرجع سابق، ص٢٧٥.

الأخرى بإستخدام برمجيات التجميد وخلافه إلى حين إصدار إذن التفتيش[١].

المطلب الثالث

المعاينة فى الجريمة المعلوماتية

مع التسليم بأهمية المعاينة فى كشف العديد من الجرائم التقليدية إلا أن دورها فى كشف غموض الجريمة المعلوماتية وفى كشف الأشياء التى قد تثبت وقوع الجريمة لا ترقى إلى الأهمية نفسها، وذلك لما أشرنا سابقاً إلى أن الجرائم التى ترتكب على نظم المعلومات قلما يكون لها آثار مادية. كما أن عدد الأشخاص المترددين على مسرح الجريمة يكون كبيراً جداً مقارنة بالجرائم التقليدية، وذلك خلال الفترة من إكتشاف الجريمة وحتى الإبلاغ عنها، مما يؤدى لحدوث تغيير أو تبخر لتلك الأدلة لطبيعتها الخاصة، فيثير ذلك الشك فى الدليل المستمد من المعاينة.

وينبغى لتعود المعاينة فى الجرائم المعلوماتية بفائدة لجهات الضبط القضائى ، مراعاة العديد من الأمور الفنية ، كتصور الحاسبات الآلية والأجهزة المتصلة بها ، وملاحظة طبيعة النظام المستخدم، وعدم نقل المواد المعلوماتية إلا بحرص شديد بعيداً عن كل ما يؤثر فيها كالمجالات المغناطيسية.

مدى صلاحية مسرح الجريمة المعلوماتية للمعاينة:

عند الحديث عن معاينة مأمور الضبط القضائى لمسرح الجريمة المعلوماتية يجب التفرقة بين حالتين هما[٢]:

١- الجرائم الواقعة على المكونات المادية للجريمة المعلوماتية (كالحاسب الآلى)

فتقع هذه الجرائم على الأجزاء المادية التى تحوى المعلومات بطبيعتها كجهاز الحاسب الآلى وأجهزة الإتصال المختلفة والكابلات

---

[١] () ومن تلك التشريعات التشريع الأمريكى بالمادة ١٨ US CODE SEC 2703 (F) مشار إليه لدى د. سليمان أحمد محمد فضل: مرجع سابق، ص٢٧٦.

[٢] () فتوح الشاذلى وعفيفى كامل عفيفى: جرائم الكمبيوتر ، بدون دار نشر ، ص٣٣٥

الخاصة بها، أو على شاشات العرض والأقراص الممغنطة التى تحتوى على المعلومات وغيرها من مكونات الحاسب الآلى ذات الطابع المادة المحسوس. فلا يثير الأمر أدنى صعوبة للقول بصلاحية المعاينة لمسرح الجريمة من قبل مأمور الضبط القضائى والتحفظ على الأشياء التى تعتبر أدلة مادية تدل على إرتكاب الجريمة ونسبتها إلى شخص معين، وكذلك وضع الأختام فى الأماكن التى تمت بها المعاينة[١]. إلا أن البحث وكما أشار سابقاً يرى أن الجرائم التى ترتكب على المكونات المادية للحاسب الآلى تخرج من نطاق جرائم المعلومات.

٢- الجرائم الواقعة على المكونات المعنوية للجريمة المعلوماتية (كالبيانات):

فالمعاينة المنصبة على الأجزاء المادية كمكونات الحاسب الآلى لا تشكل أدنى صعوبة فهى عملية سهلة، أما إذا ما تمت الجريمة بإستخدام الحاسب الآلى على سبيل المثال وكانت تقع على برامج الحاسب الآلى أو المعلومات التى تحتويه فإنها تشكل صعوبات فنية وقانونية يمكن أن تتلخص هذه الصعوبات فى عدة عوامل رئيسية منها[٢]:

-قلة الآثار المادية التى تخلفها الجريمة المعلوماتية، خاصة تلك التى تتعلق بالمعلومات والبيانات، أو التى تقع على برامج الحاسب الآلى وبياناته أو بواسطته.

-الأعداد الكبيرة من المترددين على مسرح الجريمة المعلوماتية خلال المدة الزمنية التى غالباً ما تكون طويلة نسبياً، وهى المدة الواقعة بين إقتراف الجريمة والكشف عنها، الأمر الذى يعطى فرصة كبيرة لتغيير تلك الآثار أو تلفيقها أو العبث بها، مما يلقى بظلال الشك على الدليل المستقى من المعاينة[٣].

-عدم دراية مأمور الضبط القضائى بالجوانب الفنية الكافية لطبيعة أجهزة تقنية المعلومات لإختلاف أنواعها وأنظمتها.

---

[١] () فتوح الشاذلى وعفيفى كامل عفيفى: مرجع سابق ذكره، ص٣٣٦.
[٢] () هشام فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٩٥ وما بعدها.
[٣] () فتوح الشاذلى وعفيفى كامل عفيفى: مرجع سابق، ذكره ص٣٣٧.

-كما في إستطاعة المتهم التدخل لإحداث تغيير وتلاعب بالبيانات عن بعد[١].ونظراً لحداثة الجرائم المعلوماتية وحداثة الأجهزة المختصة بمكافحتها والكشف عنها، وللخروج من تلك الصعوبات لتسهيل عمل مأمور الضبط القضائى يقترح بعض الفقه[٢] إتباع إجراءات وقواعد وإرشادات فنية عند إجراء المعاينة فى مسرح الجريمة المعلوماتية، للقيام بواجبهم على النحو الأمثل وهى[٣]:

-تصوير النظام المعلوماتى وما قد يتصل به من أجهزة طرفية، وتصوير محتوياته، وأوضاع المكان الذى يوجد به بصفة عامة، مع العناية بصفة خاصة بتصوير أجزائه الخلفية وملحقاته الأخرى، مع تسجيل الزمان والمكان والتاريخ الذى التقطت فيه الصور.

-ملاحظة طريقة إعداد النظام المعلوماتى بعناية بالغة.

-إثبات حالة التوصيلات والكابلات المتصلة وبمكونات النظام للقيام بالمقارنة والتحليل عند عرض الموضوع على المحكمة.

-عدم التسرع فى نقل أى مادة معلوماتية قبل إجراء الإختبارات اللازمة للتيقن من عدم وجود مجالات مغناطيسية لكى لا يحدث إتلاف للبيانات المخزنة.

-حفظ الأوراق الملقاة والممزقة والأقراص غير السليمة، وحفظ مخرجات الأجهزة المعلوماتية.

ويجب أن نشير فى النهاية إلى أن هناك العديد من القضايا التى طمست أدلتها أو ضاعت بسبب قلة الخبرة الفنية لدى مأمورى الضبط القضائى، كمسحهم للدليل الرقمى بدون قصد، لذلك فإن الإعداد والتدريب الأمثل لمأمورى الضبط على التعامل مع مثل تلك الجرائم له الآثر الأكبر فى ضبط مرتكبيها وتطبيق القانون بشكل فعا

---

[١] () سليمان أحمد محمد فضل: المواجهة التشريعة والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولة (الإنترنت)، ص٢٨٩.

[٢] () هشام رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٩٥.

[٣] () عبدالله حسين على محمود: إجراءات جمع الأدلة فى مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات المعلوماتية، إمارة دبى بدولة الإمارات العربية المتحدة ٢٦-٢٠٠٣/٤/٢٨ المجلد الأول، ص٥٩٨.

المطلب الرابع
التحفظ فى الجريمة المعلوماتية

يتمثل الدليل المعلوماتى فى جرائم المعلومات عامة فى ذبذبات أو نبضات إلكترونية، فإذا لم يكن مأمور الضبط القضائى مؤهلاً ومدركاً لطبيعة عمل النظام المعلوماتى الذى إرتكبت الجريمة من خلاله فقد يغفل أو يهمل الدليل، أوقد يتسبب فى إتلافه وإفساد دلالته[١].

فالتحفظ على الأدلة المعلوماتية من العمليات التى يلزمها الدقة دائماً، للتوصل إلى رصد قيمتها فيما يعرف فى القانون بـ "التصرف فيها" سواء بإستمرار الحفظ بقصد عرضها على جهات التحقيق المختصة، أو مصادرتها (بحكم قضائى عادة) أو أن ينتهى الحال إلى الإفراج عنها وإعادتها إلى أصحابها إذا لم تكن ذات قيمة فى كشف الجريمة[٢].

وفى إطار الجرائم المعلوماتية يجب أن نميز بين الأدلة التى يلزم التحفظ عليها داخل الحاسب أو جهاز تقنية المعلومات ، والتى يلزم بقاؤها فى العالم الإفتراضى، وبين الأدلة التى تنتمى إلى العالم الرقمى ويمكن إخراجها من إطار الحاسب بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة[٣]، فالتحفظ على الأدلة داخل الحاسب من العمليات المعقدة كونها تحتاج لرصد دقيق لمدى سلامة وصحة البيانات التى تحتويها تلك الأجهزة، وهذا الأمر يستدعى قيام الخبير التقنى بالكشف بداية عليها[٤].

وتتم عملية حفظ الأدلة داخل الحاسب بأساليب متعددة تتشكل فى أسهلها فى أسلوب الحفظ العادى، ومن أقوى مظاهرها عمليات حجز الحاسب على الدليل الموضوع فيه، كون الدليل الرقمى[٥] يحتوى على

---

[١] () هشام فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص١٢٧-١٣٢.

[٢] () عمر بن يونس: الدليل الرقمى، الطبعة الأولى، الجمعية العربية لقانون الإنترنت، القاهرة، ٢٠٠٧، ص١٢٤.

[٣] () عمر بن يونس: الدليل الرقمى، مرجع سابق ذكره ، ص١٢٤.

[٤] () حسن بن سعيد بن سيف: السياسة الجنائية فى مواجهة جرائم الإنترنت، ص٣٥٨.

[٥] () الدليل الرقمى هو الديل الناتج عن إستخدام الوسائل الإلكترونية فى إرتكاب الأفعال غير المشروعة التى تقع على الجريمة المعلوماتية. د. على مجمود على حمودة: الأدلة المتحصلة من الوسائل الإلكترونية فى إرتكاب الأفعال غير المشروعة التى تقع على الجريمة المعلوماتية.

- على محمود على حمودة: الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائى، (بحث منشور على الموقع www.arablawinfo.com)، ص٢٢.

بيانات رقمية تعطى مظهراً معلوماتياً محدداً غير قابل للتحويل إلى مظهر آخر إلا بإجراء تعديلات رقمية فى البيانات المذكورة[١].

كما قد يتطلب الأمر اللجوء الى الخادم الرئيسى إذا كانت الجريمة مرتكبة من خلال شبكة المعلومات (الإنترنت) والتى تشمل مظاهر مختلفة، فيتوصل إلى الخادم الرئيسى لحفظ البيانات المطلوبة بإستخدام برامجيات مساعدة عادة ما يقوم بها الخبير، كحجز وتشفير المواقع بعد تحديد جديتها ودقتها ومسارها، وهذا أمر يترتب عليه عدم إمكانيه حذفها من العالم الرقمى[٢]، وفى حالة قيام الخبير بحفظ تلك المعلومات عن طريقه فقد يستدعى ذلك إستمرار لمرحلة المحاكمة أحياناً، وقد يتطلب الوضع إستمراره إلى ما بعد المحكمة[٣].

أما فيما يتعلق بعملية الحصول على المخرجات من تلك المواد المحفوظة فإنها تعد أدلة أصلية على الرغم من كونها نسخاً من دليل أصلى موجود بالعالم الإفتراضى أو أجهزة تقنية المعلومات، حيث يتم إخراجها بأشكال مختلفة. ومن أبرز تلك الأشكال النسخ الورقية، فمخرجات البيانات هى الأصل الرقمى للموضوع المعلوماتى دائماً، بحيث لا يكون للمعلومات وجود ما لم يكن لها أصل رقمى يتم بمقتضاه هيكلة المعلومة[٤]، وعلى سبيل المثال فإن سجل الزيارات فى أحد المواقع ما هو إلا قاعدة بيانات يسهل التحكم فيه من خلال عرض المعلومات المطلوبة وإخفاء غير ذلك، فيقوم مأمور الضبط برصد قاعدة البيانات تلك بإستخدام الشفرة الملائمة، وإنزال وطباعة قاعدة البيانات كمخرجات بقصد تقديمها إلى المحكمة[٥]. كما أنه من الأشياء التى يتم التحفظ عليها الورق المتواجد بالقرب من أجهزة تقنية المعلومات، وجهاز الحاسب الآلى وملحقاته، والبرمجيات إذا كان الدليل ينشأ بسبب برنامج خاص ليس واسع الإنتشار كبرامج الإختراق، ووسائط التخزين المتحركة كأقراص الليزر والأقراص المرنة، كونها قد

---

[١] () عمر بن يونس: الدليل الرقمى، مرجع سابق، ص١٢٥.

[٢] () عمر محمد أبو بكر بن يونس: الإثبات الجنائى عبر شبكة الإنترنت، ورقة بحثية مقدمة إلى ورشة العمل الإقليمية حول تطوير التشريعات فى مجال مكافحة الجرائم الإفتراضية خلال الفترة ٢-٢٠٠٦/٤/٤، مسقط، سلطنة عمان، ص٤٣.

[٣] () كأن يرفع الموضوع إلى المحكمة أعلى درجة كالإستئناف أو النقض.

[٤] () عمر بن يونس: الدليل الرقمى، مرجع سابق، ص١٢٦.

[٥] () المرجع السابق، ص ٤٤.

تحتوى على عنصر من عناصر الجريمة، لذا فيجب أن يراعى مأمور الضبط القضائى عند القيام بالتحفظ النقاط التالية[١]:

- حفظ الدعائم الأصلية للبيانات وعدم الإكتفاء بحفظ النسخ.
- مراعاة ظروف الحرارة والرطوبة المناسبة لتخزين المعلومات.
- تأمين البرامج المتحفظ عليها فنياً قبل تشعيلها.
- إحكام حلقة التسلسل المعلوماتى لصيانتها من العبث.

وقد تناولت إتفاقية بودابيست لمكافحة جرائم المعلومات التحفظ فى الجريمة المعلوماتية بشيء من التفصيل من خلال نص المادتين "١٦ و"١٧" تحت عنوان "التحفظ العاجل على البيانات المعلوماتية المخزنة"، حيث نصت على ضرورة الاحتفاظ بالبيانات المخزنة عن طريق حائزى البيانات – مثل مقدمى الخدمات – والتحفظ المستقبلى على البيانات المتعلقة بالمرور والولوج فى الوقت الفعلى إلى محتوى الاتصالات.

فالإجراءات المقررة فى هاتين المادتين لا تطبق إلا إذا كانت البيانات المعلوماتية أو بيانات الحاسب موجودة من قبل وفى طور التخزين. وتشير عبارة "يتحفظ على البيانات **Data Preservation**" إلى حفظ بيانات سبق وجودها فى شكل مخزن وحمايتها من كل ما يمكن أن يؤدى إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة.

في حين أن عبارة "الاحتفاظ بالبيانات **Data Retention**" تعنى حفظ البيانات لدى حائز بالنسبة لمستقبل البيانات التي في طور الإنتاج والتوليد، فأرشفة البيانات تشير إلى تجميعها في الوقت الحاضر وحفظها وحيازتها في أرشيف البيانات تشير إلى تجميعها في الوقت الحاضر وحفظها وحيازتها فى أرشيف للاحتفاظ بها للمستقبل، فهي عملية تخزين على عكس "التحفظ على البيانات" والتي تعني النشاط الذى يضمن للبيانات سلامتها وسريتها.

وعلى ضوء التفرقة السابقة فإن نطاق المادتين يقتصر على "التحفظ على البيانات" ولا يمتد إلى "الاحتفاظ بها"، وإجراءات التحفظ على البيانات تنطبق على بيانات معلوماتية أو بيانات الحاسب التي تم تخزينها عن طريق

[١] () عبدالله حسين محمود: إجراءات جمع الأدلة، مرجع سابق، ص٥.

نظام معلوماتي، وهو ما يفترض أن البيانات موجودة من قبل وتم تجميعها وتخزينها.

وينعقد ذلك الإجراء بهدف التنقيبات أو الإجراءات الجنائية النوعية، وبالتالي فيتقيد تطبيقه على تحقيق معين فى قضية معينة، وعندما يقوم طرف ما بتطبيق إجراءات التحفظ عن طريق إصدار أمر فإن هذا الأمر يكون مقتصراً على بيانات نوعية لدى شخص أو تحت سيطرته.

وتقر المادتان "١٦" و "١٧" من نص الاتفاقية سالفة الذكر أن سلطة طلب التحفظ على بيانات متواجدة ومخزنة فى انتظار الكشف عن محتواها تمنح للسلطات سلطة قانونية بمناسبة التنقيبات والتحقيقات الجنائية النوعية.

والالتزام بضمان التحفظ على البيانات يقصد منه إلزام الأطراف بقصر تقديم أو استخدام خدمات لا يستعملونها بشكل منتظم في التجميع أو الاحتفاظ ببعض نماذج من البيانات، مثال ذلك بيانات المرور أو المشتركين.

وبالنسبة لغالبية الدول فإن التحفظ على البيانات يعد إجراءً قانونياً جديداً في القانون الداخلي، فهو أداة جديدة للتنقيب المهم فى مجال مكافحة الجرائم المعلوماتية للمبررات التالية:

١. قابلية البيانات المعلوماتية للتلاشي والتلاعب ، وهكذا يسهل فقدان عناصر إثبات الجريمة من خلال الإهمال وممارسات التخزين غير الدقيقة، أو من خلال التغيير العمدي لها، أو محوها من أجل تدمير عناصر الإثبات.
٢. الجرائم المعلوماتية غالباً ما يتم ارتكابها عن طريق الاتصال بواسطة نظام معلوماتي، وهذه الاتصالات يمكن أن تحوى محتوى غير مشروع مثل الصور الإباحية والفيروسات، فالتحقق من هوية مصدر أو منتهي هذه الاتصالات الخارجية يمكن أن يساعد على تحديد هوية مرتكب هذه الجرائم.
٣. عندما تقدم هذه الاتصالات محتوى غير مشروع أو دليل أفعال جنائية فإن التحفظ على هذه الاتصالات عن طريق

مقدم الخدمة يكون مهماً من أجل عدم فقد عناصر الإثبات الجوهرية.

لذا فالتحفظ على البيانات يعد إجراءً أولياً يتم تبنيه انتظاراً لاتخاذ إجراءات قانونية أخرى تستهدف الحصول على البيانات أو الكشف عنها.

كما أن السرية تفرض من أجل تجنب أن يقوم أشخاص آخرون بتغيير أو محو البيانات بالنسبة للشخص الصادر إليه أو الشخص المعنى أو الأشخاص الآخرين الذين قد يشار إليهم أو يكونوا معروفين من خلال البيانات، فلا بد أن هناك حداً زمنياً لهذا الإجراء.

كما أن الالتزام المزدوج لضمان أمن البيانات والسرية يخضع للشروط والضمانات، بحيث يكفل الحق فى الحياة الخاصة للشخص المعنوى أو الأشخاص الطبيعيين المشار إليهم والمحددة أوصافهم.

المطلب الخامس

الاستعانة بالخبراء في الجريمة المعلوماتية

مع ظهور هذا النوع الجديد من الجرائم تستعين سلطات الضبط القضائي وسلطات التحقيق والمحاكم بالخبرة بغرض كشف غموض الجريمة، أو تجميع أدلتها والحفاظ عليها، للتغلب على الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق، ويلاحظ أن نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهناً بكفاءة وتخصص هؤلاء الخبراء.

ويشكل الكم الهائل للبيانات التي يجرى تداولها في الأنظمة المعلوماتية أحد مصادر الصعوبة التي تعوق التوصل لمرتكبى الجرائم التي تقع عليها أو بواسطتها. وبالإمكان تقليص تلك الصعوبات من خلال الاستعانة بأصحاب الخبرات الفنية لتحديد ما يجب فعله، فاستعانة مأمور الضبط القضائى بالخبراء للتعامل مع الجرائم التي تقع فى مجال تكنولوجيا المعلومات تكاد تكون ضرورية لا غني عنها؛ نظراً للطابع الفنى الخاص لأسباب ارتكابها والطبيعة غير المادية لمحل الاعتداء، ونجاح هذه الجهات فى أداء رسالتها يتوقف إلى حد كبير على حسن اختيار الخبير.

فالحاسبات وشبكات الاتصال لها أنواع وطرازات متعددة، وما يتصل بها من علوم وتقنيات يتوزع على تخصصات علمية وفنية دقيقة ومتنوعة، فالتطور فى مجالها سريع لدرجة أنه يصعب على المتخصص تتبعها واستيعابها. لذلك لا وجود لخبير لديه معرفة متعمقة فى كافة أنواع الحاسبات وبرمجياتها وشبكاتها، ولا لخبير القدرة على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها، لذا يجب أن يكون للخبير الإمكانيات والقدرات العلمية والفنية في مجال التخصص الدقيق للحقل الذى تقتضيه المسألة أو النشاط موضوع الخبرة، وحصول الشخص على درجة علمية لا يكفى وحده ليكون هو المطلوب، فلا بد من توافر الخبرة العملية بالإضافة إلى الخبرة العلمية.

كما تكمن أهمية الاستعانة بالخبرة فى مجال الجريمة المعلوماتية عند غيابها، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه.

والتزام الخبير هو الالتزام ببذل عناية، فلا يسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبراته، أو بسبب ما واجهه من عقبات أثناء أداء مهمته، كما يلتزم بالمحافظة على سر المهنة، ويعاقب فى حالة إفشائه للسر بالعقوبات المقررة.

الفرع الأول
الشاهد المعلوماتي

يقصد بالشاهد المعلوماتي "الفني صاحب الخبرة والتخصص فى تقنية الحاسب وعلومه، والذى تكون لديه معلومات جوهرية لازمة لولوج نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضى التنقيب عن أدلة الجريمة داخله"[1].

ويمثل الشاهد المعلوماتي بهذا المعنى عدة طوائف تشمل كلا من: القائمين على تشغيل الحاسب الآلى، وخبراء البرمجة، والمحللين ومهندسي الصيانة والاتصالات، ومديري النظم.

---

[1] () هلالي عبداللاه أحمد ، التزام الشاهد بالاعلام في الجرائم المعلوماتية ، دراسة مقارنة ، دار النهضة العربية ، ٢٠٠٦

إلا أنه هل يوجد التزام قانوني على الشهود فى الجريمة المعلوماتية بطبع ملفات البيانات المخزنة فى الحاسب أو الإفصاح عن كلمات المرور السرية؟

يتمثل جوهر الالتزام بالإعلام فى الجريمة المعلوماتية في أنه في حال كان الشاهد المعلوماتي حائزاً على معلومات قد تساهم فى السير في عملية التحقيق فإنه مطالب بأن يعلم بها سلطة الاستدلال أو التحقيق ليتسنى لها أداء المهام المناط بها، إلا أنه لا وجود لنص قانوني صريح لمثل ذلك الالتزام لدى المشرع المصري ، ويرى الباحث ضرورة أن يتدارك المشرع المصري ذلك بالنص على الالتزام بتقديم المعلومات الجوهرية والمهمة نظراً للطبيعة الخاصة للجريمة المعلوماتية.

والالتزام بالإعلام عن الجريمة المعلوماتية هو أن يبلغ الشاهد المعلوماتي سلطة الاستدلال عن المعلومات الجوهرية اللازمة لولوج النظام للتنقيب عن الأدلة بداخله، ويرتكز ذلك من خلال الإعلام عن البيانات المخزنة فى أجهزة تقنية المعلومات، والإفصاح عن كلمات المرور السرية، والتشفيرات والأوامر الخاصة بتنفيذ البرامج. وينبغى أن تكون الشهادة فى الجريمة المعلوماتية على نحو بسيط ومفهوم لسلطات الاستدلال لتستطيع فهمه، كما يجب أن تكون الشهادة محددة ودقيقة من دون زيادة أو نقصان بالقدر الذى يساعد مأموري الضبط القضائي على اتخاذ الإجراءات المناسبة.

ويشترط فى انعقاد الالتزام أن تكون بصدد جريمة قد وقعت، وأن يكون الشاهد على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة، وأن تقتضى مصلحة التحقيق الحصول على هذه المعلومات الجوهرية للبحث عن الأدلة.

الفرع الثاني

الشهادة الإلكترونية عن بعد [1]

يطلق مصطلح الشهادة الإلكترونية على نوعين من الشهادة لا يكون بها الشاهد حاضراً بذاته المادية (أي جسدياً) وإنما تتم عبر وسائل إلكترونية أو رقمية من خلال شبكة المعلومات مثلا. ويثار التساؤل حول مدى قابلية وصحة مثل هذه الوسائل لعرض الشهادة أمام سلطات الاستدلال. يجب التمييز بين نوعين من أنواع استخدام الوسائل الإلكترونية للقول بصحة الشهادة، ومن ثم قبول ما ينتج عنها من أدلة.

أولاً: حالة الشهادة المسجلة مسبقاً :

يفترض أن يقوم مأمور الضبط القضائى بتسجيل الشهادة مسبقاً لعرضها على المحكمة، لتكون حجة بأوراق الدعوى، كما أنها تشكل ضمانة أساسية في عدم وجود إكراه على الشهود. ويرى الباحث أن الشهادة المسجلة مسبقاً تأخذ حجية الشهادة المكتوبة فى محضر استدلال مأمور الضبط القضائى أمام القضاء.

ثانياً: حالة الشهادة الإلكترونية الفورية:

وهي تتم من خلال اتصال صوتي ومرئى بين الجلسة وبين الشاهد، فتفترض حدوث هذه النوعية من الشهادة فى التحقيق النهائى، حيث يمكن من خلالها الحصول على أقوال الشاهد بشكل سمعي بصري.

وهذه الشهادة تخرج عن نطاق سلطة الاستدلال كونها من إجراءات التحقيق التي تمارس أمام المحكمة، إلا أنه يجب أن نشير هنا إلى أن المحكمة الفيدرالية الأمريكية العليا قد قررت قبول نظام الشهادة عبر الدوائر المرئية المغلقة على أساس أن قاعدة المواجهة الشخصية في الجلسة قد تعدلت بما هو مقرر فى امتداد الاستثناءات المقررة فى قاعدة شهادة السماع التي تسمع فى حالات محددة. كذلك قامت المحكمة العليا الأمريكية بتعديل تفسير القواعد الفيدرالية بحيث حثت على الأخذ بالشهادة عبر الدوائر المغلقة عن بعد.

---

[1] () خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي ، الاسكندرية ، ٢٠٠٩ ، ص ٢٦٠

المطلب الخامس

التلبس بالجريمة المعلوماتية

مدى إنطباق حالات التلبس بالجريمة على الجرائم المعلوماتية

التساؤل الذى يطرح نفسه هنا هو: هل يمكن تصور قيام حالة التلبس بالجريمة المعلوماتية؟

الجريمة المعلوماتية كغيرها من الجرائم التى يمكن أن تتوافر فيها شروط الجريمة المتلبس بها، كما أن أغلب جرائم المعلومات هى بالأصل جرائم تقليدية إلا أن أسلوب إرتكابها تطور بإستخدام التكنولوجيا الحديثة.

وحتى يكون التلبس بالجريمة المعلوماتية متفقاً وصحيح القانون فإننا لا وأن نكون بصدد جريمة معلوماتية مما يعتبرها القانون جناية أو جنحة. ويستوى أن يكون النظام المعلوماتى محل هذه الجرائم كموضوع للجريمة أو أن يكون أداة لها.

ومن أمثلة هذه الجرائم جريمة دخول النظام بدون وجه حق، والإضرار بالبيانات من خلال إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر البيانات الخاصة والسرية، والإستيلاء على المال المنقول من خلال النظام المعلوماتى.

فقد يتم التلبس بالجريمة المعلوماتية من خلال الصور التالية:

-فيتصور التلبس فى حالة مشاهدة مأمور الضبط القضائى للجريمة حال إرتكابها، كأن يكون رجل الضبط القضائى فى أحد مقاهى الإنترنت ويلاحظ وجود شخص يقوم بتصفح مواقع إباحية أو ممنوعة.

-أو كما هو في حالات التلبس من خلال مشاهدة الشخص حاملاً معه أدوات تقنية تثير الريبة يستخدمها أمام أجهزة الحاسب الآلى بطريقة مختلفة عن الطريقة الطبيعية لسحب النقود، مما يثير الريبة فى إرتكابه لفعل غير مشروع.

ويشترط أن تتوافر فى حق الشخص المتلبس بالجريمة دلائل كافية تدعو إلى الإعتقاد بأنه قد ساهم فى إرتكاب الجريمة المعلوماتية سواء بصفته فاعلا أصلياً لها أو شريكاً فيها، بالإضافة إلى باقى شروط التلبس.

ويرى الباحث أنه بسبب طبيعة التقنية المستخدمة يمكن لمأمور الضبط القضائى مشاهدة لحظة إرتكاب جريمة الشبكات المحمية، ويتعرف من خلال أنظمة الحماية على عنوان وموقع الشخص المخترق.

فشرط التلبس فى مشاهدة الجريمة قد يتم بصورة مباشرة أو غير مباشرة، كما هو الحال فى سرقة الكهرباء، لنصل بالنهاية إلى نتيجة قوامها أنه يتصور التلبس بالجريمة المعلوماتية، وبالتالى ينعقد على إثره الإختصاص الإستثنائى لمأمور الضبط المتمثل فى التفتيش والضبط.

ونظراً لطبيعة الجريمة المعلوماتية فسوف تقتصر دراستنا على الدور الإستثنائى لمأمور الضبط القضائى فى حالة التلبس بالجريمة المعلوماتية على كل من إجراء التفتيش والضبط، كون القبض لا يختلف بالجريمة المعلوماتية عن الجريمة التقليدية.

والتفتيش فى مدلوله القانونى بالنسبة للجرائم المعلوماتية لا يختلف عن مدلولة السائد فى فقه الإجراءات الجنائية، فيقصد به "أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة، لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات، لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد فى إثبات الجريمة ونسبتها إلى المتهم بإرتكابها"(١).

ويعد تفتيش نظم المعلومات من أخطر المراحل حال إتخاذ تلك الإجراءات الجنائية ضد مرتكب جريمة ناشئة عن إستخدام تكنولوجيا المعلومات نظراً لطبيعة الدليل وصعوبة الوصول إليه.

) هشام رستم: الجوانب الإجرائية، مرجع سابق، ص ٦٢ وما بعدها.([1]

- هلالى عبدالله أحمد: تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى دراسة مقارنة ، دار النهضة ،٢٠٠٦ ، ص٧٣ وما بعدها

وتخضع عملية التفتيش للأحكام المقررة قانونا تبعاً لطبيعة المكان الموجود فيه النظام، فإذا كان الحاسب أو الأجهزة والوسائل التقنية المادية محل التفتيش موجوة فى مكان خاص كمسكن المتهم وجب أن يتم التفتيش وفق أحكام تفتيش المنازل، مع توفر الضمانات المقررة قانوناً لمثل هذا النوع من التفتيش، أما أن تواجد النظام فى مكان عام، فهو على الأغلب يكون موجوداً فى حوزة المتهم ذاته، كما فى حالة الحاسب المحمول، ففى هذه الحالة فإن التفتيش يخضع لأحكام تفتيش الأشخاص بوصف النظام في حيازة الشخص غير المرتبطة بالمكان الموجودة فيه.

الفرع الاول
مدى خضوع المكونات المادية للنظام المعلومات للتفتيش

لا توجد صعوبة تذكر فى حالات تفتيش المكونات المادية للحاسب الآلى مثل الشاشة وأجهزة الإدخال والإخراج، مثل الطابعات وأجهزة الماسحات الضوئية والفارة والكابلات والأسطوانات ولوحة المفاتيح وجهاز الحاسب نفسه، وأجهزة الإتصالات بالشبكة مثل المودم، والأشرطة الممغنطة وأدوات التخزين وحفظ البيانات، والأجهزة ذات الكيان المادي الأخرى، لأن عملية التفتيش فى مثل هذه الحالات تكون طبقاً للإجراءات التقليدية لتفتيش المكونات المادية، فينبغى لإنعقاد الإختصاص الإستثنائى لمأمور الضبط القضائى بإجراء التفتيش قيام حالة التلبس[١].

ويترتب على جواز تفتيش الكيانات المادية لنظم المعلومات خضوعها لأحكام التفتيش، ومقتضى أعمال هذه الأحكام هو توقف حكم تفتيش تلك الأشياء على مكان وجودها، فالولوج للمكونات المادية للمعلومات بغرض التفتيش عن جريمة معلوماتية وقعت لكشف الحقيقة عن مرتكبيها يخضع للإجراءات القانونية الخاصة بالتفتيش من حيث طبيعة المكان الموجودة به كالأماكن العامة أو الخاصة[٢]، حيث أن لصفة المكان وطبيعته أهمية قصوى كما أشرنا سابقاً.

فالأماكن الخاصة لا يجوز تفتيشها إلا فى الحالات والضمانات والإجراءات التى يجوز فيها تفتيش المساكن، أما لو وجود شخص يحمل

---

[١] () هلالى عبد اللاه أحمد: تفتيش نظم الحاسب الآلى، مرجع سابق، ص١٠٥.
[٢] () هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٦٩ وما بعدها.

مكونات الحاسب الآلى أو أياً من أدوات تقنية المعلومات المادية، أو كان مسيطراً عليها، أو حائزاً لها فى مكان ما من الأماكن العامة، سواء أكانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أو كانت من الأماكن العامة بالتخصيص كالمقاهى والمطاعم والسيارات العامة، فإن تفتيشها لا يكون إلا فى الحالات التى يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها فى هذا المجال، بإعتبار أن تفتيش الشخص يشمل بوجه عام تفتيش ذاته وكل ما فى حوزته وقت تفتيشه، سواء أكان مملوكاً له أم لغيره[١].

الفرع الثانى

مدى خضوع المكونات المنطقية المعنوية للنظام المعلوماتى للتفتيش

آثار تفتيش المكونات المنطقية للنظام المعلوماتى للتفيش خلافاً بين الفقه حول مدى خضوع المكونات ذات الطبيعة المعنوية "**Software**" من برامج وشبكات معلومات وغيرها من برامج نظم المعلومات للتفتيش، فيرى جانب من الفقه أن الأدلة الجنائية لا بد أن تكون ذات كيان مادى يمكن مشاهدتها وإستخدامها بسهولة. ومن المتعارف عليه أن المعلومات الإلكترونية ذات كيان معنوى غير محسوس، وبالتالى يصعب خضوع هذه البيانات المعنوية وغير المرئية للتفتيش طبقاً لقوانين الإجراءات الجنائية المطبقة حالياً فى معظم الدول، بإستثناء بعض الدول التى سنت تشريعات جزائية حديثة قادرة على مواكبة التطور السريع فى مجال نظم المعلومات الحديثة، فالبيانات منفردة عن دعامتها المادية لا تعد أشياء ليتم ضبطها[٢].

بينما ذهب رأى آخر إلى جواز تفتيش البيانات المعنوية بمختلف أشكالها كون القوانين الإجرائية عندما تصدر الإذن بضبط الشيء، فإن ذلك يجب تفسيره بحيث يمثل البيانات المحسوسة وغير المحسوسة[٣].

---

[١] عبدالله حسين: مرجع سابق، ص٣٧٠.

(2) Motuenshclager "Manfred": computer crimes and other crimes against information technology in Germany. Rev. inter. De. Dr. Pen 1993. P.351.

(3) Vassilaki (Irini): computer crimes and other crimes. Against information technology in Greece. Rev. intern de. Dr. pen. P.371.

فالتشكيك فى الطبيعة المادية للبيانات والمعلومات الإلكترونية قد لا يكون لها مسوغ قانونى، لأنها ولأسباب تقنية وقانونية يجب أن ينظر إليها عل أساس أن المعلومات شيء كما وصفها القانون الفرنسى، وبذلك تعتبر البيانات والمعلومات نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية يمكن تخزينها على وسائط متعددة، ويمكن نقلها من مكان إلى آخر، كما يمكن تقييمها وقياسها، أى أنها كما وصفتها محكمة بروكسل أشياء محسوسة ومادية يمكن أن ترد عليها عملية التفتيش عند الإعتداء عليها(١).

فالوقوف بمصطلح "الأشياء" عند الأشياء المادية، قد يصطدم مع المذهب السائد اليوم فى تفسير النصوص الجنائية، والذى لا يعتمد على التفسير الحرفى للفظ فقط، وإنما يعتمد وبشكل أوسع على مذهب التفسير المنطقى، والذى يطبق اذا كان النص محل التفسير غامضاً أو خافياً فى المعنى المقصود منه(٢).

فإذا كان التفسير المنطقى يتم بدراسة رمز معين يعبر عن حقيقة موضوعية معينة، وذلك بقصد الوصول إلى تلك الحقيقة(٣)، فإنه يلزم لإنضباط التفسير بالنسبة للفصل الجنائى إقامة علاقة بين المعنى العام المجرد للقاعدة الجنائية بغرض الوصول إلى المعنى الحقيقى الذى يكمن فى مضمونها لتطبيقه عليها(٤)، فالمادة تعرف بأنها كل ما يشغل حيزاً مادياً بفراغ معين، والحيز يمكن قياسه والتحكم به، وبما أن المعلومات تشغل ذلك الحيز فى دعامتها المادية ويمكن قياسها بمقياس معين، كما أنها تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها تعد طبقاً لذلك كياناً مادياً تتشابه به مع التيار الكهربائى الذى إعتبره الفقه والقضاء من قبيل الأشياء المادية(٥).

---

(١) هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٦٨.

(٢) على محمود على حمودة: الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائى، (بحث منشور على الموقع www.arablawinfo.com)، ص٤٤.

(٣) مأمون سلامة: حدود سلطة القاضى فى تطبيق القانون، دار الفكر العربى، ١٩٧٥، ص٥١.

(4) Yves seillan: Essai Sur les methods d, interpreatation de la jurisprudence civil- these Bordeaux- 1968. P. 109.

(٥) هلالى عبد اللاه أحمد: تفتيش نظم الحاسب الآلى، مرجع سابق، ص٨.

كما أن هناك من الآثار التقليدية ما لا يمكن رؤيته بالعين المجردة وبحاجة إلى تدخل الخبراء لرفعه ومعالجته أو التعامل معه بواسطة أجهزة خاصة معدة لهذا الغرض، كالحمض النووى والتسجيلات والأفلام الموجودة فى أشرطة جهاز الفيديو المرئى أو التسجيل الصوتى.

ويقر الجميع بأنه من الممكن محو أو إتلاف أو العبث بالبيانات والبرامج الموجودة بالحاسب والإنترنت، وهذا الإقرار في حد ذاته خير دليل علي وجود تلك البيانات والبرامج ،وإلا فكيف يمكن محو وإزالة اثار معنوية لا وجود لها؟ كما أن سرعة وسهولة محو وحذف البيانات والمعلومات أو البرامج لا تحولها إلى مكونات لا آثار لها، فهناك من الآثار المادية التقليدية فى مسرح الجريمة أيضاً ما يمكن إتلافها والعبث بها وإخفاؤها.

وبالمقارنة بين الحالتين تتمثل فى أن الإختلاف بين الأشياء الخاصة والمعلومات يكمن فى نوع الوعاء الخاص بحفظ تلك المعلومات والبيانات فقط، ففى الحالة الثانية يتمثل الوعاء فى الأقراص المرنة، أو الحاسب أو الـ **Server** فى الشبكات والإنترنت، أما فى الحالة الأولى فالوعاء هو الأوراق العادية، وهذا الإختلاف مجرد إختلاف شكلى ليبين له تأثير على مضمون الوعاء من المعلومات والبيانات[١].

ويرجع ذلك الإختلاف إلى أن جرائم المعلومات ذات طبيعة تقنية– إلكترونية، وبالتالى فإن بياناتها فى الغالب ستكون أيضاً من طبيعة إلكترونية، وهذا لا يعنى أن إثباتها ببيانات أخرى من غير هذه الطبيعة أمر غير متيسر[٢].

كما أنه طبقاً لمعايير الخصوصية التى يحميها المشرع المصرى يتبين أنه قد تناول المسكن والسيارة والمحل وكل ما يتعلق بالشخص وتتمثل به خصوصياته. ولذلك فإن نظام المعلومات وما يحويه من خصوصيات لأشخاص تخضع أيضاً وبالتبعية لمعيار الخصوصية من حيث عدم جواز تداخل فيه بدون إذن من النيابة العامة، وهذا ما أكده المشرع عندما نص

---

[١] () عارف عبد الرحيم: دور ومهام اعضاء الضبط القضائي في مرحلتي التحري والتحقيق الابتدائي، رسالة دكتوراة ، جامعة المنصورة ص٢٥٤.

[٢] () يونس عرب: حجة الإثبات بالمستخرجات الإلكترونية فى القضايا المصرفية، (بحث منشور على الموقع www.arablawnfo.com).

قانون الأحوال المدنية بالمادة "١٣" فقرة "١٤" من القانون رقم ١٤٣ على أن: "تعتبر البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين التى تشتمل عليها السجلات والدفاتر أو الحاسبات الآلية أو وسائط التخزين لملحقة سرية ولا يجوز الإطلاع عليها أو الحصول على بياناتها إلا فى الأحوال التى نص عليها القانون ووفقاً لأحكامه".

وفى القانون المقارن نرى أن الولايات المتحدة الأمريكية قد قامت بتعديل القاعدة رقم ٣٤ من القواعد الفيدرالية الخاصة بالإجراءات الجنائية لعام ١٩٧٠، لتنص على السماح بتفتيش أجهزة الحاسب والكشف عن الوسائط الإلكترونية بما فى ذلك البريد الإلكترونى والبريد الصوتى[١].

كما أن المادة "٢٥١" من قانون الإجراءات الجنائية اليونانى تعطى سلطة التحقيق إمكانية القيام بأى شيء ضرورى لجمع وحماية الدليل يفسر الفقه اليونانى عبارة "أى شيء" بأنها تشمل ضبط البيانات المخزنة أم المعالجة إلكترونياً، وبذلك فإن تفتيش البيانات المخزنة فى الذاكرة الداخلية للحاسب الآلى لا تشكل أى مشكلة فى اليونان، إذ بمقدور المحقق أن يعطى أمراً للخبير بجمع البيانات التى يمكن أن تكون مقبولة كدليل فى المحاكمة[٢].

وكذلك الحال فى القانون الجنائى الكندى وبالتحديد فى المادة "٤٨٧" التى تعطى سلطة إصدار إذن لضبط أى شيء طالما تتوافر أسس معقولة للإعتقاد بأن الجريمة إرتكبت أو يشتبه فى إرتكابها بإستخدامه، أو أن هناك نية فى أن يستخدم فى إرتكاب الجريمة، أو أنه سوف ينتج دليلاً على وقوع الجريمة[٣].

ويرى الباحث أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية المساعدة فى كشف الحقيقة، فإن هذا المفهوم يمتد ليشمل البيانات المعلوماتية بمختلف أشكالها، إلا أنه كان من الأفضل لمواجهة هذا القصور

---

[١] () هلالى عبداللاه أحمد: تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى، مرجع سابق، ص٨٤.

[٢] () المرجع السابق، ص٨٢.

– عفيفى كامل: جرائم الكبيوتر وحق المؤلف والمصنفات الفنية، مكتبة الأهرام، القاهرة، ٢٠٠٠، ص٣٣٨.

[٣] () هلالى عبداللاه أحمد: تفتيش نظم الحاسب الآلى، مرجع سابق، ص٨٢.

التشريعى ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (المواد المعالجة عن طريق الحاسب الآلى أو المعلومات الإلكترونية) وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقنى الحديث هى البحث عن الأدلة المادية أو الرقمية.[١]

الفرع الثالث

مدى خضوع شبكات المعلومات للتفتيش

(التفتيش عن بعد)

إن طبيعة التكنولوجيا الرقمية قد عقدت من التحدى القائم أمام أعمال التفتيش والضبط، فالبيانات التى تحتوى على أدلة قد تتوزع عبر شبكة حاسوبية فى أماكن مجهولة بعيدة تماماً عن الموقع المودي للتفتيش، وإن كان من الممكن الوصول إليها من خلال حاسبات تقع فى الأبنية الجارى تفتيشها، إلا أنه قد يكون الموقع الفعلى للبيانات داخل إختصاص قضائى آخر أو حتى فى بلد آخر، ونستطيع أن نميز فى هذه الصورة الإحتمالات التالية:

الإحتمال الأول: إتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة فى مكان آخر داخل الدولة

يثور هنا التساؤل حول مدى إمكانية إمتداد الحق فى التفتيش إذا تبين أن الحاسب أو النهاية الطرفية فى منزل المتهم متصلة بجهاز أو نهاية طرفية فى مكان آخر مملوك لشخص غير المتهم؟

يرى الفقه الألمانى إمكانية إمتداد التفتيش إلى سجلات البيانات التى تكون فى موقع آخر إستناداً إلى مقتضيات القسم ١٠٣ من قانون الإجراءات الجزائية الألمانى[٢].

---

[١] () عبدالله حسين على محمود: سرقة المعلومات المخزنة فى الحاسب الآلى، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠١، ص٢٦٥.

(٢) Kaspersen (W.K. Henrik): "computer crime and other crime against information technology in Netherlands" R. L. D. P. 1993, P. 479.

والشيء ذاته نجده فى القانون الإتحادى الإسترالى، حيث لم تعد صلاحيات التفتيش المتصلة بالأدلة الحاسوبية تقتصر على مواقع محددة، فلا توجد حدود جغرافية محددة، ولا أى اشتراط بالحصول على موافقة طرف ثالث.

وفى هولندا ينص مشروع قانون جريمة الحاسب الآلى على إمكانية أن يمتد التفتيش إلى الأجهزة المعلوماتية الموجودة فى مواقع آخر شريطة أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة[١].

الإحتمال الثانى: إتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة فى مكان آخر خارج الدولة:

من المشكلات التى تواجه سلطة الإدعاء فى جمع الأدلة قيام مرتكبى الجرائم بتخزين بياناتهم فى أنظمة تقنية خارج الدولة، مستخدمين فى ذلك شبكة الإتصالات البعيدة، مستهدفين عرقلة الإدعاء فى جميع الأدلة والتحقيقات[٢]، وفى هذه الحالة فإن إمتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافى للدولة التى صدر من جهتها المختصة الإذن ودخوله فى المجال الجغرافى لدولة أخرى وهو ما يسمى بالولوج أو التفتيش عب الحدود قد يعتذر القيام به بسبب تمسك كل دولة بسيادتها.

إذ لابد لإنعقاد الإختصاص بالتفتيش من أن يتم فى إطار إتفاقيات خاصة ثنائية أو دولية تجيز هذا الإمتداد تعقد بين الدول المعنية، أو على الأقل الحصول على إذن الدولة الأخرى، وهذا يؤكد على أهمية التعاون الدولى فى مجال مكافحة الجرائم التى تقع فى المجال الإلكترونى[٣].

ومع ذلك أجازت المادة ٣٢ من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية والتى أعدها المجلس الأوروبى وتم التوقيع عليها فى بودابست

---

[١] هلالى عبداللاه أحمد: مرجع سابق، ص٨٣.

[٢] Sieber (Urich): "computer crime and other crime against information technology- Commentary and Preparatory question for the colloquium of the A.I.D.P in Wurzburg" R.I.D.P, 1993, P.77.

[٣] محمد أبو العلا عقيدة: التحقيق وجمع الأدلة فى مجال الجرائم الإلكترونية، المؤتمر العلمي الاول حول الجوانب القانونية والامنية للعمليات الالكترونية ، دبي ، ٢٠٠٣ ، ص٣٥.

فى ٢٠٠١/١١/٣٢م إمكانية الدخول بغرض التفتيش والضبط فى أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها فى حالتين:

الأولى: إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور.

والثانية: إذا رضى صاحب أو حائز هذه البيانات بهذا التفتيش.

ويجب أن نشير هنا إلى أن قانون الإجراءات الجنائية المصرى جاء خالياً من تنظيم عمليات التفتيش.

ومن أجل تخطى هذه الصعوبات، يجب برأينا ألا يكون الإذن بالتفتيش

محدداً بمكان معين، بل يجب أن يمتد إلى تفتيش أى نظام موجود فى مكان آخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول فى كشف الحقيقة، بشرط عدم إنتهاك سيادة دولة أخرى.

ويتضح فى النهاية أن تفتيش نظم الحاسبات تفتيش للفضاء الإفتراضى وأوعية التخزين، وهو أمر يتعلق بالقدرة على تحديد المطلوب مسبقاً وليس مجرد سبر غور نظام إلكترونى، لأن التعامل وفق السلطة الأخير قد يكون له عواقب قانونية أهمها بطلان الإجراءات لأنها خارج نطاق أمر التفتيش، أو قد تنطوى الإجراءات على كشف خصوصية البيانات المخزنة فى النظام، فالبيانات المخزنة داخل النظم ليست جميعاً تتصل بجريمة الإعتاء على النظام، فمنها بيانات خاصة وأخرى ذات قيمة إستراتيجية، لهذا إهتم الخبراء القانونيون بمخاطر الإعتداء على الخصوصية أو الحياة الخاصة فى معرض الكشف عن الدليل[١].

[١]() يونس عرب: حجية الإثبات بالمستخرجات الإلكترونية فى القضايا المصرفية، (بحث منشور على الموقع (www.arablawinfo.com).

المطلب السادس
الضبط فى الجريمة المعلوماتية

الضبط فى الجريمة المعلوماتية لا يخرج عن كونه وضع اليد على شيء يتصل بجريمة وقعت على جرائم المعلومات، ويفيد فى كشف الحقيقة عنها وعن مرتكبيها، سواء فى ذلك أن يكون هذا الشيء عقاراً أو منقولاً، فقد بينا فى المبحث السابق أن المشرع أجاز لمأمور الضبط القضائى أن يضبط ما لدى المتهم أو فى مسكنه من الأشياء التى إستخدمت فى إرتكاب الجريمة الجارى التفتيش بصددها، وكذلك الأشياء الناتجة عن إرتكابها، أو الأشياء التى وقعت عليها الجريمة، أو أى شيء يفيد العدالة فى ظهر الحقيقة.

وسنتاول هذا المبحث من خلال المطلبين التاليين:

الفرع الأول: مفهوم الضبط فى جرائم المعلومات.

الفرع الثانى: محل الضبط فى جرائم المعلومات

الفرع الأول
مفهوم الضبط فى جرائم المعلومات

تختلف طبيعة الضبط فى نطاق جرائم المعلومات، ومرد ذلك أن تقنية المعلومات تنطوى على حالات مختلفة من حيث ظروفها وأحوالها، فهى تتطلب لإجراء الضبط بها تقنيات خاصة تغاير حالات الضبط على الموجودات التقليدية. ولم يتطرق قانون الإجراءات الجنائية المصرى إلى قواعد الضبط فى الجريمة المعلوماتية مكتفياً بالقواعد العامة للضبط فى الجرائم، فيما تناولت الإتفاقية الأوروبية بوادابست السابق الإشارة إليها أحكام الضبط فى الجريمة المعلوماتية من خلال المادة "١٩"، فأستخدمت المصطلح التقليدى لذلك الإجراء وهو الضبط، وأضافت إلى جانب ذلك عبارة "الحصول بأى وسيلة مماثلة على البيانات المعلوماتية" للإشارة إلى أساليب أخرى مستحدثة للضبط، فمصطلح الضبط يمكن أن يشمل المكونات المادية التى يتم تخزين من تلك البيانات، بالإضافة إلى إستخدام أو ضبط بيانات ضرورية من أجل الولوج إلى البيانات وضبطها، فمصطلح الحصول بطريقة مشابهة يشير إلى الأخذ بالإعتبار الطرق الأخرى رفع

البيانات غير المادية والتى لا يسهل الوصول إليها، وبالتالى فإن سلطات الضبط يجب أن تتخذ ما يلزم إتخاذه من أجل الحصول على البيانات والمحافظة على سلامتها، فيجب أن تكون تلك البيانات متحفظاً عليها فى الحالة التى تم العثور عليها فيها لحظة الضبط، وعدم تغييرها من خلال ترميزها عن طريق أى وسيلة إلكترونية[1]

الفرع الثانى

محل الضبط فى جرائم المعلومات

الضبط بطبيعته وبحسب تنظيمه القانونى وغايته لا يرد إلا على الأشياء، أما الأشخاص فلا يصلحون ملحاً للضبط بالمعنى الدقيق، وإذا كان قانون الإجراءات يتحدث فى بعض المواد عن ضبط الأشخاص وإحضارهم فإنه يعنى القبض عليهم وإحضارهم، والقبض نظام قانونى يختلف تماماً عن ضبط الأشياء.

وتنقسم الأدلة التى يجوز ضبطها فى الجريمة المعلوماتية والتى لها قيمة خاصة فى إثبات جرائم الحاسب الآلى ونسبتها للمتهم إلى أدلة مادية وأدلة معنوية، بالإضافة إلى المراسلات الإلكترونية.

أولاً: المكونات المادية محل الضبط:

ليس هناك صعوبة فى تطبيق المادة "٥٥" من قانون الإجراءات الجنائية المصرى فى شأن ضبط متحصلات الجريمة المادية سواء ما إستعمل فيها من أدوات أو ما وقعت عليه.

وتشمل تلك المتحصلات المادية كلا من الأوراق، وجهاز الحاسب الآلى وملحقاته، وأقراص الليزر والشرائط الممغنطة، والبطاقات الممغنطة وبطاقات الإئتمان، بالإضافة إلى جميع المكونات المادية الأخرى التى تساهم فى ارتكاب تلك الجرائم لإعتباها من القرائن التى تساهم فى إثبات جرائم المعلومات.

---

[1] () دهلالى عبد اللاه أحمد: إتفاقية بوادابيست لمكافحة جرائم المعلومات، دار النهضة العربية ، ٢٠٠٧ ، ص٢٥٠ إلى ص ٢٥٣.

ثانياً: المكونات المعنوية محل الضبط:

ويتمثل ذلك في برامج الحاسب الآلى والبيانات الخاصة بها، ولا يختلف الحديث عن مدى صلاحية ضبط المكونات المعنوية للجريمة المعلوماتية عما تم سرده سابقاً في الحديث عن مدى صلاحية تلك المكونات المعنوية للتفتيش، فقد ثار الجدل وانقسم الفقه إلى اتجاه يري عدم صلاحية البيانات المخزنة آلياً لأن تكون محلاً للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية، لانتفاء الطابع المادى عن هذه البيانات فى حال تجردها عن الدعامة المادية.

فيما يرى اتجاه آخر أن البيانات المخزنة آلياً حال كونها مجردة من الدعامة المادية التي تحويها لا يوجد ما يمنع من صلاحيتها بهذه الصورة لأن تكون محلا للضبط المنصوص عليه بمقتضى النصوص التقليدية.

وقد توصلنا إلى قناعة بأن تلك المكونات المعنوية تصلح لأن تكون محلا للتفتيش، وهي بالتالى ومن باب أولى تصلح للضبط . فالرأى الراجح هو أن البيانات المخزنة آلياً حال كونها مجردة من الدعامة المادية التي تحويها لا يوجد ما يمنع من صلاحيتها بهذه الصورة لأن تكون محلا للضبط المنصوص عليه بمقتضى النصوص التقليدية.

كما يعزز هذا الرأى بأن البيانات والمعلومات المخزنة على الحاسب الآلى ذات طبيعة مختلفة، يسهل محوها أو التلاعب فيها بسهولة وسرعة فائقة، وخاصة المعلومات المتاحة على أحد المواقع عبر شركة الإنترنت، الأمر الذى يتطلب سرعة فى الحفظ بذاكرة الحاسب ومن ثم ضبطها، فالشخص الذى يقيم موقعاً على شبكة الإنترنت بغرض النصب وسرقة أرقام بطاقات الائتمان يمكنه بسهولة محو الموقع بالكامل بحيث لا يكون هناك أي دليل يثبت إدانته، فكيف يتم إثبات الإدانة ما لم يتم تخويل مأمور الضبط القضائى ضبط تلك البيانات والمعلومات.

إلا أنه لا مفر من تدخل تشريعي يوسع من نطاق الأشياء الممكن ضبطها لتشمل بالإضافة للأشياء ذات الطابع المادى الأشكال الأخرى التي تفتقد هذا الطابع.

ثالثاً: ضبط المراسلات:

تحظر المادة "٥٢" من قانون الإجراءات الجنائية المصري[١]، اطلاع مأمورى الضبط القضائى على الأوراق المختومة أو المغلقة فى منزل المتهم أثناء تفتيشه، وتقابلها فى المعني نفسه المادة "٥٨" من قانون الإجراءات الجزائية الإماراتي.

فإذا كان محل الأشياء المضبوطة أوراقاً مغلقة بأى طريقة فيجوز لمأمورى الضبط القضائى أن يضبطوها، إلا أنه لا يجوز لهم فضها؛ لأن ذلك الأمر يتطلب إذناً من قاضى التحقيق بذلك مع حضور المتهم والحائز لها أو المرسلة إليه، وتدون ملاحظتهم عليها، وهذا القيد ينطبق سواء ضبطت هذه الأوراق مع المتهم حال تلبسه بإرتكاب جريمة يجوز فيها القبض والتفتيش قانوناً أو ضبطت فى منزل المتهم بناءً على تفتيش قانونى سليم[٢].

والتساؤل الذى يطرح نفسه هنا هو: ما مدى سريان القيد الخاص بعدم جواز قيام عضو الضبط القضائى بفض الأوراق المختومة أو المغلقة بأية طريقة كانت والإطلاع عليها، على إطلاعه على محتويات الكمبيوتر أو الأقراص المرنة من معلومات وبيانات، وضبطه للبيانات الإلكترونية المتحصلة من الجريمة المعلوماتية؟

ذهب رأى فقهى إلى أن حكم هذه المادة يسرى على إطلاع مأمورى الضبط القضائى على محتوى نظام المعالجة الآلية للبيانات استناداً إلى سببين[٣]:

أولهما: أن العلة التى اقتضت تقرير هذا الحكم بالنسبة إلى الأوراق المختومة أو المغلقة تتوافر بالنسبة لمحتويات نظام المعالجه الآلية للبيانات: حيث أن الغلق أو التغليف يضفى عليها مزيداً من السرية ويفصح عن رغبة صاحبها فى عدم إطلاع الغير على مضمونها بغير إذنه، وهو ما تحققه

---

[١] () تنص المادة "٥٢" من قانون الإجراءات الجنائية المصرى على أنه: "إذا وجدت فى منزل المتهم أوراق مختومة أو مغلقة بأية طريقة أخرى فلا يجوز لمأمور الضبط القضائى أن يفضها".

[٢] () عفيفى كامل عفيفى: مرجع سابق، ص٣٧١.

[٣] () سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام الإنترنت، مرجع سابق، ص٣٢٣.

البيانات فى نظام معلوماتى؛ لأن محتواه لا يكون مكشوفاً بل محجوباً من الغير ولا يتاح الوصول والإطلاع عليه بغير معرفة طريقة ومفاتيح تشغيله.

ثانيهما: أن المادة ٥٢ إجراءات ترسى قاعدة عامة وضمانات بالنسبة للأسرار التى تتضمنها سائر وسائط وأوعية حفظ وتخزين المعلومات سواء ما كان تقليدياً كالأوراق أو مستحدثاً كالأقراص المرنة والأشرطة الممغنطة وذاكرات الحاسبات، ومتى كان معنى الغلق متحققاً فى الأوعية الأخيرة– وهو ما يكون بأية وسيلة ملائمة لطبيعتها وخصائصها لم يكن لمأمور الضبط القضائى أن يقوم سواء بنفسه إذا توافرت لديه المعرفة العلمية والمهارة الفنية أم بمعاونة من يراه من أهل الخبرة، بإزالة أو إختراق سياج الحماية الفنية للنظام للإطلاع على محتوياته[1].

ويؤيد الباحث ما ذهب إليه الفقه من سريان هذه القيود الإجرائية على محتوى الحاسب أو الإنترنت من معلومات أو رسائل إلكترونية، وعدم جواز إطلاع أعضاء الضبط القضائى على المعلومات والبيانات التى بها، وذلك لصراحة النص على هذه القيود فى قانون الإجراءات الجنائية.

إلا أنه يجب تعديل تلك النصوص المتعلقة بالجريمة المعلوماتية، فهذا القيد يعيق ضبط تلك الأدلة كون أغلبها يحمل تلك الصفة. كما أن عدم السماح لعضو الضبط القضائى بالقيام بفض الأوراق المغلقة يعنى عدم الثقة فيه، فالقانون منحه سلطة تفتيش باقى أرجاء المنزل والذى يعتبر مستودع أسرار الشخص، وبالتالى فهل للأوراق المغلقة أهمية أو سرية خاصة لا تتمتع بها أوراق أخرى غير مغلقة والموضوعة مثلاً فى اخلزينة المغلقة أو أدراج المكتب المغلقة، والتى لم يعطها القانون هذه الأهمية؟

فليس من المنطقى أو المعقول أن يجمع عضو الضبط القضائى جميع الأوراق المختومة والمغلقة، ثم يعرضها على النيابة العامة، فهذا الإجراء فيه إضاعة للجهد والوقت ، كما أن قانون الإجراءات الجنائية فى مصر قد قرر حماية المشتبه بهم من خلال المعاقبة على إفشاء المعلومات الخاصة بهم.

---

[1] () هشام فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص١٠١.
– نبيلة هبه هروال: مرجع سابق، ص ٢٦٠.

بالإضافة إلى أن ضبط البيانات والمعلومات الإلكترونية التى فى الأجهزة الرقمية الحديثة يتطلب أولاً الإطلاع عليها؛ لأن هذه الأجهزة وملحقاتها كالأسطوانات والأقراص المدمجة تحتوى على معلومات وبيانات بكميات هائلة، فلا يعقل أن يقوم عضو الضبط القضائى بضبط هذه الأقراص والإسطوانات، ثم عرضها على النيابة العامة مباشرة(١).

لذا كان من الافضل تعديل ذلك النص ليتناسب مع الطبيعة الخاصة لضبط أدلة الجريمة المعلوماتية، حتى يستطيع عضو الضبط القضائى أن يباشر سلطة فى ضبط هذه الاشياء.

المطلب السابع
صعوبات الضبط فى جرائم المعلومات وطرق التغلب عليها

أولاً: صعوبات الضبط فى جرائم المعلومات :

توجد عدة عوائق تعترض مأمور الضبط القضائى أو الملحق الجنائى عند ضبط البيانات المعالجة آليا، وذلك بصرف النظر عن الخلاف القانونى الدائر حول طبيعتها فيما ان كانت من الأشياء القابلة للضبط من عدمه.

فالجريمة المعلوماتية تتم فى بيئة أو اطار لا علاقة له بالأوراق أو المستندات، بل تتم بواسطة الحاسب الالى أو الشبكة العالمية، ويمكن للجانى عن طريق نبضات الكترونية لا ترى البعث فى بيانات الحاسب الالى أو برامجة وذلك وقت قياسى قد يكون جزءً من الثانية كما يمكنه محو هذه البيانات أو المعلومات فى زمن قياسى قبل أن تصل إليها يد العدالة(٢).

---

(١) هشام محمد فريد رستم: "الجرائم المعلوماتية أصول التحقيق الجنائى الفنى وآلية التدريب التخصصى للمحققين"، (مجلة الأمن والقانون، السنة السابعة، العدد الثانى، يوليو ١٩٩٩، تصدرها كلية شرطة دبى)، ص٨٥.

(٢) عبد الفتاح بيومى حجازى: القانون الجنائى والتزوير فى جرائم الكمبيوتر والانترنت دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٥،ص٢٤

وتكمن تلك الصعوبات العملية التى تحول دون ضبط البيانات التى تشكل دليلا على ارتكاب جريمة ما فى بيئة المعالجة الآلية للبيانات فى الاتى[١]:

١. قلة خبرة بعض العاملين فى الأجهزة الأمنية.
٢. عدم وجود دليل مرئى يمكن فهمه بالقراءة.
٣. تتصف أغلب الجرائم التى يكون محلها بيانات المعلومات بعدم تركها لأية اثار مادية يمكن الاستدلال بها على مرتكب الجريمة.
٤. كما يمكن للجانى محو أو تدمير البيانات التى يمكن التواصل اليها فى فترة زمنية بسيطة لاتتعدى ثوانى معدودة من خلال استخدام وسائل فنية كالفيروسات أو تهيئة وبرمجة الجهاز للتفجير أو التدمير الذاتى بمجرد تشغيلة من قبل الغير.
٥. ضخامة البيانات التى يجب فحصها من قبل المحقق الجنائى.
٦. طبيعة مسرح الجريمة، فالشبكات تنتشر على مستوى العالم، لذا فقد لا يكون ممكنا الحصول على الدليل فى حالة توزيع مسرح الجريمة بين أكثر من دولة[٢].
٧. اخفاء الهوية وذلك من خلال القيام ببعض الأجراءات أو استخدام بعض البرامج والتطبيقات التى تؤدى لطمس الهوية، مما يشكل عائقاً أمام مأمورى الضبط القضائى.
٨. اخفاء المعلومات والبيانات من خلال استخدام برامج خاصة لخلق ما يعرف بنظام (ملفات آمن) مما يجعل من عملية استعادة الأدلة أو اعادة تركيبها أمراً فى غاية الصعوبة.

ثانيا: طرق التغلب على صعوبات الضبط فى جرائم المعلومات.

---

[١] () عفيفى كامل غفيفى: مرجع سابق، ص٣٥٥ وما بعدها.

[٢] () عبد الناصر محمد فرغلى، د.محمد عبيد سيف (الاثبات الحنائى بالأدلة الرقمية من الناحية القانونية والفنية)، منشور ضمن اعمال المواد العلمية للمؤتمر الثالث للتشريعات الجنائية ، جامعة نايف للعلوم الامنية، الرياض ، ص٣٢.

٩. ويتضح مما تقدم أن ضبط الجريمة المعلوماتية أمر فى غاية الصعوبة، وللتغلب على تلك الصعوبات ينصح البعض باتباع الاجراءات التالية(١).

١- **ان يقوم بالتفتيش المختصصون:**

فاذا شاهد مأمور الضبط القضائى جريمة من جرائم المعلومات المتلبس بها فيجب ألا يقوم بالتفتيش على تلك الأجهزة، وانما يجب عليه ضبطها وارسالها الى المختصين، أو طلبهم فى موقع الحادث للتأكد منها وفحصها لكى لا يفقد الدليل.

٢- **عدم تغير الدليل الأصلى:**

فمن السهل عدم تغيير أدلة الأجهزة والبرامج عندما لا تكون الأجهزة قيد الاستخدام، إلا أن المشكلة تكمن عندما تكون تلك الأجهزة فى وضع التشغيل، فقد يؤدى البعث بها أو أى تفاعل بين المستخدم والحاسب إلى تغيير فى حالة الدليل ، وقد يكون لتلك التغيرات اثاراً على الدليل الالكترونى ، بالتالى فيجب ان يكون مأمور الضبط القضائى حريصا على تقليل جميع التفاعلات لتقليل احتمال تغيير تلك الأنظمة.

٣- **عدم تنفيذ البرامج على حاسب مسرح الجريمة:**

ان تنفيذ أى برامج مباشرة على أنظمة المعلومات بمسرح الجريمة قد يسبب الضرر للأدلة الموجودة عليه ، أو على الأقل قد يغير حالة الذاكرة أو الملفات، وإذا كان لا بد من تنفيذ البرامج على حاسب مسرح الجريمة فيجب التعامل معه من قبل متخصص.

٤- **عدم السماح للمشتبه فيه بالتعامل مع حاسب مسرح الجريمة:**

إن الأدلة المعلوماتية من السهل شطبها أو اتلافها لدى العمل على جهاز الحاسب؛ لذلك يجب عدم السماح للمشتبة به بالعمل على هذه الأجهزة، فيجب ألا يكون هناك أى سماح له بالتعامل مع أى جزء فى الجهاز أو حتى الوصول الى مصدر الطاقة.

---

(١) كمال أحمد الكركى: التحقيق فى جرائم الحاسوب (بحث منشور على الموقع www.arablawinfo.com)، ص٣٠ الى ص.٣٢.

٥- **اعداد نسخة من وسائط تخزين المعلومات الموجودة فى مسرح الجريمة**:

إن اعداد نسخة احتياطية ضرورة للعمل الجنائى، فيجب ان تقتصر نشاطات التحقيق على النسخ الاحتياطية لضمان المحافظة على الدليل الاصلى.

٦- **توثيق جميع نشاطات التحقيق**:

يجب توثيق كل مايفعله المحقق بما فى ذلك الشهود ومساعدو التفتيش ومواقع الأجهزة والوسائط منذ لحظة فتح القضية الى لحظة اغلاقها، وعمل سجل للأدلة الالكترونية يحتوى على وصف موجز للأجهزة والوسائل خلال التفتيش عن الأدلة لاعتبار ذلك من ضمن اجراءات مخصص الاستدلال، ولإكساب الإجراءات المتخذة حجيتها القانونية

٧- **التخزين الجيد الحاسب**:

يجب تخزين أدلة الأجهزة والبرامج فى بيئة مناسبة، ويجب الحذر من المجالات الكهرومغناطيسية والكهرباء الساكنه والغبار، كونها تؤثر فى اتلاف الدليل.

الخلاصة:

بعد ان انتهينا من تعريف الجريمة المعلوماتية وسماتها وسمات المجرم المعلوماتي واستعرضنا بشكل مفصل الدور العملي لوزارة الداحلية المتمثل في دور مامور الضبط القضائي في تحقيق الجرائم المعلوماتية بصفته المنوط به ذلك ولما لدور وازرة الداخلية من دور فعال في انفاذ القانون وضنط الجرائم ومكافحتها فنري أننا :-

فى حاجة الى التنظيم التشريعى لجوانب الضبط فى حقل جرائم المعلومات ومسائل حماية البيانات الشخصية أيضا نجد وجها فى الحاجة الى توفير معيار مقبول يقيم توازناً بين حقوق وحريات الافراد وحماية خصوصياتهم، وبين موجبات المكافحة وحاجتها إلى قواعد استثنائية فرضتها تحديات هذه الجرائم التى تزيد عن تحديات غيرها.

وفى ظل الحاجة للتدخل السريع لضبط متعلقات الجريمة فى المكافحة الفاعلة قد تنطوى على اهدار لكثير من الحقوق والحريات فى ضمانات المتهم وما توجبه قرينة البراءة المقرر له ، وهذا التناقض لا مجال لفضه إلا باقامة معيار تعكسه القواعد التشريعية، فالإستثناء على الحرية والقيد المقرر عليها يغدو مقبولا فى ضوء اعتبارات مصلحة المجتمع وأمنه متى توفر بحق هذا المبرر، ومتى كان المعيار مدركاً أن الاستثناء لا يجوز التوسع فيه، ويتعين تقييده بالقيد التشريعى الواضح الذى لا يتيح للسلطات التوغل فيما قرره القانون من حقوق، أو بما تفسره هى وفق رؤيتها لما قرره القانون من حقوق ، أو بما تفسره هى وفق رؤيتها لما قرره القانون من حقوق ، أو بما تفسره هى وفق رؤيتها لما قرره القانون لها من صلاحيات[1].

[1]() يونس عرب: جرائم الكمبيوتر والإنترنت، مرجع سابق، ص٥٢٣.

قائمة المراجع

الكتب المتخصصة :

١. جميل عبد الباقي الصغير : أدلة الإثبات الجنائي والتكنولوجيا الحديثة ، دار النهضة العربية ، القاهرة ، ٢٠٠٢ .

٢. حسين ابراهيم : الاستدلال ، كلية الشرطة ، القاهرة ، ٢٠٠٤

٣. خالد ممدوح ابراهيم : فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٩

٤. فتوح الشاذلي ، وعفيفي كامل عفيفي : جرائم الكمبيوتر، بدون دار نشر.

٥. مأمون سلامة : حدود سلطة القاضي في تطبيق القانون ، دار الفكر العربي ، ١٩٧٥ .

٦. مصطفي محمد موسي : التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الاولي ، مطابع الشرطة ، القاهرة ، ٢٠٠٩ .

٧. ممدوح عبد الحميد عبد المطلب : جرائم استخدام شبكة المعلومات العالمية ، الجريمة عبر الإنترنت ، الطبعة الاولي ، دار الفتح ، الشارقة ، ٢٠٠٠٠ .

٨. نائلة عادل محمد فريد قورة : جرائم الحاسب الإقتصادية – دراسة نظرية وتطبيقية ، دار النهضة العربية ، القاهرة ، ٢٠٠٤ .

٩. نبيلة هبه هروال : الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلال دراسة مقارنة ، الإسكندرية ، دار الفكر الجامعي ، ٢٠٠٧

١٠. هدي حامد قشقوش : جرائم الحاسب الإلي في التشريع المقارن ، دار النهضة العربية ، القاهرة ١٩٩٢ .

١١. هشام محمد فريد رستم : قانون العقوبات ومخاطر تقنية المعلومات ، الطبعة الاولي ، مكتبة الالات الحديثة ، اسيوط ، ١٩٩٢

١٢. ـــــــ : الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الألات الحديثة ، اسيوط ، ١٩٩٤ .

١٣. هلالي عبداللاه احمد : التزام الشاهد بالإعلام في الجرائم المعلوماتية ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠٠٦ .

١٤. ـــــــ : تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ، ادار النهضة العربية ، القاهرة ، ٢٠٠٦ .

١٥. يونس عرب : الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، الطبعة الثانية ، دار النهضة العربية ، ٢٠٠٦

الرسائل العلمية :

١. أيمن عبد الحفيظ : إستراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي ، رسالة دكتوراه ، أكاديمية الشرطة

٢. حسن بن سعيد بن سيف الغافري : السياسة الجنائية في مواجهة جرائم الإنترنت – دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق ، جامعة عين شمس ، القاهرة .

٣. سليمان أحمد محمد فضل : المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت) ، رسالة دكتوراه ، أكاديمية الشرطة ، القاهرة ، ٢٠٠٧ .

٤. عارف محمد عبد الرحيم : دور مهام أعضاء الضبط القضائي في مرحلتي التحري والتحقيق الأبتدائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة المنصورة ، ٢٠٠٧

٥. عبد الله حسين علي محمود : سرقة المعلومات المخزنة في الحاسب الآلي ، رسالة دكتوراه ، جامعة عين شمس ، ٢٠٠١ .

المؤتمرات و الندوات :

١. عبدالله حسين على محمود إجراءات جمع الادلة فى مجال سرقة المعلومات ، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية و الأمنية للعمليات المعلوماتية ، إمارة دبى بدولة الإمارات العربية المتحدة ٢٦-٢٨/٤/٢٠٠٣ المجلد الأول .

٢. عبد الناصر محمد فرغلى ، د. محمد عبيد سيف ، الإثبات الجنائى بالأدلة الرقمية من الناحية القانونية والفنية–دراسة تطبيقية مقارنة ، منشور ضمن أعمال المواد العلمية للمؤتمر العربى لعلوم الأدلة الجنائية والطب الشرعي، المحور الثالث التشريعات الجنائية ، جامعة نايف العربية للعلوم الأمنية، الرياض ، في الفترة من ١٢ إلى ١٤ -١١-٢٠٠٧ م .

٣. عمر محمد أبو بكر بن يونس : الإثبات الجنائى عبر شبكة الإنترنت ، ورقة بحثية مقدمة إلى ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الافتراضية خلال الفترة ٢-٢٠٠٦/٤/٤، مسقط ، سلطنة عمان.
٤. غنام محمد غنام : عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر ، مؤتمر القانون ، جامعة الإمارات العربية المتحدة ٢٠٠٠ .
٥. محمد أبو العلا عقيدة ، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية، دبي ، ٢٠٠٣ .
٦. محمد الأمين البشري : التحقيق في الجرائم الحاسب الآلى ، جامعة الامارات ، كلية الشريعة والقانون ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، ٢٠٠٤ .
٧. هشام محمد فريد رستم : الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إ اشاء آلية عربية موحدة للتدريب التخصصي ، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت ، كلية الشريعة والقانون ، جامعة الإمارات ، ٢٠٠٤ .

المجلات والدوريات :

١. باسم منصور : الآليات الأمنية لمواجهة جرائم الحاسب والإنترنت ، مجلة مركز بحوث الشرطة ، عدد ٣٥ ، يناير ٢٠٠٩
٢. جمال توفيق وآخرون : دراسة مركز بحوث الشرطة حول الجرائم المعلوماتية وطرق مواجهتها ، مركز بحوث الشرطة ، أكاديمية الشرطة ، الاصدار الثالث ، يونيو ٢٠٠٥ ، القاهرة.
٣. غنام محمد غنام : عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر ، مؤتمر القانون والككمبيوتر والإنترنت ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، سنة ٢٠٠٠ .
٤. سليمان أحمد فضل : البعد الدولي للجرائم المعلوماتية وطرق مواجهتها ، ورقة عمل مقدمة لندوة الواقع الإمني مسئوليات – إنجازات ، مركز بحوث الشرطة ، أكاديمية الشرطة ، القاهرة ٢٠١١/١/٩ .

٥. كريستوفر بينتر : التهديد الذي تفرضه الجريمة المعلوماتية والحاجة الي التعاون الدولي ، ورقة عمل مقدمة للمؤتمر الدولي السادس للجرائم المعلوماتية الذي نظمته المنظمة الدولية للشرطة الجنائية "الإنتربول "، القاهرة ١٣-٢٠٠٥/٤/١٥ ترجمة مركز بحوث الشرطة ، القاهرة
٦. هشام محمد فريد رستم : الجرائم المعلوماتية اصول التحقيق الجنائي الفني وآلية التدريب التخصصي ، مجلة الأمن والقانون ، تصدرها كلية شرطة دبي ، السنة السابعة ، العدد الثاني ، يوليو ١٩٩٩ .

أبحاث علي الشبكة الدولية للمعلومات :

١. علي محمود علي حمودة : الادلة المتحصلة من الوسائل الإلكترونية في إطار الإثبات الجنائي (بحث منشور علي الموقع www.arablawinfo.com)
٢. يونس عرب : جرائم الكمبيوتر والإنترنت – المعني والخصائص والصور وإستراتيجية المواجهة القانونية ، (بحث منشور علي الموقع www.arablawinfo.com)
٣.ـــــــ : حجية الإثبات بالمستخرجات الإلكترونية في القضايا المصرفية ، (بحث منشور علي الموقع www.arablawinfo.com)