الجوانب الإجرائية لجرائم المعلوماتية

د. مقداد ايوب سعدي القره لوسي
الامانة العامة لمجلس الوزراء

د. غسان شاكر محسن أبو طبيخ
الامانة العامة لمجلس الوزراء

المقدمــة

شهد القرن الحادي والعشرين العديد من التطورات في مجال المعلومات والاتصالات، وقد انعكس ذلك على جميع نواحي الحياة، وكان من نتائج هذا التطور ظهور الجريمة الالكترونية، والتي تضاعفت بصورة كبيرة وفي مختلف دول العالم، حيث بات العديد من المجرمين الذين يسخرون التقنية الحديثة في ممارسة اعمالهم الاجرامية على الشبكة العالمية باستخدام جهاز الحاسب الآلي.

إن ثورة الاتصالات والمعلومات دفعت عدداً هائلاً من الأفراد والمؤسسات ارتياد هذه الشبكة فقد بات العالم في قرية إلكترونية واحدة، وما تبلور عنها بظهور التجارة الالكترونية، والحكومة الالكترونية وغيرها من مجالات وانتقال العمليات الادارية والمصرفية من اسلوبها التقليدي واجراءاتها الورقية ، واصبحت مجالاً خصباً لكثير من الشبكات الاجرامية التي تمارس نشاطها الاجرامي من السرقة والتجسس والابتزاز وهتك العرض وغيرها من جرائم. وأصبح من السهل وفق ما تقدم ارتكاب أبشع الجرائم بحق مرتادي شبكة الانترنت، من خلال اختراق نظام الامن وفك الشفرات لأجهزة الحاسوب، ولم تتمكن تقنيات الامن المستخدمة من حماية المستندات والبيانات بشكل كامل، مما يستدعي تدخل المشرع لحماية الافراد والمؤسسات من خلال نظام جنائي صارم للحد من هذه الانتهاكات والجرائم.

ان قانون الاجراءات الجنائية ينتمي الى طائفة القوانين المنظمة لأعمال القضاء، لأنه يهدف الى فاعلية العدالة الجنائية، والتي تتوقف على التطبيق القضائي لقانون العقوبات فضلاً عن أن القضاء هو الحارس الطبيعي للحريات. فقانون الاجراءات الجنائية يهدف الى حل نزاع يتعلق بتطبيق قانون العقوبات وهو مسألة ترتبط بمصلحة الدولة، فضلاً عن حماية الحرية الشخصية للمتهم[١].

لذا سوف نحاول معالجة هذا الموضوع من خلال تقسيمه الى الخطة الآتية:

تقسيم البحث

المبحث الاول: ماهية الجريمة المعلوماتية
المطلب الاول: مفهوم الجريمة المعلوماتية
المطلب الثاني: خصائص الجريمة المعلوماتية
المبحث الثاني: ضبط وتفتيش محتويات الحاسب الآلي
المطلب الاول: المعاينة
المطلب الثاني: الضبط والتفتيش
المطلب الثالث: المراقبة
الخاتمة

(١)راجع: د.أحمد فتحي سرور، الشرعية الدستورية وحقوق الانسان في الإجراءات الجنائية، دار النهضة العربية-القاهرة، طبعة معدلة،١٩٩٥، ص٥٣و ٥٧.

المبحث الأول
ماهية الجريمة المعلوماتية

ان التقدم التقني والمعلوماتي مكن مستخدمي شبكة الانترنت من حفظ واجراء تعاملاتهم بطريقة اليكترونية وايداع أوراقهم ومستنداتهم الكترونياً لما يوفره هذا النظام من جهد ووقت من خلال استخدام الحوسبة السحابية على شبكة الانترنت[١]، ولا يمكن اغفال الاهمية الكبيرة لهذا التقنية والمتمثلة في حفظ البيانات وحمايتها من الفقدان أو التلاعب أو التلف، من خلال تشفيرها، وذلك بتحويل الكلمات المكتوبة أو المستندات إلى أرقام أو رموز لا يمكن معرفة مضمونها، إلا عن طريق فك الشفرة ذاتها. إلا إن هذا التطور كان له انعكاساً سلبياً يتمثل في اقدام البعض ذوي الميول الاجرامية من اختراق أجهزة الحاسوب من خلال كسر الشفرة والاستيلاء على البيانات والمعلومات أو تحريفها أو اتلافها.

ومما هو جدير ذكره، فإن جريمة الاحتيال واستخدام أجهزة الحاسوب بقصد التضليل أو الغش وافشاء أسرار وبيانات المشتركين للغير واستخدام شبكة الانترنت بقصد الغش علامة تجارية تعود للغير تعد أكثر الجرائم شيوعاً على شبكة الانترنت، وهذه الجرائم يعاقب عليها قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل[٢].

لذا فإن القانون العراقي يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعاً من الحماية الجنائية ضد الافعال الشبيهة بالأفعال المكونة لأركان جريمة المعلوماتية.

ونتناول فيما يأتي التعريف بالجريمة المعلوماتية وخصائص هذه الجريمة.

المطلب الأول
مفهوم الجريمة المعلوماتية

نتيجة لاتساع ظاهرة الاستغلال المقترنة بسوء نية عند التعامل مع التقنية الحديثة ادى لنشوء ما يسمى بالإجرام المعلوماتي بوصفه أحد الاوجه العديدة للتعدي المؤثر على التقنية في العمليات الادارية والمصرفية والامنية، بحيث أصبح الاجرام المعلوماتي حقيقة اجتماعية مادية[٣].

مما يستدعي وضع الحلول ومعالجة أي استخدام سيء لثورة تقنية المعالجة الالية للمعلومات المتعلقة في أغلبها بالتلاعب بالحاسب الآلي وتعطيله والتجسس عليه.

ومما تجدر الاشارة اليه، ان هناك صعوبة في وضع تعريف معين لمفهوم الجريمة المعلوماتية خشية حصرها في مجال ضيق وخصوصا لعدم الاتفاق على مصطلح معين للدلالة على هذه الظاهرة الاجرامية[٤].

ونظراً لعدم وجود اجماع على تعريف هذه الجريمة، فقد تعددت التعاريف في هذا المجال، فمنهم من يستند في تعريفها على وسيلة ارتكاب الجريمة وهو جهاز الحاسوب، اذ يعرفها: كل أشكال السلوك غير المشروع

---

(١) يعرّف البعض الإنترنت بشبكة الشبكات، وبعبارة أخرى ((شبكة الشبكات)) حيث تتكون الإنترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرة في أنحاء كثيرة من العالم. ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى ((بروتوكول تراسل الإنترنت(TCP/IP) . انظر: محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، مقال منشور على شبكة الانترنت (http://www.khayma.com).

(٢) القاضي كاظم عبد جاسم الزيدي ، مكافحة الجرائم المعلوماتية في التشريع العراقي ، بحث منشور على موقع السلطة القضائية(http://www.iraqja.iq).

(٣) قسم مشروع الاتفاقية الأوروبية لجرائم الحاسب الآلي "الكمبيوتر" والإنترنت لعام ٢٠٠٠-٢٠٠١ جرائم الانترنت الى:

١- الجرائم التي تستهدف عناصر المعطيات والنظم وتضم :

(أ) الدخول غير القانوني "غير المصرح به".(ب) الاعتراض غير القانوني.(ج) تدمير المعطيات.(د) إساءة استخدام الأجهزة.

٢- الجرائم المرتبطة بالحاسب الآلي:(أ) التزوير المرتبط بالحاسب الآلي.(ب) الاحتيال المرتبط بالحاسب الآلي.

٣-الجرائم المرتبطة بالمحتوى : وتضم طائفة واحدة وفقاً لهذه الاتفاقية (مشروع الاتفاقية الأوربية لجرائم الحاسب الآلي) وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.

4 -الجرائم المرتبطة بالإخلال وبحقوق الملكية الفكرية وعلى وجه التحديد الجرائم المرتبطة بالتعدي على حق المؤلف والحقوق المجاورة أو فيما يعرف بقرصنة البرمجيات.

(٤) انظر: محمد علي سالم وحسون عبيد هجيج، الجرائم المعلوماتية، بحث منشور في مجلة العلوم الانسانية، جامعة بابل، المجلد ١٤، العدد٢، ٢٠٠٧، ص٨٧.

أو الضار بالمجتمع الذي يرتكب باستخدام الحاسوب. ويعرفها البعض الآخر بالاستناد الى موضوع الجريمة: بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تخول عن طريقه[١].

وعرفها جانب آخر كمصطلح عام لجميع اشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات(ITC) دوراً أساسياً. وهنا تقع الكثير من الجرائم ضمن هذا التعريف فقد قدم هذا الفريق قائمة بـ ٢٨ جريمة بدءاً من قرصنة الانظمة الرقمية وتثبيت برامج التجسس للاحتيال باستخدام الخدمات المصرفية عبر الانترنت[٢].

وتتعدد صور ارتكاب جرائم الانترنت: فمنها ما يمس أمن وسلامة البلاد(جرائم الارهاب الالكتروني)[٣]، أو في ارتكاب جرائم الاتجار بالبشر والمخدرات والممارسات الجنسية والاحتيال والتزوير والقرصنة الالكترونية أو يتعلق بالحقوق المالية للدولة او الشركات او الافراد[٤].

المطلب الثاني

خصائص جرائم المعلوماتية

تميزت الجرائم المعلوماتية عن غيرها من الجرائم التقليدية بعدة خصائص يمكن اجمالها بما يأتي:

أولاً- انها جريمة عابرة للحدود:

شبكة المعلومات لا تعترف بالحدود الجغرافي، حيث لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، نتيجة للقدرة الفائقة لأجهزة الحاسوب وشبكاتها في نقل كميات كبيرة من البيانات والمعلومات وتبادلها بين نظم معلومات يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد. مما ولد امكانية ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى[٥].

ثانياً- صعوبة اكتشافها واثباتها:

فهي تمتاز بصعوبة كشفها، حيث ان المجنى عليه لا يلحظها غالباً إلا بعد مدة من ارتكابها، وذلك لاحترافية الجاني من جهة، ولكون المجنى عليه يتعامل مع نبضات الكترونية غير مرئية ولا يمكن قرائتها من جهة اخرى.

ولغياب الاثر المادي في كثير من الاحيان فان اثبات هذه الجريمة أمر بالغ الصعوبة، لكون هذه الجريمة تتعامل مع أنظمة معلوماتية معالجة بواسطة نبضات الكترونية على الحواسيب، وهذه من السهولة اختراقها والتلاعب فيها أو محوها[٦].

---

(١) انظر:http://www.blog.saeeed.com

(٢) د.ذياب موسى البداينة، الجرائم الالكترونية: المفهوم والاسباب، بحث مقدم الى الملتقى العلمي(الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية)، للفترة من ٢-٢٠١٤/٩/٤ في عمان-الاردن.

(٣) يلجأ الارهابين الى استخدام أجهزة الحاسوب وشبكة المعلومات بقصد ارتكاب الجرائم التي تمس أمن البلاد ومصالحها الاقتصادية أو السياسية أو العسكرية، أو تسهيل الاتصال بقيادات وأعضاء الجماعات الارهابية والترويج للأفكار والأعمال الارهابية. انظر: القاضي كاظم عبد جاسم الزيدي، مكافحة الجرائم المعلوماتية في التشريع العراقي، مقال منشور على موقع السلطة القضائية(http://www.iraqja.iq).

(٤) وبالرغم من تعدد التعاريف لمفهوم الارهاب لكننا لم نقف على تعريف جامع مانع لحقيقة الارهاب، فقد عرف قانون الارهاب رقم ١٣ لسنة ٢٠٠٥ في مادته الأولى العمل الارهابي بأنه: (كل فعل اجرامي يقوم به فرد او جماعة منظمة استهدف فرداً أو مجموعة افراد أو جماعات أو مؤسسات رسمية أو غير رسمية اوقع الاضرار بالممتلكات العامة أو الخاصة بغية الاخلال بالوضع الامني أو الاستقرار والوحدة الوطنية أو ادخال الرعب أو الخوف والفزع بين الناس أو اثارة الفوضى تحقيقاً لغايات ارهابية). ومن مدلول هذا النص يمكننا اعتبار كل ما يدخل في نطاق الارهاب من جرائم المعلوماتية مشمولة بنص القانون المذكور.
كما اننا نجد أن مشروع قانون التجارة الالكترونية المصري، جرم في المادة ٢٦ منه أفعال الغش أو التدليس التي تقع على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيعات الإلكترونية، وكذلك فقد جرمت هذه المادة أفعال الاتصال أو الابقاء على الإتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة.

(٥) نهلا عبد القادر المومني، الجرائم المعلوماتية، بحث منشور على شبكة الانترنت(http://kenanaonline.com).

(٦) القاضي محمد عبدالله سعيد، الجرائم المعلوماتية، بحث مقدم الى مجلس القضاء الاعلى وهو جزء من متطلبات الترقية لسنة ٢٠١١، ص١١-١٢.

ثالثاً- الجاني في الجرائم المعلوماتية :
قد يكون الجاني الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي شخصاً طبيعياً يعمل لحسابه، ويهدف إلى تحقيق مصلحة خاصة به من وراء الجريمة التي يرتكبها ضد أحد نظم المعالجة الآلية للبيانات والمعلومات، أو عن طريق الاستعانة بأحد نظم المعالجة الآلية للبيانات والمعلومات ، ولكن يحدث كثيراً أن يقترف الشخص الطبيعي الفعل المؤثم جنائياً ليس لحسابه الخاص ، وإنما لحساب أحد الأشخاص المعنوية ، كشركة عامة أو خاصة تعمل في مجال المعلوماتية ، أو تعمل في مجال آخر ، ولكن تقدم على السطو على أحد أنظمة المعلوماتية، أو تحدث ضرراً للغير عن طريق اللجوء لأحد نظم المعالجة الآلية للمعلومات((١)) .
رابعاً- اقل عنفاً بالتنفيذ:
تعد جرائم هادئة لا تحتاج الى عنف لتنفيذها مقارنة بالجرائم التقليدية فيكفي لارتكابها وجود جهاز حاسوب مع شبكة انترنت، في حين أن الجرائم التقليدية تكون مصحوبة بعنف غالباً كما في جرائم القتل والخطف.

المبحث الثاني
ضبط وتفتيش محتويات الحاسب الآلي

يعد اختراق الحاسوب عمل غير قانوني يحاسب عليه القانون، فاختراق الحاسوب من قبل البعض أمر خطير للغاية، لأنه يجعل المعلومات والبيانات كلها متاحة للغير، فلن يكون هناك سرية في المعلومات، مما يمكن الغير من استخدام هذه البيانات بطريقة مخلة تضر كثيراً بصاحبها. الحماية من هذه الاعتداءات واثبات قدرة النظام على التعامل الآمن مع البيانات يثير مشكلات إجرائية عديدة في معرض تفتيش نظم الحاسوب أو تقديم الدليل في الدعوى الجزائية، طبعاً في النظم القانونية التي تنص على تجريم افعال الاعتداء على المعلومات، وهذا ما سنتناوله في المطالب الآتية:

المطلب الأول
المعاينة

كما أشرنا آنفاً فأن طول الفترة الواقعة بين ارتكاب الجريمة المعلوماتية وبين وقت ارتكابها قد يؤدي الى ضياع الادلة المادية بسبب اتلاف أو تحريف أو محو جميع تلك الآثار.
لذا فأن البعض يرى بأن اهمية معاينة مسرح الجريمة في مثل هذه الحالة تتضاءل لندرة تخلف آثار مادية.
وفي كل الأحوال وعند تلقي بلاغ بوقوع إحدى الجرائم المعلوماتية يتم الانتقال إلى مسرح الجريمة لمعاينته، ومسرح الجريمة المعلوماتية يختلف عن مسرح الجريمة التقليدية كالقتل والسرقة، والجريمة المعلوماتية قد تكون جريمة مستمرة كما في حالة الجرائم الاقتصادية– السرقة والاحتيال –وقد يكون مسرحها جرائم اخرى كما في جريمة التزوير وإتلاف البرامج. ففي الحالة الاولى تكون المعاينة هدفها المداهمة وضبط الأدلة على الطبيعة، وفي الحالة الثانية وبعد وقوع الجريمة فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم وكذلك شهادة الشهود والقرائن(٢).
لذا يرى البعض بأن أهمية المعاينة بعد وقوع الجريمة الالكترونية لا تقل عن أهميتها بالنسبة للجرائم التقليدية، ومرد ذلك إلى ان هناك على الدوام تقريباً، مسرحاً للجريمة جرت عليه الاحداث وتركت آثارها المادية. بينما لا يوجد عادة مسرح مماثل للجريمة الالكترونية، واقرب تشبيه لمسرحها، قد يكون الموقع أو المكتب الذي توجد فيه المعدات والانظمة المعلوماتية التي كانت محلاً للجريمة(٣).

المطلب الثاني
الضبط والتفتيش

---

(١) المستشار الدكتور محمد ياسر أبو الفتوح خصائص وتصنيفات الجريمة المعلوماتية، بحث منشور على موقع منتدى كلية الحقوق-جامعة المنصورة.
(٢) د. محمد عبيد سيف، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية-دراسة تطبيقية مقارنة، بحث مقدم للمؤتمر العربي الاول لعلوم الادلة الجنائية والطب الشرعي، ٢٠٠٧.
(٣) د.صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة دكتوراه مقدمة الى كلية الحقوق والعلوم السياسية-جامعة مولود معمري في العام ٢٠١٣، ص٨٤.

يعد التفتيش وسيلة الاثبات المادي للجريمة الواقعة، ومحله اشياء مادية تتعلق بالكشف عن الجريمة، وهذه الطبيعة المادية تتعارض مع الطبيعة غير المادية لمحتويات وبرامج الحاسب الآلي وشبكة الانترنت[١]، والتي ليس لها أي مظهر محسوس[٢].

إن الولوج إلى مكونات الحاسب الآلي المادية بحثاً عن شيء يتصل بجريمة من جرائم الانترنت، يفيد بلا شك في كشف الحقيقة عن الجريمة ومرتكبها، ويخضع للإجراءات القانونية الخاصة بالتفتيش.

هناك تشريعات قليلة قد نصت على قواعد خاصة بتفتيش مكونات الحاسبات الآلية، من ذلك المادة ٢٥١ من قانون الإجراءات الجنائي اليوناني ، والمادة ٤٧٨ من القانون الجنائي الكندي. كذلك فإن القانون الإنجليزي الصادر في سنة ١٩٩٠ والذي طبق اعتبارا من ٢٩ أغسطس سنة ١٩٩٠ نظم صراحة تفتيش مكونات الحاسب الآلي، فنص هذا القانون على أن الجرائم المدرجة في القسم الثاني والقسم الثالث والتي تشتمل على أفعال الدخول غير المصرح به على نظام الحاسب الآلي لتسهيل إرتكاب أفعال غير مشروعة عن عمد، أو التعديل غير المصرح به في نظام الحاسب عن عمد، والتي يعاقب عليها بعقوبة السجن لمدة لا تزيد على خمس سنوات، تجيز القبض على المتهم دون حاجة لإذن قضائي، كما تجيز تفتيش محل إقامة المتهم بحثا عن أدلة مادية تكون ذات قيمة في إثبات الجريمة محل القبض[٣].

ويرى الفقه الالماني إمكانية امتداد التفتيش الى سجلات البيانات التي تكون في موقع آخر استناداً الى مقتضيات القسم ١٠٣ من قانون الاجراءات الجنائية الالماني[٤].

ويمكننا اجمال القواعد العامة في التفتيش الجنائي للجريمة المعلوماتية بما يأتي:

أولاً- تفتيش وضبط نظم المعلومات:

يعتبر التفتيش إجراء من إجراءات التحقيق يتطلب أوامر قضائية لمباشرته، ويهدف للبحث عن الأدلة المادية التي ترتبط بالجريمة مدار التحقيق ولا يشمل لذلك الأدلة الشفوية أو القولية لاتصال الأخيرة بعنصر الشخص – الشاهد، ويجري التفتيش بخصوص جرم تحقق وقوعه، ويوجه التفتيش إلى مكان يتمتع بالحرمة، أو يتجه إلى الشخص المشتبه به، ويخضع التفتيش في وجوده وإجراءاته التنفيذية إلى أحكام القانون والتي من أبرزها صدور أمر التفتيش أو مذكراته الكتابية عن الجهة التي حددها القانون، مع بيان الأسباب الموجبة لذلك ومحل التفتيش المخصوص.

ثانياً- التعامل مع الادلة الرقمية:

هنالك عدة نواحي من منظور العلم الجنائي لمعاينة وفحص الأدلة الرقمية وهي:

أ -تمييز الأدلة الرقمية : وهي عملية تتكون من عنصرين، أولاً يجب على المحقق أن يميز الأجهزة Hardwareمثل جهاز الحاسوب والأقراص المرنة وكوابل الشبكات والتي تحتوي على المعلومات الرقمية، وثانياً يجب على المحقق أن يميز بين المعلومات غير المهمة والمعلومات المرتبطة بالجريمة[٥].

---

(١) اختلفت أنظمة الإثبات في تقديرها لحجية المخرجات ففي القوانين ذات الصياغة اللاتينية، ومنها القانون الأردني والفرنسي والمصري والسوري واللبناني، فإن حجية الأدلة الإلكترونية لا تثير صعوبات لمدى حرية تقديم هذه الأدلة لإثبات جرائم الحاسوب والإنترنت ، ولا لمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية، وفي فرنسا مشكلة حجية المخرجات المتحصلة من الحاسوب على مستوى القانون الجنائي ليست ملحة أو عاجلة في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة. نقلاً عن: د.علي حسن الطوالبة، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي-دراسة مقارنة، بحث منشور على شبكة الانترنت(http://www.omanlegal.net).

(٢) د.اسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، بحث منشور في المجلة العربية للدراسات الامنية والتدريب، مجلد٢٩، عدد٥٨، ص٨٧.

(٣) د.علي محمود علي حمودة، الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث منشور على منتدى كلية الحقوق-جامعة المنصورة.

(٤) راجع: د.صغير يوسف، مرجع سابق، ص٧٩.

(٥) يوجد للحاسب الآلي مكونات مادية (Hardware) ، وأخرى معنوية أو برامجية (Software)،كما أن له شبكات اتصال (Network Telecommunications) سلكية ولاسلكية محلية ودولية . ويقصد بالتفتيش هنا التفتيش عن معطيات الحاسب الآلي غير المادية والمخزنة في جهاز الحاسب الآلي، أو المخزنة في الأقراص ، كما يقصد بالتفتيش، البحث في النظم المعلوماتية محل التحقيق. انظر: د.اسامة بن غانم العبيدي، المرجع السابق، ص٨٨.

ب -حفظ وجمع وتوثيق الأدلة الرقمية: يجب حفظ الادلة الرقمية بحالتها الأصلية لأن القانون يطلب أصالة الأدلة وعدم تغيير الحالة الأصلية للأدلة ومن هنا يجب طباعة الدليل وفي هذه الحالة فإن للنسخة المطبوعة قيمة قانونية كدليل إلا إذا كان الدليل الأصلي محل شك.
ج - توفير الوقت والجهد وتجنب تدمير أو مقاطعة عمل فرد أو مؤسسة ما: فبعض أجهزة الحاسوب حساسة لإدارة مؤسسات وقد يؤدي أخذ الجهاز إلى توقف عمل المؤسسة، مثل أجهزة المستشفيات.
كما إن توثيق الادلة مهم لإثبات أن الدليل أصيل ولم يتغير ، كذلك يستخدم التوثيق للتفريق بين الدليل الأصلي والنسخة المأخوذة عنه، وأيضاً يلزم التوثيق وبالذات توثيق هوية الأشخاص الذين جمعوا الدليل وتعاملوا معه من أجل الحفاظ على سلسلة الوصاية.
د- تصنيف ومقارنة وإفراد الدليل الرقمي: وهذه المرحلة هي عملية إيجاد الخصائص التي تصف الأدلة بشكل عام وتميزها عن غيرها، وبناء الدليل الرقمي المخفي أو المشفر يعتد على نوع الدليل الرقمي ونوع الحاسوب ونظام التشغيل وإعدادات الحاسوب.
ومن التحديات الأخرى، الملفات المشفرة حيث أن برامج التشفير أصبحت شائعة وأصبح بإمكان المجرمين بعثرة الدليل الذي يدينهم باستخدام شيفرة غير مقروءة وبالتالي يصبح فك التشفير مسألة صعبة ويتطلب فك التشفير كلمة سر خاصة ويمكن في عدة حالات فك التشفير باستخدام الخبرة والأجهزة المناسبة ولكن محاولة فك التشفير غير عملية في بعض التحقيقات لأنها تأخذ وقتاً خالياً[١].
ومما تقدم يتضح لنا إن وسائل جهاز الشرطة في مجال الضبط القضائي تتنوع إلى عدة أنواع أهمها هي:
أولاً- البحث والتحري عن الجرائم والجناة : ويقصد بها مجموعة الإجراءات التي يقوم بها المتحري عبر الشبكة بواسطة التغطية الالكترونية الرقمية وكذلك على أجهزة الحاسب الآلي، وذلك للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء حسب طبيعتها لضبط جرائم الكمبيوتر والانترنت.
ثانياً- الإرشاد الجنائي عبر الانترنت : يلعب الإرشاد دورا كبيرا في التقصي والكشف عن الجرائم.
ثالثاً- دور الشرطة في معاينة مسرح جرائم الحاسب الآلي : المعاينة هي إثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة.
رابعاً- دور الشرطة بالتفتيش في جرائم الحاسب الآلي : يعد التفتيش من إجراءات التحقيق التي يختص بها أصلا سلطة التحقيق ومأموري الضبط القضائي على سبيل الاستثناء وهو ليس غاية في حد ذاته وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول إليه من خلاله إلى أدلة مادية تسهم في بيان وظهور الحقيقة.
خامساً- الدور الشرطي في ضبط أدلة جرائم الحاسب : أن الضبط لا يعد من إجراءات الاستدلال إلا إذا تم في مكان يجوز لمأموري الضبط دخوله ، أما إذا تم نتيجة تفتيش المتهم أو مسكنه ففي هذه الحالة يعد من إجراءات التحقيق لا الاستدلال ، والضبط ينصب على الأشياء المادية ، إما الأشياء غير المادية فلا يرد عليها الضبط إلا استثناء بموجب نصوص خاصة[٢].
ومما تجدر الاشارة اليه، انه وبعد ضبط الأدلة الجرمية لا بد من المحافظة عليها وفق أسس علمية مدروسة تكفل بقائها على حالتها لحين انتهاء مرحلة المحاكمة، وقد أحال مشروع قانون الجرائم المعلوماتية العراقي إجراءات الضبط إلى قانون اصول المحاكمات الجزائية في المادة(٢٤/ثالثاً) والتي تنص على: (يتولى قاضي التحقيق إو المحقق المباشرة في إجراءات الضبط وجمع الأدلة أو أي إجراء تحقيقي نص عليه قانون أصول المحاكمات الجزائية) [٣].

المطلب الثالث
المراقبة

(١) جمال احمد الكركي، التحقيق في جرائم الحاسوب، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والامنية للعمليات الالكترونية-اكاديمية شرطة دبي، للفترة من ٢٠٠٣/٤/٢٦ ولغاية ٢٠٠٣/٤/٢٨.
(٢) نقلاً عن: د.عفيفي كامل عفيفي، جرائم الكمبيوتر والانترنت ودور الشرطة في مكافحتها، بحث منشور على شبكة الانترنت، http://www.omanlegal.net.
(٣) نقلاً عن: القاضي محمد عبدالله سعيد، المرجع السابق، ص٨٦.

من الحقوق الأساسية للإنسان هي حرمة حياته الخاصة التي تصون كل خصوصياته، وأسراره الخاصة به، وإن هذا الحق متباين الإباحة والتجريم بين الشريعة والقانون[١].

الكثير من الدول أجازت التصنت والمراقبة الإلكترونية للحاسبات الآلية، ففي فرنسا أجاز قانون ١٠ يوليو سنة ١٩٩١ فرض الرقابة على الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات. وفي أمريكا تجوز الرقابة على الاتصالات الإلكترونية والتي تدخل عدادها شبكات الحاسب الآلي بشرط الحصول على إذن بالتفتيش من القاضي المختص، أما في كندا فإن القوانين العادية التي تنظم أعمال المراقبة الإلكترونية يمكن أن تطبق على أنواع عديدة من اتصالات الحاسب الآلي[٢].

تعد مراقبة المكالمات السلكية واللاسلكية تحت رقابة القضاء من الوسائل الملائمة لضبط ما يفيد في كشف الحقيقة احياناً، ويجب أن تحاط المراقبة بضمانات فلا يجوز إجرائها إلا بأمر مسبب من القضاء.

ومما تجدر الإشارة إليه، إن التسجيل الصوتي الممغنط باستخدام وسائل عالية الدقة لا يمكن التلاعب فيه ولا يحتمل أي خطأ، وبالتالي فأن التسجيل الصوتي الممغنط يعتبر دليلاً وحجة قاطعة في الاثبات الجنائي.

ويشترط الفقه لمشروعية الدليل المستمد من المراقبة أن تتوافر فيه جملة من الشروط تتمثل في:

أولاً- اذا لم يتضمن التسجيل اعتداء على حق يحميه القانون فيكون الدليل وهذه الحالة مشروعاً ويمكن للمحكمة أن تستند اليه عند اصدار حكمها.

ثانياً- يفيد في تحديد شخصية المشتبه فيه وبدقة عند تسجيل صوته أو مراقبة بريده الالكتروني.

ثالثاً- تحديد نوع الجريمة والجهة المرخص لها اتخاذ الإجراءات القانونية والمدة المسموح فيها تسجيل الصوت[٣].

لقد كشف حكم محكمة القضاء الإداري في مصر الصادر عام ٢٠١١ في قضية قطع الاتصالات خلال أحداث ثورة ٢٥ يناير أن هناك محاولات للمراقبة بدأت وفقاً لأقل التقديرات عام ٢٠٠٨ عندما قامت وزارات الداخلية والاتصالات والإعلام بمشاركة شركات المحمول بإجراء بعض تجارب المراقبة كانت إحداها في ٦ أبريل عام ٢٠٠٨ والأخرى في ١٠ أكتوبر ٢٠١٠ وقد استهدفت التجربتين قطع الاتصالات عن مصر وكيفية حجب بعض المواقع الرقمية، وأسلوب منع الدخول على شبكة الإنترنت "لمدينة أو لمحافظة أو لعدة محافظات" ، وكذلك إبطاء مواقع رقمية محددة، ووضع خطة لسرعة الحصول على بيانات مستخدمي الشبكة عقب استخدامها خلال فترة لا تقل عن ثلاثة أشهر[٤].

الخاتمة

بعد ان انتهينا من موضوع بحثنا، توصلنا إلى إن الزيادة المطردة في اعداد مستخدمي شبكة الانترنت ادت بالنتيجة الى زيادة حجم الجرائم المرتكبة بواسطة هذه الشبكة. كما اننا وجدنا ان القوانين العقابية وقوانين الإجراءات الجنائية التقليدية كانت غير كافية لمواجهة ومكافحة هذه الجرائم بسبب الطبيعة الخاصة لهذا النوع من الجرائم، كما إننا وجدنا إن التحري والضبط والتفتيش بالنسبة لهذه الجرائم ليس بالسهل ويتطلب استخدام وسائل تقنية عالية الجودة.

---

(١) المادة(١٧)اولاً من دستور العراق نصت على: (لكل فردٍ الحق في الخصوصية الشخصية، بما لا يتنافى مع حقوق الآخرين، والآداب العام).

أما الدستور المصري لعام ٢٠١٤ فقد نص في مادته(٥٧) على: للحياة الخاصة حرمة، وهى مصونة لا تمس . وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. تنظيم جمع الأدلة. الاتصالات كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك.

(٢) د. علي محمود علي حمودة، مرجع سابق.

(٣) د. علي حسن الطوالبة، مرجع سابق.

(٤) أيضا أصدرت ذات المحكمة حكماً في عام ٢٠١٠ بصدد مراقبة خدمة رسائل المحمول المجمعة"BULK SMS" ، حيث قضت بوقف تنفيذ قرار الجهاز القومي لتنظيم الاتصالات بإخضاع خدمة الرسائل النصية القصيرة المجمعة للرقابة المسبقة أو اللاحقة، وبحظر تعليق مباشرة الشركات المرخص لها لنشاطها المتعلق بتقديم تلك الخدمة على وجوب الحصول على موافقات مسبقة قبل تقديم الخدمة تقوم على (رقابة محتوى الرسائل) محل الترخيص من أية جهات. نقلاً عن موقع:http://www.madamasr.com

ويحلو لنا في ختام ذلك أن نتقدم بالتوصيات الآتية:
أولاً- ضرورة تدخل المشرع العراقي لسد النقص الحالي من خلال تشريع قانون خاص بجرائم المعلوماتية بما يتلائم وثورة الاتصالات والتقنية الحديثة التي يشهدها العالم. ويكفل في نفس الوقت حماية حرمة الحياة الخاصة لمستخدمي الشبكة العنكبوتية.
ثانياً- نرى من المفيد الاتفاق على مفهوم واحد للجرائم المعلوماتية وبما يساعد على تعزيز التعاون بين دول العالم للقضاء أو الحد من هذه الجرائم على المستوى الدولي.
ثالثاً-ضرورة تطوير الجهاز القضائي من خلال النهوض بقدرات الافراد العاملين في هذا الجهاز ورفده بالتخصصات العلمية والفنية وبما يمكنه من التعامل مع هذا النوع من الجرائم.
رابعاً- لا بد من احاطة البينات والمعلومات بنظام قانوني يمنع أو يحد من اختراقها أو التلاعب فيها أو محوها.