السياسة الجنائية في مواجهة القرصنة المعلوماتية

إعـــداد الطالـبـــة

فائزة سليمان عمر السنوسي

إشـــــراف

الأستاذ الدكتور : موسى مسعود ارحومة

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير
في القانون الجنائي

جامعـة بنغـازي

كلية القانون

يوليو 2020

جامعة بنغازي

كلية القانون

قسم الجنائي

السياسة الجنائية في مواجهة القرصنة المعلوماتية

اعداد

فائزة سليمان عمر السنوسي

نوقشت هذه الرسالة واجيزت بتاريخ:22.07.2020

تحت اشراف

أ. د. موسى مسعود ارحومة

التوقيع:.....

الأستاذ الدكتور: أحمد الصادق الجهاني (ممتحنا داخليا)

التوقيع:.....

الأستاذ الدكتور: .شحاته اسماعيل أحمد (ممتحنا خارجيا)

التوقيع:.....

عميد الكلية

مدير ادارة الدراسات العليا والتدريب بالجامعة

بِسْمِ اللهِ الرَّحْمَنِ الرَّحِيمِ

﴿ وَمَنْ يَتَّقِ اللَّهَ يَجْعَلْ لَهُ مَخْرَجًا (2) وَيَرْزُقْهُ مِنْ حَيْثُ لَا يَحْتَسِبُ وَمَنْ يَتَوَكَّلْ عَلَى اللَّهِ فَهُوَ حَسْبُهُ إِنَّ اللَّهَ بَالِغُ أَمْرِهِ قَدْ جَعَلَ اللَّهُ لِكُلِّ شَيْءٍ قَدْرًا (3) ﴾

صَدَقَ اللهُ العَظِيمِ

الآيتان (2،3) من سورة الطلاق

الإهـداء

إلى من رباني على حب العلم وسعى لأنعم بالراحة ولم يبخل بشيء من أجل دفعي إلى طريق المعرفة أطال الله في عمره

(والدي العزيز)

إلى التي غرست في نفسي حب العلم وكانت مصدراً للحب والعطف والحنان والتشجيع طوال حياتي والتي لولا توجيهاتها ووقوفها اللامحدود معي لما كانت هذه الرسالة لتصل إلى هذا المستوى أطال الله في عمرها

(أمي الغالية)

إلى الذي دَلّل الصعاب ، ومهد لي الطريق ، حتى تمكنت من إتمام هذا العمل . . .

وفقه الله ورعاه

(زوجي)

الباحثة

الشكر والتقدير

الحمد والشكر لله وحده الذي منحني بلطفه وعطفه العون والصبر على تحدي الصعوبات التي واجهتني لانجاز هذا العمل المتواضع .

وبداية أدين بوافر الشكر والتقدير إلى الأستاذ الدكتور المشرف (موسى مسعود ارحومة) وذلك لتشجيعه المستمر وتوجيهاته العلمية البناءة في هذه الرسالة سواء بتصويباته المنهجية أو اللغوية حتى تجسدت هذه الرسالة على ارض الواقع في صورتها النهائية .

وعرفاناً وتقديراً لكل من ساعدني في إعداد هذا العمل، كما أتقدم بالشكر لجميع أعضاء هيئة التدريس بقسم القانون الجنائي لما أتاحوا لي من فرص التحصيل العلمي.

وفي الختام أتقدم بخالص الشكر والتقدير لكل من ساهم معي في انجاز هذه الرسالة سواءً بالكلمة الطيبة أو النصيحة .

الباحثة

قائمة المحتويات

الموضـــــوع	رقم الصفحة

رقم الصفحة

الموضـــــوع

الفصل الثاني

ملامح السياسة الجنائية الإجرائية للجريمة المعلوماتية

رقم الصفحة | **الموضـــــوع**

السياسة الجنائية في مواجهة القرصنة المعلوماتية

إعداد

فائزة سليمان عمر السنوسي

المشرف

أ. د. موسى مسعود أرحومة

الملخص

يعتبر الحاسب الآلي وشبكة المعلومات الدولية في يومنا المعاصر من أهم متطلبات الحياة، وتكمن أهمية هذه الدراسة في أن أي اختراع حديث له إيجابياته كما له سلبياته والمتمثلة في سوء استخدام هذه التقنية الحديثة.

وتهدف هذه الدراسة إلى تسليط الضوء على صور القرصنة المعلوماتية وبيان ماهيتها، ومدى إمكانية التصدي لهذه الظاهرة الإجرامية من الناحية الموضوعية والإجرائية.

ولتنفيذ هذه الدراسة تم الاعتماد على المنهج "الوصفي التحليلي"، وتوصلت الدراسة إلى العديد من النتائج أهمها ما يلي:

1. إن صور القرصنة المعلوماتية هي ذات طبيعة خاصة، تتسم بخصائص مميزة لها عن الجرائم التقليدية.
2. هناك فراغاً تشريعياً في مجال الجرائم المعلوماتية، حيث عجزت عدد من التشريعات النافذة في الدول وخاصة العربية منها عن مواجهتها إذ لم تقم بتجريم هذه الاعتداءات الواقعة على النظم المعلوماتية من الأساس مثل ما هو حاصل في دولة ليبيا. أو لم تقم بإدخال تعديلات على تشريعاتها بما يكفل التصدي لها بشكل جيد ومتكامل.
3. استحداث أجهزة خاصة تُكلف بمهمة مكافحة الإجرام المعلوماتي مكونة من عناصر ذات تأهيل عالي في مجال التكنولوجيا المعلوماتية.

هناك العديد من التحديات في جانبها الإجرائي، أهمها في مجال إثبات الجريمة المعلوماتية من حيث صعوبة اكتشافها بسبب طبيعتها المعنوية، مما أدى إلى ظهور ما يُعرف "بالأدلة الرقمية". وكذلك في مجال إجراء التفتيش والضبط الواقع على مكونات الحاسب الآلي المعنوية "المنطقية" وذلك خلافاً للأصل في التفتيش حيث يقع على الأشياء ذات الطبيعة المادية.

المقدمة

إن الحاسب الآلي قد أصبح من المتطلبات الأساسية في حياتنا المعاصرة، فلم يعد اقتناؤه من الأمور الترفيهيَّة للإنسان، بل هو من أهم لوازمه، بحيث لا يستطيع الاستغناء عن خدماته سواء في منزله أو في مكتبه في العمل. [1]

ويُعرف الحاسب الآلي بأنه: "عبارة عن مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة البيانات الداخلة طبقاً للبرنامج الذي تم وضعه مسبقاً للحصول على نتائج معينة".[2]

ومع ظهور عصر الإنترنت "الشبكة المعلوماتية" وذلك كنتيجة للاندماج الحاصل بين تقنيتي الحوسبة والاتصالات، ازدادت أهمية تقنية المعلومات وأصبح العالم قرية صغيرة يتواصل فيه كل الأفراد والمؤسسات المختلفة مع بعضها البعض بكل سهولة ودون أي اعتبار للحدود الجغرافية بين الدول، فقد أحدث التطور العلمي وهذا التقدم الهائل في مجال تقنية المعلومات وتدفُّقها عبر حدود الدول والقارات ثورة إلكترونية تطبق في كافة مجالات الحياة والمرافق الحيوية الهامة مثل: المستشفيات والمطارات والبنوك وغيرها، فأضحى من الصعوبة الاستغناء عن خدماتها وفوائدها العظيمة والمتنامية. [3]

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مجلة دراسات قانونية، كلية القانون، جامعة قاريونس، العدد السابع عشر، اكتوبر 2008، منشورات جامعة قاريونس، ص 80.

(2) هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، د.ط، دار النهضة العربية، القاهرة، 1992م، ص6.

(3) علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، د.ط، المكتب الجامعي الحديث، 2012، ص5.

ثم بعد ذلك ظهر الهاتف المحمول وتم تطويره حتى أصبح بمثابة جهاز حاسوب مصغر، لذا فإن ما يُقال بالنسبة للحاسب الآلي يُقال كذلك بالنسبة للهاتف المحمول، خاصة في ظل الاستخدام الشائع والواسع له في هذه الأيام، إذ أصبح كل شخص – كبيراً أم صغيراً – يستعمله، وليس من الممكن تركه أو الاستغناء عنه، ولذلك كان يجب على كل مشرّع يقوم بسن أو تقنين تشريع خاص بجرائم الإنترنت أو يقوم بتوسيع النصوص التقليدية بتعديلها أو إضافة نصوص جنائية خاصة جديدة للقانون الجنائي المُطبق أو القائم حالياً أن يأخذ في حسبانه هذا الأسلوب من أساليب ارتكاب جرائم الإنترنت، حيث نجد أنه في هذا الأسلوب قد اختلفت فقط وسيلة ارتكاب الجريمة من الحاسب الآلي إلى الهاتف النقال.

ولم يتفق الفقهاء على مصطلح واحد للدلالة على الجرائم المرتبطة بتقنية المعلومات، فظهرت العديد من المصطلحات أهمها: جرائم الحاسوب وجرائم الحاسب الآلي والإنترنت وجرائم أنظمة المعلومات وجرائم التكنولوجيا المعلوماتية والجرائم السيبرانية والجرائم المعلوماتية...الخ. [1]

أولاً: أهمية البحث:

إن لهذا الموضوع أهمية متزايدة سواء من الناحية النظرية أو العلمية، كما أن لكل اختراع أو اكتشاف إيجابيات وسلبيات فمثلاً: الشبكة المعلوماتية تعتبر سلاح ذو حدين لها عدة إيجابيات منها القفزات النوعية التي حققتها والتغيرات الإيجابية الكبيرة التي حدثت بسببها سواء على صعيد الدول أو الأفراد في العديد من المجالات الاقتصادية والسياسية والاجتماعية. [2]

(1) حمزة محمد أبو عيسى، جرائم تقنية المعلومات، ط1، دائرة المكتبة الوطنية، عمان، 2017، ص 7-8.

(2) جمال الدين كرابيج، الجريمة المعلوماتية، الصحيفة القانونية الإلكترونية، سوريا، 2011-2010م، متاح على الرابط "Vie.gov.sy>index.ph" تاريخ الزيارة 2017/01/17م.

إلا أنها لها كذلك سلبياتها والمتمثلة في سوء استخدام هذه التقنية الحديثة بحيث أصبحت المعلومات أو البيانات المخزنة في شبكة الإنترنت أو التي يتم انسيابها عبرها هدفاً للاعتداء عليها سواء باختراق المواقع الإلكترونية الخاصة بالأفراد أو المؤسسات أو بتدمير أو إتلاف البيانات عن طريق بث الفيروسات من قبل الحاقدين والمتطفلين "الهاكرز" أو القيام بأعمال القرصنة المعلوماتية وذلك بالاستيلاء على تلك البيانات أو البرامج بعد اختراق المواقع الإلكترونية وتقليدها أو نسخها...الخ. [1]

ومن خطورة هذه الظاهرة المستحدثة أنها من الممكن ارتكاب الجرائم التقليدية بواسطة الشبكة المعلوماتية أو تسهيل ارتكابها مستغلين الإمكانيات الهائلة لهذا الاختراع، مثل القيام بإرسال رسائل تحتوي على كلمات سب أو قذف للآخرين عبر البريد الإلكتروني "E.mail" أو القيام بالاستيلاء على الأموال أو تحويلها وغيرها.

وكذلك ارتكاب الجرائم المعلوماتية البحتة، بحيث تكون الشبكة المعلوماتية هي موضوع الجريمة أو هدفها وليس مجرد الوسيلة لارتكابها، مثل جرائم إتلاف البيانات عن طريق بث الفيروسات وغيرها من طرق الإتلاف المعلوماتي وجرائم الغش المعلوماتي وبالتالي تم استحداث صور أخرى من الإجرام يرتبط بهذه التقنية المعلوماتية الحديثة المتطورة والتي تكون محلاً لهذه النوعية من الإجرام المستحدث وهو "الإجرام المعلوماتي".

وقد تزايدت معدلات ارتكاب هذا النوع من الإجرام في العقدين الأخيرين على وجه الخصوص، وهذا ما أدى إلى بزوغ فجر هذه الظاهرة الإجرامية وأخذها في الانتشار السريع في كل بقاع العالم، وتكمن خطورتها في سهولة ارتكابها على هذه الأجهزة الإلكترونية أو بواسطتها، فإن

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص81.

عملية تنفيذها لا يستغرق في أكثر الأحيان إلا دقائق معدودة فقط، وغالباً ما يلجأ الجاني عقب ارتكابه للجريمة إلى محو آثار جريمته وإتلاف أدلتها بكل سرعة وسهولة، مما يُصعب من عملية اكتشافها. [1]

ولأن هذه الظاهرة من الظواهر الحديثة والخطيرة في آنٍ واحدٍ وينجم عنها أضرار بالغة ، ونظراً لطبيعتها الخاصة، كان لابد من التصدي لها بكل حزم وشدة للحد من مخاطرها وأضرارها على الفرد والمجتمع، وذلك من خلال تبني جملة من الآليات والتدابير الفعالة على الصعيد الوطني أولاً بسن التشريعات الجزائية الرادعة والتي تكفل توفير الأمن المعلوماتي للوقاية من هذه الجرائم وضمان الحماية الكافية للنظم المعلوماتية وتحد بقدر الإمكان من حالات اقترافها.

وتبعاً لذلك يجب أن تطور المنظومة الإجرائية فيما يخص قواعد الضبط والتفتيش والتحقيق والاختصاص الجنائي وما إلى ذلك من الإجراءات التي يتطلبها تعقب الجناة وملاحقتهم والتحري عنهم بغية تقديمهم للعدالة وإنزال الجزاء المناسب بحقهم.[2]

وكذلك يجب تطوير أجهزة العدالة الجنائية ورفع كفاءتها وقدراتها من أجل القدرة على التصدي للجريمة المعلوماتية، ولأنها تعتبر من ضمن الجرائم العابرة للحدود بل وللقارات فإن مكافحتها أو مواجهتها على الصعيد الوطني فقط أصبحت قاصرة وغير ناجعة ما لم تعززها الجهود الدولية في هذا المجال وذلك من خلال إبرام الاتفاقيات الدولية أو الإقليمية وعقد المؤتمرات الدولية بهذا الخصوص. [3]

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 5.
(2) موسى مسعود أرحومة، السياسة الجنائية في مواجه جرائم الإنترنت، مرجع سابق ذكره، ص 82
(3) ذات المرجع السابق، ص 124.

فضلاً عن ضرورة اللجوء لوسائل التعاون الدولي عند التعامل معها في حالة ارتكاب السلوك المجرم في بلد ما وحدوث أو تحقق النتيجة في بلد آخر، فهذا ما يستلزم التعاون فيما بين الدول في مجالات التفتيش والتحقيق وجمع الأدلة وتسليم المجرمين والإنابة القضائية وتنفيذ الأحكام الأجنبية الصادرة في هذا المضمار، وذلك لأنها من ضمن الجرائم المنظمة عبر الوطنية والتي تعد من أهم وأخطر التحديات التي يواجهها المجتمع الدولي. [1]

ثانياً: نطاق البحث:

يتجه هذا البحث بشكل خاص إلى دراسة عدة نقاط مهمة تتعلق بالجريمة المعلوماتية منها:

أولاً: تسليط الضوء على طائفة من الجرائم ذات طبيعة خاصة وهي جرائم "القرصنة المعلوماتية" وبيان صورها، بالإضافة إلى دراسة خصائص المجرم المعلوماتي والتي تميزه عن غيره من المجرمين.

ثانياً: التركيز على محاولات وجهود مكافحة هذه الطائفة من الجرائم ومواجهتها من حيث الجانب التشريعي "الموضوعي والإجرائي"، فقد تم تسليط الضوء على الجهود التشريعية المبذولة من جانب بعض الدول العربية والغربية في سبيل مواجهة هذا الإجرام المعلوماتي وذلك بعرض بعض النصوص التجريمية التي نصت عليها قوانين هذه الدول في هذا المضمار، وبالتدريج التشريعي لها.

ثالثاً: تطرقنا إلى الجانب الإجرائي للجريمة المعلوماتية وذلك من حيث صعوبة اكتشافها ومدى حجية الدليل الرقمي في الإثبات وكذلك بيان إجراءات التحري وجمع الأدلة وإجراءات التحقيق الابتدائي في الجريمة المعلوماتية.

(1) سناء خليل، الجريمة المنظمة والعبر الوطنية "الجهود الدولية ومشكلات الملاحقة القضائية"، المجلة الجنائية القومية، العدد الثاني، المجلد التاسع والثلاثون، يوليو، 1996م، ص87.

وعلى ضوء ما تقدم سنركز من خلال هذا البحث على دراسة الجانب "الموضوعي والإجرائي للجريمة المعلوماتية" فقط دون "الجانب الدولي" (الاتفاقيات والمؤتمرات الدولية وصور التعاون الدولي)، وذلك تفادياً لطول ودسامة هذه الدراسة أكثر من اللازم.

ثالثاً: إشكالية البحث:

يُثير هذا الموضوع العديد من الإشكاليات والتساؤلات يمكن إيجازها في النقاط التالية:

1. مدى إمكانية التوفيق بين الحق في الاستخدام الحر لشبكة الإنترنت وبين ضمان عدم المساس بالحياة الخاصة وبالحقوق الشخصية للإنسان.
2. مع هذه الطفرة اللامتناهية في مجال تقنية المعلومات وما صاحبها من انعكاسات سلبية متمثلة في سوء استخدام هذه التقنية الحديثة وأمام تطور عقلية المجرم المعلوماتي فأصبح يبتكر أساليب جديدة في ارتكابه لهذا النوع من الإجرام المستحدث، وبالتالي ظهور أنماط وصور جديدة ومعقدة للجريمة المعلوماتية بحيث يكون الحاسب الإلكتروني فيها هو موضوع الجريمة وليس فقط مجرد وسيلة لارتكابها.

وهذا ما جعل الأمر يصطدم مع الواقع التشريعي القاصر للعديد من الدول لاسيما دول العالم الثالث وفي مقدمتها دولة ليبيا، حيث لم يقم المشرّع الليبي حتى وقتنا هذا بمعالجة تشريعية لهذا النوع من الإجرام المستحدث والخطير، وبالتالي تقف مثل هذه الدول عاجزة عن مواجهة هذه الأفعال المتمثلة في سوء استخدام شبكة المعلومات الدولية، خاصةً وأن القواعد والنصوص التقليدية القائمة غير كافية بذاتها لمواجهة هذا النوع من الإجرام ، لأنها قد وضعت في زمن سابق على ظهور هذه التكنولوجيا المتقدمة. فما هو الحل لهذا الفراغ التشريعي؟

3. مدى إمكانية الأجهزة العاملة في مجال مكافحة الجريمة "أجهزة العدالة القضائية" من مواجهة هذا النوع من الإجرام المستحدث ومدى معرفتها لكيفية التعامل مع هذه الطائفة من الجرائم

المعلوماتية، وذلك من حيث تتبعها وإثباتها ، وبالتالي القيام بإجراءات الضبط والتفتيش بشأنها، وهذا ما قد تقف هذه الأجهزة عاجزة عن القيام به على أكمل وجه وذلك بسبب الطبيعة التقنية الخاصة لهذه الظاهرة من الإجرام، فهي تختلف عن طبيعة الجرائم التقليدية مثل "القتل والسرقة...الخ" والتي اعتادت "أجهزة العدالة القضائية" على كيفية التعامل معها.

وكذلك بسبب عدم القيام بإجراء دورات نظرية وتدريبية لهذه الكوادر البشرية في هذا المجال، وذلك لكي يكونوا على علم ودراية بكل جوانب الجريمة المعلوماتية وعلى معرفة تامة بكيفية التعامل معها بعد وقوعها.

4. أثارت ظاهرة الإجرام المعلوماتي العديد من المشكلات في نطاق القانون الجنائي الإجرائي، حيث إن الجرائم التقليدية لا توجد صعوبات كبيرة في إثباتها والتحقيق فيها وجمع الأدلة المتعلقة بها خاصة مع خضوعها لمبدأ حرية القاضي الجنائي في تكوين عقيدته وصولاً للحقيقة الموضوعية بشأن الجريمة والمجرم، في حين أن الجرائم المعلوماتية وهي تتعلق في كثير من الأحيان ببيانات معالجة إلكترونية وكيانات منطقية غير مادية، وهذا ما يُظهر لنا العديد من الإشكاليات والصعوبات، فمثلاً يصعب كشف هذه الجرائم من ناحية، كما يستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة القيام بإجراءات جمع الأدلة والتحقيق الابتدائي بشأنها سرعة ودقة تنفيذ هذه الجرائم المعلوماتية مع إمكانية محو آثارها بسرعة فائقة وإخفاء الأدلة المتحصلة منها عقب تنفيذها مباشرة. ومن هنا تظهر مشكلة صعوبة الإثبات بشأنها ومدى حجية المخرجات الإلكترونية" الدليل العلمي أو الرقمي" في الإثبات نظراً لطبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية.

فكان لابد من تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية لهذا النوع من الإجرام وذلك لتحقيق الغرض المطلوب منها وهو اقتضاء حق الدولة في العقاب

من الجاني، بكشف الجريمة، والتوصل إلى مرتكبيها والتحقيق معهم وجمع الأدلة بشأن الجريمة المعلوماتية وتقديمهم للمحاكمة العادلة.

رابعاً: منهج البحث:

قد اعتمدنا في دراسة هذا الموضوع منهجاً يتماشى وطبيعته وهو المنهج "الوصفي التحليلي".

- **الوصفي:** لأن هذه الدراسة اعتمدت على وصف صور وأشكال هذه الظاهرة من الإجرام المستحدث ووصف شخصية وخصائص مرتكبيها وهو ما يُطلق عليه مصطلح "المجرم المعلوماتي".
- **وتحليلي:** لأن هذه الدراسة قد تناولت بعض النصوص التجريمية ذات العلاقة بالموضوع في بعض التشريعات العربية والغربية بالتحليل بغية معرفة الشروط والأركان الواجب توافرها في الاعتداء المعلوماتي المجرم لقيام الجريمة المعلوماتية وبالتالي استحقاق العقاب.

فهذا المنهج الوصفي التحليلي يسعى إلى وصف وتحليل وتشخيص موضوع البحث أو الدراسة من مختلف جوانبه وأبعاده، بهدف التوصل إلى نظرة واضحة عن الآليات الملائمة لمكافحة ومواجهة هذه الظاهرة الإجرامية الخطيرة.

خامساً: خطة البحث:

تتضمن خطة الدراسة تناول موضوع السياسة الجنائية في مواجهة القرصنة المعلوماتية وذلك من خلال فصلين:

الفصل الأول: يتناول ملامح السياسة الجنائية الموضوعية للجريمة المعلوماتية.

والفصل الثاني: يتناول ملامح السياسة الجنائية الإجرائية للجريمة المعلوماتية.

الفصل الأول
ملامح السياسة الجنائية الموضوعية
للجريمة المعلوماتية

الفصل الأول

ملامح السياسة الجنائية الموضوعية للجريمة المعلوماتية

تمهيد وتقسيم:

إن التطور الذي شهدته تكنولوجيا المعلومات وما أفرزته من آثار في مختلف جوانب الحياة الاقتصادية والسياسية والاجتماعية أظهر الحاجة المُلحة والملموسة لمواكبة تشريعية حمائية لما أفرزته هذه الثورة التقنية من قيم مستحدثة لم تكن متصورة فيما مضى، ولمكافحة أنماط الإجرام المعلوماتي والذي تمرد على حدود الزمان والمكان، بات المشتغلين في حقل القانون من مشرعين وفقهاء وقُضاة أمام تحدٍ كبير يتطلب منهم ضرورة استيعاب لإفرازات أو مخرجات هذا الانفجار التكنولوجي المعلوماتي وذلك من خلال اتباع سياسة تشريعية موضوعية لا يقل الجانب الحمائي فيها أهمية عن الجانب العقابي.[1]

ومن هنا كان من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في جرائم المعلوماتية المختلفة والتي تأتي في مقدمتها الدخول غير المشروع على شبكات الحاسبات والتحايل على نظم المعالجة الآلية للبيانات وإتلاف البرامج والمعلومات واعداد ونشر برامج فيروسات الحاسب الآلي ...الخ.

(1) طاهر جمال الدين كرابيج، بحث "الجريمة المعلوماتية" 2010-2011 ، متاح على الرابط vle.gov.sy>indexphp ، تاريخ الزيارة : 2017/01/28م

غير إن هذه المواجهة تظل قاصرة حتى الآن وكأن الجرائم المعلوماتية مارداً جباراً خرج من القمقم تستعصي عليه أية مواجهة تشريعية، أو بعبارة أخرى المواجهة التشريعية تسير بسرعة السلحفاة في مواجهة الجرائم المعلوماتية التي بدورها تنطلق كالصاروخ بسرعة الضوء.[1]

ومن المؤسف أن المشرّع الليبي لم يستجيب بعد للتطور التكنولوجي وما قد يحدث من اعتداءات على النظم المعلوماتية، فيجب إذاً أن يشمل بالحماية الجنائية هذه الأموال والنظم المعلوماتية، لأن النصوص الجنائية التقليدية غير ملائمة للتطبيق أحياناً على جرائم الحاسب الآلي، أو أن عقوبتها غير مناسبة للفعل المرتكب.

وبالتالي نلاحظ وجود نقص تشريعي في هذ المجال وندعو المشرّع الليبي إلى سد هذا النقص التشريعي.

ولذا فإنه من المفيد أن نتطرق في هذا الفصل إلى صور القرصنة المعلوماتية وذلك في المبحث الأول، ومن ثم نقف على الوضع القانوني للجريمة المعلوماتية والسياسية التشريعية التي انتهجتها التشريعات المختلفة العربية منها والغربية للتصدي لهذه الجرائم، فقد استجابت العديد من التشريعات لمتطلبات الثورة التكنولوجية، وقامت بإصدار قوانين ستكون هي المنصة التي ننطلق منها في تناول بعض صور القرصنة المعلوماتية بحيث تكفل قدر الإمكان حماية الأنظمة المعلوماتية ومكوناتها وخاصة البرمجية منها من ناحية، والحد من الجرائم الواقعة عليها أو بواسطتها من ناحية أخرى، وهذا ما سنوضحه في عرض تدريجي لبعض التجارب التشريعية التي قامت بها بعض الدول العربية والغربية في هذا الصدد وذلك من خلال المبحث الثاني من هذا الفصل.

(1) ماهية الجريمة الالكترونية، قسم أرشيف منتديات الجامعة، متاح على الرابط www.djelfo>showthread، تاريخ الزيارة 2017/02/02م.

المبحث الأول

صور القرصنة المعلوماتية والمجرم المعلوماتي

تمهيد وتقسيم:

لاشك في أن الجرائم المعلوماتية بصفة عامة هي كثيرة ومتنوعة ولا يمكن حصرها، فتكنولوجيا الحاسبات الآلية متطورة ومتغيرة وهذا ما يؤثر بدره على الجريمة المعلوماتية، ويظهر ذلك بصفة خاصة في هذه الطائفة من الجرائم لارتباطها الوثيق بهذه التكنولوجيا المتقدمة.[1]

إلا أن نطاق هذا البحث لا يتسع للتعرض لكافة أنواع أو صور الجرائم المعلوماتية، ولذا سوف يكون تعرضنا بالدراسة لأهم الجرائم المحتمل وقوعها في نطاق المعاملات الإلكترونية، وهي التي تُكون مكونات الحاسب الآلي المعلوماتية" المكونات المعنوية" مثل البرامج المستخدمة والبيانات والمعطيات المخزنة في ذاكرة الحاسب الآلي هي محلاً أو موضوعاً للجريمة المعلوماتية.

حيث من المتصور عملياً أن يقوم أحد الأشخاص بالاعتداء على برنامج معلوماتي في الحاسب الآلي أو أن يدعي ملكيته أو يقوم بسرقته أو تقليده أو إتلافه بشتى طرق الإتلاف المعلوماتي، أما البيانات فيستطيع العبث بها عن طريق "تحريفها أو تزويرها أو نسخها".[2]

وكل هذه الأنشطة أو الأفعال هي ما يُطلق عليها مصطلح "القرصنة المعلوماتية"، والجدير بالذكر في هذا المضمار أن معظم صور الجرائم المعلوماتية لا يمكن أن ترتكب دون الدخول إلى النظام المعلوماتي ابتداءً، ففعل الدخول غير المصرح به، فعلى سبيل المثال من أراد أن يتلف أو

(1) نسرين عبدالحميد نبيه، الإجرام المعلوماتي، د. ط.، منشأة المعارف، الإسكندرية، 2007م، ص 139.
(2) فتوح الشاذلي – عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف و د. ط. ، د. ت.، ص 23.

يسرق برنامجاً معيناً في أي نظام معلوماتي، لابد له من اختراق هذا النظام أولاً ومن ثم القيام بفعل الإتلاف أو السرقة، وعليه فإن الاختراق يُعتبر أول مرحلة لارتكاب أغلب الجرائم المعلوماتية.[1]

وكما أن الجرائم المعلوماتية هي ظاهرة إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها ، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع على المستويات الاقتصادية والاجتماعية والثقافية والأمنية.[2]

فلا شك أن مستخدمي الشبكة المعلوماتية في ارتكاب جرائمهم قد تجاوزوا الطرق التقليدية لما تتطلبه هذه الجرائم من ثقافة وخبرة تكنولوجية ومعلوماتية هائلة وهو أمر يقتضي التعرف على خصائص هؤلاء المجرمين وطبيعة جرائمهم.[3]

ومن هذا المنطلق سيتم تقسيم هذا المبحث إلى مطلبين:-

نتناول في المطلب الأول: صور القرصنة المعلوماتية.

وفـــــي المطلب الثاني: المجرم المعلوماتي.

(1) حمزة محمد أو عيسى، مرجع سابق ذكره، ص 27.
(2) خالد ممدوح إبراهيم، أمن الحكومة الإلكترونية، د. ط. ، الدار الجامعية ، الإسكندرية، 2010م ، ص 149.
(3) علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، د. ط. ، دار اليازوري العلمية للنشر والتوزيع، الأردن – عمان، 2009م، ص48.

المطلب الأول

صور القرصنة المعلوماتية

سنتناول صور القرصنة المعلوماتية في هذا المطلب في أربعة فروع وذلك على التقسيم الآتي:

الفرع الأول

الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات "النظام المعلوماتي"

يُعرف الدخول غير المشروع أو الاختراق أو الانتهاك للنظام المعلوماتي بأنه "الولوج غير المصرح به أو بشكل غير مشروع إلى نظام معالجة آلية للبيانات باستخدام الحاسوب ويتحقق الدخول غير المشروع إلى النظام المعلوماتي بالوصول إلى المعلومات والبيانات المخزنة داخل النظام المعلوماتي ودون رضا أو قبول من المسؤول عن هذا النظام أو المعلومات التي يحتوي عليها". [1]

وفي تعريف آخر بأنه "إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات المخزنة بداخله للاطلاع عليها أو لمجرد التسلية أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي على الرغم من الاحتياطات التقنية التي يحتوي عليها نظامه".[2]

كما يُعرف الدخول غير المشروع أو الاختراق للنظام المعلوماتي بأنه: "هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الآخرين وشبكاتهم الإلكترونية تتم من خلال برامج متطورة

(1) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 152.
(2) أيمن عبدالله فكري، جرائم نظم المعلومات، رسالة مقدمة لاستكمال الحصول على درجة الدكتوراه، جامعة المنصورة، د.ط. 2005-2006م، ص 164-165.

متوفرة على الإنترنت، وبواسطة أشخاص غير مصرح لهم بالدخول إليها وقد أطلق على هؤلاء مصطلح القراصنة "Hackers" فيقومون بتوجيه هجمات إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى والتكاملية أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالهم".[1]

أولاً: المقصود بفعل الدخول للنظام المعلوماتي:

إن معنى الدخول ينصرف في إطار المعلوماتية ليشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة أو السيطرة على البيانات التي يتكون منها أو الخدمات التي يقدمها، والدخول لا يقصد به المعنى المادي لهذا المصطلح كالدخول إلى مكان أو منزل أو حديقة، إنما يجب أن يُنظر إليه كظاهرة معنوية أي دخول منطقي أو برامجي معلوماتي يُشبه فكرة الدخول لملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات.[2]

وليس هناك وسيلة للدخول أو طريقة لكي يتم الدخول بها إلى النظام المعلوماتي، فقد يلجأ الفاعل إلى التلاعب بعناصر النظام المادية لكي يصل إلى هدفه وهو الدخول فيقوم بإجراء الاتصال بالنظام محل الحماية باستخدام طرق فنية متعددة كاستخدام كارت ممغنط أو اتصال تليفوني أو باستخدام الرقم الكودي أو أرقام سرية تسمح بهذا الدخول، أو أن يربطه بجهاز تنصت يستطيع من خلاله اختراق النظام أو استقبال المعلومات، أو عن طريق تجاوز نظام الحماية خاصةً إذا كان ضعيفاً وفي حالة وجود مثل هذا النظام يستوي أن يتم الدخول مباشرةً أم بطريقة غير

(1) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 151-152.
(2) أيمن فكري، مرجع سابق ذكره، ص 165.

مباشرة، كما هو الحال في الدخول عن بُعد وذلك عن طريق شبكات الاتصال التليفونية أو الطرفيات سواء كانت محلية أو عالمية.[1]

ويقع فعل الدخول من كل إنسان أياً كانت صفته، سواء كان يعمل في مجال الأنظمة المعلوماتية أم لا يعمل بها، وسواء كان يستطيع أن يستفيد من الدخول أم لا"، وسواء تم الدخول إلى النظام كله أو إلى جزء منه فقط.[2]

ويتم فعل الدخول غير المشروع للنظم المعلوماتية عندما يقوم الشخص باختراق الشبكات والحواسيب الإلكترونية التي ترتبط بشبكة الإنترنت وذلك باختراق نظام الأمن المعلوماتي في الشبكة المعلوماتية والدخول إلى الجهاز والكشف عن محتوياته لأي غرض كان.[3]

بالإضافة إلى أن الولوج أو الدخول غير المشروع للنظم المعلوماتية يضم الاختراق الذي يحدث للنظام بأكمله أو لجزء منه.

ويضم أيضاً الاختراق الذي يحدث لنظام معلوماتي متصل بشبكات اتصال عامة، أو لنظام معلوماتي متصل بنفس الشبكة، أي شبكة محلية أو إنترنت، وسواء كانت طريقة الاتصال عن بُعد بما في ذلك الاتصال اللاسلكي، أم كانت على نطاق قريب.[4]

فيكفي أن يكون الفاعل ليس ممن يكون لهم الحق في الدخول إلى النظام المعلوماتي، أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، فيتحقق الدخول غير المشروع للنظام

(1) عبدالفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، د. ط. ، 2009م، ص 355 – 356.
(2) علي عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، د. ط.، الدار الجامعية للطباعة والنشر، الإسكندرية، 1999م، ص 131.
(3) محمود أحمد القرعان، الجرائم الالكترونية، ط1، دار وائل للنشر والتوزيع، الأردن، عمان، 2017، ص 42.
(4) هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2003م، ص 72.

المعلوماتي متى كان هذا الدخول مخالفاً لإدارة صاحب النظام أو من له حق السيطرة عليه، مثل تلك الأنظمة التي تتعلق بأسرار الدولة أو دفاعاتها، أو سر المهنة أو أسرار الحياة الخاصة.[1]

وخلاصة فكرة الدخول غير المشروع للنظام المعلوماتي ، تُعرف بدلالة المكان بأنها "التسلل إلى داخل النظام المعلوماتي".

أما الدخول من حيث الزمان فأنه يتمثل في تجاوز حدود التصريح أو الترخيص داخل النظام والممنوح لفترة زمنية محددة عن طريق تجاوز هذه الفترة الزمنية.[2]

ونجد بأن أغلب القوانين العربية ومنها القانون المصري والعماني والإماراتي ونأمل أن ينضم قريباً القانون الليبي إليها، قد قامت بتجريم الدخول أو البقاء غير المشروع في النظام المعلوماتي سواء في صورته البسيطة "الدخول المجرد" أي دون اشتراط تحقق نتيجة معينة من وراء فعل الدخول غير المشروع إلى النظام المعلوماتي، فمثلاً لا يشترط لقيام هذه الجريمة التقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها أو استعمال تلك المعلومات أو البيانات، بل أن الجريمة تتوافر حتى ولو لم يكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام المعلوماتي.[3]

(1) عبدالفتاح بيومي حجازي، مرجع سابق ذكره، ص 356.
(2) ذات المرجع السابق، ص 362.
(3)علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 132-133.

لـذا فأنـه مـن الحكمـة التشـريعية تجـريم فعـل الاختـراق بحـد ذاتـه، إذ أن السياسـة العقابيـة المعاصرة تتبنى مبدأ منع الجريمة قبل وقوعها، ولكي نمنع الجريمة قبل وقوعها لابد أن نسد الطرق المؤدية إليها.[1]

كما قد يتحقق الدخول أو البقاء غير المشروع في النظام المعلوماتي بصورته المشددة، وهو في حالة إذا ما ترتب أو نتج على فعل الدخول أو البقاء في النظام المعلوماتي محو أو تغيير أو إتلاف أو نسخ في المعطيات الموجودة في النظام المعلوماتي.[2]

ثانياً: المقصود بفعل البقاء داخل النظام المعلوماتي:

يقصـد بفعـل البقـاء داخـل النظـام المعلومـاتي هـو التواجـد داخـل نظـام المعالجـة الآليـة للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.[3]

كما يُعرف فعل البقاء داخل نظام المعالجة الآلية للمعطيات بأنه: " مشاركة ذات سيطرة من المخترق على عمليات الحاسوب – النظام المعلوماتي– خلال حركة الدخول والخروج فالبقاء في نظام المعالجة الآلية للبيانات هو فعل مستقل ذات طابع خاص يختلف عن فعل الاختراق لكون الأخير يمكن أن يخضع لمعدلات حركة الدخول والخروج، فمن يحاول الدخول قد يفشل وقد ينجح إلا إن من يحاول البقاء فهو قد أتم الاختراق فعلاً ثم استقر في النظام المعلوماتي، ولا يشترط فيه إحداث نتائج معينة كإتلاف أو تخريب أو تعديل أو غير ذلك، وإنما مقصود هذا الفعل هو التحكم في نظام المعالجة الآلية للبيانات".[4]

---

(1) حمزة محمد أبو عيسى، مرجع سابق ذكره، ص 28.
(2) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 130.
(3) ذات المرجع السابق، ص 133.
(4) طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني لحماية المعلومات"، د. ط. دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2009، ص 303-304.

ومن واقع الملفات القضائية حادثة المواقع الإستراتيجية، ففي 19 من شهر نوفمبر 1999م تم إدانة "Eric Burns" من قبل محكمة فيرجينيا الغربية بالحبس لمدة 15 شهراً والبقاء تحت المراقبة السلوكية لمدة 3 سنوات بعد أن أقر بذنبه وأنه قام وبشكل متعمد باختراق كمبيوترات محمية ألحق فيه ضرراً بالغاً في كل من ولايات فيرجينيا و واشنطن وإضافة إلى لندن في بريطانيا، وقد تضمن هجومه الاعتداء على مواقع لحلف الأطلسي إضافة إلى الاعتداء على موقع نائب رئيس الولايات المتحدة الأمريكية، كما اعترف بأنه قد أطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق كمبيوترات البيت الأبيض.[1]

وفي حادثة أخرى تمكن أحد الهاكرز "الإسرائيليين" من اختراق أنظمة معلومات حساسة في كل من الولايات المتحدة الأمريكية والكيان الصهيوني، فقد تمكن أحد المبرمجين الإسرائيليين في مطلع عام 1998م من اختراق عشرات النظم لمؤسسات عسكرية ومدنية وتجارية في الولايات المتحدة وإسرائيل.[2]

وأن فعل البقاء داخل النظام المعلوماتي المعاقب عليه في قوانين بعض الدول التي أبدت اهتمامها بموضوع الجريمة المعلوماتية بعكس دولة ليبيا التي لم تهتم حتى وقتنا الحاضر بمعالجة هذا الموضوع ، قد يتحقق مستقلاً عن الدخول إلى النظام ، وقد يجتمعا ويكون فعل البقاء معاقباً عليه استقلالاً حين يكون الدخول إلى النظام مشروعاً، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فوراً فإذا بقى رغم ذلك فإنه يُعاقب على جريمة البقاء غير المشروع إذا توافر لها

(1) يونس عرب، جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10-2002/02/12م، ص 19.
(2) ذات المرجع السابق، ص 19-20.

الركن المعنوي، فهو عبارة عن نشاط إيجابي بطريق الامتناع عن قطع الاتصال مع النظام المعلوماتي.[1]

ويُعتبر البقاء جريمة أيضاً في الحالة التي يستمر فيها الجاني باقياً داخل النظام بعد المدة المحددة له للبقاء داخله أي تجاوز الوقت المسموح به للبقاء داخل النظام فيتخذ صورة الجريمة المستمرة، وفعل البقاء يمكن أن يكون لاحقاً على دخول غير مشروع، ويمكن أن يكون لاحقاً على دخول مشروع إذا تجاوز الوقت المسموح به أو الغرض الأساسي لهذا الدخول. [2]

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معاً وذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام ويدخل إليه فعلاً ضد إرادة من له حق السيطرة عليه ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الغرض الاجتماع المادي للجرائم بين الجريمتين. [3]

فقد ذهبت محكمة استئناف باريس في حكمها الصادر في 15 أبريل 1994م إلى أن القانون يجرم البقاء غير المشروع داخل نظام الحاسب الآلي سواء أكان الدخول تم عن طريق الخطأ أم بطريقة مشروعة إلا أنه اكتسب بعد ذلك صفة عدم المشروعية كما لو فقد الفاعل حقه بالبقاء نتيجة لخطأ من جانبه.[4]

ولكن تثور في هذا الفرض مشكلة متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؟

ذهب رأي في الفقه إلى أن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها إلى البرنامج وإن كان الدخول في نظر هذا الرأي يفترض بالضرورة البقاء فترة قصيرة من الزمن تنتهي عندها جريمة الدخول وتكتمل وبعد تلك اللحظة تبدأ جريمة البقاء داخل النظام وتنتهي بانتهاء حالة

(1) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 133.
(2) أيمن عبدالله فكري، مرجع سابق ذكره، ص 177.
(3) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 133-134.
(4) أيمن عبدالله فكري، مرجع سابق ذكره، ص 178.

البقاء، ويُؤخذ على هذا الرأي أنه لا يحدد لحظة بداية جريمة البقاء بطريقة حاسمة ، ولهذا ذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه المتدخل أن بقاءه داخل النظام غير مشروع، كما أخذ على هذا الرأي أيضاً صعوبة إثبات علم المتدخل. [1]

ولذلك ذهب رأي ثالث إلى أن جريمة البقاء داخل النظام المعلوماتي تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع ، فإذا لم ينسحب يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام. وهذا الرأي وإن كان له وجاهته إلا أنه يفترض وجود جهاز إنذار يقوم بهذه المهمة، وهو إن أمكن توفيره فنياً فإنه لن يكون متاحاً إلا بالنسبة للشركات أو المؤسسات الكبيرة فقط، ولذا ظهر رأي آخر يرى بان الحل الأفضل في مثل هذه الظروف هو الذي يعتبر أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام؛ ويستمر في التجول داخله بعد انتهاء الوقت المحدد، لأن الفرض يتعلق بدخول غير مشروع أي مع علم الجاني أنه ليس له حق الدخول، فإذا دخل وظل ساكناً تظل الجريمة جريمة دخول إلى النظام أما إذا بدأ في التجول فإن جريمة البقاء داخل النظام تبدأ منذ تلك اللحظة وهو يعلم مسبقاً أن مبدأ دخوله فيه غير مشروع، ويكفي لتحقيق الجريمة البقاء داخل النظام كله أو في جزء منه[2]، وأعتقد بأن هذا الرأي هو الرأي الأصوب من بين هذه الآراء.

ونلاحظ بأنه يكفي مجرد البقاء داخل النظام بالمعنى السابق بيانه لقيام هذه الجريمة، دون اشتراط أن يُضاف إليه ضرورة التقاط معلومات أو أي شكل من أشكال الضرر، فهي تعد من الجرائم الشكلية دون اشتراط تحقق نتيجة.[3]

(1) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 134.
(2) ذات المرجع السابق، ص 134-135
(3) حمزة محمد أبوعيسى، مرجع سابق ذكره ، ص 38.

وإذا كانت تلك الجريمة على هذه الصورة تهدف أساساً إلى حماية نظام المعالجة الآلية للبيانات أو المعطيات بصورة مباشرة، إلا أنها تحقق أيضاً وبصورة غير مباشرة حماية للمعطيات أو المعلومات ذاتها. بل ويمكن من خلالها تجريم سرقة وقت الماكينة "الحاسب الإلكتروني" وذلك بالنسبة للموظف أو العامل حيث يسرق وقت الماكينة ضد إرادة من له حق السيطرة على النظام، ويقوم بطبع أو نسخ بعض المعلومات أو البرامج كما يمكن أن تطبق كذلك على الاستخدام غير المشروع للكارت الممغنط إما بسرقته أو تزويره ثم استخدامه أو حتى إذا استخدمه صاحبه في سحب مبالغ دون أن يكون لديه رصيد كافٍ، وتكون الجريمة في هذه الحالة هي جريمة البقاء غير المشروع داخل النظام بشرط أن يكون صاحب الكارت يعلم مقدماً بأنه ليس له رصيد أو ليس له رصيد كافٍ، كما يمكن تطبيقها على التصنت على المحادثات التليفونية طالما أن أرقام التليفونات معالجة آلياً في نظام خاص بها.[1]

ثالثاً: طبيعة جريمة الدخول أو البقاء داخل النظام المعلوماتي:

هي من ضمن جرائم السلوك المجرد أي أنها تقع وتكتمل أركانها بمجرد الانتهاء من السلوك المكون لها وهو الدخول أو البقاء داخل النظام المعلوماتي دون أن يتطلب المشرّع في نموذجها القانوني حسب نصوص التجريم أية نتيجة إجرامية. وإذا كان الاتجاه الغالب في الفقه يعتبر جريمة الدخول أو جريمة البقاء ذات سلوك مجرد، إلا أن الفقه لم يتفق على كون هذه الجريمة وقتية أم مستمرة أم متتابعة الأفعال.[2]

(1) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 133-134.
(2) ذات المرجع السابق، ص 136.

فقد ذهب رأي في الفقه إلى اعتبار أن كُلاً من جريمة الدخول وجريمة البقاء جريمة مستمرة أي أن النشاط فيها يتطلب بطبيعته الاستمرار، فتستلزم نشاطاً متجدداً من قبل الجاني، بعكس الجريمة الوقتية التي يبدأ فيها النشاط وينتهي عادةً في الحال.[1]

بينما ذهب رأي آخر إلى اعتبار جريمة الدخول للنظام المعلوماتي هي جريمة متتابعة الأفعال بينما جريمة البقاء هي جريمة مستمرة ويقصد بالجريمة المتتابعة الأفعال هي الجريمة التي تتكون من عدة أفعال، كل فعل منها يُعتبر جريمة في ذاته، إلا أنه يجمع بينها وحدة المشروع الإجرامي "الغرض الإجرامي" وخرق نفس النص القانوني ولذا اعتبرها القانون جريمة واحدة.[2]

كما ذهب رأي ثالث في الفقه – واتفق مع هذا الرأي – إلى أن جريمة الدخول هي جريمة وقتية ذات أثر ممتد، فالجاني يكون فيها قد استنفذ نشاطه الإجرامي ولكن الأثر المترتب عليها يظل باقياً ومستمراً دونما الحاجة إلى تدخل جديد من قبل الجاني. بينما جريمة البقاء هي جريمة مستمرة وهذا ما أتفق عليه الفقه. ولعل أهمية التفرقة بين أنواع الجرائم السابقة تتعلق بمرور الزمن "التقادم" والاختصاص المكاني والعفو.[3]

(1) موسى مسعود ارحومه، الأحكام العامة لقانون العقوبات الليبي، الجزء الأول، النظرية العامة للجريمة، ط1، 2005م، ص 163.
(2) محمد رمضان باره، شرح القانون الجنائي الليبي، الأحكام العامة، الجريمة والجزاء، الجزء الأول، الجريمة، ط3، 2000م، ص172.
(3) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 136.

الفرع الثاني

إتلاف برامج ومعلومات الحاسب الإلكتروني

أولاً: ماهية الإتلاف المعلوماتي:

يعرف الإتلاف في قانون العقوبات الليبي بأنه : "هو إفناء مادة الشيء ، أو على الأقل إدخال تغييرات شاملة عليها، بحيث تعتبر غير صالحة إطلاقاً للاستعمال في الغرض الذي من شأنه يستعمل فيه الشيء، فتقل تبعاً لذلك قيمته بالنسبة إلى مالكه".[1]

عرف جانب من الفقه الإتلاف المعلوماتي باعتباره المعنِي الأول والأخير بوضع التعريف للشيء وليس من جوهر عمل المشرعين القانونيين ، بأنه : ..." الفعل المادي الذي يتمثل في التأثير على مادة الشيء على نحو يُذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له".[2]

كما عرفه جانب آخر من الفقه بأنه: ..."إتلاف أو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسب الآلي أياً كان شكلها سواء استيلاء على أموال أو اطلاع على معلومات ولكن إلى إحداث الضرر بالنظام المعلوماتي وإعاقته عن أداء وظيفته.[3]

---

(1) رحاب علي عميش، الجرائم المرتكبة بواسطة الحاسب الآلي ، المشكلات التي تثيرها جرائم الحاسب الآلي في النظرية العامة لقانون العقوبات الليبي"، رسالة دكتوراه، جامعة قاريونس، 2006-2007م، ص 150.

(2) أيمن عبدالحفيظ عبدالحميد سليمان، إستراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي "دراسة مقارنة"، رسالة مقدمة للحصول على درجة الدكتوراه في علوم الشرطة، 2003م، ص 5.

(3) أيمن عبدالله فكري، مرجع سابق ذكره، ص 112.

ويُطلقون على هذا التعريف مصطلح أو تعبير "تدمير النظم المعلوماتية". كما ويُعرف الإتلاف المعلوماتي بأنه هو محو المعلومات كلياً وتدميرها إلكترونياً، أو القيام بتشويه المعلومة أو البرنامج على نحو فيه إتلاف بها ومن ثم يجعلها غير صالحة للاستعمال.[1]

وقد أدى التطور التكنولوجي وتقدير عنصر الوقت والجهد إلى جعل هذه الأجهزة للحاسب الآلي تحتوي على قدر كبير من المعلومات ذات الأهمية والسرية فباتت تُشكل في أيامنا هذه قيمة اقتصادية كبيرة فهي سلعة تباع وتشترى، فالمعلومات هي المحور الأساسي الذي تدور حوله المعلوماتية التي تمثل المعالجة الآلية للبيانات والمعلومات.[2]

ونظراً لما لهذه المعلومات من قيمة اقتصادية كبيرة وكسلعة تباع وتشرى وكمعطيات يمكن تبادلها بين الجهات وأن لها قيمة مالية قابلة للاستثثار والانتشار، بل وباعتبارها أساس عمل النظام المعلوماتي فينتج عن ذلك أن تكون هدفاً للجرائم المعلوماتية من ناحية التلاعب بها أو إتلافها.[3]

ثانياً: صور الإتلاف:

إن المعلومات التي يختزنها النظام المعلوماتي تمثل هدفاً أساسياً بالنسبة للجناة الذين يُحاولون الاستيلاء عليها بشتى الطرق والوسائل فتتخذ جرائم الإتلاف المعلوماتي صوراً عديدة سواء أكان الحاسب الآلي ذاته محلاً لارتكاب الجريمة أم كانت المعلومات هي هدف الجاني، ولذلك سيتم البحث في صور ارتكاب تلك الجريمة من خلال ما يلي:

1. الإتلاف المادي:

وتتحقق هذه الصورة من الإتلاف عندما يكون الحاسب الآلي محلاً لارتكاب الجريمة كما في حالة قيام الجاني بإتلاف الجهاز أو أحد ملحقاته دون المساس بالمعلومات داخل الجهاز

(1) حمزة محمد أبو عيسى، مرجع سابق ذكره، ص 65-66.
(2) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص5.
(3) أحمد خليفة الملط، الجرائم المعلوماتية "دراسة مقارنة" د. ط. ، جامعة الإسكندرية، 2005م، ص 123 – 209.

وبالتبعية قد تتلف المعلومات، ولكن الجريمة هنا تكون واقعة على الجهاز في حد ذاته أو أحد ملحقاته وهذا ما يتحقق حتى قبل تشغيل الجهاز.[1]

وسائل الإتلاف المادي:

لا يتطلب إتلاف الأجهزة أشخاص خبراء في مجال الحاسب الآلي ، فقد تقع الجريمة من أي من الأشخاص العاديين دون تطلب معرفة فنية على الإطلاق، بل باستخدام الوسائل العادية، وذلك عن طريق ضرب وحدات تشغيل المعلومات بأدوات ثقيلة أو حادة أو إغراقه بالزيت أو الماء أو إشعال الحريق بها أو تفجيرها بشحنات ناسفة أو العبث بمفاتيح التشغيل أو بمحو بطاقة التعريف بما فيها المعلومات المختزنة أو بمسح البرنامج أو إخفاء بعض البطاقات، وكذلك يمكن إفساد المعلومات المُخزنة مغناطيسياً بإخضاعها لقوى مغناطيسية مُتلفة.[2]

وقد يصل الأمر إلى تطلب معرفة الجاني ببعض الجوانب الفنية "معرفة بسيطة" دون اشتراط كونه محترفاً في مجال المعلومات، حيث يأتي ببعض الأساليب التي تؤدي إلى تحقق فعل الإتلاف عن طريق ما يلي:

1. لصق ورقة صنفرة على بعض أجزاء من البطاقات المثقبة لتخريب الأجهزة القارئة لها.
2. إدخال قطع أو اسطوانات ورق في فتحات أجهزة الحاسب الآلي لتعطيله.
3. إدخال غازات تُسبب تآكل في الأسلاك والأجهزة.
4. استخدام القوى المغناطيسية لمحو محتويات الأشرطة والاسطوانات الممغنطة.[3]

مع ملاحظة أن كل هذه الصور والأشكال المتعددة والتي تؤثر على ماديات النظام المعلوماتي بتعطيلها أو إيقافها عن العمل هي تخرج عن نطاق بحثنا ، حيث يقتصر فقط على

(1) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 6.
(2) جميل عبدالباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية للنشر، القاهرة، 1992م، ص26.
(3) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 6.

الطرق التقنية في الإتلاف الواقع على البيانات والمعلومات والبرامج المخزنة داخل الحاسب الإلكتروني.

2. الإتلاف المعنوي:

وهو ما يطلق عليه مصطلح الإتلاف المعلوماتي وتتحقق هذه الصورة من الإتلاف عندما تكون البيانات والمعلومات محلاً لارتكاب الجريمة، أي هي الهدف من وراء الاعتداء على النظام المعلوماتي ، وفي هذا الشأن لابد أن يكون الجاني متخصصاً في مجال المعلومات، ويتمتع بقدر كبير من المعرفة الفنية، فلا يحتاج إلى القيام بسلوك عنيف أو عدواني فهذا الاعتداء المعلوماتي يُرتكب فقط بواسطة استعمال تقنيات التدمير الناعمة والتي تتمثل في التلاعب بالمعلومات أو البيانات أو إتلافها.[1]

ويتخذ الإتلاف المعلوماتي عدة صور منها ما ينصب على إعداد البرامج، فيتم إتلاف المعلومات عن طريق التلاعب في البرامج في مرحلة المعالجة عن طريق محو أو إزالة أو تعديل البيانات التي تحويها البرامج مما يؤدي إلى تعطيل تشغيل النظام، والتعطيل هو إتلاف جزئي يؤدي إلى إعاقة نظام المعالجة الآلية للبيانات عن بلوغ غايته.[2]

ومن صور أو أشكال الإتلاف المعلوماتي:

أ. الاعتداء على البرامج المعلوماتية بما يؤدي إلى إعاقة وتعطيل النظام المعلوماتي عن العمل:

إن إعاقة سير عمل النظام المعلوماتي هو فعل يتسبب في تباطؤ أو ارتباك عمل نظام المعالجة الآلية للمعلومات، ويترتب على ذلك تغير في حالة عمل النظام ويُساوي البعض بين عرقلة النظام عن العمل ومحو أو تعديل أو إلغاء المعلومات، في حين إنه لكي تتحقق تلك النتيجة

(1) فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق ذكره، ص 33.
(2) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 15-16

فيجب أن يكون الإتلاف المعلوماتي موجه لبرامج تشغيل النظام المعلوماتي التي تقوم بوظائف عمل النظام وليس المعلومات بالمعنى الضيق، وذلك كبرامج تشغيل النظام أو البرامج التطبيقية التي يستند إليها النظام المعلوماتي في القيام بعمله على الأنواع الأخرى من المعلومات.[1]

ويستوي أن يكون التعطيل أو التوقيف دائماً أو مؤقتاً ، فقد يؤدي إلى توقف دائم للنظام كما في حالة إدخال فيروس تدميري، وقد يكون التوقف مؤقتاً أو متقطعاً على فترات منتظمة، كما إذا تم إدخال قنبلة معلوماتية زمنية مبرمجة ينجم عنها شلل للنظام عند البدء في تشغيله مثلاً أو عند استخدام أحد برامج التطبيق.[2]

كما أن الإتلاف المعلوماتي يؤثر في تلك الحالة بالضرورة على المعلومات المرتبطة بهذا البرنامج، والتي يتم الاعتماد عليها في تشغيله سواء بتخزينها أو التعديل فيها أو نقلها أو غير ذلك من وظائف البرامج مع المعلومات التي يتعامل عليها النظام المعلوماتي سواء كانت مالية أو تجارية أو اقتصادية أو شخصية.[3]

ب. استبدال المعلومات

إن استبدال المعلومات من الأمور السهلة في جرائم إتلاف المعلومات، كاستبدال رقم بآخر أو إحلال رقم محل آخر وهو نوع من جرائم التزوير على درجة كبيرة من الخطورة لأنه في حالة نجاحه يستمر فترة طويلة ويستولي على مكاسب كبيرة.[4]

فهناك مجموعة من المستخدمين الإداريين استطاعوا تقاضي ساعات إضافية لم يتم تنفيذها على الإطلاق وذلك عن طريق استبدال قوائم الحسابات بساعات عمل.[5]

(1) أيمن عبدالله فكري، مرجع سابق ذكره، ص 122.
(2) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 140.
(3) أيمن عبدالله فكري، مرجع سابق ذكره، ص 122-124.
(4) أحمد خليفة الملط، مرجع سابق ذكره، ص 213-214.
(5) فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق ذكره، ص 27.

وهناك قضية شهيرة في إسرائيل تتلخص وقائعها في قيام شخص يُدعى " Vladimir Lorilditt" وهو مُهاجر روسي يعمل بوزارة المالية بإدخال فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي اصطنعها، فيمكن للمسؤولين عن حفظ المعلومات أن يتلفوا المعلومات المكلفين بحفظها داخل النظام المعلوماتي وتشكل هذه العمليات عنصراً هاماً من عناصر جرائم التزوير في مجال المعلومات.[1]

وفي الواقع أنه بإمكان أي شخص يشغل منصباً على قدر من الأهمية في مركز المعلومات بالمنشآت والبنوك ولديه الكفاءة الفنية في استخدام النظام المعلوماتي أن يحصل على كل ما يريده من معلومات ويطوعها إلى مصلحته الخاصة.[2]

ج. العدوان على المعلومات المخزنة بالنظام المعلوماتي:

في هذه الصورة من صور الإتلاف المعلوماتي يتحقق بتدمير وإتلاف وتخريب المعلومات المخزنة داخل النظام المعلوماتي بحيث يصبح بلا معنى ولا يمكن الاستفادة منها أياً كان نوعها دون أن يترتب على هذا الفعل إلحاق ضرر بالنظام المعلوماتي أو برامجه، حيث يستمران في العمل بنفس الكفاءة التي كانت قبل وقوع الإتلاف المعلوماتي على المعلومات والبيانات.[3]

ونكون هنا بصدد إتلاف البرامج والمعلومات بمعناها الفكري أي المحتوي ذاته المسجل على دعامة ما أياً كان نوعها، وهذا الإتلاف قد يكون بمحو المعلومات كلياً وتدميرها إلكترونياً، أو بتشويه المعلومة أو البرنامج على نحو فيه إتلاف بها يجعلها غير صالحة للاستعمال.[4]

وتشمل جريمة تدمير وإتلاف البيانات عمليات اختراق للحاسوب بهدف تدمير البرامج والبيانات الموجودة في الملفات المخزنة في الحاسوب، وتُعد هذه الجريمة من أخطر جرائم

(1) عبدالفتاح بيومي حجازي، مرجع سابق ذكره، ص 380.
(2) ذات المرجع السابق، ص 389.
(3) أيمن عبدالله فكري، مرجع سابق ذكره، ص 123.
(4) هدى حامد قشقوش، مرجع سابق ذكره ، ص 43.

الحاسوب إذ تحدث لدى قيام شخص ما بوضع أمر معين لبرامج الحاسوب الإلكتروني وعند تنفيذ هذا الأمر يتم مسح كلي أو جزئي للملفات المرتبطة بهذا البرنامج، وفي بعض الأحيان يكون المجرمون أكثر اهتماماً بإساءة استخدام أجهزة الحاسوب ونظم الاتصالات من مجرد تحقيق أرباح من ورائها ، فعلى سبيل المثال: قام أحد الطلبة في جامعة ويسكونسن الأمريكية بتعطيل نظام الحاسوب التابع للجامعة متعمداً ولأكثر من مرة، بُغية تدمير المشروعات النهائية لعشرات الطلبة وقد حكم عليه القاضي بعقوبة لمدة سنة واحدة سجن مع إيقاف التنفيذ ومغادرة الجامعة.[1]

ونظراً للطبيعة الخاصة التي تتسم بها المكونات المعنوية للنظام المعلوماتي والتي يغلب عليها الطابع الفني المستحدث، فقد يُطلق على إتلاف المكونات المنطقية للنظم المعلوماتية تعبير لدى بعض الفقهاء يُسمى "تدمير المعلومات" ويقصد بتدمير النظم المعلوماتية: إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ، ولا يهدف التدمير هنا إلى مجرد الحصول على منفعة النظام المعلوماتي أياً كان شكلها استيلاء على نقود أو اطلاع على معلومات ، ولكن يبقى ببساطة إحداث ضرر بالنظام المعلوماتي وإعاقته عن أداء وظيفته.[2]

د. تضخيم البريد الإلكتروني:

يعني تضخيم البريد الإلكتروني أن يتم إرسال نسخ مكررة بعدد كبير من ذات الرسالة لنظام البريد الإلكتروني الخاص بالغير بما يترتب عليه من إعاقة سير النظام التقني المعلوماتي بشكل منضبط، ويؤدي ذلك الأمر إلى إعاقة استخدام تلك الخدمة أو توقفها ، وفي الغالب يتم هذا الأمر من خلال فيروسات معلوماتية يتم بثها ونشرها عن طريق الشبكة المعلوماتية "الإنترنت".[3]

وهذا ما سنتناوله بالتفصيل في الفرع الآتي:

---

(1) وليد الزيدي، القرصنة على الإنترنت والحاسوب، ط1، دار أسامة للنشر والتوزيع، الأردن، عمان، 2003م، ص 30-31.
(2) أحمد خليفة الملط، مرجع سابق ذكره، ص 639 – 641.
(3) أيمن فكري، مرجع سابق ذكره، ص 125– 126 .

الفرع الثالث

بث الفيروسات والبرامج الشبيهة لها داخل النظام المعلوماتي

يُعتبر أسلوب ارتكاب الجرائم باستخدام برنامج الفيروس أو البرامج الشبيهة للفيروس من الطرق التقليدية في ارتكاب الجرائم المعلوماتية، على الرغم مما تنطوي عليه من آثار تدمير بحيث إنها يمكن أن تصل إلى درجة التدمير الكامل للجهاز، وترجع خطورة هذا الأسلوب إلى سهولة ارتكابه من خلال الدخول على شبكة الإنترنت أو من خلال تداول إحدى الوسائط المتعددة، وتكون مُصابة بإحدى هذه البرامج، وعند قيام أي شخص إما بإنزال البرامج من شبكة الإنترنت أو من خلال التعامل مع أي من هذه الوسائط المتعددة بتشغيله على الحاسب يتم اقتحام الجهاز ونزول أي من هذه البرامج المدمرة عليه.[1]

كما يُلاحظ بأنها برامج غير مرئية حيث تحتاج للكشف عنها إلى أسلوب علمي أكثر تطوراً ومعرفة تقنية على مستوى عالٍ لكي يمكن للمستخدم اكتشاف وجود غزو لأي من برامجه.[2]

فتقوم هذه الفيروسات بالتسلل إلى النظام المعلوماتي في صمت عند اتصالها بإحدى الشبكات الملوثة، أو عند نقل برنامج مصاب لذاكرة النظام، حيث لم يلبث ما تتكاثر فيه دون علم أو دراية من المستخدم أو من نظام التشغيل وتقوم بعملها بسرعة وحذر وما أن تتمكن من النظام المعلوماتي حتى تصيبه بالشلل التام.[3]

(1)أيمن عبدالحفيظ عبدالحميد سليمان، إستراتيجية مُكافحة جرائم استخدام الحاسب الآلي، د.ط، د.ت.، ص 289.
(2) ذات المرجع السابق، ص 289.
(3) نسرين عبدالحميد نبيه، مرجع سابق ذكره، ص 138.

وقد كان الفيروس يستهدف في بادئ الأمر غاية تجارية بحتة، حيث صممته شركات تصميم البرامج لحماية برامجها التطبيقية من النسخ غير المشروع والذي كان يفوت عليها أرباحاً طائلة غير أن هذا الاستخدام ما لبث أن تَطور تطوّراً إجرامياً كبد العالم خسائر مالية فادحة.[1]

فأصبحت تهدد وتضر بالأمن التقني الشخصي أو الرسمي ومن صوره ما يُعرف "بالهاكرز"، ولقد بدأت فيروسات الحاسوب تظهر في أواخر سنوات السبعينات وتزايدت في الآونة الأخيرة لما تشكله من خطر على الشبكة المعلوماتية لسرعة انتقالها وجسامة الضرر الناتج عنها، وقد يُعتبر إرسال الهاكرز وغيرها من صور الفيروسات جريمة إرهاب إلكتروني لا تقل خطورة عن الاختراق والتخريب.[2]

أولاً: ماهية الفيروسات المعلوماتية:

لقد عرفها مركز الحاسبات الشخصية القومي بالولايات المتحدة الأمريكية بأنها: عبارة عن برامج مُهاجمة تصيب أنظمة الحاسبات بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان، وهي في العادة برنامج صغير مكتوب بلغة متدنية المستوى مثل لغة التجميع مما يزيد من صعوبة اكتشافه ويقوم بالتجول في الحاسب باحثاً عن برنامج غير مصاب وعندما يجد واحد ينتج نسخة من نفسه للتدخل فيه، وتتم هذه العملية في جزء من الثانية حيث يقوم البرنامج فيما بعد بتنفيذ أوامر الفيروس.[3]

كما أنه هناك من يُعرف الفيروس بأنه "عبارة عن برنامج معد سلفاً لغرض إصابة الحاسوب ولإتلاف برامجه".[4]

---

(1) محمد فتحي عيد، الإجرام المعاصر، ط1، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1999م، ص 253.

(2) فائزة الباشا، سياسة التجريم في مواجهة الجرائم المعلوماتية، ورقة عمل مقدمة إلى المؤتمر الذي عقد في لبنان- منعقد في الفترة 25-2009/02/27م، ص 7-8.

(3) أيمن عبدالله فكري، مرجع سابق ذكره، ص 113.

(4) وليد الزيدي، مرجع سابق ذكره، ص 33-34.

ويُعرف أيضاً بأنه عبارة عن برنامج صغير الحجم يصعب اكتشافه ويوضع في اسطوانة ثم يقوم بنسخ نفسه في نظام تشغيل الحاسبات الآلية، وينتشر بعد ذلك في كل الدعائم الممغنطة والمستخدمة في هذه الأجهزة ويستطيع الفيروس في فترة وجيزة أن يُحطم جميع هذه البطاقات.[1]

ومن التطبيقات الواقعية لزرع برامج الفيروسات بغرض الإتلاف المعلوماتي قيام مبرمج في ألمانيا بزرع برنامج فيروس في النظام المعلوماتي للشركة التي يعمل بها، وتم برمجته على أن يبدأ التدمير والتخريب في معلومات وبرامج الشركة بعد عامين من فصله من الشركة وظل المفجر في البرنامج يعمل في حساب ساعة وسنة التنفيذ، وعندما وصل البرنامج إلى الوقت المحدد توقفت العديد من طرفيات الاتصال بنظام معلومات الشركة وصلت إلى 300 نهاية طرفية، ويُلاحظ في هذه الواقعة صعوبة اكتشاف فاعلها، وذلك بسبب التباعد الزمني بين النشاط الإجرامي وحدوث النتيجة.[2]

ثانياً: خصائص الفيروسات المعلوماتية:

تتميز الفيروسات المعلوماتية وفقاً للتعريفات المتقدمة لها بعدد من الخصائص وهي:

1. القدرة على الاختراق:

تُزود البرامج الفيروسية بما يُمكنها من اختراق النظم المعلوماتية والمواقع الإلكترونية المحاطة بنظم أمنية، فيتم استخدام كل الوسائل الممكنة من قبل المخربين التي يُزود بها الفيروس حتى يحقق أهدافه التخريبية والتدميرية للمواقع الإلكترونية. [3]

(1) عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2002م، ص 49.
(2) أيمن عبدالله فكري، مرجع سابق ذكره، ص 125-126.
(3) أيمن عبدالله فكري، ذات المرجع السابق، ص 114.

فتتعدد الأغراض المتوخاة من زراعة فيروس الحاسب الآلي إلى:

أ. اختراق النظام المعلوماتي لأحد البنوك بغرض تحويل مبلغ مالي من حسابات العملاء إلى الحساب الخاص للمجرم المعلوماتي.

ب. اختراق النظام المعلوماتي للغير لنقل المعلومات المعالجة إلكترونياً، أو لنقل برنامج من برامجه كلياً أو جزئياً إلى النظام الخاص بالمجرم المعلوماتي.

ج. اختراق النظام المعلوماتي للغير بغرض التجسس على المؤسسات الهامة في الدولة أو التجسس على الأسرار الشخصية للأفراد أو التلاعب في بياناتهم ذات الصفة الشخصية بالحذف أو الإضافة أو التعديل.

د. اختراق النظام المعلوماتي للاستفادة من إمكانيات الحاسب الآلي ذاته وهو ما يُطلق عليه سرقة وقت الحاسب.

هـ. اختراق النظام المعلوماتي للغير لتدمير ثروته المعلوماتية كلها أو جزء منها.[1]

2. القدرة على الاختفاء:

إن برنامج الفيروس له القدرة على الاختفاء حيث يستخدم عدة وسائل تمويهية منها دخوله لذاكرة الحاسب كملفات مخفية داخل النظام المعلوماتي، بحيث يصعب ملاحظتها واكتشافها من قبل المستخدم أو المواقع المستهدفة، وكذلك عن طريق الاستقرار في أماكن معينة لا يستطيع المستخدم ملاحظتها مثل ساعة الحاسب.[2]

(1) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 313-314.
(2) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 301-302.

3. القدرة على الانتشار:

تتميز الفيروسات بسرعة انتقال تفوق التصور فهي تستطيع أن تنتقل من قارة إلى أخرى في ثواني معدودة بسبب التكاثر اللانهائي ، ومما ساعد على هذا الانتشار التوافق في البرامج المستخدمة على نطاق واسع عبر دول العالم، وشبكات المعلومات الدولية.[1]

4. القدرة على التدمير:

إن الهدف الأساسي للفيروس المعلوماتي هو تدمير وتخريب المعلومات والبرامج بما يؤدي في النهاية إلى تعطيل أو توقف النظم المعلوماتية، فإن الفيروس يتجه إلى مكان ما في الذاكرة ويظل كامناً أو خاملاً حتى يتحقق الأمر أو الزمن الذي تم برمجة المفجر في الفيروس عليها، ثم ما يلبث أن يقوم بنشاطه في تدمير المعلومات.[2]

كما أن فيروس الحاسب الآلي هو برنامج مدمر يُلحق نفسه بالبرامج الشرعية الموجودة في الحاسب الآلي رغم أنف المستخدم، ويتكاثر أثناء عملية التشغيل، ويستطيع أن يُعدل نفسه أثناء ذلك، مما يُصعب من اكتشافه، كذلك فهو ينتشر عبر الشبكات والنظم بسرعة فائقة، فضلاً عن انتقاله السريع عبر الملفات وخلال ذلك يحدث حالة من الفوضى ويُربك عمل الأجهزة ، ويدمر البرامج ويعمل على مسح محتويات الملفات.[3]

ثالثاً: البرامج الشبيهة بالفيروس:

تتعرض أجهزة الحاسب الإلكتروني لكثير من المخاطر التي لا تنصب فقط على برنامج الفيروس ولكن هناك برامج شبيهة بالفيروس تنطوي على ذات الخطورة وتُسبب أضراراً بالغة ، تحتاج إلى الكثير من الوقت والمال والجهد لعلاج آثارها التدميرية، والمتمثلة في المحو الكلي أو

(1) أيمن عبدالله فكري، مرجع سابق ذكره، ص 114.
(2) أيمن عبدالله فكري، ذات المرجع السابق، ص 115.
(3) وليد الزيدي، مرجع سابق ذكره، ص 33.

الجزئي للبيانات، كما يمكن عن طريق هذه البرامج ارتكاب الكثير من الجرائم دون إحداث أي تغير أو إتلاف أو محو لبيانات داخل النظام المعلوماتي ، بل على العكس يظل النظام المعلوماتي كما هو وتكون هذه البرامج بمثابة الثغرة التي يستطيع الشخص من خلالها ارتكاب جرائم بالغة الضرر[1]. وتتمثل هذه البرامج في الآتي:

1. برامج الديدان "Worm Software"

وهي عبارة عن برامج تشغيل أية فجوات في نظم التشغيل لكي تنتقل من نظام معلوماتي إلى آخر أو من شبكة إلى أخرى عبر الوصلات التي ترتبط بينهما ويتكاثر أثناء عملية انتقالها كالبكتيريا – بإنتاج عدة نسخ منها، فهو قادر على نسخ نفسه عدة مرات أوتوماتيكياً ، ويمكن التحكم في تكرار تلك النسخ، من قِبل منتجه من مكان بعيد عن طريق الشبكات المعلوماتية، وتهدف هذه البرامج إلى شغل أكبر حيز ممكن من سعى الشبكة، ومن ثم العمل على تقليل كفاءتها، وقد تتعدى هذا الهدف لتبدأ بعد الانتشار والتكاثر في التخريب والتدمير الفعلي للملفات والبرامج ونظم التشغيل.[2]

فله القدرة الفائقة على تعطيل أو إيقاف نظام الحاسب الآلي بصورة كاملة وينتشر أساساً عبر خطوط التوصيلة الإلكترونية وتصدر معلومات غير صحيحة وتؤدي في النهاية إلى انغلاق النظام المعلوماتي فيحدث الإتلاف المعلوماتي، كما إن هذا الفيروس يُصيب جزء محدد من نظام المعالجة الآلية للبيانات وهو الجزء الخاص بنظام التشغيل، وهو ذلك النظام الذي يقصد به

(1) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 300.
(2) نسرين عبدالحميد نبيه، مرجع سابق ذكره، ص 138.

مجموعة البرامج التي تتحكم في إمكانيات الحاسب وفي العمليات التي تستخدمها هذه الإمكانيات.[1]

وعادة ما يستخدم لتحقيق آثاره المدمرة ما يلي:

أ. البريد الإلكتروني: يُعتبر وسيلة سريعة وفعالة لضمان سرعة وصول برنامج الديدان إلى الأجهزة الأخرى مشابهاً في ذلك برنامج الفيروس.[2]

والبريد الإلكتروني هو من أبرز الخدمات التي تقدمها شبكة الإنترنت، لما يمثله من سرعة في إيصال الرسالة وسهولة الإطلاع عليها وقراءتها في أي مكان من العالم.[3]

ب. حسابات الأشخاص: وتتمثل أهمية ذلك بأنه إذا أمكن للشخص الدخول إلى النظام الخاص بأي بنك يقوم البرنامج بقراءة العناوين في الفهرس ثم يبدأ نشاطه المدمر عليها.[4]

2. برنامج حصان طروادة: "Trojan Horse"

هو برنامج فيروسي ضار له قدرة كبيرة على الاختفاء داخل البرنامج الأصلي الذي ظاهره مفيد ولكن محتوياته مدمرة وعندما يتم تشغيل البرنامج الأصلي ينشط الفيروس المتمثل في حصان طروادة وينتشر ليبدأ نشاطه التدميري الذي يؤدي إلى تعديل ومحو بعض البيانات من الجهاز بل وقد يصل به الحد إلى تدمير النظام بأكمله.[5]

كما يُعرف كذلك بأنه نوع من البرمجيات الخبيثة التي لا تتناسخ من تلقاء نفسها بعكس برنامج الديدان المعلوماتية. فهو أداة فعالة في ميدان خرق الأمن المعلوماتي ويمكن القول بأنه:

أ. برنامج غير مرخص متضمن في برنامج شرعي.

(1) هدى حامد قشقوش، مرجع سابق ذكره، ص 104.
(2) أيمن عبدالحفيظ عبدالحميد، مرجع سابق ذكره، ص 302.
(3) محمود أحمد القرغان، مرجع سابق ذكره، ص 186.
(4) متاح على الرابط: allthetec8oudebjimohamed.blogspot.com 2013م، تاريخ الزيارة 2016/11/05م.
(5) نسرين عبدالحميد نبيه، مرجع سابق ذكره، ص 138.

ب. برنامج شرعي تم تغييره بإدخال شفرات غير مرخصة داخل هيكلته البرمجية، فيقوم بعمله وهو جملة من الأنشطة غير المشروعة.

ج. يوفر خدمة مفيدة أو مثيرة لاهتمامات الآخرين. [1]

3. برنامج القنبلة الموقوتة: "Time bomb"

هو اصطلاح يُطلق على أنواع من الفيروسات المعلوماتية التي تهدف إلى تدمير المعلومات والبرامج كوسيلة لارتكاب جريمة الإتلاف، وتعني إن الفيروس ينشط ويبدأ في التدمير عند حدوث واقعة معينة أو في تاريخ محدد.[2]

وتنقسم القنابل المعلوماتية الموقوتة إلى قسمين:

أ. قنابل منطقية. [3]

ب. قنابل زمنية.[4]

ومن الأمثلة الواقعية أو النماذج التطبيقية لوضع برامج قنابل منطقية أو زمنية في الأنظمة المعلوماتية الآتي:

أ. قيام مبرمج فرنسي بدافع الانتقام على أثر فصله من العمل، بوضع قنبلة زمنية على شبكة المعلومات الخاصة بالمنشأة بحيث تنفجر بعد مضي ستة أشهر من رحيله عن المنشاة وترتب على ذلك إتلاف كل البيانات المتعلقة به.

---

(1) محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، د.ط. الإسكندرية، دار الجمهورية للصحافة، أكتوبر، 2010م، ص120.

(2) هدى حامد قشقوش، مرجع سابق ذكره، ص 103-104.

(3) القنابل المنطقية: هي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو في كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام لتسهيل القيام بالعمل غير المشروع. نسرين عبدالحميد نبيه، مرجع سابق ذكره، ص 138.

(4) القنابل الزمنية: وهي عبارة عن كود معين يتم زرعه في برنامج محدد ويتم تحديد موعد معين بالساعة واليوم والسنة لبدء الهجوم من خلال برمجته بدقة متناهية على تشغيله عند الموعد المعين سلفاً. أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص303.

ب. في ولاية لوس أنجلوس الأمريكية تمكن أحد العاملين بإدارة المياه والطاقة من وضع قنبلة منطقية في النظام المعلوماتي الخاص بها مما أدى إلى تخريب النظام عدة مرات.[1]

ج. قيام مبرمج بإحدى الشركات بتصميم قنبلة منطقية من شأنها تدمير بيانات الملف بأكمله، إذا ما تم رفع اسمه من الملف، أي إذا تم فصله وإلغاء خدماته من هذه المؤسسة. [2]

(1) نسرين عبدالحميد نبيه، مرجع سابق ذكره، ص 138-139.
(2) رحاب علي عميش، مرجع سابق ذكره، ص 153..

الفرع الرابع

السرقـــة المعلوماتيـــة

أولاً: سرقة المعطيات والبيانات:

ترجع البدايات الأولى لظاهرة سرقة المعلومات والتي أصبحت موضوعات لأبحاث أكثر تعمقاً في الفترة الزمنية الأخيرة إلى فترة الستينات، والتي تناولت ما يُطلق عليه بصفة عامة "جريمة نظم المعلومات"، حيث تعالج هذه البيانات في غالبيتها التلاعب بالحاسب الآلي وتعطيله، وسرقة المعلومات المختزنة فيه، علاوة على التجسس عليه واستخدامه على النحو غير المشروع.

ويُلاحظ من الاطلاع على الأبحاث والدراسات التي أجريت في هذا الخصوص عدم اتفاقها على مصطلح بذاته للتعبير عن هذه الظاهرة الإجرامية المستحدثة، فهناك من يطلق عليها ظاهرة "الغش المعلوماتي" أو "الجريمة المعلوماتية" أو "الاختلاس المعلوماتي".[1]

وقد نص المشرّع الليبي على جريمة السرقة في المادة (444) من قانون العقوبات الليبي بأنها: "كل من اختلس منقولاً مملوكاً لغيره يعاقب بالحبس ويعد من الأموال المنقولة في حكم قانون العقوبات الطاقة الكهربائية وجميع أنواع الطاقة ذات القيمة الاقتصادية".[2]

فنجد هنا أن المقصود بفعل الاختلاس هو ذلك الواقع على شيء ماديٍ ملموسٍ، بعكس ذلك في جريمة سرقة المعلومات فمحل السرقة فيها هو ذو طبيعة معنوية متمثلة في بيانات ومعلومات مهمة يحتويها الحاسب الآلي.[3]

(1) عبدالله حسين علي محمود، مرجع سابق ذكره، ص 41-42.
(2) محمد رمضان بارة، شرح قانون العقوبات الليبي، القسم الخاص، ج2، جرائم الاعتداء على الأموال، د.ط، 2013م، ص35.
(3) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 95.

ومن هنا كان من الضروري معرفة مدى قابلية الأحكام التقليدية الخاصة بجريمة السرقة للتطبيق في حالة الحصول غير المشروع على المعلومات سرقة المعطيات والبيانات وهل تُعتبر المعلومات محلاً يقبل وقوع فعل السرقة عليها أم لا؟

فمثلاً يشترط في السرقة التقليدية أن يكون فعل الاختلاس واقعاً على شيء مادي منقول ومملوكاً للغير، فهل تنطبق هذه العناصر على سرقة المال المعلوماتي المعنوي أم لا؟ ومدى اختلاف الآراء في هذا الشأن؟ إذاً وفقاً للقواعد العامة يجب أن يكون الشيء موضوع السرقة مادياً أي له كيان مادي ملموس لكي يثير كيفية انتقاله إلى حيازة شخص آخر عن طريق الاختلاس المكون للركن المادي في جريمة السرقة ، وبالتالي تستبعد من مجال السرقة واقع مجرد الأفكار ما لم تكن معروفة بطريقة تسمح بالاستيلاء عليها فيكون محل السرقة واقع على الشيء المدونة عليه.[1]

مثل أن تكون هذه المعطيات أو البيانات مسجلة على اسطوانات أو على شرائط ممغنطة أو على أوراق، فهنا يكفي الاستيلاء مادياً على الدعامة.[2]

وفي هذه الحالة يُعتبر من السهل تطبيق الأحكام العامة لجريمة السرقة عليها بما أنها قد أخذت شكلاً مادياً، فيصبح محل السرقة هنا قابل لأن يخضع لنص المادة المُعالج لجريمة السرقة التقليدية، وكذلك الحال بالنسبة للمال المعلوماتي ذو الطبيعة المادية في الأصل مثل آلات وأدوات الحاسب الآلي كوحدة الغرض البصري ووحدة الإدخال. وفعل الأخذ أو الاختلاس في جريمة السرقة هو الاستيلاء على الحيازة الكاملة للشيء بدون رضاء المالك أو الحائز السابق.[3]

(1) هدى حامد قشقوش، مرجع سابق ذكره، ص 49-50.
(2) جميل عبدالباقي الصغير، مرجع سابق ذكره، ص 24.
(3) محمد رمضان باره، شرح قانون العقوبات الليبي، القسم الخاص ، الجزء الثاني، مرجع سابق ذكره، ص 37-38.

وهو ما ينتج عنه خروج الشيء المستولى عليه من ذمة ودخوله في ذمة أخرى، وبعبارة أخرى، إفراغ ذمة وإشغال أخرى بحيث لا يوجد مجال للتزاحم بين الذمتين في الاستيلاء على الشيء.[1]

وهذا المعنى للاستيلاء في جريمة السرقة وهو نقل الشيء محل جريمة السرقة من حيازة المجني عليه إلى حيازة الجاني يتعارض مع طبيعة المعلومات إذا ما نظرنا إليها منفصلة عن إطارها المادي، حيث إن الحصول عليها لا يعني انتقالها من حيازة المجني عليه إلى حيازة الجاني لأنها تظل على الرغم من ذلك في حيازة المجني عليه وتحت سيطرته.[2]

فكيف يتصور أن يرد فعل الأخذ أو الاختلاس الذي هو من طبيعة مادية على شيء معنوي، ومن هنا انقسم الفقه حول مدى صلاحية وقوع فعل الاختلاس على المعلومات من عدمها إلى اتجاهين:

1. الاتجاه القائل بصلاحية المعلومات للاختلاس أو الأخذ:

يرى هذا الاتجاه إن طبيعة الشيء المختلس هي التي تحدد الطريقة أو الأسلوب الذي يجب أن يتبعه الجاني للقيام بالنشاط الإجرامي المحقق لفعل الاختلاس، وهكذا يختلف الأسلوب الذي ينفذ به هذا النشاط باختلاف الشيء الواقع عليه فعل الاختلاس سواء من حيث طبيعته أو حجمه أو وزنه أو مقاومته أو وظيفته أو قيمته. فالاستيلاء على سيارة مثلاً يختلف في الأسلوب الذي يتم به عن الاستيلاء على تيار كهربائي، والسرقة من المحلات الكبرى تختلف عن السرقة في الأسواق العادية، وبالمثل فإن سرقة شيء مادي تختلف عن سرقة شيء معنوي، فإذا كانت الأشياء المادية يتم اختلاسها من خلال نشاط مادي يصدر عن الجاني فإن الأمر يختلف بالنسبة للأشياء المعنوية

(1) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 98.
(2) نسرين عبدالحميد نبيه، مرجع سابق ذكره، ص132.

فهذه الأخيرة يمكن اختلاسها عن طريق اختلاس الدعامة ودون الاستعانة بها، بمعنى أن برامج الحاسب الآلي والمعلومات يمكن التقاطها ذهنياً دون أي نشاط مادي ملموس وخاصة عن طريق السمع أو النظر.[1]

ولكن هذا القول لا يمكن التسليم به – بلا جدال – في مجال القانون الجنائي إذ لابد من نشاط مادي يصدر عن الجاني للقول بتوافر فعل الاختلاس، هذا لأن القانون لا يُعاقب على مجرد الأفكار والنوايا أياً كانت جسامتها، وللخروج من هذا المأزق يذهب أصحاب هذا الاتجاه إلى أن أخذ أو اختلاس المعلومات يجب أن يتم بنشاط مادي، وهو عملية النسخ أو التصوير التي عن طريقها تنتقل المعلومات من الأصل إلى الصورة وبالنسبة للمعلومات التي يتم التقاطها ذهنياً فإن الاختلاس لا يتحقق بالنسبة لها إلا إذا وضعت موضع التنفيذ أو تم بيعها أو نقلها إلى الغير على دعامة مادية أو إذاعتها لأن هذا النشاط المادي هو الذي ينتج عنه انتقال المعلومات من ذمة إلى أخرى ويقوم بها فعل الاختلاس، وتتحقق الغاية منه وهي إنقاص الذمة للمجني عليه ولو لم يخرج الشيء محل السرقة من ذمته بنقله أو تحريكه من مكانه.[2]

وهذا ما يؤيده الفقه والقضاء الفرنسي، فقد اعتبر مؤخراً أن المعلومات والبيانات هي طائفة جديدة من الأموال قابلة بأن يقع عليها فعل الاختلاس المكون لجريمة السرقة الواقعة على المال المعلوماتي[3]. وفي كل الأحوال فإن السرقة المعلوماتية لا يترتب عليها خروج المعلومات من حيازة أصحابها أو الحائز القانوني لها ولكن تخرج فقط نسخة من هذه المعلومات على حين أنه في السرقة التقليدية تخرج الحيازة من الحائز القانوني إلى السارق[4].

(1) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 94.
(2) ذات المرجع السابق، ص 98-99.
(3) فائزة الباشا، مرجع سابق ذكره، ص10.
(4) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص167.

2. الاتجاه القائل بعدم صلاحية المعلومات للاختلاس أو الأخذ:

استبعد هذا الاتجاه الفقهي أن تقع جريمة السرقة على البرامج والمعلومات مستقلة عن دعامتها نظراً للطبيعة غير المادية للمعلومات، ولكن أنصار هذا الاتجاه لم يكن لهم رأي واحد، منهم من رأى أن السرقة قد وقعت على الأصل، ومنهم من اعتبر أنها وقعت على الماكينة لنسخ صور لبرامج أو للمعلومات الأصلية من خلالها، ولو كان هذا الاستيلاء لم يستمر لفترة طويلة من الزمن، ففي الحالتين لا تَعدو أن تكون سرقة استعمال مؤقت.[1]

ولكن هذان الرأيان يصطدمان بعقبة مؤداها أنه من الممكن أن يتم الحصول على صورة البرنامج أو نسخ صور منه دون الاستيلاء على الأصل أو الماكينة وذلك إذا تم هذا النسخ من خلال طرفية تتصل بالحاسب المركزي سلكياً أو لاسلكياً، بحيث لا يُحرم صاحب الآلة أو البرنامج ولو لفترة قصيرة من استعمال أيهما، في حين أنه في السرقة التقليدية تخرج الحيازة من الحائز القانوني إلى السارق.[2]

ولتفادي هذه العقبة اتجه رأي آخر إلى أن السرقة هنا وقعت على قدر من التيار الكهربائي اللازم لاستخراج الصورة من خلال الومضات والإشعاعات التي يترتب عليها فنياً استخراج هذه الصورة.

إلا أن هذا الرأي نفسه لا يرى في هذا التفسير حلاً للمشكلة لأن كمية الكهرباء المستهلكة لا تكاد تذكر فهي من الأقلية بمكان بحيث لا يوجد وجه للمقارنة بينها وبين جريمة سرقة التيار الكهربائي المعروفة.[3]

(1) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 101-102.
(2) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 163.
(3) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 104.

إذاً نستنتج من كل هذه الآراء أنه إذا ما سلمنا بها سنواجه نتيجة غير مقبولة وهي عدم المعاقبة على وقوع فعل السرقة على المال المعلوماتي ، خاصة وأن الحاسب الآلي أصبح يؤدي وظيفة أو خدمة تتعاظم أهميتها يوماً بعد يوم في كل أنحاء العالم، ومن هنا يجب النص على تجريم الاعتداء على هذه الخدمة، وذلك حتى يتم تجنب الجدل حول سرقة المعلومات وسرقة وقت الآلة وسرقة استعمال الأصل، وبالتالي تتحقق كذلك الحماية الجنائية المباشرة للبرامج والمعلومات بصفة عامة لكي يتم الاستثمار والاستغلال بشأنها على الوجه الأكمل[1]. وهذا ما نذهب إلى تأييده.

فإن الأمر لا يخلو من الحاجة إلى ضرورة إصدار القوانين المعالجة لأي ظاهرة حديثة نسبياً، قد تضر بالمصالح الاجتماعية أو الاقتصادية أو السياسية...الخ.

وبالتالي فإن القوانين الجديدة سوف تتجنب الرؤيا القانونية التي تسعى إلى استخدام تشريعات جنائية أخرى ليست ذات علاقة وذلك لتطبيقها على جرائم الحاسوب والانترنت، وبهذا يمكن إدانة المتهمين عن ارتكابهم لجرائم الحاسوب بشكل مباشر.[2]

كما أنه انطلاقاً من مفهوم السياسة التشريعية الجنائية والتي ترتبط باحتياجات المجتمع ومن المؤكد أن الخدمات الإلكترونية أصبحت شديدة الالتصاق بالمجتمع، كما من المنطقي أن تتجه السياسة التشريعية في معظم قوانين العالم إلى حماية الأشخاص والأموال عن طريق تجريم الاعتداء على الأموال المعلوماتية معنوية كانت أو مادية، وما قد يتسبب عن هذه الاعتداءات من مساس بالأشخاص أو الأموال. [3]

(1) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 105.
(2) أورين كير، "مؤلف"، نطاق الجريمة الافتراضية، عمر محمد بن يونس، "مترجم"، د.ط، جامعة الإسكندرية، د.ت، 2004، ص 52.
(3) هدى حامد قشقوش، مرجع سابق ذكره، ص 89.

وهذا ما نأمل من المشرّع الليبي الاتجاه إليه، وبالتالي يجب عليه أن يبادر بضرورة النص على تجريم جميع صور ظاهرة الجريمة المعلوماتية وبمختلف أشكال الاعتداءات على النظم المعلوماتية من دخول أو اختراق للنظام المعلوماتي ومن ثم إتلاف البيانات أو البرامج أو سرقتها أو تزويرها أو نسخها...إلخ.

ثانياً: موقف القضاء من جريمة سرقة المعلومات:

كان أول حكم أصدرته محكمة النقض الفرنسية في هذا الشأن هو حكم "لوجاباكس" والذي تتلخص وقائعه في أن أحد مهندسي شركة "لوجاباكس" قد فُصل من عمله ، وفي الدعوى المرفوعة منه ضد رب العمل قدم للمحكمة تأييداً لدعواه صورتين كان قد نسخهما لمستندين من مستندات الشركة أمكنه الحصول عليها بمناسبة وظيفته السابقة وقبل فصله من العمل، قدم للمحاكمة بتهمة سرقة هذه المستندات وبرأته محكمة أول درجة وتأيد حكم البراءة في الاستئناف على أساس أن المتهم لم يحمل هذه المستندات إلى منزله على سبيل التملك، ولكن محكمة النقض الفرنسية نقضت الحكم السابق لمخالفته صحيح القانون، لأن القانون لم يشترط لتحقق الأخذ أو الاختلاس في جريمة السرقة أخذ أو انتزاع الشيء وأن الاختلاس يمكن أن يتحقق ولو كان الشيء بين يدي الجاني – قبل الاستيلاء عليه – على سبيل اليد العارضة، ولأن الجاني استولى على المستندين التابعين للشركة المذكورة، التي كان يعمل فيها لمصلحته الشخصية من دون علم ومن دون رضى رب العمل المالك لهما أثناء الوقت اللازم لتصويرها.[1]

كما صدر حكم آخر من محكمة الجنح الفرنسية متعلق بموظف سابق كان يعمل لدى شركة "بيجو" للسيارات، حيث قام المتهم بتسجيل المعلومات والبرامج المعلوماتية التي كان قد ساهم

(1) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 100-105.

فيها قبل تركه العمل على قرص مغناطيسي كان قد حمله معه خصيصاً لهذا الغرض ، وكان هذا التسجيل أو النسخ بعد مدة من الاستغناء عنه في العمل "فصله" وأثناء عمله لدى شركة أخرى.

فأدانته المحكمة بجريمة السرقة على أساس أنه اختلس المعلومات المسجلة على قرص مغناطيسي والتي تتضمن برامج معلوماتية تخص شركة "بيجو" ومن الواضح أن في هذا الحكم قرر منطوقه أن المعلومات ملكاً للشركة، ولا يقلل من أهمية هذا الحكم صدوره من محكمة الجنح، ولا يمكن كما أدعى معارضو سرقة المعلومات والبرامج أن الحكم قصد به تجريم التسجيل وليس سرقة المعلومة في حد ذاتها فإنه على كل الأحوال يعتبر خطوة تمهيدية من جانب القضاء.[1]

ثالثاً: صور ارتكاب جريمة السرقة المعلوماتية:

لعل من بين أهم الصور أو الطرق التي تتم بواسطتها ارتكاب جريمة سرقة المعلومات أو جرائم النصب والاحتيال المعلوماتي هي وسيلة:

1. اختراق المواقع الإلكترونية:

الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة وذلك عن طريق ثغرات في نظام الحماية الخاص بالهدف ، وغالباً ما تكون تلك الثغرات في المنافذ "Ports" الخاصة بالجهاز وهذه المنافذ يمكن وصفها بأبسط شكل على أنها بوابات للجهاز على الإنترنت.[2]

ويمكن تعريف الاختراق بأنه قوة المخترق على الدخول إلى جهاز شخص ما بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول إلى جهاز آخر فهو "مخترق" أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو "مخرب".[3]

---

(1) هدى حامد قشقوش، مرجع سابق ذكره، ص 59-60.

(2) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص152..

(3) متاح على الرابط: www.aliy.yosh.comishowthread منتديات جيوش الهاكرز، تاريخ الزيارة 2016/11/18م ، الساعة 10:30 م.

كما يُعرف الاختراق بأنه هو عبارة عن عملية دخول غير مصرح به إلى أجهزة وشبكاتهم الإلكترونية، وذلك بواسطة برامج متطورة يستخدمها كل من يملك خبرة في استعمالها.[1]

وهناك طرق عديدة للاختراق والتي يمكن للمبتدئين استخدامها وأبسطها هي البرامج التي تعتمد على نظام "الزبون/الخادم" حيث تحتوي على ملفين أحدهما يسمى "Server" وهو الذي يرسل إلى جهاز الضحية بطريقة ما والملف الآخر يسمى "Client" ويتم تشغيله من قبل المخترق للتحكم في الجهاز المصاب، وعند تشغيل ملف الـ"Server" من قبل الضحية يصبح جهازه عرضة للاختراق حيث يتم فتح أحد المنافذ في جهازه، وبذلك يستطيع المخترق يتوصل بجهاز الضحية باستخدام إحدى البرامج المتخصصة في هذا المجال، ومن ثما يستطيع المخترق أن يفعل كل ما يحلو له في جهاز الضحية مثل : سرقة الملفات المهمة والأرقام السرية وتخريب وإتلاف الملفات، كما يستطيع أشخاص آخرون فعل نفس الشيء والدخول لجهاز الضحية نظراً لوجود منفذ مفتوح في جهازه ويكون بذلك عُرضة للاختراق من قبل الأشخاص الذين يقومون بعمل مسح للمنافذ المفتوحة لدى الأجهزة المصابة بملفات الباتش وهذه الطريقة هي أبسط أشكال الاختراق، وهناك طرق أخرى عديدة تمكن المتطفلين من الاختراق ومباشرة من دون إرسال ملفات لدرجة أن جمعية للمقرضين في أمريكا ابتكرت طريقة للاختراق متطورة للغاية ، حيث يتم عن طريق حزم البيانات التي تتدفق مع الاتصالات الهاتفية عبر الإنترنت فيتم اعتراض تلك البيانات والتحكم في جهاز الضحية.[2]

(1) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 152.
(2) متاح على الرابط: www.aliy.yosh.comishowthread منتديات جيوش الهاكرز، تاريخ الزيارة 2016/11/18م، الساعة 10:59.

فمثلاً نجد أنه في حرم بعض الجامعات في أرجاء العالم المختلفة استطاع لصوص المعلوماتية من اختراق الحواسيب الخاصة بتلك الجامعات، والتي تحتوي على بيانات بدرجات الطلبة الامتحانية وسرقوا معلوماتها ومعظم تلك الجامعات كانت في الولايات المتحدة الأمريكية.

ومن الجدير بالذكر أن تلك الجريمة تتداخل بين كونها جريمة سرقة نظراً لوقوعها على بيانات ومعطيات ومعلومات من الحواسيب الآلية وبين كونها من جرائم التنصت والتجسس على الحياة الخاصة للأفراد أو في طبيعة عمل شركات أو مؤسسات.[1]

ولعل من أشهر صور النصب والاحتيال هي النصب ببطاقات الائتمان مما بدأ يُسبب قلق المتعاملين مع الإنترنت بهذا النوع من البطاقات، فلو أن شخصاً ما قد أخذ أو عرف رقم بطاقة ائتمان شخص آخر، فيمكن له حينها أن يشتري بها بطريقة السحب نفسها من قبل صاحبها الأصلي، لذلك طالبت شركات بطاقات الائتمان العاملين بها بعدم استخدام رقم البطاقة في المعاملات عبر الإنترنت إلا بعد تشفيرها.[2]

كما أن هناك عدة أدوات لفك كلمة المرور المشفرة مثل أداة مصدع كلمات العبور "Passwords cracker" وهي تشمل أي برنامج تطبيقي يمتلك القدرة على تجاوز عقبة شيفرة كلماتها أو إحباط آليات الحماية المصاحب لها ويُتيح إمكانية تجاوز الجدار الأمني الذي توفره لصاحبها في درء أي نشاط يسعى إلى تجاوز الحدود الشخصية للملكة المعلوماتية الخاصة.[3]

والجدير بالذكر أن هذه البرامج التي يعتمد عليها القراصنة في مجال كسر كلمات السر موجودة واستخدامها مشروع بهدف كسر كلمات السر للملفات في حالة نسيانها من قبل صاحبها،

(1) وليد الزيدي، مرجع سابق ذكره، ص 38-39.
(2) وليد الزيدي، ذات المرجع السابق، ص 65-67.
(3) طارق إبراهيم الدسوقي، مرجع سابق ذكره، ص 529.

كما أن هناك شركات متخصصة في بيع تلك البرامج ويلجأ إليها القراصنة لكسر كلمات السر وبمقابل مادي، ولكن وجود مثل هذه البرامج في أيدي القراصنة يُعتبر خطراً كبيراً لإمكانية استغلالها في الدخول على الأنظمة الخاصة بالأشخاص أو الجهات المختلفة ومن ثم ارتكاب الكثير من الجرائم عليها. [1]

2. انتحال الشخصية:

هناك وسيلتان لانتحال الشخصية هما:

أ. انتحال الشخصية البدائي: وفي هذه الوسيلة يستخدم فيها المخترق تقنيات غير عالية الكفاءة كأن يستخدم بطاقة أو كارت خاص بشخص مسموح له بالدخول، وهذا النوع يُعتبر بسيطاً من الناحية التقنية على الرغم مما يسببه من أخطار ونتائج ضارة.

ب. انتحال الشخصية باستخدام تقنيات عالية أو ما يطلق عليها "التنكر الإلكتروني"، وفيها ينتحل الشخص شخصية آخر وذلك باستخدام اسم هذا الشخص عن طريق إرسال بريد إلكتروني مدعياً أنه شخص آخر، وقد يتطور الأمر باستخدام بطاقة الائتمان الخاصة بشخص آخر، وبالتالي ارتكاب الكثير من الجرائم مثل السرقة والنصب والاحتيال وغيرها من الجرائم، وتتمثل خطورة هذه الوسيلة في عدم قدرة جهاز الحاسب الآلي في التفرقة بين المستخدم الأصلي ومنتحل الشخصية.[2]

3. البريد الإلكتروني E-Mail:

وهو من بين أبرز الوسائل المستخدمة من قِبل المجرمين عبر شبكة الإنترنت في جرائم النصب والاحتيال، وذلك عن طريق إرسال رسائل غير مرغوب فيها إلى المشتركين في الخدمة وبكم هائل ، يُطلق على هذه الرسائل تسمية "القائمة القذرة".[3]

(1) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 529-530.
(2) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 331-313.
(3) وليد الزيدي، مرجع سابق ذكره، ص66.

فهذه الرسائل المزعجة تبطئ من نظام البريد الإلكتروني وينطوي أغلبها على عمليات نصب واحتيال وتضم هذه القائمة الرسائل التي تتحدث عن الموضوعات التالية:

أ. فرص تجارية وإغراءات تجني المال من خلال إرسال الرغبات بالبريد الإلكتروني على نطاق واسع.

ب. توجيه خطابات تزعم أنه بالإمكان كسب مبالغ طائلة في مدة قصيرة .

ج. الترويج لجوائز الإجازات.

د. تقديم قروض بشروط ميسرة.

وغير ذلك من الموضوعات التي لا يجد لها المشترك فيما بعد أساساً من الصحة، فلا تعدو أن تكون سوى وسائل لارتكاب جرائم مثل السرقة والنصب والاحتيال. [1]

4. مزادات الإنترنت:

وهي أسلوب آخر من أساليب النصب والاحتيال يجرى عبر شبكة الإنترنت وبهدف السرقة ففي الولايات المتحدة الأمريكية مثلاً يقول 41% من مستخدمي الإنترنت أنهم تعرضوا إلى الاحتيال والسرقة خلال مشاركتهم في المزادات التي تتم عبر الشبكة المعلوماتية والتي في أغلب الأحيان تتعلق بسلع ذات أسعار مرتفعة، وهو ما يعني أن حجم المخاطرة المالية للمشاركين فيها مرتفع أيضا.[2]

(1) وليد الزيدي، مرجع سابق ذكره، ص 66-67

(2) ذات المرجع السابق، ص 67-68.

المطلب الثاني

المجـرم المعلوماتــي

من المعروف بأن في كل جريمة هناك شخصان رئيسيان: شخص إيجابي وهو "الجاني" وشخص سلبي وهو المجني عليه فيها.

فالجاني هو ذلك الشخص الذي يرتكب الفعل غير المشروع، أم المجني عليه فهو شخص أو عدة أشخاص قد أصابهم العدوان وهو محل الجريمة، فجعل منه مجنياً عليه في الجريمة أو مجنياً عليهم إذا كانوا عدة أشخاص.[1]

وبما أن لكل جريمة طرفان ففي الجريمة المعلوماتية "محل الدراسة" يكون الطرف الأول : هو "الجاني" والذي يُطلق عليه اسم "المجرم المعلوماتي" والطرف الثاني: هو "المجني عليه" سواء كان من الأشخاص الطبيعية أو المعنوية أو العامة أو الخاصة، مثل المنشآت المالية والمنشآت التجارية والصناعية والعسكرية.[2]

إلا أن المستهدف من هذه الدراسة هو فكرة المجرم المعلوماتي وهذا ما سيتم تسليط الضوء عليه في الفروع الآتية:

الفرع الأول

شخصية المجرم المعلوماتي

إن فكرة المجرم المعلوماتي هي فكرة جديدة على الفقه الجنائي، ففي الجرائم المتعلقة بالحاسب الآلي نحن لسنا بصدد سارق أو محتال عادي ولكن بصدد مجرم ذو مهارات تقنية ودراية بالتكنيك المستخدم في نظام الحاسب الآلي، قادر على استخدام هذا التكنيك لاختراق الكود السري لتغيير المعلومات أو لتقليد البرنامج أو التحويل من الحسابات عن طريق استخدام الحاسب نفسه،

(1) جلال ثروت، نظم القسم العام في قانون العقوبات ، نظرية الجريمة، د. ط.، دار الجامعة الجديدة، الإسكندرية، 2010م، ص 115.
(2) أحمد خليفة الملط، مرجع سابق ذكره، ص 119.

وهذا شيء منطقي حيث ترك عالم المجرمين البؤساء ليدخل إلى عالم مجرمي المهارات المعلوماتية، فشخصية المجرم وميكانيكية ارتكابه للجريمة له صفاته الخاصة بهذا النوع الجديد من الإجرام.[1]

ولذلك يمثل المجرم المعلوماتي بالنسبة للمجموعات التقليدية للإجرام شخصية مستقلة بذاتها فهو من ناحية إنسان ذكي ومن ناحية أخرى إنسان اجتماعي بطبيعته.[2]

وهذا ما سيتم ايضاحه بالشرح في الآتي:

أولاً: المجرم المعلوماتي "إنسان ذكي":

من المعروف أن مرتكبي جرائم الحاسب الآلي يتمتعون بقدرة عالية من الذكاء وأغلبهم ينتمون إلى التخصصات المتصلة بالحاسب الآلي من الناحية الوظيفية.[3]

كما أن جرائم التكنولوجيا الحديثة لا تتطلب لارتكابها إجراءات تميل إلى العنف بقدر ما تتطلب مقدرة عقلية وذهنية خاصة لدى الجاني. [4]

لذا يُقال عادة عن الإجرام المعلوماتي بأنه هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى استخدام القوة والعنف في تنفيذه.[5]

فالجرائم المعلوماتية تتطلب إلماماً كافياً بالمهارات والمعارف الفنية ذات الصلة بالحاسب الآلي وأنظمته، وبالتالي فمن المنطقي أن يكون مرتكبي هذه الجرائم في الغالب من المتخصصين في المعالجة الإلكترونية للبيانات، حيث يمكن في مرحلة المعالجة القيام بإدخال أي تعديلات من

(1) هدى حامد قشقوش، مرجع سابق ذكره، ص 27.
(2) أحمد خليفة الملط، مرجع سابق ذكره، ص 114.
(3) عبدالله حسين علي محمود، مرجع سابق ذكره، ص 48.
(4) فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق ذكره. ص 33.
(5) جميل عبدالباقي الصغير، مرجع سابق ذكره، ص 15.

شأنها تحقيق ما يبغيه الجاني من جراء التلاعب في برنامج الحاسب الآلي كدس معلومات غير مصرح بها فيها أو تشغيل برامج تلغي جزئياً أو كلياً عمل البرامج الأصلية.[1]

كما يمكن تصور وقوع هذه الجرائم في مرحلة الإدخال ، حيث تترجم المعلومات والبيانات المراد معالجتها أو تخزينها بالحاسب الآلي إلى لغة يفهمها هذا الحاسب، ومن ثم يقوم الجاني بإدخال بيانات أو معلومات غير صحيحة وعدم إدخال الوثائق الأساسية والمعلومات المطلوبة، كما قد تقع مثل هذه الجرائم في مرحلة الإخراج، وذلك بسبب وقوع تغيير أو تلاعب في النتائج التي يخرجها النظام المعلوماتي "البيانات المخرجة" والتي سبق وإن كانت صحيحة عند إدخالها ومعالجتها.[2]

وإذا كان من السهل معرفة الإجرام العنيف الموجه ضد المعلومات والذي يتبلور في إتلاف الحاسب الآلي أو الدعائم الممغنطة، إلا أنه لا يستنتج من ذلك أن الإتلاف المعلوماتي بحاجة إلى سلوك عنيف أو عدواني، فهو ينشأ في أغلب الأحوال من تقنيات التدمير الناعمة والتي تتمثل في التلاعب بالمعلومات أو البرامج أو البيانات، وذلك عن طريق ما يُعرف بالقنابل المنطقية أو بالفيروسات المعلوماتية [3]. والتي سبق وأوضحناها بالشرح.

ثانياً: المجرم المعلوماتي "إنسان اجتماعي":

يمكن القول بأن المجرم المعلوماتي هو من الأشخاص الذين يرتكبون الجرائم المعلوماتية من أجل تحقيق دافع اجتماعي كدافع اللهو أو لمجرد إظهار تفوقهم على النظام المعلوماتي أو على البرامج المخصصة لأمن النظام، وليس لتحقيق أي منفعة مادية من جراء جرائمهم، ولكنهم يكتفون بالتفاخر بأنفسهم أو أن يظهروا لضحاياهم ضعف أنظمتهم ، وهكذا يشاع في بعض

(1) فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق ذكره، ص 30
(2) أحمد خليفة الملط، مرجع سابق ذكره، ص 104.
(3) عبدالله حسين علي محمود، مرجع سابق ذكره، ص 49.

المنشآت التي يضبط بها أحد قراصنة النظام المعلوماتي بأنه يسعى إلى ضمه للفريق المعلوماتي المكلف بضمان أمن النظام المعلوماتي فيها.[1]

كما نجد أن المجرم المعلوماتي هو إنسان متوافق مع المجتمع فلا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، ذلك لأنه أساساً إنسان مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، ولكن ذلك لا يعني التقليل من شأن المجرم المعلوماتي بل إن خطورته الإجرامية قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه. [2]

(1) أحمد خليفة ملط، مرجع سبق ذكره، ص 115.
(2) عبدالله حسين علي محمود، مرجع سابق كره، ص 50.

الفرع الثاني

خصائص وصفات المجرم المعلوماتي

اختلف الباحثون في تحديد الصفات المميزة للمجرم المعلوماتي كما اختلفوا أيضاً في مدى انطباق وصف جرائم ذوي الياقات البيضاء على مجرمي المعلوماتية، فيُعد الأستاذ "Parker" واحداً من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي بصفة خاصة، فهو يرى أن المجرم المعلوماتي وإن كان يتميز ببعض الصفات الخاصة إلا أنه لا يخرج عن كونه مرتكباً لفعل إجرامي يتطلب توقيع العقاب عليه.[1]

فكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في صفاتها من جرائم ذوي الياقات البيضاء ، فهو يقترب منهم في أنه ينتمي في أكثر الحالات لوسط اجتماعي متميز وكما أنه على درجة من العلم والمعرفة ولا يعتبر سلوكه جريمة أو فعل يتنافى مع الأخلاق، ولكن الاختلاف يكمن في أن المجرم المعلوماتي ليس من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي.[2]

ويتمتع مجرمي المعلوماتية بخصائص وصفات تميزهم بصفة عامة عن غيرهم من المجرمين، وذلك انعكاس حتمي لما تتطلبه عمليات استخدام هذه الشبكة من قدرات تقنية وفنية هائلة وثقافة وخبرة تكنولوجية ومعلوماتية عالية المستوى. [3]

(1) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 174.
(2) ذات المرجع السابق، ص175.
(3) علي جبار الحسيناوي، مرجع سابق ذكره، ص 48.

وهذه الخصائص هي:

1. المهارة:

تعد المهارة المتطلبة لتنفيذ النشاط الإجرامي من أبرز خصائص المجرم المعلوماتي، فتنفيذ الجريمة المعلوماتية بصفة عامة يتطلب قدراً من المهارة يتمتع بها الفاعل ، والتي قد يكتسبها عن طريق الدراسة المتخصصة في مجال تكنولوجيا المعلومات أو عن طريق الخبرة المكتسبة في هذا المجال.[1]

وتقع هذه الجريمة كما ذكرنا سابقاً سواء في مرحلة الإدخال للبيانات والمعلومات أو في مرحلة المعالجة أو حتى في مرحلة الإخراج، فتقع مثلاً الجريمة على أثر وقوع تغيير في البيانات المخرجة والتي سبق وإن كانت صحيحة عند الإدخال المعالجة.[2]

إلا أن ذلك لا يعني ضرورة أن يكون لدى المجرم المعلوماتي خبرة كبيرة في هذا المجال، بل أن الواقع العملي قد أثبت أن من أخطر مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال. [3]

2. المعرفة:

وهي تعني التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، فالجناة غالباً ما يمهدون لارتكاب جرائمهم بالتعرف على كافة الظروف المحيطة، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنها.[4]

(1) طارق إبراهيم الدسوقي، مرجع سابق ذكره، ص 176.
(2) فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق ذكره، ص 30-31.
(3) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 176.
(4) ذات المرجع السابق، ص 176.

3. الوسيلة:

ويراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته، فالوسائل المتطلبة للتلاعب بأنظمة الحاسب الآلي هي في أغلب الحالات تتميز نسبياً بالبساطة وبسهولة الحصول عليها. [1]

4. السلطة:

وهي الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فأغلب مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وهذه السلطة قد تكون مستمدة من مجال عملهم، فقد يكون المجرم المعلوماتي من العاملين في مراكز الحاسوب الرئيسية. [2]

5. الباعث:

وهو الدوافع المحركة للمجرم المعلوماتي فهي متباينة وتختلف من مجرم إلى آخر ومن أهمها:

أ. تحقيق الكسب المادي:

إن النفع المادي والمتمثل في المكاسب والأرباح الطائلة الناتجة من ارتكاب الجرائم المعلوماتية وعلى وجه الخصوص جرائم الاحتيال المعلوماتي ، كثيراً ما تُغري مقترفها فتجعله يُقدم على ارتكابها وذلك من أجل سداد الديون المستحقة ، أو لحل مشاكل عائلية راجعة للنقود أو إدمان ألعاب القمار أو المخدرات ...الخ. [3]

(1) ذات المرجع السابق، ص 177.
(2) وليد الزيدي، مرجع سابق ذكره، ص 39.
(3) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره ، ص88.

ب. تحقيق الإثارة والمتعة والتحدي "دوافع شخصية":

يتمثل هذا الباعث في قهر النظام وحب المغامرة والإثارة وإثبات القدرة على اختراق التعقيدات التقنية والأنظمة الأمنية أكثر من الرغبة في تحقيق النفع المادي وكسب المال، مثل قيامهم باختراق مواقع الإنترنت والاستخدام غير المصرح به لأنظمة المعلومات، وذلك لما تثيره من تحدي عقلي وذهني لهم.[1]

ونجد بأن هذا الدافع يتزايد شيوعاً لدى فئات صغار السن من مرتكبي جرائم الكمبيوتر والإنترنت الذين يمضون وقتاً طويلاً أمام حواسيبهم الشخصية وذلك في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وبالتالي إظهار تفوقهم على وسائل التكنولوجيا مثل قيامهم بفك الشفرة أو الرقم السري. [2]

ج. الانتقام:

وقد يكون الباعث من وراء اقتراف جرائمهم هو الانتقام من غيرهم سواء كانوا من المنافسين لهم أو من رجال الأعمال، وذلك مثل قيامهم بجرائم إتلاف البيانات والبرامج وتدمير نظم المعلومات بمختلف الوسائل والطرق بما في ذلك زرع الفيروسات.[3]

والمثال على ذلك الموظفون الساخطون على أرباب أعمالهم في شركاتهم او مؤسساتهم فيلجأون إلى الثأر منهم وذلك مثلاً بالعودة إلى مواقع العمل بعد فترات العمل الرسمية أما لغرض سرقة المعلومات أو لغرض تخريب وإتلاف البيانات وإخفاء المعلومات المخزنة على الحواسيب الآلية. [4]

وبالإضافة إلى ما سبق فثمة دوافع أخرى، سياسية أو أيديولوجية أو تنافسية أو إرهابية وما شاكل ذلك.

---

(1) فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق ذكره، ص 31.
(2) عبدالله حسين علي محمود، مرجع سابق ذكره، ص 74-75.
(3) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 178.
(4) وليد الزيدي، مرجع سابق ذكره، ص 40.

الفرع الثالث

طوائف وفئات المجرم المعلوماتي

لا يمكن أن نحصر مرتكبي الجرائم المعلوماتية في طبقة أو فئة معينة أو جنس معين، فمرتكبها قد يكون من البالغين أو الأحداث والمتعلمين منهم أو المثقفين ومن الفقراء والأغنياء ومن الرجال أو النساء، ولا يمكننا أن نحصر جرائم الإنترنت في نوع معين من الجرائم فقد تكون من الجرائم الماسة بأمن الدولة من الداخل أو من الخارج وقد تكون من جرائم الاعتداء على الأشخاص أو جرائم الاعتداء على الأموال.[1]

ويقسم مجرمي المعلوماتية إلى مجموعة من الطوائف والفئات المختلفة، ولا يعني ذلك بطبيعة الحال أن كل مجرم يندرج تحت طائفة معينة دون غيرها بل يكون المجرم الواحد مزيجاً من أكثر من طائفة أو فئة.[2]

فيُصنف الباحثون مرتكب جرائم نظم المعلومات "مجرمي المعلوماتية" إلى الفئات التالية:

أولاً: القراصنة "Hackers"

1. الهواة "العابثين":

وهم الذين ليس لديهم سلطة أو حق شرعي في استخدام الحواسيب الآلية إلا أنهم مغرمون بالعبث ببرامجها وبياناتها، فيكون الباعث أو الدافع من وراء اختراق النظم المعلوماتية هو مجرد الفضول وحب المغامرة والتسلية في أغلب الأحيان، فلا تتوافر لديهم أي نية إجرامية مثل الحصول على معلومات معينة أو إتلافها...الخ. [3]

(1) علي جبار الحسيناوي، مرجع سابق ذكره، ص 48.
(2) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص179.
(3) وليد الزيدي، مرجع سابق ذكره، ص 40.

ويغلب على هؤلاء أنهم من صغار السن أو المراهقين ممن نبغوا في هذا المجال أو على الأقل توافر لديهم قدر من المهارة في استخدام هذه التقنية العالية، وفي الغالب لا يتوفر لدى هؤلاء أي دوافع حاقدة أو تخريبية "دوافع إجرامية" ، بخلاف غرهم من الطوائف الأخرى.[1]

ولكن هذه الفئة هي من أكثر المجموعات خطورة ، فيكمن هذا الخطر في احتمال تحول هذا العابث من مجرد هاوٍ صغير للأفعال غير المشروعة إلى محترف لأعمال السلب والاحتيال المعلوماتي. أو إمكانية احتضان منظمات أو أفراد غير شرفاء لهؤلاء الشباب واستغلالهم في ارتكاب العديد من الجرائم. [2]

فهم من الفضوليين والمراهقين المولعين بالشبكة العنكبوتية، حيث يدفعهم الفضول إلى معرفة كلمة سر بعض الأشخاص والدخول على نظامهم المعلوماتي.[3]

2. المحترفون "Crackers" :

تتميز هذه الفئة من مجرمي المعلوماتية بأن لديهم مهارة كبيرة وخبرة عالية بأنظمة الحاسوب والإنترنت. وهؤلاء يُعتبرون أكثر خطورة من الفئة السابقة، لأن كثيراً ما ينجم عن أفعالهم أضرار بالغة بالنظام المعلوماتي، وذلك بسبب ارتكابهم لجرائم التخريب والإتلاف للبرامج والمعلومات المخزنة على الحواسيب الآلية، وفي الغالب ما يكون هدفهم هو تحقيق الكسب المادي[4]. كما قد يؤلفون أندية لتبادل المعلومات فيما بينهم، وتعكس اعتداءاتهم ميولاً جرمية خطيرة.[5]

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 86.
(2) أحمد خليفة الملط، مرجع سابق ذكره، ص 117-118.
(3) محمود أحمد القرعان، مرجع سابق ذكره، ص 37.
(4) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت ، مرجع سابق ذكره، ص 86.
(5) علي جبار الحسيناوي، مرجع سابق ذكره، ص 49.

ثانياً: "المخادعون":

وهؤلاء يتمتعون غالباً بقدر عالٍ من المهارة وبقدرات وكفاءات فنية عالية باعتبارهم من الأخصائيين في نظم المعلومات، وجُل جرائمهم تتمثل في الاستيلاء على الأموال أو تحويلها بإساءة استخدام بطاقات الائتمان، مثل اعتراض أرقام بطاقات الائتمان وتزويرها أو سرقة قوائم الزبائن في المتاجر أو الفنادق أو غيرها. أو لغرض تخفيض الأسعار في الأسواق أو رفعها لنشر الفوضى في تلك الأسواق أو لشل موقع منافس. [1]

كما يقومون بالتلاعب بحسابات البنوك أو فواتير الكهرباء والتليفون وهذه الفئة من المجرمين لها موهبة خاصة في الاستحواذ على ثقة الناس، مما تلزمهم بالتفاني في العمل لتحقيق مصالح ورغبات هؤلاء الناس، فالغاية في وجهة نظرهم تبرر الوسيلة والاشتراك في أعمال غير شرعية يبررها توصلهم إلى إرضاء الناس. [2]

ثالثاً: الجواسيس:

وهم الذين يهدفون عادة إلى اختراق النظم المعلوماتية من أجل الحصول على بعض المعلومات والبيانات لمصلحة بعض الجهات كالشركات أو لفائدة دول معينة. [3]

رابعاً: الموظفون الحاقدون الساخطون:

وهم الذين تحركهم في العادة رغبة الانتقام من أرباب الأعمال الذين يعملون طرفهم [4]. فيقومون بالعودة إلى مواقع العمل في شركاتهم أو مؤسساتهم وذلك بعد فترات العمل الرسمية، إما

(1) وليد الزيدي، مرجع سابق ذكره، ص 41.
(2) عبدالله حسين علي محمود، مرجع سابق ذكره، ص 58.
(3) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت ، مرجع سابق ذكره، ص 87.
(4) ذات المرجع السابق، ص 87.

لغرض سرقة المعلومات أو لغرض التخريب وإتلاف البيانات واختفاء المعلومات المخزنة على الحواسيب الآلية. [1]

كما أن الغالبية من مرتكبي الجريمة المعلوماتية هم من العاملين بالمؤسسات التي تتعرض لهذه الجرائم، وهذا ما يُسهل لهم الأمر حيث يقومون بشكل أساسي بإدخال البيانات غير الصحيحة أو بالتلاعب ببيانات قائمة لإتمام العمل الإجرامي. [2]

خامساً: الفئة التي تعمل في مجال الجريمة المنظمة باستخدام الحواسيب الآلية:

وهم مجرمين في مجال الجريمة المنظمة ويستفيدون من أنظمة المعلومات في اقتراف جرائمهم وتسهيل ارتكابها والتخطيط لها [3]. فيعملون على استخدام الحاسب الآلي بشكل غير قانوني من أجل معرفة بعض المعلومات المتعلقة بأساليب أمنية معينة تنتهجها بعض المؤسسات التي يستهدفون السطو عليها وتنفيذ عملياتهم الإجرامية، ليسهل عليهم إتمام جرائمهم. [4]

سادساً: لصوص نظم المعلومات:

تعد هذه الفئة إحدى فئات الإجرام المعلوماتي وتعتبر ثمرة تكنولوجيا المعلومات الحديثة ونظم الاتصال الجديدة، ومع مرور الأيام زاد اقتحام هؤلاء المجرمين لنظم الاتصالات، ولم يتوقف هذا الاقتحام على التعدي المادي وإنما أمتد أيضاً إلى البرامج التي تتحكم في تشغيل تلك النظم وإن مرتكب هذه الجرائم ليس بالضرورة من ذوي الياقات البيضاء أو من أصحاب المهن، فالكثير منهم طلبة في الجامعات أو المدارس ولم يسبق القبض عليهم ، وهم مكتشفون غير شرعيين لتلك النظم ويبحثون عن الشهرة أو الحصول على المال. [5]

---

(1) وليد الزيدي، مرجع سابق ذكره، ص 40.
(2) نسرين عبدالحميد النبيه، مرجع سابق ذكره، ص 131.
(3) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت ، مرجع سابق ذكره، ص 87.
(4) وليد الزيدي، مرجع سابق ذكره، ص 40-41.
(5) عبدالله حسين علي محمود، مرجع سابق ذكره، ص 61-64.

المبحث الثاني

موقف القوانين الوضعية من القرصنة المعلوماتية

تمهيد وتقسيم:

لقد أجمع المتخصصون في تكنولوجيا المعلومات على أن أفعال الاختراق والقرصنة للنظام المعلوماتي، باتت تهدد الأمن القومي للدول، وهذه القضية هي ذات أبعاد أمنية وقانونية واجتماعية واقتصادية وسياسية، فرأت العديد من الدول أنّه لمواجهة هذه الاعتداءات على النظام المعلوماتي، لابد من سد الفراغ التشريعي بخصوص هذا الشأن، وذلك بإصدار التشريعات اللازمة للحماية من خطر مجموعات الهاكرز التي تقوم بعمليات تسلل واختراق للشبكات؛ لكشف الأسرار ومعرفة الخصوصيات وإتلاف المعلومات أو تزويرها عن طريق التنصت والتجسس، إضافة إلى الاستيلاء على أموال غيرهم بالتسلل لحساباتهم...الخ.[1]

وبالتالي يجب على كل الدول عدم الاتجاه إلى تطبيق أو تطويع التشريعات التقليدية القائمة على هذه الجرائم المعلوماتية المستحدثة لعدم كفايتها لمواجهة هذه النوعية من الجرائم العابرة للحدود، فكان لابد من رجال القانون الجنائي خاصة أن يهتموا بتنظيم المناخ القانوني وإعداده لمواكبة هذا التطور التكنولوجي وحماية الجديد في مجال الحاسب الآلي، ومنع العبث به، ومكافحة الإجرام الذي تولد عن هذا الاكتشاف العلمي الجديد. [2]

ولهذا فقد برزت العديد من التجارب والمحاولات وبأساليب مختلفة وذلك من أجل مكافحة هذه الظاهرة، ولعل من أبرز التجارب العربية في هذا الصدد تجربة دولة الإمارات والتي سنفرد لها

(1) محمد علي سكيكر، مرجع سابق ذكره، ص 136
(2).جميل عبدالباقي الصغير، مرجع سابق ذكره، ص 18-19.

فرعاً خاصاً بها، لما يمثله الواقع التشريعي المعلوماتي فيها من مثال أو نموذج متطور يمكن للدول العربية الأخرى الاستفادة من تجربتها في هذا المجال.

وذلك في المطلب الأول من هذا المبحث، ومن ثم ننتقل إلى محاولات وضع قوانين تعالج الجريمة المعلوماتية في بعض الدول الغربية مثل دولة الولايات المتحدة الأمريكية ودولة بريطانيا وفرنسا، فكانت هذه الدول هي السباقة في إصدار قوانين خاصة في هذا الشأن. وذلك في المطلب الثاني من هذا المبحث.

وعلى ضوء ذلك سنعرض في المطلب الأول: موقف بعض القوانين العربية وفي المطلب الثاني: موقف بعض القوانين غير العربية "التشريعات الغربية" في مكافحة القرصنة المعلوماتية.

المطلب الأول

موقف بعض القوانين العربية من القرصنة المعلوماتية

تقسيم:

سيتم استعراض موقف بعض القوانين العربية من القرصنة المعلوماتية وذلك من خلال الفروع الآتية:

الفرع الأول

موقف القانون المصري

تعتبر دولة مصر في بادئ الأمر من ضمن الدول العربية التي لم تعمل على سن قوانين جديدة خاصة بها في هذا المجال ولم تقم حتى بإدخال بعض التعديلات بهذا الخصوص على قانونها الجنائي القائم، وإنما كانت السلطة القضائية في مصر غالباً ما تحاول تطبيق قواعد القانون الجنائي التقليدية "الموضوعية والإجرائية" على الجرائم المعلوماتية وذلك عن طريق القياس، وهي تلك التي تفرض نوعاً من الحماية الجنائية ضد الأفعال المشابهة بالأفعال المكونة لأركان الجريمة المعلوماتية. [1]

فلم يكن يوجد نظام قانوني خاص يحكم هذه النوعية من الجرائم في دولة مصر العربية، وظلت هذه الجرائم مع ازدياد مخاطرها متروكة لاجتهاد الفقه والقضاء. [2]

والواقع أن القواعد القانونية التي يحاول الفقه والقضاء في مصر تطويعها لكي تنطبق على الجرائم المعلوماتية يمكن تقسيمها إلى طائفتين:

(1) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، د. ط، دار الفكر الجامعي، 2006م، ص191.

(2).جميل عبدالباقي الصغير، مرجع سابق ذكره، ص 18-19.

1. الطائفة الأولى:

وتشمل مجموعة القواعد التي يحتويها قانون العقوبات والخاصة بحرمة الحياة الخاصة أو النصوص الخاصة بالاعتداء على الأموال مثل السرقة وخيانة الأمانة والإتلاف العمدي وإفشاء الأسرار المهنية وغير ذلك من الأفعال التي قد تتشابه أركانها مع الأفعال التي قد ترتكب ضد نظم المعلوماتية وبرامج الحاسب الآلي. [1]

2. الطائفة الثانية:

وتشمل مجموعة من القواعد الموجودة خارج إطار قانون العقوبات ولكنها تقرر نوع من الحماية الجنائية ضد أفعال شبيهة بالأفعال المكونة للجريمة المعلوماتية، فيلجأ إليها القاضي في حسم المشاكل التي تنشأ عن الجرائم الموجهة ضد نظم وبرامج المعلوماتية، مثل: القوانين المتعلقة بحماية الملكية الفكرية والأدبية كالقانون رقم 82 لسنة 2002م في شأن حماية حقوق الملكية الفكرية متى وقعت الجريمة عن طريق الحاسب الآلي وشبكة الإنترنت، وحماية الحقوق الذهنية وحق المؤلف، وحماية الملكية الصناعية وحماية براءات الاختراع والرسوم والنماذج الصناعية[2].

وكذلك من بين هذه القوانين الخاصة:

1. مشروع قانون التجارة الإلكترونية المصري:

قد تضمن هذا المشروع نصوصاً تتعلق بتجريم الدخول بطريق الغش أو التدليس على نظام معلومات أو قاعدة بيانات أو قاعدة تتعلق بالتوقيعات الإلكترونية، دون اشتراط تحقيق نتيجة معينة

(1) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 207-271..
(2).ذات المرجع السابق، ص 271.

من جراء هذا الدخول، بل كل ما اشترطه أن يتم هذا السلوك إما بطريق الغش أو التدليس أو من خلال الاتصال غير المشروع أو الإبقاء على الاتصال الذي حدث بطريق الخطأ. [1]

كما عاقب هذا المشروع على استخدام نظام أو برنامج للحيلولة دون إتمام المعاملات التجارية بالوسائل الإلكترونية وذلك بالتعديل فيها أو محو بياناتها أو إفسادها أو تدميرها أو بتعطيل أنظمتها. [2]

فالمشرّع هنا حاول أن يوفر نوع من الحماية الجنائية ضد الإتلاف المعلوماتي وكذلك تناول الوسيلة الأخطر في الإتلاف المعلوماتي في هذا المشروع وهي الفيروسات ليجرم إدخالها للنظام المعلوماتي سواء كان الفعل بطريق العمد أو كان بطريق الخطأ. [3]

ولكن نلاحظ على هذا المشروع بأن الحماية الجنائية للنظام المعلوماتي فيه كانت قاصرة على نوع معين من المعلومات والبيانات وهي تلك التي تتعلق بالتجارة الإلكترونية والتوقيع الإلكتروني دون غيرها من المعلومات والبيانات.

2. القانون رقم "15 لسنة 2004" بشأن تنظيم التوقيع الإلكتروني:

قد ضم هذا القانون "30 مادة"، ويعني بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا للمعلومات وكان لصدور هذا القانون صدى واسع في حسم العديد من المشكلات القانونية ، والتي كان يتصدى لها القضاء بالاجتهاد والقياس، فجاء هذا القانون بتعريفات واضحة ومحددة لماهية المحرر الإلكتروني والوسيط الإلكتروني، وقد عاقب هذا القانون بالحبس وبالغرامة

(1) عبدالفتاح بيومي حجازي، مرجع سابق ذكره، ص 326.
(2) أيمن عبدالله فكري، مرجع ساقب ذكره، ص139.
(3) ذات المرجع السابق، ص 139.

أو بإحدى هاتين العقوبتين كل من أتلف أو عيب توقيعا أو وسيطاً أو محرراً إلكترونياً، أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر. [1]

كما جرم الحصول بأي وسيلة ومن دون وجه حق على توقيع أو وسيط أو محرر إلكتروني أو اختراق هذا الوسيط أو اعتراضه أو عطله عن أداء وظيفته. [2]

وكذلك المشرّع في هذا القانون لم يقتصر في التجريم على الشخص الطبيعي فقط بل اتجه إلى تجريم ومعاقبة الشخص المعنوي والمتمثل في الشخص المسؤول عن الإدارة الفعلية مادام فعله هو الذي أدى إلى ارتكاب الفعل المجرم، إلا أن هذا القانون كذلك كانت الحماية الجنائية فيه محصورة داخل نطاق التوقيع الإلكتروني والمحرر أو الوسيط الإلكتروني دون غيرها. [3]

إذاً ومن خلال ما سبق يتضح أن المشرّع المصري بهذه القوانين الخاصة لم يكفل حماية كاملة وشاملة للمعلومات والبيانات الإلكترونية ضد الكثير من الأفعال التي قد تكون محلها المعلومات مثل: الإتلاف وسرقة المعلومات وغيرها، أي أنه قد اقتصر على كفالة حماية جزئية للحق في سلامة المعلومات وعلى نطاق ضيق فكانت حمايته قاصرة على نوع معين من المعلومات ونظمها دون أن يشمل الأنواع الأخرى من المعلومات والبيانات بالحماية الجنائية من الإتلاف المعلوماتي بجميع صوره وأشكاله. [4]

ونتيجة لهذا القصور والفراغ التشريعي في مجال حماية ومكافحة جرائم تقنية المعلومات، فقد رأى المشرّع ضرورة إفراد تشريع مستقل يشتمل على تلك النوعية الحديثة من الجرائم ذات الأركان المادية الجديدة وغير المألوفة للقضاء الجنائي، فلا تختلط بغيرها من الجرائم التقليدية والتي

(1) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 282-283.
(2) عبدالفتاح بيومي حجازي، مرجع سابق ذكره، ص 343.
(3) أيمن عبدالله فكري، مرجع سابق ذكره، ص 142.
(4) ذات المرجع السابق، ص 142.

قد تكون وسيلة الاتصال الحديثة هي مجرد أداء لارتكابها ليس أكثر، فاستمرت المحاولات جاهدة لوضع مشروع قانون في شأن مكافحة جرائم تقنية المعلومات حتى "سنة 2015م" ، حيث وضع مشروع قانون بموجب قرار رئيس جمهورية مصر العربية بالقانون رقم "63" لسنة "2015" في شأن مكافحة جرائم تقنية المعلومات، حتى يواكب هذا المشروع التطور السريع والمتلاحق في عالم الجريمة الإلكترونية، والذي جاء وليداً للثورة التي حدثت في مجال الاتصالات وتكنولوجيا المعلومات في مصر وسائر دول العالم منذ بدء الألفية الجديدة.[1]

وهذا المشروع قد تضمن على "28 مادة" استهل بمادة لتعريف المصطلحات الأساسية الحديثة في مجال تكنولوجيا الاتصالات وتقنية المعلومات وتضمنت باقي مواد المشروع على مجموعة من جرائم تقنية المعلومات والتي لا يتصور وجودها من دون وسيلة الاتصال الحديثة سواء أكانت الحواسيب الآلية أو غيرها.[2]

وسنعرض للتوضيح بعض هذه المواد التي تضمنها هذا المشروع فقد نصت المادة "4" على أنه "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تتجاوز 30 ألف جنيه أو بإحدى هاتين العقوبتين كل من دخل إلى موقع أو نظام معلوماتي مستخدماً حقاً مخول له، فتعدى حدود هذا الحق من حيث ضرورة أو مستوى الدخول، فإذا وقعت الجريمة على موقع أو نظام معلوماتي يدار بمعرفة الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوك لها أو يخصها، يعاقب مرتكبها بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عند "50" ألف جنيه ولا تتجاوز "150" ألف جنيه.[3]

(1) مشروع قانون مكافحة جرائم تقنية المعلومات، متاح على الرابط: aitmagahram.or.eg.com ، تاريخ الزيارة 2016/12/30م.
(2) متاح على الرابط: Cybercrin<pdf<eipr.org تاريخ الزيارة 2020/10/2م.
(3) متاح على الرابط: Cybercrin<pdf<eipr.org تاريخ الزيارة 2020/10/2م.

فنجد أن المشرّع في هذه المادة قد جرم الدخول المجرد أي من دون اشتراط وقوع نتيجة معينة، إلا أنه قد قصر الدخول على من يستخدم حقاً يخول له ذلك ولكنه تعدى حدود هذا الحق، فضيق من نطاق التجريم، إلا أن الدخول قد يكون مشروع وقد يكون غير مشروع في الأساس كأن يقوم به من ليس له سلطة مشروعة مستمدة من القانون أو من صاحب الحق الشرعي في الدخول، مثل أن لا يأذن له بذلك.

كما نصت المادة "5" على أنه "يعاقب بالحبس مدة لا تقل عن سنتين كل من أتلف أو عطل أو دمر أو شوه أو غير أو عدل مسار، أو ألغى كلياً، أو جزئياً من دون وجه حق، البرامج أو البيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه أياً كانت الوسيلة التي استخدمت في الجريمة، فإذا كانت هذه البرامج أو البيانات أو المعلومات تخص الدولة أو أحد الأشخاص الاعتبارية العامة تكون العقوبة السجن".[1]

فهذه المادة قد تكلمت على الإتلاف المعلوماتي وقصرت العقوبة على الحبس فقط دون الغرامة، وشددت من مقدار العقوبة إذا وقعت هذه الجريمة على برامج أو بيانات تخص الدولة أو الأشخاص الاعتبارية، فقد اعتبرت هذا الأمر كظرف مشدد للعقاب. [2]

وكذلك نص المشروع في المادة "6" على أنه "يعاقب بالسجن وبغرامة لا تقل عن "50 ألف جنيه" ولا تتجاوز "250 ألف جنيه" كل من أدخل إلى شبكة معلوماتية ما من شأنه إيقافها عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو التنصت عليها أو اعتراض عملها، فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص

(1) متاح على الرابط: Cybercrin<pdf<eipr.org تاريخ الزيارة 2020/10/3م.
(2) متاح على ذات الرابط السابق.

الاعتبارية العامة أو تدار بمعرفتها تكون العقوبة السجن المؤبد أو المشدد وغرامة لا تقل عن "100 ألف جنيه" ولا تتجاوز "500 ألف جنيه".

وفي المادة "7" نص على أنه "يعاقب بالحبس مدة لا تقل عن ستة أشهر كل من التقط أو اعترض من دون وجه حق أية معلومات أو بيانات أو أرقام أو رسائل أو حروف أو شفرات أو صور، مما هو مرسل عن طريق شبكة معلوماتية، أو أحد أجهزة الحاسب الآلي وما في حكمها، أو تنصت عليها...".[1]

وأيضاً نصت المادة "8" على أنه "يعاقب بالحبس وبغرامة لا تقل عن "20 ألف جنيه" ولا تتجاوز "100 ألف جنيه" أو بإحدى هاتين العقوبتين كل من أتلف أو عطل أو أبطأ أو شوه أو أخفى أو غير تصاميم أو محتوى موقعاً خاصاً بشركة أو مؤسسة أو منشأة من دون وجه حق. فإذا وقعت الجريمة على موقع يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها أو يخصها تكون العقوبة السجن وغرامة لا تقل عن "100 ألف جنيه" ولا تتجاوز "500 ألف جنيه".[2]

والجدير بالذكر أن هذه النسخة من المشروع ليست هي النسخة الأخيرة فقد طرأت عليها بعض التغيرات والتعديلات، وقسم إلى أبواب وفصول، فنص في "الباب الثالث" منه على "الجرائم والعقوبات" ونص في "الفصل الأول" فيه على "الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات".

(1) مشروع قانون مكافحة جرائم تقنية المعلومات، متاح على الرابط aitmagahram.or.eg.com تاريخ الزيارة 2020/10/03م، الساعة 8:00 م.

(2) ذات المرجع السابق، تاريخ الزيارة 2017/01/01م، الساعة 09:00 م.

فنجد أن المادة "16" "جريمة الدخول غير المشروع"، في المشروع المُعدل هي ذات المادة "4" في المشروع السابق، فنصت على أنه "يعاقب بالحبس مدة لا تقل عن سنة وغرامة لا تقل عن "50 ألف جنيه" ولا تتجاوز "100 ألف جنيه"، أو بإحدى هاتين العقوبتين كل من دخل عمداً أو دخل بالخطأ غير العمدي وبقى من دون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه، فإذا نتج عن ذلك إتلاف أو محو أو تغير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي تكون العقوبة الحبس لمدة لا تقل عن سنتين وبغرامة لا تقل عن "100 ألف جنيه" ولا تتجاوز "200 ألف جنيه" أو بإحدى هاتين العقوبتين.[1]

فنجد أن المشرّع في هذا التعديل قد رفع من سقف عقوبة الغرامة عن سابقها، ورفع كذلك من مقدار العقوبة السالبة للحرية في حالة ما ترتب على الدخول غير المشروع إتلاف أو محو أو تغيير...الخ.

كما نص على الدخول أو البقاء في النظام المعلوماتي سواء أكان قد تم هذا الدخول بطريق العمد أو بطريق الخطأ، كما عُدلت المادة "5" بنص المادة "19" جريمة "الاعتداء على سلامة الأنظمة المعلوماتية"... فنصت على أنه "يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 200 ألف جنيه ولا تتجاوز 500 ألف جنيه كل من أتلف أو عطل أو دمر أو زور أو شوه أو غير أو عدل مساراً أو ألغى كلياً أو جزئياً من دون وجه حق، البرامج والبيانات أو المعلومات المخزنة

(1) مشروع قانون مكافحة جرائم تقنية المعلومات، متاح على الرابط aitmagahram.or.eg.com تاريخ الزيارة 2020/10/03م، الساعة 8:00 م..

أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه أياً كانت الوسيلة التي استخدمت في الجريمة".[1]

فالمشرّع في هذه المادة قد أبقى على نفس مقدار العقوبة السالبة للحرية ولكنه أضاف عقوبة الغرامة لها.

وكذلك المادة "18" هي نفسها المادة "7" في نسخة المشروع السابقة فنصت المادة "18" تحت عنوان جريمة "الاعتراض غير المشروع" على أنه "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 100 ألف جنيه ولا تتجاوز 250 ألف جنيه كل من اعترض من دون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها".[2]

نجد أن المشرّع قد رفع من سقف العقوبة السالبة للحرية وأضاف عقوبة الغرامة إليها، وهذا النهج كان أفضل من سابقه.

(1) نشر نص قانون مكافحة جرائم الإنترنت "الحق والضلال" متاح على الرابط: www.christian-dogma.com ، تاريخ الزيارة 2017/01/01م ، الساعة 10:00 م .

(2) متاح على الرابط، ذات المرجع السابق، ونفس تاريخ الزيارة.

الفرع الثاني

موقف القانون العماني

تعتبر دولة عُمان من ضمن الدول العربية القليلة التي تطرقت إلى مواجهة الإجرام المعلوماتي، وذلك عن طريق إدخال بعض التعديلات الطفيفة على قانونها رقم "7" لسنة "1974م" وذلك بموجب المرسوم السلطاني رقم "2001/72م" ، وقد تضمن هذا التعديل إضافة الفصل الثاني مكرر إلى الباب السابع تحت عنوان جرائم الحاسب الآلي، حيث اشتمل على عدة مواد مستحدثة، وهي نص المادة "276" مكرر "1" و "276" مكرر "2" و "276" مكرر "3" و "276" مكرر "4".[1]

وذلك تعبيراً عن إرادة المشرّع ورغبةً منه في مواكبة التطور السريع لتكنولوجيا المعلومات وشبكات الاتصال ، فجرم 10 صور جرمية في المادة "276" مكرر "1" متى استخدم الحاسب الآلي في ارتكابها عن عمد وهي تشمل: الالتقاط غير المشروع للمعلومات أو البيانات، الدخول غير المشروع على أنظمة الحاسب الآلي، التجسس والتنصت على البيانات والمعلومات، انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم، تزوير البيانات أو الوثائق مبرمجة أياً كان شكلها، إتلاف وتغيير ومحو البيانات والمعلومات، جمع المعلومات والبيانات وإعادة استخدامها، تسريب المعلومات والبيانات، التعدي على برامج الحاسب الآلي بالتعديل أو الاصطناع، نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين الملكية الفكرية والأسرار التجارية، وكذلك جرم الاستيلاء أو الحصول على نحو غير مشروع على بيانات شخص آخر تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات.[2]

(1) حمزة محمد أبو عيسى، مرجع سابق ذكره، ص 22.
(2) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق ذكره، ص 94.

وقد شدد المشرّع العقوبة بموجب المادة "276" مكرر "2" في حالة ما يكون مرتكب الجرائم السابقة من مستخدمي "الحاسوب أو الكمبيوتر".[1]

كما جرمت المادة "276" مكرر "3" ثلاث صور من صور الاعتداء على بطاقات الوفاء أو السحب تمثلت في تقليد أو تزوير بطاقات الوفاء، استخدام أو محاولة استخدام بطاقات الوفاء المزورة أو المقلدة مع العلم بذلك، قبول الدفع ببطاقات الوفاء المقلدة أو المزورة مع العلم بذلك، والعقوبة المقررة للأفعال السابقة تتمثل في السجن بحد أقصى خمس سنوات وغرامة مالية بحد أقصى ألف ريال عُماني. [2]

وقام المشرّع من خلال المادة "276" مكرر "4" بالنص على نوع آخر من التشديد شدد فيها العقوبة الأصلية لتصل إلى السجن بحد أقصى ثلاث سنوات والغرامة ثلاثة آلاف ريال وذلك في حالة تم ارتكاب الأفعال المنصوص عليها في المادة "276" مكرر "3" من قبل المتهم بمناسبة أداء عمله أو أثناء عمله. [3]

والجدير بالتنويه هنا بأن هذه الخطوة من قبل المشرّع العماني كانت بداية وخطوة جيدة ومحاولة جادة منه لبسط الحماية الجنائية للنظام المعلوماتي، خاصةً بالمقارنة مع غيره من التشريعات العربية الأخرى التي لم يطرأ على قوانينها أي تعديل يذكر بالخصوص ومنها القانون الليبي. [4]

إلا أن هذه النصوص تظل غير كافية، فهناك الكثير من الأفعال الخطيرة لم يتضمنها التعديل السالف الذكر، فلم يواجه جميع صور إساءة استخدام تقنية المعلومات، فنجد أنه نص على

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق ذكره، ص 204.
(2) ثقافة قانونية – جهود سلطنة عمان في مكافحة جرائم تقنية المعلومات، متاح على الرابط : hussain-alghafri.blogspot.com تاريخ الزيارة: 2017/01/03م، الساعة 9:20 م.
(3) متاح على الرابط hussain-alghafri.blogspot.com /2012/01/blog-spot25html ، تاريخ الزيارة 2014/09/14م.
(4) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ذكره، ص 95.

بعض صور جرائم الخصوصية أو انتهاك حرية الشخص في بياناته الخاصة المعالجة آلياً، ولم ينص على بقية صور الاعتداء على الخصوصية مثل نقل البيانات دون إذن أو استغلالها في نشاط غير المعد له.[1]

كما أن المادة "276" مكرر "1" قد نصت على تجريم صور إضافية وهي الاستيلاء على البيانات ولكنها لم تنص على سرقة وقت الحاسب الآلي أو "الكمبيوتر" أو صور أخرى متصلة بتعطيل عمل الأنظمة الإلكترونية، وأيضاً لم تتضمن النصوص السابقة الاحتيال المعلوماتي وإن كانت قد تضمنت بعض صوره من الناحية الفنية وكذلك المادة "276" مكرر "4" قد عالجت ثلاث صور من صور إساءة استخدام بطاقات الوفاء الإلكترونية، ولكن يؤخذ على هذا النص تقيده بمصطلحات مقيدة وضيقة في حين كان يمكنه أن يكون أكثر اتساعاً وشمولاً حين يجرم صور الاعتداء المذكورة على كل أنواع البطاقات منعاً للدفع بأن البطاقة محل الاعتداء ليست بطاقة وفاء. [2]

ومن هذا المنطلق سارع المشرّع العماني إلى إصدار تشريع خاص لمواجهة هذه الفئة من الإجرام المستحدث، وذلك بغض النظر عن سلسلة التشريعات العمانية الخاصة ذات العلاقة بهذا الموضوع مثل قانون تنظيم الاتصالات رقم "2002/30م" وقانون المعاملات الإلكترونية رقم "2008/69م"، فكل هذه القوانين الخاصة لم تعد مواكبة لمواجهة ذلك التطور المتزايد لهذه النوعية من الإجرام، لذا قام المشرّع بإصدار قانون "مكافحة جرائم تقنية المعلومات" رقم "2011/12م". الصادر في 2011/02/06م تضمن "35" مادة والذي نص مرسوم إصداره صراحة في مادته

(1) يونس عرب، الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وسلطنة عمان، ورقة عمل، هيئة تنظم الاتصالات، مسقط، سلطنة عمان، الأردن، 2-4 أبريل 2006م، ص 34.

(2) ذات المرجع السابق، ص35.

الثانية على إلغاء الفصل الثاني مكرر من الباب السابع من قانون الجزاء العماني المشار إليه سابقاً، كما يُلغى كل ما يُخالف هذا القانون أو يتعارض مع أحكامه.[1]

ويتكون هذا القانون من "سبعة فصول" عالج "الفصل الأول" منه "التعريفات والأحكام العامة" أما "الفصل الثاني" فعالج موضوع "التعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية والنظم المعلوماتية"، بينما يختص "الفصل الثالث" من هذا القانون بموضوع "إساءة استخدام وسائل تقنية المعلومات" وجاء "الفصل الرابع" ليجرم "التزوير والاحتيال المعلوماتي"، أعقبه "الفصل الخامس" والذي خصص "للجرائم الخاصة بالمحتوى"، في حين أفرد "الفصل السادس" منه لموضوع "التعدي على البطاقات المالية" وفي النهاية خصص "الفصل السابع" لبيان الأحكام الختامية لهذا القانون. [2]

وسنعرض بعض مواد هذا القانون العماني مثل المادة "الثانية" من "الفصل الثاني" المتعلق "بالتعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية والنظم المعلوماتية".

فقد نصت على أنه " يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين ، كل من دخل عمداً ودون وجه حق موقعاً إلكترونياً أو نظاماً معلوماتياً أو وسائل تقنية المعلومات أو جزءاً منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك.[3]

(1) حمزة محمد أبو عيسى، مرجع سابق ذكره، ص 22.
(2) مصطفى السيد علي بلاس، رئيس محكمة، وخبير قانوني، ملامح قانون مكافحة جرائم تقنية المعلومات، متاح على الرابط: 2015.omandaily.com تاريخ الزيارة : 2017/02/20م.
(3) مرسوم سلطاني رقم 2011/12 في شأن إصدار قانون مكافحة جرائم تقنية المعلومات، متاح على الرابط qanoon.0m.com قانون، تاريخ الزيارة 2020/10/4م، الساعة 12:00 م.

فإذا ما ترتب على ما ذكر في "الفقرة الأولى" إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات، أو إلحاق ضرر بالمستخدمين أو المستفيدين، تكون العقوبة السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين، كما شدد المشرّع من العقوبة فرفعها إلى السجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات، وغرامة لا تقل عن ألف ريال عماني ولا تزيد على عشرة آلاف ريال عماني أو بإحدى هاتين العقوبتين على كل من ارتكب أحد الجرائم المنصوص عليها في المادة سالفة الذكر أثناء أو بمناسبة تأدية عمله.[1]

ونلاحظ بأن المشرّع قد نص في المشروع المصري السالف الذكر في شأن "مكافحة جرائم تقنية المعلومات" على ذات الموضوع وذلك في المادة "16" منه.

ولكن اتجاه المشرّع المصري كان أشد حزم من المشرّع العماني ، بحيث نص على عقوبة أشد بخصوص جريمة "الدخول غير المشروع" عنها في القانون العماني، وذلك سواء فيما يتعلق بالعقوبة المقيدة للحرية أو الماسة بالذمة المالية أي "السجن أو الحبس والغرامة".

واتفقا على نفس محتوى ظرف التشديد إذا ما ترتب عن ذلك الدخول "إلغاء أو تغيير أو تعديل...الخ"، إلا أن الاختلاف كان كذلك في مقدار التشديد، فكان مقداره مرتفع بالمقارنة مع مقدار التشديد في القانون العماني.

وكما جرم القانون العماني في المادة "6" كل من دخل عمداً ومن دون وجه حق موقعاً إلكترونياً أو نظاماً معلوماتياً بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية

(1) مرسوم سلطاني رقم 2011/12 في شأن إصدار قانون مكافحة جرائم تقنية المعلومات، متاح على الرابط qanoon.0m.com قانون، تاريخ الزيارة 2020/10/4م، الساعة 5:30 م

وعاقب عليها بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحداهما.[1]

ورفع من مقدار العقوبة إذا ما ترتب على هذا الفعل تغيير أو إلغاء أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر البيانات أو المعلومات الإلكترونية، فجعل من ذلك ظرف تشديد للعقوبة، فنجد أن المشرّع العماني قد اتخذ اتجاه موسع في تحديد محل جريمة الاختراق بأن جعله يشمل بالإضافة إلى المواقع الإلكترونية، الأنظمة المعلوماتية.[2]

وكذلك قام بتجريم الاعتراض عمداً ومن دون وجه حق وباستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات المرسلة عبر الشبكة المعلوماتية أو قطع بثها أو تنصت عليها أو إدخال ما من شأنه إيقاف أو تعطيل العمل في النظام المعلوماتي أو إتلاف أو تشويه أو تدمير البرامج والبيانات، وكما جرم التزوير المعلوماتي وذلك بتغيير الحقيقة في البيانات أو المعلومات وذلك بالإضافة أو الحذف أو الاستبدال لتحقيق منفعة لنفسه أو لغيره أو إلحاق ضرر بغيره.

وكذلك قام المشرّع العماني بإفراد حكماً خاصاً لاستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات مثل الهواتف النقالة المزودة بآلة تصوير في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بالتقاط صور أو نشر أخبار أو تسجيلات صوتية أو مرئية تتصل بها ولو كانت غير صحيحة أو في التعدي على غيرنا بالسب والقذف، كما جرم إنشاء موقع إلكتروني لتنظيم إرهابي، أو استخدام الشبكة المعلوماتية لأغراض إرهابية أو في عملية غسل الأموال أو الاتجار بالبشر أو في الأعضاء البشرية أو في الأسلحة...الخ.[3]

(1) متاح على الرابط: polick www.mohe.gov.om تاريخ الزيارة 2020/10/4م، الساعة 6:20م.
(2) حمزة محمد أبو عيسى، مرجع سابق ذكره، ص 35.
(3) قانون جرائم تقنية المعلومات، قوانين وإجراءات سلطنة عمان موافدين، مرسوم السلطاني رقم 2011/12م متاح على الرابط http"//m.facebook.com/permalink تاريخ الزيارة 2017/1/4م، الساعة 5:30م.

وكذلك جرم تزوير بطاقة مالية وعاقب كل من استولى على بيانات بطاقة مالية أو استعمل أو قدمها لغيره أو سهل له الحصول عليها أو استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في الوصول دون وجه حق إلى أرقام أو بيانات بطاقة مالية أو قبل بطاقة مالية مزورة وهو عالم بذلك، وذلك بقصد الاستيلاء أو تسهيل الاستيلاء على أموال غيره أو ما تتيحه البطاقة من خدمات، كما أفرد نصوصاً خاصة بمعاقبة الشخص المعنوي إذا ارتكبت باسمه أو لحسابه وبغرامة تعادل ضعف الحد الأعلى لعقوبة الغرامة المقررة قانوناً للجريمة في حال ارتكبها الشخص الطبيعي.[1]

أما بالنسبة للعقوبات في هذا القانون فكانت العقوبات الأصلية هي السجن لحد أدنى شهر ولا تزيد على خمس سنوات وغرامة لا تقل عن ألف ريال عماني ولا تزيد على عشرة آلاف ريال عماني، أما العقوبات التكميلية في هذا القانون ، فقد تضمن العديد منها مثل مصادرة جميع الأجهزة والأدوات والبرامج وغيرها مما استعمل في ارتكاب الجرائم المعلوماتية، وكذلك الأموال المتحصلة منها، وغلق الموقع الإلكتروني والمحل الذي ارتكبت فيه الجريمة أو الشروع فيها إذا ارتكبت بعلم مالكه وعدم اعتراضه، وطرد الأجنبي المحكوم عليه بعقوبة إرهابية أو بعقوبة تأديبية إذا كانت الجريمة معلوماتية مسيئة للمجتمع. [2]

(1) قانون جرائم تقنية المعلومات، قوانين وإجراءات سلطنة عمان للوافدين، المرسوم السلطاني رقم 2001/12م متاح على الرابط: https://m.facebook.com/permalink تاريخ الزيارة : 2017/01/08م، الساعة : 10:30 م.

(2) ذات الرابط، ونفس تاريخ الزيارة.

الفرع الثالث

موقف القانون الإماراتي

في بادئ الأمر دولة الإمارات العربية لم تُصدر تشريعاً خاصاً بجرائم تقنية المعلومات، مما جعل القُضاة يلجأون إلى تطويع بعض نصوص قانون العقوبات العام على القضايا التي تُعرض أمامهم والمتعلقة بإساءة استخدام شبكة الإنترنت وتكنولوجيا المعلومات.

ولكن بعد ارتفاع معدل ارتكاب مثل هذا النوع من الإجرام المعلوماتي واتجاه الحكومة إلى إدخال وتطبيق فكرة الحكومة الإلكترونية ومباشرة العمل بها على مستوى جميع الإدارات في إمارة دبي بشكل خاص وإنشاء مدينة دبي للإنترنت، تم تكليف لجنة خاصة من وزارة العدل لتعديل قانون العقوبات الاتحادي رقم "3" لسنة "1987م" ليواكب المستجدات ، فقامت هذه اللجنة بإضافة فصل جديد إلى فصول الباب الثامن من الكتاب الثاني ليجرم الأفعال المشار إليها بعنوان "الجرائم الواقعة على الحاسوب" في الفصل الثاني مكرر وكان يحتوي هذا الفصل على أربع مواد مكررة بأرقام "403" مكرراً "1" و "403" مكرراً "2" و "403" مكرراً "3" ومكرراً "4".[1]

وتعاقب هذه النصوص على عدة أفعال منها: الدخول إلى جهاز أو نظام أو شبكة حاسوب بغرض الحصول على معلومات أو تغييرها أو حذفها، وتشدد العقوبة في حالة استعمالها للحصول على مال أو خدمة أو منفعة، وكذلك عاقبت كل من قام عمداً بنقل أو إرسال برنامج معلومات أو شفرة أو أمر إلى جهاز أو نظام شبكة حاسوب بقصد إحداث تلف في ذلك الجهاز أو النظام أو

(1) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، د. ط.، دار النهضة العربية، القاهرة، د. ت.، ص 12.

المعلومات أو البيانات أو البرامج المخزنة عليها، وشدد العقوبة في حالة اتجاه إرادته إلى توقف الشبكة أو الحاسوب أو النظام المعلوماتي عن العمل.[1]

كما نصت هذه المواد على جريمة إتلاف المعلومات أو البيانات أو البرامج المخزنة في جهاز أو نظام أو شبكة حاسوب بطريق الخطأ مما أدى إلى توقف عمل ذلك النظام أو الشبكة عن العمل.[2]

أما عن العقوبات فكانت تتراوح ما بين السجن والحبس حده الأدنى ستة أشهر وحده الأقصى خمس سنوات، بينما عقوبة الغرامة فلم ينص عليها إلا في نص المادة الأخيرة "403" مكرراً "4" في صورتها الخطائية، فنص على المعاقبة بالحبس وبالغرامة أو بإحدى هاتين العقوبتين من تسبب بخطئه في إتلاف معلومات أو بيانات أو برامج مخزنة في جهاز أو نظام أو شبكة حاسوب أو أفضى فعله إلى توقف ذلك النظام أو الشبكة عن العمل.[3]

إلا أن هذا التعديل قد وجهت إليه انتقادات كثيرة من القانونيين الذين وجدوا فيه أنه مواجهة ضعيفة لجرائم الإنترنت، ولا يتناول سوى جزء بسيط من هذه الجرائم، الأمر الذي حدا بالمشرّع إلى إيجاد بديل لذلك، فتم إعداد مشروع قانون اتحادي لمكافحة جرائم تقنية أنظمة المعلومات وهو القانون رقم "2 لسنة 2006م" جاء في "29 مادة"، وكانت بهذا المشروع أول دولة عربية بادرت بإصدار تشريع خاص بهذا النوع من الإجرام المستحدث، فبدأ هذا القانون بتعريفات لكلمات وعبارات وردت فيه تجنباً لما قد تثيره من خلاف على تفسيرها، وكما تناول معظم الجرائم التي قد تنشأ عن التقنية الحديثة وبالأخص الإنترنت. [4]

(1) ذات المرجع السابق، ص 12.
(2) محمد عبيد الكعبي، مرجع سابق ذكره، ص 13- 14.
(3) ذات المرجع السابق، ص 14.
(4) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق ذكره، ص 96.

فجرم تقريباً كل صور إساءة استخدام الحاسب الآلي والإنترنت، حيث ركز بصورة أساسية على حماية الشبكات المعلوماتية مما قد يستهدفها من اعتداءات من قبل مستخدميها لتعطيلها أو اختراق البيانات أو المعلومات المخزنة بها أو التلاعب بها على أي وجه كان، لذا فقد جرم هذا القانون اختراق النظم المعلوماتية للوصول إلى البيانات أو المعلومات السرية من دون وجه حق، وتزوير مستندات الحكومة الاتحادية والمتعلقة بالهيئات والمؤسسات العامة م4، وإعاقة الوصول إلى الخدمة بتعطيل الشبكة أو تدمير أو إتلاف أو حذف أو تعديل البرامج أو البيانات أو المعلومات المخزنة بها، وهذا هو ما نصت عليه المادتان "5، 6" من هذا المشروع. [1]

وقد اعتبر المشرّع ظروفاً مشددة، أن يترتب على فعل الولوج أو الاختراق إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات.[2]

كما أفرد حكماً خاصاً لتعديل أو إتلاف الفحوص الطبية والتشخيص أو العلاج الطبي تقديراً من المشرّع لما يمكن أن يترتب على ذلك من أضرار فادحة بسلامة المرضى، ولم يكتفِ بذلك، بل حظر التنصت أو التقاط أو اعتراض كل ما هو مرسل عبر الشبكة المعلوماتية بدون وجه حق وذلك في المادة "8" منه. [3]

وكذلك جرم استخدام الشبكة المعلوماتية في ارتكاب بعض الجرائم الخطيرة كالتهديد والابتزاز أو الاستيلاء على الأموال والمستندات بطريقة احتيالية والوصول إلى أرقام أو بيانات البطاقة الائتمانية أو غيرها من البطاقات الإلكترونية، وقد قرر هذا المشروع مجموعة من الجزاءات

(1) دولة الإمارات العربية المتحدة، قانون مكافحة جرائم تقنية المعلومات، شبكة المعلومات القانونية، متاح على الرابط: www.gcc-legal.org>LawASPPF>Law تاريخ الزيارة: 2017/01/10م، الساعة 11:00م.

(2) عبدالفتاح بيومي حجازي، مرجع سابق ذكره، ص 344.

(3) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 96-97.

من أجل زجر مرتكبي الأفعال المذكورة وهي تتراوح بين الحبس والغرامة أو الاكتفاء بأي منهما وذلك بالنسبة لجل الجرائم الواردة فيه. [1]

وهناك طائفة أخرى من صور التجريم نجد أن المشرّع الإماراتي قد واجهها بعقوبات مغلظة نوعاً ما بحيث تصل إلى السجن لوحده أو بإضافة الغرامة إليه، كما عزز حمايته لنظم المعلومات بالنص على بعض التدابير والعقوبات التكميلية الأخرى، ومنها مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، وإغلاق المحل كلياً أو مؤقتاً للمدة التي تقدرها المحكمة أو الموقع الذي يرتكب فيه أي من هذه الأفعال المذكورة. [2]

كما أن هذا القانون في سبيل تسهيل كشف الجرائم المنصوص عليها فيه وضبط مرتكبيها وتعقبهم، قام بإضفاء صفة مأموري الضبط القضائي على بعض الموظفين الذين يصدر بتحديدهم قرار من وزير العدل والشؤون الإسلامية والأوقاف وذلك في المادة "27" منه. [3]

إلا أن هذا القانون وإن كان في السنوات الماضية أي في وقت صدوره نموذجاً كان ينبغي أن تقتدي به باقي الدول العربية في تجريم كل الأفعال الناجمة عن سوء استخدام الشبكة المعلوماتية بجميع صورها وأشكالها، وذلك لكي تتماشى مع التطور التكنولوجي، إلا أن الواقع العملي قد أثبت قصور هذا القانون على مواكبة التطورات السريعة والمخاطر الناجمة عن هذا التقدم المذهل في وسائل التقنية الحديثة وظهور نوعية معينة من الجرائم التي لم يشملها هذا القانون

(1) عصام عبدالفتاح مطر، التشريعات الإلكترونية الدولية والعربية، د.ط. المكتب الجامعي الحديث، 2010م، ص860.
(2) ذات المرجع السابق ، 858-864..
(3) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق ذكره، ص 94-95.

بالمعالجة، وهذا الأمر هو الذي دفع المشرّع إلى إلغائه واستبداله بالمرسوم بقانون اتحادي رقم "5" لسنة "2012م" في شأن "مكافحة جرائم تقنية المعلومات".[1]

واشتمل هذا القانون على "51" مادة، نص في مادته "الأولى" على عدد من التعريفات وفي المادة "الثانية" نص جريمة اختراق موقع إلكتروني أو نظام معلوماتي بدون تصريح أو تجاوز حدود التصريح أو البقاء فيه بصورة غير مشروعة، وحدد في هذا القانون قيمة الغرامة بأن لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم وأبقى على نفس العقوبة السابقة في قانون رقم "2" لسنة "2006م" وهي "الحبس والغرامة" أو بإحداهما إلا أنه حدد قيمة الغرامة فرفع من السقف الأدنى لعقوبة الغرامة في كل الفقرات الثلاثة السابقة، كما شدد من العقوبة إذا ما ترتب على ذلك إتلاف أو إلغاء أو تعديل...الخ.[2]

وقد تضمن هذا المرسوم العديد من المواد التي من شأنها توفير الحماية القانونية لخصوصية ما يتم نشره وتداوله على الشبكة المعلوماتية من معلومات وبيانات وأرقام تتعلق بالبطاقات الائتمانية وأرقام وبيانات الحسابات المصرفية أو أية وسيلة من وسائل الدفع الإلكتروني، وكذلك جرم كل استخدام لأي من وسائل تقنية المعلومات في تزوير أو تقليد أو نسخ البطاقات الائتمانية أو البطاقات المدنية، وكذلك يُعاقب بموجب هذا القانون كل من أبتز أو هدد شخصاً آخر لحمله على القيام بفعل معين أو الامتناع عنه، وذلك باستخدام شبكة معلوماتية أو أي وسيلة من وسائل تقنية المعلومات.[3]

(1) جمال الدين كرابيج، بحث "الجريمة المعلوماتية" 2010- 2011 م متاح على الرابط vle.gov.sy>indexphp تاريخ الزيارة 207/02/08م، الساعة 12:00م.

(2) ذات المرجع السابق، نفس تاريخ الدخول.

(3) متاح على الرابط: www.emaratalyoum.com تاريخ الزيارة 2020/10/03م، الساعة 9:20م.

كما عاقب بموجب المادة "21" منه كل من استخدم شبكة معلوماتية أو إحدى وسائل تقنية المعلومات في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً، سواء تم هذا الاعتداء عن طريق استراق السمع أو اعتراض أو تسجيل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية، أو التقاط صور للغير أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها أو نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة ودقيقة، وكذلك عاقب على غسل الأموال والترويج للإرهاب بواسطة استخدام وسائل تقنية المعلومات. [1]

وقد تضمن هذا المرسوم بقانون اتحادي رقم (5) لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات على عدد من العقوبات الأصلية تصل إلى السجن والغرامة التي لا تتجاوز مبلغ 2 مليون درهم، كما عاقب على الشروع في الجنح المنصوص عليها في المرسوم بقانون ينصف العقوبة المقررة للجريمة التامة، فإن هذه التعديلات الجديدة على القانون تعتبر مغلظة تتضمن عقوبات رادعة على مرتكبيها ومنها الجرائم الماسة بأمن الدولة، وكذلك اشتمل على عدداً من العقوبات التكميلية، فنص على سلطة المحكمة في مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من هذه الجرائم، وكذلك إغلاق المحل أو الموقع الذي ارتكبت فيه الجريمة إغلاقاً كلياً أو لمدة محددة، بالإضافة إلى إبعاد الأجنبي الذي يحكم عليه بأي من هذه الجرائم وذلك بعد تنفيذ العقوبة.[2]

كما يجوز للمحكمة أن تأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه من استخدام شبكة المعلومات أو النظام المعلوماتي الإلكتروني ووضعه في مأوى علاجي أو مركز

(1) بشأن تعديل الرسوم بقانون اتحادي رقم (5) لسنة 2012م في شأن مكافحة تقنية المعلومات، متاح على الرابط ArtclesDetails<site.eastLaws.com. تاريخ الزيارة 2020/10/4م، الساعة 8:00 م

(2) متاح على الرابط: www.albayanae/across.the-uae/assident. تاريخ الزيارة : 2017/02/19م، الساعة: 11:00م.

تأهيل للمدة التي تراها المحكمة مناسبة، كما أنه بناءً على طلب من النائب العام للمحكمة أن تقضي بتخفيف العقوبة أو الإعفاء منها عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقاً لأحكام هذا المرسوم متى أدى ذلك إلى الكشف عن الجريمة ومرتكبها وإثباتها عليهم أو القبض على أحدهم. [1]

(1) متاح على الرابط: www.hrw.org>news تاريخ الزيارة 2020/10/05م، الساعة 10:00 ص.

الفرع الرابع

موقف القانون الليبي

نستخلص من موقف بعض القوانين العربية بصدد موضوع القرصنة المعلوماتية، بأنها قد سدت بعض العجز الملحوظ في مجال المعلوماتية، واتجهت سياستها التشريعية إلى الحد من هذه الظاهرة الإجرامية الحديثة، ففي بداية محاولتها للحد من هذه الظاهرة ومكافحتها، قمت بعض الدول مثل دولة الإمارات العربية المتحدة وسلطنة عمان بإدخال بعض التعديلات الجزئية في تشريعاتها الجنائية القائمة، بما يكفل توفير الحماية المناسبة ضد التحديات الجديدة التي ظهرت مع شيوع استخدام هذه التكنولوجيا الحديثة.

ثم خطت بعض ذلك خطوات متقدمة في هذا المجال، فمثلاً قام المشرّع الإماراتي والعماني بسن تشريع جنائي خاص في شأن مكافحة جرائم تقنية المعلومات، كما وضع مشروع قانون بموجب قرار رئيس جمهورية مصر العربية بالقانون رقم (63) لسنة 2015م في شأن مكافحة جرائم تقنية المعلومات، وذلك لمواكبة التطور السريع في مجال تكنولوجيا المعلومات.

وفي المقابل ثمة طائفة أخرى من الدول في طريقها إلى إصدار تشريعات مماثلة في هذا الخصوص، ويعمل القضاء فيها على تطويع قوانينها النافذة بحيث يجري تطبيقها على الأفعال التي تمثل إساءة استخدام الحاسوب الآلي أو الإنترنت، وهذه الطائفة الأخيرة تشمل أغلب الدول العربية وكذلك جل دول العالم الثالث.[1]

وعلى رأسها دولة ليبيا، فنجد أن المشرّع الليبي لم يقم بأي خطوة إيجابية ومتقدمة حتى وقتنا الحاضر في مجال تجريم الاعتداءات الواقعة على النظم المعلوماتية.

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 92.

بالرغم من أن الجريمة المعلوماتية هي ظاهرة إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم منها على كافة المستويات الاقتصادية والاجتماعية والثقافية والأمنية، كما أن أي تطور تقني له انعكاساته على المستوى القانوني بصفة عامة، وفي إطار القانون الجنائي على وجه الخصوص، فالجريمة المعلوماتية قد تحولت إلى ظاهرة عالمية يصعب التحقق من وقوعها، كما يصعب القبض على مرتكبها، ولو قُبض عليه قد يصعب محاكمته لعدم توفر أدلة مادية أو شهود، بالإضافة إلى التطور السريع والمستمر في تقنيات النظام المعلوماتي وفي المقابل لم يواكبها تعريفات واضحة ومحددة وتشريعات تناسب هذا التطور.[1]

فكان من المنطقي أن تهدف أو تتجه السياسة التشريعية في دولة ليبيا للحد من ظاهرة الإجرام المعلوماتي، خاصة بعد ازدياد جرائم الحاسب الآلي والإنترنت على المستوى العالمي في الفترة الأخيرة، وتفاقم مخاطرها.

ولما كانت أنماط الجريمة المعلوماتية ومهما اختلف الدور الذي يلعبه الحاسب الآلي فيها، سواء كان وسيلة متطورة لارتكاب الجرائم التقليدية، أو كان الهدف التي تتوجه إليه الأنماط الحديثة من السلوك الإجرامي للحصول على المعلومات ذاتها، أو كان هو البيئة التي تُسهل ارتكاب الجرائم خاصة الجرائم عابرة الحدود، لما تتيحه من توفير مخازن للمعلومات والأنشطة الإجرامية لسرقة البنوك وتزوير المحررات والتوقيعات ...الخ.[2]

تستهدف جميعها مصالح معترفاً بحمايتها، وتستهدف محلاً يتسم بطبيعة مغايرة لمحل الجريمة التقليدية التي عرفتها قوانين العقوبات القائمة حالياً، والقدرة على ارتكابها عبر الحدود، والقدرة على إتلاف أدلة الجريمة فإن القواعد الإجرائية المتمثلة في جمع الأدلة والتفتيش والضبط

(1) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 149.
(2) محمد علي سكيكر، مرجع سابق ذكره، ص 133.

والمعاينة والخبرة والتي سيتم التطرق إلى دراستها لاحقاً، يتعين أن تواكب هذا التغير، وتضمن تحقيق التوازن بين حماية الحق وفعالية نظام العدالة الجنائية في الملاحقة والمساءلة ، لذا فإن تأثير التقنية الحديثة على قواعد قانون العقوبات وقانون الإجراءات الجنائية هي الأبرز والأكثر تميزاً من بين تأثيرات تلك التقنية على بقية فروع القانون الأخرى.[1]

كما يستلزم قبل توافر تلك النصوص القانونية، وجود شرطة فنية ورجال نيابة ورجال قضاء ومحاميين مدربين فنياً وتكنولوجياً على كيفية التعامل مع ذلك النوع من جرائم التكنولوجيا الحديثة، هذا من جهة ومن جهة أخرى يُلزم توافر الأجهزة الفنية كذلك لهم ليتمكنوا من القيام بما هو منوط بهم من واجبات لتيسير التعامل معها ومساعدتهم على القيام بمهامهم.[2]

وإن كان في الوقت السابق وفي إطار تطوير الأجهزة المعنية بمكافحة هذه الجرائم أنشأت ليبيا إدارة خاصة لمكافحة جرائم تقنية المعلومات تابعة للإدارة العامة للأدلة والبحث الجنائي وذلك بموجب قرار أمين اللجنة الشعبية العامة للأمن العام رقم (63) لسنة 2005م بشأن تقرير حكم في القرار رقم (131) لسنة 2004م بشأن التنظيم الداخلي للجهاز الإداري للجنة الشعبية العامة للأمن العام، وقد كان من أهم اختصاصات هذه الإدارة مكافحة جرائم الحاسوب والإنترنت وجرائم تقنية المعلومات الأخرى، فضلاً عن تقديم الدعم الفني للمؤسسات العامة في مجال الأمن المعلوماتي بالتنسيق مع الجهات ذات العلاقة، والقيام بأعمال البحث والتحري وجمع الاستدلالات في الجرائم المذكورة [3] وغيرها من الاختصاصات ذات العلاقة بموضوع الجريمة المعلوماتية.

(1) محمد علي سكيكر، مرجع سابق ذكره، ص 133- 134.
(2) منير محمد الجنيهي، ممدوح محمد الجنيهي، مرجع سابق ذكره، ص 216-217.
(3) موسى مسعود ارحومة، السياسة الجنائية في مواجهة الإنترنت، مرجع سابق ذكره، ص 108-109.

ولكن هذه الخطوة من جانب دولة ليبيا وإن كانت جيدة إلا أنها تظل غير كافية بذاتها لمواجهة ومكافحة الجريمة المعلوماتية، بل لابد من تدخل تشريعي "موضوعي وإجرائي" لمعالجة هذه الظاهرة الإجرامية الخطيرة، ومن ثم تطوير الأجهزة المعنية بمكافحة هذا الإجرام المعلوماتي.

والحقيقة أن القانون الجنائي لا يتطور بنفس السرعة التي تتطور بها التكنولوجيا، فنتيجة لكل ذلك كان على المشرّع الجنائي الليبي أن يتدخل لتوفير الحماية لجنائية الكافية لنظم المعلومات وتطوير المنظمة الإجرائية لكي تتماشى مع هذا التطور التكنولوجي ومن ثم تم ضمان مكافحتها على أكمل وجه.

فلا يكفي من حيث المبدأ اللجوء إلى تطويع النصوص العقابية المتعلقة بالجرائم التقليدية كالسرقة والنصب وخيانة الأمانة والتزوير والإتلاف والتجسس لكي يتم إعمالها بصدد إساءة استخدام تقنية المعلومات ، فقد أسفرت الدراسات والأبحاث التي أجريت في هذا الخصوص بأن النصوص التقليدية غير كافية لمواجهة الجرائم المستحدثة، ويصعب قبول تطبيق هذه النصوص بشأنها وذلك لأكثر من اعتبار، فمن ناحية أن جرائم الإنترنت تستهدف في المقام الأول: المعطيات وهي البرامج والمعلومات والبيانات المخزنة في جهاز الحاسب الآلي أو المنقولة عبر الإنترنت منه أو إليه، ومن ناحية ثانية أن مبدأ شرعية الجرائم والعقوبات يتنافى ومسألة إعمال القواعد المتعلقة بالجرائم التقليدية على أنماط السلوك المستحدثة دون النص على تجريمها والعقاب عليها بصورة واضحة وصريحة، ومن ناحية ثالثة أن القياس محظور في مسائل التجريم والعقاب، ومن ثم لا يجوز قياس إساءة استخدام الحاسوب والإنترنت على الجرائم التقليدية أو العادية.[1]

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 93.

ولذا فإنه في حالة لو سلمنا بأن قانون العقوبات الليبي الحالي لا يكفي لمواجهة هذا الإجرام المستحدث، فهل هذا يعني أن نقف مكتوفي الأيدي أمام هذا الفراغ أو النقص التشريعي، ونترك بدون عقاب أفعال تمثل اعتداءات خطيرة على نظم المعلومات، أم نسمح للقضاء بأن يتدخل لسد هذا النقص التشريعي بما ينطوي عليه ذلك من انتهاك لمبدأ الشرعية الجنائية، أم يجب على المشرّع أن يتدخل لمعالجة ومكافحة الجريمة المعلوماتية من مختلف جوانبها وأبعادها.

في الواقع أن المشرّع الجنائي هو الوحيد الذي يتدخل – كما دعت الحاجة إلى ذلك – ليتناول بالتجريم والعقاب ما يستجد من أفعال لم تكن تقع من قبل تحت سلطانه، وذلك تطبيقاً للمبدأ المعروف "شرعية الجرائم والعقوبات"، والذي يعني حصر مصادر التجريم والعقاب في نصوص القانون ، فالمشرّع دون القاضي هو المختص دائماً بتحديد الأفعال التي تُعد جرائم وبيان أركانها وعناصرها، وكذلك العقوبات المقررة لها سواء من حيث نوعها أو مقدارها.[1]

وفي النهاية ونتيجة لكل ما سبق ذكره من شرح لهذه الظاهرة الإجرامية الحديثة والخطيرة في آن معاً، ندعو المشرّع الليبي من هذا المقام إلى ضرورة أن يسارع ويستعجل في معالجة ظاهرة الجريمة المعلوماتية بمختلف أنماطها وجوانبها وأبعادها، لتفادي مخاطرها وذلك سواء بإصدار تشريع خاص ومستقل لمعالجتها أو على الأقل إدخال تعديل على القانون الليبي النافذ حالياً وذلك بعمل باب مستقل بخصوص الجريمة المعلوماتية، بحيث تكون نصوص التجريم في هذا المجال صريحة وواضحة لكونه مجالاً جديداً ومتميزاً سواء بمصطلحاته الجديدة أو بطبيعته الخاصة وذلك بحكم الوسيلة المستخدمة وبحكم طبيعة المال المعتدي عليه والمراد حمايته، ووضع عقوبات خاصة بهذه الجريمة المعلوماتية بحيث تتلاءم وإياها، ذلك لأن التجريم والعقاب في هذا المجال سوف

(1) جميل عبدالباقي الصغير، مرجع سابق ذكره، ص 18-20.

يحقق بـلا شـك وظيفتـي الـردع العـام والـردع الخـاص، فضـلاً عـن ضـرورة وضـع إجراءات جنائيـة تنسجم مع طبيعة نمط هذا الإجرام المعلوماتي المستحدث.

وإن كان المشرّع الليبي قد نص على عقوبة لإساءة استخدام شبكة المعلومات الدولية وعقوبة لإساءة استخدام وسائل الاتصالات ، وذلك في القانون رقم "22" لسنة 2010 م بشأن الاتصالات ، حيث نصت المادة "35" (يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تزيد على خمسة آلاف دينار وسحب الترخيص ومصادرة الآلات والأجهزة المستخدمة وذلك كل من أساء استخدام شبكة المعلومات الدولية في نشر معلومات أو بيانات تمس الأمن السياسي أو الاقتصادي أو الاجتماعي أو الموروث الثقافي في للمجتمع العربي الليبي أو استخدام الفيروسات أو أي طرق أخرى لإيذاء الغير. [1]

كما نصت المادة "36" من ذات القانون على أنه "مع عدم الإخلال بأحكام المادة "35" من هذا القانون ، يعاقب بغرامة لا تقل عن مائة دينار ولا تزيد على خمسمائة دينار كل من أساء استخدام وسائل الاتصال للإضرار بالغير". [2]

والجدير بالذكر هنا أن هذه الخطوة أو المحاولة للمشرّع الليبي في شأن تجريم إساءة استخدام شبكة المعلومات الدولية ووسائل الاتصالات في قانون الاتصالات الليبي السالف ذكره ، هي محاولة يتيمة لا نظير لها في التشريع الليبي ، فضلا عن أنها قاصرة وغير جامعة لكل صور الجريمة المعلوماتية بما فيها القرصنة المعلوماتية .

لذا فلا غنى عن سن نصوص قانونية بخصوص الجريمة المعلوماتية تعالج كل صورها وأنماطها المختلفة ، وذلك لكل الاعتبارات السابق ذكرها بهذا الخصوص .

(1) شبكة قوانين الشرق EASTLWS.COM.، متاح على الرابط: http://security-Legislation.ly/sites تاريخ الزيارة: 2020/11/1م، الساعة 10:00 صباحاً.
(2) ذات المرجع السابق، على الرابط.

المطلب الثاني

موقف التشريعات الغربية من القرصنة المعلوماتية

تمهيد وتقسيم:

قد تنبهت الدول الغربية وخصوصاً في أوروبا في وقت مبكر بالمقارنة مع غيرها من الدول الأخرى لمخاطر الجريمة المعلوماتية وصورها المختلفة ، ولعل ذلك سببه دخول الحاسب الإلكتروني وتطبيقاته في وقت مبكر في مختلف مجالات الحياة، ومختلف القطاعات من حكومية وغير حكومية، الأمر الذي جعل لهذه الدول الأسبقية في استصدار التشريعات المتعلقة بمكافحة الجريمة المعلوماتية. [1]

ولذا سنعرض في هذا المطلب لتجربة كل من "المشرّع الفرنسي" في الفرع الأول و"المشرّع الإنجليزي" في الفرع الثاني و"المشرّع الأمريكي" في الفرع الثالث على التوالي، وذلك في مجال مكافحة الجريمة المعلوماتية.

(1) الجريمة المعلوماتية، بحث منشور على الإنترنت، الصحيفة القانونية، متاح على الرابط: jle-gov.sy>index.php تاريخ الزيارة: 2017/01/02م.

الفرع الأول

موقف التشريع الفرنسي

عندما اتضح جلياً للمشرّع الفرنسي أن المعلوماتية أصبحت من وسائل ارتكاب الجرائم ضد الأشخاص والأموال، وبالتالي اتسع نطاق النظام المعلوماتي وتدخل في كافة نواحي الحياة الاقتصادية والسياسية والحياة الخاصة والحريات والأسرار، بحيث أصبح لازماً عليه أن يتدخل بالأسلوب التشريعي لحماية مصالح الناس وحرياتهم، فقام المشرّع بإضافة مجموعة من القواعد الخاصة بالجريمة المعلوماتية إلى قانون العقوبات الفرنسي وذلك على مراحل ثلاثة:

في المرحلة الأولى: صدر قانون "6 يناير 1978م" المتعلق بالمعلوماتية والحريات والواقع أن هذا القانون كان قاصراً على حماية ما يسمى بالمعلومات الإسمية والحرية وسرية الحياة الخاصة للأفراد ، وقد استحدث هذا القانون أنواعاً من الجرائم وهي:

1. عدم احترام الشكليات اللازمة والسابقة على معالجة المعلومات الإسمية.
2. جمع المعلومات الإسمية والاحتفاظ بها بصورة غير شرعية.
3. إنشاء المعلومات الإسمية.[1]

في المرحلة الثانية: لاحظ المشرّع استفحال ظاهرة الإجرام المعلوماتي، ولذلك كان لابد من التدخل ثانية لتضمين قانون العقوبات نصوص جديدة من شأنها مواجهة هذه الظاهرة، ولهذا الغرض تم التفكير في تقديم مشروع لتعديل قانون العقوبات، وقُدم هذا المشروع بالفعل إلى البرلمان الفرنسي تحت عنوان " بعض الجرائم في مواد المعلوماتية" ، وتم اعتماده وصدر به قانون "1988م" الذي تم إدماجه في قانون العقوبات الفرنسي وخصص له الفصل الثاني المواد من

(1) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 268.

"2/462" إلى "9/462" أي تسع مواد جديدة تحت عنوان : "بعض الجرائم في مواد المعلوماتية" وتم إلحاق هذا الفصل بالباب المخصص "للجنايات والجنح ضد الأشخاص".[1]

وقد احتوى هذا القانون على عدة أنواع من الجرائم يمكن تقسيمها إلى ثلاث طوائف رئيسية:

الطائفة الأولى: تشمل ثلاثة أنواع من الجرائم تضمنتها المواد من "462/ف2" إلى "462/ف4" من قانون العقوبات وتهدف هذه الجرائم والعقوبات المقررة لها إلى حماية نظم المعلومات ذاتها وتشتمل هذه الطائفة بدورها على ثلاث جرائم مختلفة وهي:

1. الدخول أو البقاء غير المشروع داخل النظام المعلوماتي.
2. الاعتداء على سير نظام المعلوماتية.
3. إدخال معلومات بصورة غير شرعية في نظام المعلوماتية أو إتلاف المعلومات الموجودة فيه. [2]

أما **الطائفة الثانية:** فتشمل نوعين من الجرائم تكلمت عنها المواد "462/ف5" و"462/ف6" وهاتان الجريمتان هما:

1. تزوير الوثائق المعالجة معلوماتياً.
2. استخدام الوثائق المعالجة معلوماتية المزورة. [3]

و**الطائفة الثالثة:** وهي تشتمل على عقوبتين تهدفان إلى الردع وتغليظ العقاب في المقام الأول، ونصت عليها المواد "462/ف7" إلى "462/ف9" وهما الحبس "حده الأدنى شهرين والأقصى 5 سنوات"، والغرامة حدها الأدنى 200 فرنك والأقصى 2 مليون فرنك وهذه العقوبات

(1) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 155..
(2) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 268.
(3) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 117.

المغلظة تهدف إلى ردع النشاط الإجرامي لعصابات المعلوماتية، وهي نفس العقوبة بالنسبة حتى للشروع في الجرائم السابقة. [1]

إلا أن هذا القانون كذلك قد تعرض لعدة انتقادات منها: أنه لم ينص على تجريم سرقة البرامج والمعلومات، كما أنه لم ينص صراحةً على تجريم سرقة وقت الآلة، وإن كان ممكن تضمينها لمحتوى نص المادة "462 ف2" والتي تُعالج جريمة "التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات".

ولذا يرى جانب من الفقه الفرنسي إمكانية تفسير النص تفسيراً يسمح بانطباقه على سرقة وقت الآلة حيث إن هذه الجريمة الأخيرة تعني الاستخدام غير المصرح به لإمكانيات نظام المعالجة الآلية للبيانات وأن هذا التفسير لا يمثل أي إخلال بمبدأ الشرعية. [2]

في المرحلة الثالثة: نتيجة لهذه الانتقادات لم يكتفِ المشرّع الفرنسي بهذا بل قام بتعديل آخر لقانون العقوبات الفرنسي وضمنه أحكام جديدة للحد من هذا النوع من الإجرام المعلوماتي، فتم تعديل القانون في عام 1994م تحقيقاً لهذا الغرض، وكان مقتضى هذا التعديل إضافة فصلٍ ثالثٍ للباب الثاني من القسم الثالث من قانون العقوبات وتم تسميته "الاعتداءات على نظم المعالجة الآلية للمعلومات"، ويتكون من المواد رقم "323/ف1" حتى "323/ف7".[3]

وقد عالجت المادة "323/ف1" من هذا القانون مسألة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية وهي ترديد للمادة "462/ف2"، وكذلك نفس ظرف التشديد الوارد بها إلا أنها أتت بعقوبة مضاعفة لها، حيث اتجه المشرّع الفرنسي نحو تشديد العقاب المنصوص عليه للفعل

(1) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 273.
(2) هدى حامد قشقوش، مرجع سابق ذكره، ص 84.
(3) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق ذكره، ص 189.

الإجرامي مما كان عليه في التعديل السابق، وذلك لزيادة الردع العام في مواجهة الإجرام المعلوماتي. [1]

وتعالج المادة "323/ف2" من هذا القانون الاعتداءات الإدارية على سير نظام المعالجة الآلية للمعلومات بحيث يترتب على ذلك تعطيل سير النظام، وذلك بالاعتداء المادي على النظام أو بنشر فيروسات داخل النظام المعلوماتي، أو إعاقته بصورة دائمة أو مؤقتة، وعقوبة هذه الجريمة هي السجن لمدة "3 سنوات" والغرامة التي تصل إلى "300 ألف" فرنك فرنسي. [2]

كما نصت المادة "323/ف3" على الاعتداءات التي تقع على البيانات والمعلومات داخل نظام المعالجة الآلية للمعلومات، وقرر لها نفس العقوبة التي نصت عليها المادة "323/ف2" سالفة الذكر، وهي السجن لمدة "3 سنوات" والغرامة التي تصل إلى "300 ألف" فرنك فرنسي.

ومن خلال نص المادة "323/ف3" يظهر أن المشرّع الفرنسي لا يحمي النظام المعلوماتي من الناحية المادية والبرامج أو التطبيقات فقط، بل يحمي كذلك المعلومات المخزنة فيه وذلك ضد أي اعتداء أو نشاط إجرامي يترتب عليه إتلاف المعلومات وهو ما يطلق عليه "القرصنة المعلوماتية" وعلى ذلك فهذا النص يُعاقب على إتلاف المعلومات المخزنة في ذاكرة الحاسب أو على وسيط التخزين المعلوماتي. [3]

فنلاحظ أنه إذا كان نشاط الجاني ذا طبيعة ذهنية أو غير مادية فإنه ينطبق عليه نص المادة "323/ف3" الخاصة بالإتلاف المعلوماتي، ومتى كان نشاط الجاني ذا طبيعة مادية في القيام بالسلوك الإجرامي فإنه ينطبق عليه نص المادة "323/ف2" والخاصة بإعاقة سير أنظمة

(1) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 155.
(2) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 138-139.
(3) عبدالفتاح بيومي حجازي، مرجع سابق ذكره، ص 333-334.

المعلومات، هذا وتعالج المادة "323/ف4" الأفعال الصادرة عن عصابات الإجرام المعلوماتي في حالة لو كانت هذه الأفعال تشكل واحدة أو أكثر من الجرائم المنصوص عليها في المواد السابقة.[1]

كما عاقب فيها على الأعمال التحضيرية قبل وقوعها، وذلك لخطورة هذا النوع من الإجرام وتهديده لتطبيقات التجارة الإلكترونية، فنصت المادة "323/ف4" على مساهمة أكثر من شخص في ارتكاب أفعال مادية تحضيرية تهدف إلى ارتكاب إحدى الجرائم المنصوص عليها في المواد "1/323" إلى "3/323" أي جرائم الاعتداء على نظم المعالجة الآلية للمعلومات. [2]

بالإضافة إلى ذلك فقد نصت المادة "323/ف5" في سبعة بنود منها على مجموعة من العقوبات التكميلية إلى جانب العقوبات الأصلية، وهي كثيرة تتراوح بين الحرمان من الحقوق المدنية المتعلقة بالأسرة لمدة 5 سنوات، والحرمان من الحقوق السياسية ونشر القرار الصادر بالإدانة في الجرائد والأماكن المعدة للنشر. [3]

وكذلك مصادرة الأشياء المستخدمة في الجريمة أو التي أُعدت للاستعمال فيها أو تحصلت منها، عدا تلك التي تكون محلاً للرد، وإغلاق الأماكن أو المشروعات التي استخدمت في ارتكاب الجريمة لمدة لا تتجاوز 5 سنوات".[4]

(1) أحمد خليفة الملط، مرجع سابق ذكره، ص 659-660.
(2) علي عبدالقادر القهوجي، مرجع سابق ذكره، ص 127.
(3) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 272-274.
(4) عبدالفتاح بيومي حجازي، مرجع سابق ذكره، ص 335-336.

الفرع الثاني

موقف التشريع الانجليزي

تعتبر دولة بريطانيا هي من أوائل الدول الأوروبية التي أولت اهتمامها بهذا الموضوع في وقت مُبكر، فكانت ثَالث دولة تسن قانوناً خاصّاً بجرائم الإنترنت، حيث أصدرت سنة 1981م قانوناً لمكافحة التزوير والتزييف باستخدام وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق الإلكترونية أو التقليدية أو أي طرق أخرى. [1]

ثم في سنة 1990م أصدرت قانوناً يُعالج مسألة إساءة استخدام نظم المعلومات تحت عنوان قانون إساءة استخدام الكمبيوتر ودخل حيز التنفيذ في أغسطس عام 1990م.

حيث جرم الدخول إلى البيانات المختزنة بالحاسب الآلي أو البرامج، وكذلك إجراء أي تعديل عليها بصورة غير مشروعة أو محاولة فعل ذلك[2]. فهذا القانون قد وضع جرائم إساءة استخدام الكمبيوتر في ثلاثة بنود هي:

البند الأول: الدخول المحظور على مواد الكمبيوتر

وهذا النص يحدد صور السلوك الإجرامي الذي تقوم به جريمة حظر الدخول إلى مواد الكمبيوتر كما يلي:

1. يُعد الشخص مذنباً إذا:

أ. قام بفعل يؤثر بسبب على أي وظيفة بالنسبة لتأمين إدخال بيانات برنامج أو بيانات موجودة في الكمبيوتر.

(1) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق ذكره، ص 188-190.
(2) موسى مسعود ارحومة، مرجع سابق ذكره، ص 104.

ب. تعمد الدخول المحظور للكمبيوتر.[1]

ج. إذا علم الشخص أنه حينما يقوم بهذه العملية أنه يرتكب جريمة.

2. يجب أن تتجه نية الشخص الذي يرتكب جريمة تحت هذا القسم إلى الاعتداء على:

أ. أي برنامج أو بيانات محددة.

ب. أي برنامج أو بيانات محددة النوع.

ج. أي برنامج أو بيانات موجودة في أي كمبيوتر محدد.

3. الشخص المذنب في جريمة تحت هذا القسم يكون معرضاً للإدانة العاجلة وإلى عقوبة السجن لفترة لا تتجاوز ستة أشهر أو الغرامة التي لا تتجاوز المستوى الخامس العادي أو إلى كليهما.[2]

البند الثاني: الدخول المحظور بقصد التسهيل والتحريض على الجرائم:

وينص هذا البند على الاشتراك في جريمة الدخول المحظور والذي يتخذ صورة التحريض والتسهيل، ويعتبر المشرّع الإنجليزي هذه الصور جريمة إضافية وتعد من قبيل الجنح.

ويُعاقب الشخص المذنب بسبب جريمة تحت هذا البند كما يلي:

1. في حالة الاعتراف يعاقب بالسجن لفترة لا تتجاوز الحد الأقصى القانوني المقرر لهذه العقوبة أو الغرامة أو كلاهما.

2. في حالة ثبوت الاتهام يعاقب بالسجن لفترة خمس سنوات أو الغرامة أو كلاهما.[3]

---

(1) اختلفت تشريعات الدول في تحديد محل الدخول غير المصرح به إلى نظام الكمبيوتر، فنجد أن القانون الفرنسي هو مثالاً يقتدى به في الاتجاه الموسع ، حيث جمع بين المعلومات وأنظمة الكمبيوتر وشبكات المعلومات، بينما القانون الإنجليزي لسنة 1990م فقد استبعد شبكات المعلومات من نطاق التجريم، حيث نصت المادة الأولى من هذا القانون على الدخول غير المصرح به إلى البرامج والمعلومات التي يحتوي عليها أي كمبيوتر. أنظر خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 156.

(2) قانون إساءة استخدام الكمبيوتر البريطاني ، متاح على الرابط:
COMPUTERMISUSEACT.1990(UK)COMMENCEMENT29AUGUST1990<GALAN.2184445.COM الساعة 10:00م

(3) متاح على ذات الرابط السابق.

البند الثالث: حظر تبديل أو تحويل مواد الكمبيوتر:

في هذا البند نص المشرّع على جريمة الاعتداء على البرامج والبيانات بإتلافها أو استبدالها، فنص على أن يكون الشخص مذنباً إذا:

1. تسبب في تعديل محظور لمحتويات أي كمبيوتر وتوفر لديه القصد والمعرفة حينما قام بهذا التعديل.
2. يجب أن يتوفر لدى المذنب بالإضافة إلى القصد، سبب لتعديل المحتويات بأي عمل يؤدي إلى:
3. الشخص المذنب بسبب هذه الجريمة معرضاً لـ:
4. السجن لمدة لا تتجاوز ستة أشهر أو غرامة لا تتجاوز الحد الأقصى القانوني أو كلاهما في حالة الاعتراف.
5. في حالة ثبوت الاتهام تكون العقوبة السجن لمدة لا تتجاوز خمس سنوات أو غرامة أو كليهما.[1]

ويتبين لنا من خلال استعراض الأسلوبين الفرنسي والانجليزي أن المشرّع الفرنسي تصدي للجريمة المعلوماتية من خلال خطوتين:

الأولى: تتجلى بإقرار المشرّع والقضاء الفرنسي بإمكانية انطباق النصوص القانونية في قانون العقوبات على الجرائم التي تقع بواسطة النظام المعلوماتي.

الثانية: تتمثل في إضافة نصوص قانونية جديدة إلى قانون العقوبات لتغطي بشكل خاص الجرائم الواقعة على الكيان البرمجي للنظام المعلوماتي.

(1) طاهر جمال الدين كرابيج، الجريمة المعلوماتية، الصفحة القانونية، بحث منشور على الإنترنت، للعام الدراسي 2010 - 2011.م، متاح على الرابط: vle.gov.sx>index.php تاريخ الزيارة: 2017/01/29م، الساعة 11:38 م.

في حين أن المشرّع الإنجليزي تصدى لهذه الجريمة من خلال إصدار قانون خاص بها عام 1990م تحت عنوان "قانون إساءة استخدام الكمبيوتر".[1]

بالرغم من أن الاستجابة البريطانية للتدابير التشريعية الجديدة في حقل تقنية المعلومات، وصفت بأنها متأخرة عن غيرها من الدول الأوروبية ومتأخرة بالتأكيد عن الاستجابة الأمريكية، إلا أن السنوات الأخيرة وتحديداً الأعوام من 1998م وحتى الآن تشهد تميزاً في التجربة البريطانية سواء من حيث محتوى التنظيم أو الحلول التشريعية المقررة، ليس في نطاق أمن المعلومات فحسب بل في نطاق حماية البيانات الشخصية والخصوصية وتنظيم حرية البيانات والمعلومات وفي مختلف الفروع الأخرى لقانون تقنية المعلومات.[2]

(1) متاح على ذات الرابط.
(2) التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات مركز هردو لدعم التعبير الرقمي، القاهرة 2018م، متاح على الرابط hrdegypt.org> تاريخ الزيارة 2020/10/5م، الساعة 11:30م.

الفرع الثالث

موقف التشريع الأمريكي من القرصنة المعلوماتية

كانت الولايات المتحدة الأمريكية هي الدولة التالية التي تبعت دولة السويد في إصدار قوانين خاصة بها تجرم الاعتداءات الإلكترونية، فتميزت بسن عدة تشريعات على المستوى الفيدرالي وحزمة معتبرة من التشريعات على مستوى الولايات، حيث شرعت قانوناً فيدرالياً خاصاً بحماية أنظمة الحاسب الآلي تحت مسمى "قانون التحايل المعلوماتي" سنة "1984م" وفي عام "1985م" حدد معهد العدالة القومي الأمريكي خمسة أنواع رئيسية للجرائم المعلوماتية وهي:

- جرائم الحاسب الآلي الداخلية.
- جرائم التلاعب بالحاسب الآلي.
- جرائم الاستخدام غير المشروع عن بعد.
- جرائم دعم التعاملات الإجرامية.
- جرائم سرقة البرامج الجاهزة والمكونات المادية للحاسب الإلكتروني.[1]

وفي عام 1986م صدر قانون آخر يحمل الرقم "1213" عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الضرورية اللازمة لتطبيقه، وعلى أثر ذلك قامت الولايات الداخلية بإصدار التشريعات الخاصة بكل منها على حدة للتعامل بها مع تلك الجرائم الإلكترونية، وقد خولت وزارة العدل الأمريكية في عام 2000م خمس

(1) الجريمة عبر الإنترنت (3) تشريعات ضد الجرائم الإلكترونية على مستوى العالم. صوت الأمة، رئيس التحرير : يوسف أيوب، مدير التحرير: هشام السروجي، أيمن عبدالتواب، متاح على الرابط: Article<www.soutalomma.com

جهات حكومية للتعامل مع جرائم الإنترنت والحاسب الآلي في سبيل تفعيل مكافحة هذه الجرائم منها مكتب التحقيقات الفيدرالي"FBI".[1]

كما عملت الولايات المتحدة الأمريكية على تطوير نظامها الإجرائي فيما يتعلق بالبحث عن الدليل المستمد من شبكة المعلومات الدولية "الإنترنت" من خلال إصدار قانون خصوصية الاتصالات الإلكترونية المعدل سنة 2001م، والذي ينظم أحكام الضبط والتفتيش في نطاق الفضاء المعلوماتي أو في بيئة الحواسيب، كما رسم القانون المشار إليه الآليات التي يستلزم اتخاذها من قِبل مأموري الضبط القضائي أو المدعيين العموميين، وهذه المتطلبات تتفاوت بتفاوت المصالح المحمية، بالإضافة إلى إقراره لعدد من القواعد التي تحمي الخصوصية فيما يتخذ من إجراءات جنائية في ميدان جرائم التقنية وما يمكن تسميته بضمانات المتهم المعلوماتي. [2]

وبالرجوع إلى الاتجاه التشريعي الفيدرالي نجد أن القانون الخاص بإساءة استخدام الحاسب الآلي الصادر سنة "1984م" قد نص في مادته "1030" بالبندين "1، 2" فقرة "3" على أن "يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة التي لا تزيد على خمسة آلاف دولار أو على ضعف القيمة التي حصل عليها الجاني أو الخسارة التي سببها بجريمته وبكلا العقوبتين كل من توصل عن علم ومن دون تصريح إلى نظام الحاسب أو استغل فرصة وصوله إليه على نحو مصرح به لتحقيق أغراض لا يمتد إليها التصريح الممنوح له إذا تمكن بهذا السلوك من استخدام أو تعديل أو تدمير أو كشف المعلومات المخزنة داخله عن علم بذلك، أو منع الاستخدام المصرح به لنظام

(1) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق ذكره، ص 186-187.
(2) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 101-102.

الحاسب، وذلك إذا ما كان الحاسب يعمل لأجل أو بالنيابة عن حكومة الولايات المتحدة وكان من شأن سلوك الفاعل التأثير في تشغيل الحاسب الآلي. [1]

فقد جرمت هذه المادة الحصول على المعلومات عن طريق الدخول غير المصرح به إلى الحاسبات الآلية وكذلك جرمت الدخول المجرد إلى الحاسبات الآلية التابعة لحكومة الولايات المتحدة الأمريكية أو تلك التي يؤدي الدخول غير المشروع إلى المساس بأعمال تتعلق بالحكومة، وتشمل الحاسبات وفق هذا القانون كل جهاز إلكتروني أو كيميائي كهربائي أو جهاز لمعالجة المعلومات، وكذلك كل وسائل الاتصالات التي تعمل بالاتصال مع أي من هذه الأجهزة ووفقاً لهذا النص فإن المحل الذي تنصب عليه جريمة الدخول غير المشروع يتسع ليشمل المعلومات وأنظمة الحاسبات الآلية وشبكات المعلومات ولكن المشرّع الأمريكي قد قيد هذا الأمر بوضع بعض القيود مثل أن تكون المعلومات متعلقة بأمور الائتمان، كما تتطلب أن تكون تلك الأنظمة تابعة أو متعلقة بحكومة الولايات المتحدة الأمريكية. [2]

كما أن القسم "1462" من الفصل "18" من قانون الولايات المتحدة يحظر استخدام الكمبيوتر لاستيراد مواد مخلة بالآداب إلى داخل الولايات المتحدة الأمريكية.

في حين أن القسم "1028" من الفصل "18" من قانون الولايات المتحدة الأمريكية يعتبر إنتاج أو نقل إدارة جهاز يتضمن نظام كمبيوتر بقصد استخدامه بتزوير الوثائق أو إنتاج وثائق تعريف مزورة جريمة. ويعتبر القسم "2319" من ذات الفصل الإخلال بحق المؤلف جريمة فيدرالية[3].

(1) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 240-241.
(2) أيمن عبدالله فكري، مرجع سابق ذكره، ص 192-195.
(3) متاح على الرابط : www.arablaw-orylowoffcanol.com-jo، تاريخ الزيارة: 2017/02/29م.

ثم زاد اهتمام المشرّع الأمريكي بهذه الظاهرة الإجرامية نتيجة التزايد الهائل والملحوظ للاعتداءات الواقعة على الحواسب الآلية، فتوالت التعديلات على القوانين المختلفة في هذا الشأن في حقبة التسعينات، فقد تم فيها تعديل عام 1994م، وتضمن ثلاثة تعديلات على قانون 1986م، فيما يتعلق بالمادة "5/أ" من القسم "1030"، حيث يغطي هذا التعديل استخدام الحاسب في التجارة بين الولايات المتحدة الأمريكية، كما أنه توسع في جريمة الدخول غير المصرح به، بحيث يمكن مساءلة العاملين داخل المؤسسة والمستخدمين المصرح لهم، كذلك تضمن تجريم حالات من الإهمال والسلوك والأفعال العمدية المعتبرة جرائم. (1)

وتدخل كذلك المشرّع سنة 1994م في الفصل "105" بالبند "2155" بالحماية ضد الإتلاف المعلوماتي في مجال الدفاع الوطني، حيث نص على عقوبة أي شخص يرتكب عن عمد أي أضرار أو يحدث أي تغيير أو تشويش أو يعترض سبيل المعلومات الخاصة بالدفاع الوطني سواء بالتعييب أو التحطيم أو الإفساد، أو يحاول الإضرار بأي ممتلكات تخص الدفاع الوطني أو المباني أو أراضي أو تسهيلات تخص الدفاع الوطني يُلزم بدفع غرامة لا تزيد عن عشرة آلاف دولار أمريكي أو بسجن مدة لا تزيد عن عشر سنوات أو كليهما. (2)

ثم في عام "1996م" صدر تشريع بمقتضى قانون البنية القومية للمعلومات والتي أُعدت له لجان الكونجرس الأمريكي الدراسات والإحصائيات المتوالية من قبل لجان متخصصة فيه، وكان الأساس في هذا القانون الأخير هو تنامي الجريمة عبر الإنترنت بشكل كبير، وتجدر الإشارة إلى أن هذا التشريع هو ما تضمنه نص القسم "1030" من التقنين الفيدرالي الأمريكي بعنوان الاحتيال والأنشطة الأخرى ذات العلاقة بالحاسب الآلي. (3)

(1) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 241.
(2) ذات المرجع السابق، ص241.
(3) أيمن عبدالله فكري، مرجع سابق ذكره، ص 199.

كما أن الخطة العامة التي سار عليها القانون الأمريكي في تعديل قانون "1996" انطلقت من ربط جرائم الإنترنت بالحاسب واعتبارها كلها جريمة واحدة مع تقرير معيار ثلاثي الأبعاد، ويتعلق بالمعيار الثلاثي لجرائم الحاسب الذي يكون موضوعاً لها والجرائم التي يكون الحاسب وسيلة إلى ارتكابها وجرائم يكون الحاسب دافعاً لارتكابها، لذلك نجد هذا النص في تعديل "1996م" يشير إلى أفعال يعتبرها القانون الأمريكي أشكالاً للاختراق من خلال الحاسب المستخدم في مؤسسة مالية، أو حاسب مستخدم من قبل الحكومة الفيدرالية أو حاسب مستخدم من قبل مؤسسة اقتصادية أو مؤسسة اتصالات في الولايات المتحدة الأمريكية أو خارج الولايات المتحدة وهذه الأشكال هي:

أ. التوصل إلى الدخول بشكل غير مشروع إلى حاسب حكومي ومن ثم يكشف معلومات سرية، وليس للمخترق الحق في الدخول إليه.

ب. يتوصل إلى الدخول بشكل غير مشروع إلى حاسوب ومن ثم يرتكب جريمة نصب.

ج. يتسبب في الأضرار بحاسب كنتيجة للدخول غير المشروع إليه بوضعه برمجية أو كود أو معلومات في الحاسب.

د. يرسل إلى مؤسسة اقتصادية في الولايات المتحدة أو في خارج الولايات تهديداً بإحداث أضرار في حاسب بقصد ابتزاز أموال أو ملكية من شخص أو حائزها الشرعي. [1]

أما على مستوى تشريع الولايات المتحدة الأمريكية، فإنه يمكن القول أن كافة الولايات قد تضمنت في تشريعاتها النص على التجريم التقني في مجالين هما الدخول غير المصرح به لحاسب بقصد ارتكاب جريمة أخرى، ثم إحداث أضرار لمادة مخزنة في الحاسب بما في ذلك المحتويات المعنوية غير المادية. [2]

(1) أيمن عبدالله فكري، مرجع سابق ذكره، ص 199-201.
(2).ذات المرجع السابق، ص 202.

أ. فمثلاً في "ولاية نيويورك": نصت المادة "25" بالبند "156" تحت عنوان "العبث بالكمبيوتر" على ما يلي:

نصت "الفقرة الأولى" على أن "يعتبر الشخص مذنباً بالعبث بالكمبيوتر من الدرجة الثانية عندما يستخدم أو يتسبب في استخدام الكمبيوتر وليس لديه الحق في القيام بذلك بقصد التغيير أو التبديل أو التعديل بأي أسلوب في البيانات أو البرامج الخاصة بالكمبيوتر وتنص الفقرة الثانية على أن يعتبر الشخص مذنباً بالعبث بالكمبيوتر من الدرجة الأولى عندما يقوم عن قصد بتغيير أو بتعديل بأي أسلوب أو تحطيم أي خامات للكمبيوتر وكانت قيمتها تزيد عن ألف دولار".[1]

ب. ولاية "فلوريدا": نص المشرّع على الجرائم المرتكبة ضد معدات الكمبيوتر ومحتوياته في المادة "05 و 815" على ما يلي:

تنص الفقرة الأولى على أن أي شخص يقوم بإرادته وعلى علم ومن دون تصريح بالعبث أو التعديل في معدات وتجهيزات مستخدمة أو سيتم استخدامها في الكمبيوتر أو نظام الكمبيوتر البرامج أو شبكة الكمبيوتر، يعتبر ارتكب جريمة ضد معدات وتجهيزات الكمبيوتر.[2]

وتنص "الفقرة الثانية" على أن ما هو موضح في "الفقرة الأولى" فإن الجريمة التي يتم ارتكابها ضد معدات أو تجهيزات الكمبيوتر تعتبر جنحة من الدرجة الأولى ويعاقب عليها كما هو موضح في البند الفرعي "082 و 775" أو "083 و 775" أو "084 و 775".

وتنص "الفقرة الثالثة" على أن المشرّع يشدد العقوبة ويعتبر الواقعة ترقى إلى درجة جناية في حالة ما إذا كانت الخسارة التي حدثت لتجهيزات أو معدات الكمبيوتر أو نظام الكمبيوتر

(1) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 241.

(2) يونس عرب، الاتجاهات التشريعية للجرائم الإلكترونية، متاح على الرابط www.ituarabic>E.crimesDoc6-jor. تاريخ الزيارة 2017/1/29م، الساعة 1:00م.

أو شبكة الكمبيوتر تعادل ألف دولار أمريكي أو أكثر أو كان هناك إعاقة أو إفساد لعمليات حكومية، ويعاقب عليها كجناية من الدرجة الثانية كما هو موضح في المواد "082 و 775" أو "083 و 775" أو "084 و 775".[1]

يتبين لنا من خلال ما سبق أوجه الاختلاف بين التشريع الفيدرالي وتشريع الولايات ، حيث يُلاحظ أن التشريع الفيدرالي اقتصر على تناول جريمة إتلاف المعلومات فقط "الإتلاف المعنوي" دون أن يتطرق إلى الإتلاف في الأجهزة ذاتها "الإتلاف المادي" وبالتالي جعل من الإتلاف الواقع على الأجهزة تخضع للقواعد العامة، ولم يراعِ تشديد العقوبة في حالة كون هذا الجهاز هو الحاسب الآلي بالرغم من أهميته لاسيما في مجال الدفاع الوطني وتعتبر العقوبة التي قررها المشرّع في المادة "1030" سنة "1984م" ضئيلة نسبياً بالرغم من أهمية حجم الجريمة المرتكبة، وهذا ما دعا المشرّع إلى التدخل وتعديل العقوبة سنة "1994م" في المادة "2155" في الفصل "105" في حالة كون المعلومات تخص الدفاع الوطني، هذا بعكس الولايات التي اهتمت بجريمة الإتلاف الواقعة على أجهزة الحاسب الآلي وجعلت العقوبة ذات العقوبة المقررة في حالة الخسارة التي هي ألف دولار عقوبة الجناية. [2]

لذا فإن مراجعة تشريعات جرائم الكمبيوتر النافذة في مختلف الولايات المتحدة الأميركية يشير إلى وجود اختلاف حقيقي في مستويات الحماية وتحديد أنماط هذه الجرائم، وكذلك وجود اختلاف في الاصطلاحات المستخدمة وأثر ذلك على توفير الحماية، إضافة إلى التباين بشأن العقوبات المقررة لهذه الجرائم، كل ذلك يدل على أهمية التوجه نحو وضع تشريع شامل وموحد لمعالجة هذه الجرائم. [3]

---

(1) يونس عرب، الاتجاهات التشريعية للجرائم الإلكترونية، متاح على الرابط www.ituarabic>E.crimesDoc6-jor. تاريخ الزيارة 2017/1/29م، الساعة 1:00م.

(2) أيمن عبدالحفيظ عبدالحميد سليمان، مرجع سابق ذكره، ص 242.

(3) هيئة تنظيم الاتصالات ، مسقط، سلطنة عمان، ورشة عمل "تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية"، من 2 – 4 نيسان / إبريل 2006م, د.يونس عرب، عنوان الورقة" الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، 2006م، ص 12، ومتاح على الرابط www.ituarabic.org تاريخ الزيارة 2020/10/6م، الساعة 9:23م

الفصل الثاني
ملامح السياسة الجنائية الإجرائية
للجريمة المعلوماتية

الفصل الثاني

ملامح السياسة الجنائية الإجرائية للجريمة المعلوماتية

تمهيد وتقسيم:

إن الطبيعة الخاصة لأنماط الجريمة المعلوماتية والقدرة على ارتكابها عبر الحدود، وإمكانية إتلاف أدلة الجريمة بكل سهولة وسرعة، فإن القواعد الإجرائية المتمثلة في جمع الأدلة والتفتيش والضبط والمعاينة والخبرة يتعين أن تواكب هي الأخرى هذا التغيير، وتضمن تحقيق التوازن بين حماية الحق وفعالية نظام العدالة الجنائي في الملاحقة والمساءلة. [1]

ولذا فإن التطور الواقع على الجرائم التي تتعلق بتكنولوجيا المعلومات يجب أن يتبعه تطور في السياسة الجنائية الإجرائية للجريمة المعلوماتية وذلك لكي يمكن تتبع هذه الجريمة وإثباتها وإلقاء القبض على مرتكبها وبالتالي إظهار الحقيقة.[2]

وسنقوم بدراسة إجراءات التحري وجمع الأدلة في الجريمة المعلوماتية في المبحث الأول من هذا الفصل، وإجراءات التحقيق الابتدائي في المبحث الثاني، وذلك على النحو التالي.

(1) محمد علي سكيكر، مرجع سابق ذكره، ص 134.

(2) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 82.

المبحث الأول

إجراءات التحري وجمع الأدلة في الجريمة المعلوماتية

تمهيد وتقسيم:

تعد مرحلة جمع الاستدلالات من المراحل المهمة في مجال الجرائم بصفة عامة، والتي يقوم بها رجال الضبط القضائي ، وقد تضمنت ذلك المادة "11" من قانون الإجراءات الجنائية الليبي، حيث نصت على أنه "يقوم مأمورو الضبط القضائي بالبحث عن الجرائم ومرتكبيها، وجمع الاستدلالات التي تلزم للتحقيق والدعوى".[1]

وهي المرحلة التي تسبق مرحلة التحقيق الابتدائي التي تقوم بها النيابة العامة، وقد أستقر الأمر في أغلب التشريعات على أهمية هذه المرحلة باعتبارها مرحلة أساسية بالنسبة للسلطات المختصة بتحريك الدعوى الجنائية، فعملية جمع الاستدلالات من اختصاص مأموري الضبط القضائي من حيث تقصي الجرائم، والبحث عن مرتكبيها، وجمع الأدلة والمعلومات اللازمة للتحقيق والاتهام، وبذلك تعتبر هذه المرحلة هي خط الدفاع الأول ضد الجرائم المرتكبة سواء كانت من الجرائم التقليدية أم من جرائم الاعتداء على نظم المعلومات.[2]

وقد أثبتت التجربة العملية بأن مرحلة التحري وجمع الاستدلالات هي من أهم وأدق المهام الملقاة على عاتق جهاز الشرطة باعتبار أن من واجبه القيام بالكشف عن الجرائم المرتكبة فضلاً عن عمليات المكافحة ذاتها ومنع الجرائم قبل وقوعها، وبالتالي يقصد بالتحري في مجال الضبط

---

(1) موسوعة التشريعات الجنائية، الجزء الثالث، قانون الإجراءات الجنائية والقوانين المكملة له، 2016م، ص5، متاح على الرابط: iteadel.gov.ly

(2) منى كامل تركي، حث منشور في مجلة الإبداع العلمي، متاح على الرابط: amdayss,blogspot.com>...blog-fage تاريخ الزيارة 2020/10/5م، الساعة: 10:33م.

القضائي البحث عن الجرائم المرتكبة والتحقق من صحة الوقائع المبلغة عنها لمأمور الضبط القضائي وجمع كافة القرائن التي تفيد في حصول الواقعة أو نفي وقوعها.[1]

كما نجد بأن هناك اختصاصات معينة لمأموري الضبط القضائي عند البدء في أعمال جمع الاستدلالات، وذلك لحرصه على سرعة ضبط الواقعة وعدم طمس الأدلة التي تدل على الفاعل وبالتالي ضياع معالم الجريمة، وصعوبة تحقيق العدالة بشأنها، وما يقتضيه ذلك من سرعة انتقال مأمور الضبط القضائي لمكان ارتكاب الجريمة، ومباشرة تلك الاختصاصات ، كما يشترط في تلك الاختصاصات عدم المساس بحرمة شخص المتهم أو مسكنه وعدم إهدار حقوقه، وذلك ما يميز هذه الاختصاصات عن إجراءات التحقيق بمعناها الضيق، والتي لا تكون إلا بعد ظهور الجريمة، ويتجه فيها التحقيق إلى متهم معين دون غيره.[2]

وتعتبر من أهم إجراءات الاستدلال والتي أقرها المشرّع ي قانون الإجراءات الجنائية الليبي وتضمنتها نص المادة "14" من هذا القانون تحت عنوان "قبول التبليغات والشكاوى" ، حيث نصت على أنه "يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم بشأن الجرائم وأن يبعثوا بها فوراً إلى النيابة العامة.

ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على جميع الإيضاحات ، ويجروا المعاينات اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم، أو التي يعلنون بها بأية كيفية كانت ، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة ، ويجب أن يثبت جميع الإجراءات التي يقوم بها مأمور الضبط القضائي في محاضر موقع عليها منهم يبين فيها وقت اتخاذ الإجراء ومكان حصوله.[3]

(1) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 408-409.
(2) ذات المرجع السابق، ص 305 – 351.
(3) موسوعة التشريعات الجنائية ، الجزءالثالث، قانون الإجراءات الجنائية والقوانين المكملة له، ص 6، متاح على ذات الرابط السابق.

والجذير بالذكر في هذا المقام، أن هناك فراغاً تشريعياً بخصوص الجريمة المعلوماتية في التشريع الليبي، بحيث لم يقم المشرّع بمعالجة هذا الموضوع لا من الجانب الموضوعي ولا من الجانب الإجرائي له، وبالتالي أرجوا من المشرّع الليبي أن يدرك مدى خطورة هذا الإجرام المستحدث ويقوم بمعالجة الجريمة المعلوماتية تشريعياً من الناحية الموضوعية والإجرائية معاً.

وسيتم تقسيم هذا المبحث إلى مطلبين: نتناول في المطلب الأول موضوع تلقي البلاغات في الجرائم المعلوماتية وفي المطلب الثاني التحري وكشف غموض الجريمة المعلوماتية على التوالي.

المطلب الأول

تلقي البلاغات في الجرائم المعلوماتية

تمهيد وتقسيم:

يُعرف البلاغ بصورة عامة بأنه: إخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع أو أن هناك اتفاقاً جنائياً على ارتكابها. [1]

كما أن البلاغ في قانون الإجراءات الجنائية الليبي قد تضمنته المادة "15" والمادة "16" من هذا القانون، حيث نصت المادة "15" تحت عنوان "تبليغ النيابة" على أنه "لكل من علم بوقوع جريمة ، يجوز للنيابة العامة رفع الدعاوى عنها بغير شكوى أو طلب ، أن يبلغ النيابة العامة أو أحد مأموري الضبط القضائي عنها".[2]

كما نصت المادة "16" تحت عنوان "واجبات الموظفين العموميين ومن في حكمهم في التبليغ" على أنه "يجب على كل من علم من الموظفين العموميين أو المكلفين بخدمة عامة أثناء تأديته عمله أو بسبب تأديته بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب، أن يبلغ عنها فوراً النيابة العامة ، أو أقرب مأمور من مأموري الضبط القضائي".[3]

فنلاحظ بأن البلاغ عن الجرائم في هاتين المادتين هو إجباري على كل من علم بوقوع جريمة ما سواء كان من عامة الناس أو من الموظفين العموميين، وعادةً ما تبقى الجريمة مستترة حتى يصل خبرها إلى السلطات المختصة، هذا الوضع ينطبق على الجرائم كافة دون استثناء، لكنه

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 11.
(2) موسوعة التشريعات الجنائية، الجزء الثالث، قانون الإجراءات الجنائية والقوانين المكملة له، ص 7، متاح على الرابط السابق.
(3) ذات المرجع السابق، وعلى ذات الرابط.

يتجلى وضوحاً بالنسبة لجرائم تقنية المعلومات نظراً لطبيعتها، حيث يصعب على الأشخاص العاديين الإبلاغ عنها لما تتطلبه من مهارات فنية غير متوافرة سوى لفئات مهنية أو تخصصية في مجال الحاسب الآلي ونظم تقنية المعلومات.[1]

والمُبلغ في الجريمة المعلوماتية لابد وأن يكون لديه معرفة مقبولة وجيدة بالجوانب الفنية للحاسب الآلي وشبكة الإنترنت حتى يستطيع أن يُقدم أو يُعطي معلومات تصف الحادث بشكل جيد، وبالتالي تُمكن المحقق من الوقوف على طبيعة الجريمة ومباشرة التحقيق فيها على أفضل وجه. [2]

كما أنه من جهة أخرى يفترض أن يكون لدى من يتلقى البلاغ المعرفة الكافية بالجوانب الفنية للحاسب الآلي والشبكات المعلوماتية حتى يستطيع مناقشة المبلغ في الكثير من الجوانب الفنية المتعلقة بالجريمة محل البلاغ. [3]

وسنتناول مشكلات البلاغ في الفرع الأول وماهية المعلومات التي يجب استيفاؤها من المبلغ في الفرع الثاني وتشكيل فريق التحقيق في الفرع الثالث وذلك على التوالي.

(1) حسين خليل مطر، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، بحث مقدم إلى مؤتمر "الإصلاح التشريعي طريق نحو الحكومة الرشيدة ومكافحة الفساد" الذي أقامته مؤسسة النبأ للثقافة والإعلام ، جامعة الكوفة ، كلية القانون 25 – 26 نيسان، 2018م، متاح على الرابط annabaa.org.com.

(2) علي عدنان الفيل، مرجع سابق ذكره، ص 11.

(3) ذات المرجع السابق، ص 11.

الفرع الأول

مشكـــلات البـــــلاغ

هنـاك بعـض المشـكلات التـي تتعلـق بعمليـة الإبـلاغ عـن جـرائم الحاسـوب الآلـي وشـبكة الإنترنـت والتـي يجـدر بـالمحقق الإلمـام بهـا ومعرفتهـا وأخـذها بعـين الاعتبـار والعمـل علـى الحـد مـن تأثيرها بالوسائل المناسبة، ومن هذه المشكلات:

أولاً: الإحجام عن الإبلاغ:

فقد يحجم البعض عن إبلاغ السلطات المختصة عن الجرائم التي ارتكبت بحقهم، خاصة المؤسسات والشركات التجارية، حتى في الدول المتقدمة من الناحية التقنية والتي ترتفع فيها معدلات هذا النوع من الجرائم، ففي دراسة أجراها معهد أمن الحاسوب "CSI" بالاشتراك مع مكتب التحقيق الفيدرالي "FBI" في الولايات المتحدة الأمريكية إلى أن حوالي "70%" من الجرائم التي يتم اكتشافها لا يتم الإبلاغ عنها لسلطات العدالة. [1]

وهناك عدة أسباب تؤدي إلى إحجام البعض عن الإبلاغ من أهمها:

1. عدم إدراك خطورة الجرائم المعلوماتية من قبل الأفراد والمسؤولين بالمؤسسات، وهذا يرجع إلى اغفال جانب التوعية لإرشاد المستخدمين إلى خطورتها[2]، وبالتالي يحجم بعض الأفراد ومدراء الأنظمة الحاسوبية ومسؤولي الشركات عن الإبلاغ عن جرائم وقعت وتم اكتشافها نتيجة عدم إدراكهم بأن مثل هذه الأفعال تعتبر جرائم ويمكن معاقبة مرتكبها بموجب التشريعات والأنظمة المطبقة ضمن إقليم الدولة. [3]

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص 236.
(2) حسين خليل مطر، مرجع سابق ذكره، متاح على ذات الرابط السابق.
(3) محمود أحمد القرعان، مرجع سابق ذكره، ص 237.

2. تخوف الجهات التي وقعت عليها الجرائم، خاصةً المؤسسات والشركات المالية أن يؤثر انتشار خبر الحادث على سمعتها وثقة السوق في خدماتها، الأمر الذي قد ينعكس سلباً على أرباحها وقيمة أسهمها. [1]
3. احتجاز الحواسيب الآلية أو تعطيل الشبكات المعلوماتية للمؤسسات والشركات التجارية بسبب أعمال التحقيق التي تقوم بها الشرطة والتي قد تستمر لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية من جراء هذا التحقيق الجنائي بخصوص وقوع إحدى جرائم المعلوماتية. [2]
4. وإلى جانب كل ذلك ، فإن المجني عليه قد يتردد أحياناً في الإبلاغ عن هذه الجرائم، خوفاً من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي إلى تكرار وقوعها بناء على تقليدها من قبل الآخرين، كما أن الإعلان عن هذه الجرائم يؤدي إلى الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي، مما يُسهل عملية اختراقه. [3]
5. الشكوك التي قد تساور بعض الضحايا حول مدى قدرة الشرطة على التعامل مع جرائم الحاسب الآلي والإنترنت من حيث توافر الخبرة الفنية لدى ضباطه أو مدى توافر المعدات والتجهيزات اللازمة للتحقيق في هذا النوع من الجرائم. [4]

ثانياً: الطبيعة الفنية الخاصة للجرائم المعلوماتية:

إن هذه الطبيعة الفنية تستلزم أن يكون المبلغ عنها على قدر من الإلمام بمبادئ الحاسوب والشبكات ومعرفة أساسيات عمل شبكات الحاسب الآلي وأهم مصطلحاته حتى يستطيع المحقق

(1) حسين خليل مطر، مرجع سابق ذكره، متاح على ذات الرابط السابق..
(2) محمود أحمد القرعان، مرجع سابق ذكره، ص 237.
(3) ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، دراسة تأصلية تطبيقية، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، الرياض، 2012م، ص 25-26..
(4) محمود أحمد القرعان، مرجع سابق ذكره، ص 237-238..

استيفاء المعلومات اللازمة عن طبيعة الجريمة وملابساتها، فعدم معرفة المبلغ للأبعاد الفنية المتعلقة بالجريمة بالقدر الكافي يجعل من الصعب عليه الإبلاغ عنها بشكل كامل ودقيق. [1]

ثالثاً: عدم وجود تعريف محدد ودقيق لجرائم الحاسوب والإنترنت بالإضافة إلى قصور الكثير من التشريعات الحالية محلياً وعربياً بل وفي كثير من دول العالم، مما قد يؤدي ذلك إلى ورود بلاغات عن سلوكيات مرتبطة بالحاسوب وشبكة الإنترنت قد لا تعتبر في واقع الأمر جرائم تعاقب عليها التشريعات، والتشريع الليبي خير مثال على ذلك ، وإن كان بعضها يتنافى مع العادات والتقاليد السائدة في المجتمع المحلي، وهذا الأمر يتطلب ممن يتلقى البلاغ من رجال الشرطة الوعي والمعرفة بكافة جوانب هذه الجرائم بحيث يمتلك القدرة على توضيح الأمر للمبلغ وإقناعه بعدم وجود جريمة مُعاقب عليها قانوناً. [2]

(1) منى كامل تركي، مرجع سابق ذكره، متاح على ذات الرابط السابق..
(2) محمود أحمد القرعان، مرجع سابق ذكره، ص 238.

الفرع الثاني

ماهية المعلومات التي يجب استيفاؤها من المبلغ

تتباين المعلومات التي ينبغي أن يدونها المحقق عند تلقي البلاغ بتباين فئات جرائم الحاسوب والإنترنت وبحسب الطبيعة الفنية التي تتميز بها كل فئة عن غيرها، وعلى الرغم من أن لكل فئة من هذه الجرائم المستحدثة معلوماتها الخاصة التي ينبغي الحرص قدر الإمكان على استيفائها عند تلقي البلاغ، إلا أن هناك معلومات تكاد تكون مشتركة بين معظم هذه الفئات، ويمكن الحصول عليها بطرح أسئلة تتناول جوانب محددة منها ما يلي:

1. تاريخ ووقت تلقي البلاغ.
2. المعلومات الخاصة بالمبلغ.
3. المعلومات الخاصة بمتلقي البلاغ.
4. طبيعة ونوع جريمة الحاسب الإلكتروني محل البلاغ.
5. الأسئلة الستة المشهورة والمتعلقة بالجريمة وهي ماذا؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟
6. المعلومات ذات العلاقة بالأنظمة الحاسوبية، مثل طبيعة العتاد ونوعية البرمجيات والمسؤولين عن الأنظمة وطريقة الاتصال بهم وغيرها. [1]

وفي جميع الأحوال فإن أي بلاغ عن جريمة سواء كان فاعلها مجهولاً أم معلوماً ينبغي أن يتضمن على الأقل معلومات أولية عن الجريمة مثل تحديد محل الجريمة ومكان وقوعها ونوعها، إذ تُعد هذه العناصر مهمة وضرورية لمساعدة رجال الضبط القضائي في أي بلاغ متعلق بجرائم

(1) علي عدنان الفيل، مرجع سابق ذكره، ص12..

تقنية المعلومات بحيث تُمكنهم من تحديد معالم الجريمة ووضع خطة للتعامل معها من الناحيتين الفنية والقانونية. [1]

ومما يجدر التنويه عليه أن عملية تلقي البلاغ لا تعدو أن تكون محادثة قصيرة وسريعة تهدف إلى تمكين المحقق من وضع تصور مبدئي عن ظروف وملابسات الحادث قبل الانتقال إلى مسرح الجريمة، كما أن دقة وتكامل المعلومات محل البلاغ على درجة كبيرة من الأهمية، حيث إنه من الممكن أن تسهم في مساعدة المحقق على ما يلي:

1. تحديد ما إذا كان السلوك محل البلاغ يعد سلوكاً إجرامياً يندرج ضمن جرائم الإنترنت والحاسب الآلي أم لا.
2. وضع تصور مبدئي عن خطة العمل المناسبة للتحقيق في الواقعة.
3. تحديد نوع الخبرة الفنية التي يحتاجها في المعاينة ورفع وتحريز الأدلة من موقع الحادث، والعمل على سرعة استدعاء الخبراء القادرين على إنجاز ذلك. [2]

كما أن هناك وسيلتان لأعضاء الضبط القضائي لغرض الحصول على البيانات المتعلقة بارتكاب الجريمة من نظام حاسوب، وهما تستندان إلى معايير تقنية وقانونية، وتتمثل بما يأتي:

1. يتم الحصول على المعلومات من الموقع نفسه الذي تم من خلاله ارتكاب الجريمة بعد أن يتم اكتشافه باستخدام البرمجيات الحديثة.
2. يتم الحصول على المعلومات عن طريق اعتراض أو رصد البيانات المنقولة من الموقع أو إليه أو في إطاره. [3]

(1) حسين خليل مطر، مرجع سابق ذكره، متاح على ذات الرابط السابق.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص 12-13.
(3) حسين خليل مطر، مرجع سابق ذكره، متاح على ذات الرابط السابق..

الفرع الثالث

تشكيل فريق التحقيق

يوجد الكثير من المحققين الجنائيين ذوي خبرة طويلة في هذا المجال، وكما أن هناك خبراء في الحاسوب والشبكات المعلوماتية ذوي معرفةٍ واسعةٍ في مجال عملهم، ولكنه من النادر أن يوجد شخص واحد يمتلك مهارات عالية في المجالين معاً. خاصةً وأن مجالات الحاسوب والإنترنت متعددة ومتشعبة وعلى درجة كبيرة من التعقيد وسرعة التطور، ولذلك كان من الضروري أن يستعين المحقق بخبراء في هذا المجال بحسب ما تفرضه ظروف كل قضية وملابساتها. [1]

وكما هو معروف أن المحقق الجنائي غالباً ما يستعين بالخبراء في مجالات عدة تتعلق بالتحقيق في الجرائم التقليدية، مثل الأطباء الشرعيين وخبراء الأدلة الجنائية وخبراء التصوير، وغيرهم من الخبراء الذين تعتمد الشرطة على قدراتهم المتنوعة في تنفيذها لأعمالها. [2]

فإن تشكيل فريق متخصص بالتحقيق في الجرائم بشكل عام قد يعد أمراً ضرورياً، ويرجع تقدير ذلك للجهة التحقيقية، أما على مستوى الجرائم الإلكترونية فالأمر مختلف، إذ يُعد تشكيل هكذا فريق للتحقيق في الجرائم المعلوماتية هو من الاعتبارات التي لا مناص منها وله أهمية خاصة نظراً لطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية عن غيرها من الجرائم، وذلك لأن هذه الجرائم مرتبطة بمسائل فنية وعلمية بحتة، بحيث يصبح لازماً على القائم بالتحقيق الاستعانة بالخبراء والمختصين، لأن تصدي المحقق لفحص شيء وإبداء الرأي فيه دون أن تتوافر لديه المعرفة اللازمة يجعل قراره معيباً يضر بمصلحة التحقيق ويعوق الوصول إلى الحقيقة، وكل ذلك

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص 245.
(2) ذات المرجع السابق، ص 245.

يصب في أهمية التقارير التي يُنجزها خبراء تقنية المعلومات في مجال الجرائم المعلوماتية ويُعطيها مكانة متميزة من حيث الإلزام. [1]

وكذلك الحال بالنسبة لجرائم الحاسوب والإنترنت، فإن التحقيق فيها قد يتطلب أيضاً الاستعانة ببعض خبراء مسرح الجريمة التقليدية مثل خبير البصمات وخبير التصوير، بالإضافة إلى غيرهم من الخبراء الذين قد يفرضهم ارتباط جريمة الحاسوب محل التحقيق بجريمة أخرى من الجرائم التقليدية كجريمة القتل وغيرها. [2]

فضلاً عن ضرورة الاستعانة بخبير من خبراء الحاسب الآلي والشبكة المعلوماتية وذلك بحسب نوع الجريمة المعلوماتية التي وقعت. ففي مرحلة جمع الاستدلالات في الجرائم التقليدية نجد أن المشرّع الليبي قد أقر في قانون الإجراءات الجنائية اختصاصات معينة لمأموري الضبط القضائي باعتبارهم المعنيون بالقيام بأعمال الاستدلال مثل سرعة انتقال مأمور الضبط القضائي لمكان ارتكاب الجريمة لضبط الواقعة وعدم طمس الأدلة، وغيرها من الاختصاصات الواردة في المادة "14" من قانون الإجراءات الجنائية الليبي والسالفة الذكر.

وفي هذا المقام يتواجد سؤال يطرح نفسه ألا وهو: هل من الأهمية علم مأمور الضبط القضائي بتقنيات نظم المعلومات لتقدير مدى صحة التحريات التي يجريها في نطاق الجريمة المعلوماتية؟

نظراً للطبيعة المتميزة والخاصة للجرائم المعلوماتية، الأمر الذي يثير جملة من الإشكاليات القانونية والتحديات العملية أمام القائمين على مكافحتها ومن أبرزها صعوبة اكتشافها والاستدلال على مرتكبيها، وذلك بسبب استهدافها للمعنويات "البرامج والمعلومات" لا المحسوسات أو الماديات؛

(1) حسين خليل مطر، مرجع سابق ذكره، متاح على ذات الرابط السابق.
(2) محمود أحمد القرعان، مرجع سابق ذكره، ص 246.

فضلاً عن أن مباشرة الاستدلال والتحقيق فيها يتطلب دراية كبيرة بتقنية المعلومات مما يتعذر على الأجهزة الضبطية والتحقيقية التقليدية التعامل معها. [1]

ولذا كان من الضروري أن يكون مأموري الضبط القضائي على علم ومعرفة بتقنيات نظم المعلومات وذلك كدليل وسند على صحة التحريات التي يجب عليه القيام بها، وبالتالي يكون حرياً بمأمور الضبط القضائي أن يتوافر لديه هذا القدر من العلم والمعرفة بتقنيات المعلوماتية حتى تُصبغ تحرياته بشأن الجريمة المعلوماتية بالجدية المطلوبة. [2]

ولأن ليس كل مأموري الضبط القضائي على قدر من المعرفة بتقنيات نظم المعلومات، لذا كان من الأفضل إسناد هذه المهمة لفريق يشكل من ذوي الخبرة الفنية في هذا المجال نظراً لأن التحقيق في الجرائم المعلوماتية بل وكذلك القيام بجمع الاستدلالات بخصوصها يتطلب مهارات فنية خاصة وخبرات متنوعة ومتعددة قد لا تتوافر لدى كثير من رجال الشرطة، فإن تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم قد يكون أمراً ضرورياً وحتمياً، وعلى هذا الأساس يمكن تقسيم فريق التحقيق في الجرائم المعلوماتية "جرائم الحاسوب والإنترنت" إلى فئتين:

الأولى: تمثل الأشخاص الذين يتصل عملهم مباشرة بجرائم الحاسوب والإنترنت ولا يمكن التحقيق في أي جريمة تنتمي لهذه الطائفة من الجرائم الإلكترونية بدون تواجدهم، فوجودهم أمر ضروري على مسرح الجريمة كما تتوافق خبراتهم مع الطبيعة المميزة لهذا النوع من الجرائم. [3]

الثانية: تمثل الأشخاص الذين قد تتطلب ظروف مسرح الجريمة تواجدهم إلا أن دورهم ليس وثيق الصلة بالطبيعة الخاصة لجرائم الحاسب الآلي والإنترنت، مثل: أفراد حماية وتأمين

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 89.
(2) طارق إبراهيم الدسوقي عطية، مرجع .سابق ذكره، ص 410.
(3) علي عدنان الفيل، مرجع سابق ذكره، ص 17.

مسـرح الجريمـة وأفـراد القـبض وأفـراد المباحـث والمراقبـة السـرية وفرقـة الاقتحـام وفريـق أبطـال المتفجرات... وغيرهم. [1]

ويمكن تحديد أعضاء فريق التحقيق في الجرائم المعلوماتية الأساسيين الذين ينتمون إلى الفئة الأولى كما يلي:

1. قائد الفريق: وهو شخص يشترط فيه أن يكون له خبرة طويلة في مجال التحقيق الجنائي ولديه معرفة جيدة بالطبيعة الخاصة للجرائم المعلوماتية وقد تلقى دورات تدريبية كافية عن الحاسوب والشبكات المعلوماتية حتى يتولى السيطرة بشكل كامل على مسرح الجريمة وتوزيع المهام على الفريق والإشراف على قيامهم بأعمالهم والتنسيق مع الجهات ذات العلاقة واتخاذ كافة القرارات الهامة المتصلة بالتحقيق. [2]
2. محقق جنائي: وهو شخص أو أكثر بحسب ظروف الجريمة، وتكون لديه خبرة ومعرفة واسعة بأساليب التحقيق وإجراءاته والإلمام بطبيعة جرائم الحاسوب والإنترنت وكيفية التعامل مع الأدلة الرقمية ويتولي التفتيش عن الأدلة وأخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة [3].
3. خبير الحاسب الآلي والشبكات المعلوماتية: وهو شخص أو أكثر بحسب ظروف الواقعة، ويكون جامع بين المعرفة بعلوم الحاسب الآلي والشبكات وبين الإلمام بإجراءات التحقيق الجنائي وأساليبه وكيفية التعامل مع مسرح الجريمة، ويكون مسؤولاً عن رفع وتحريز الأدلة

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص247.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص 17.
(3) علي جبار الحسيناوي، مرجع سابق ذكره، ص 130.

الجنائية الرقمية بالطريقة المناسبة فنياً بحيث لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوى وعرضها على المحكمة. [1]

4. خبير مدقق حسابات: وهو شخص متخصص في المراجعة المحاسبية وعلى درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة في المؤسسات المصرفية، والآليات المختلفة التي يتم بواسطتها تبادل النقد الإلكتروني ويعمل مع خبير الحاسوب والشبكات على تحديد أسلوب الجريمة وما إذا كان هناك تلاعب في الأنظمة المتضررة بالإضافة إلى تحديد الحجم التقريبي للخسائر المادية الناجمة عن الحادث. [2]
5. خبير تصوير: وهو شخص يتولى تصوير مسرح الجريمة، كالمتبع في جميع الجرائم التقليدية، بالتصوير الفوتوغرافي والفيديو مع الاهتمام بشكل خاص بتصوير شاشات عرض الحواسيب المتضررة إذا كانت في وضع التشغيل وذلك قبل أن يقوم خبير الحاسوب بعمله.
6. خبير بصمات: وهو شخص يقوم برفع البصمات من مسرح الجريمة كإجراء عام في معظم الجرائم، مع ضرورة التركيز على المكونات المادية للحواسيب والشبكات المتضررة أو المشتبه بوجود صلة لها بالجريمة خاصة لوحة المفاتيح والفأرة وذلك بعد اتخاذ الاحتياطات الفنية اللازمة من قبل خبير الحاسب الآلي.
7. خبير رسم تخطيطي: وهو شخص يقوم بعمل رسم تخطيطي كروكي لمسرح الجريمة بطريقة فنية ودقيقة مستخدماً مقياساً مناسباً للرسم بما يوضح تقسيماته وأماكن تواجد الأدلة والأشخاص فيه. [3]

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص 248.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص 248.
(3) ذات المرجع السابق، ص248.

أما بقيمة أعضاء الفريق من الفئة الثانية فتحديدهم نوعاً وكماً، أمر متروك لتقدير المحقق على ضوء المعلومة المتوفرة لديه عن الجريمة ، وعلى حسب ما تفرضه طبيعة مسرح الجريمة وحجمها وظروفها، ومن أهمهم، قوة مناسبة لتأمين مسرح الجريمة والقبض على المتهمين وترحيلهم عند الحاجة وهذه القوة قد لا يخلو مسرح أي جريمة من وجودها. [1]

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص 247-248.

المطلب الثاني

التحري وكشف غموض الجريمة المعلوماتية

تمهيد وتقسيم:-

تتسم الجرائم ذات الصلة بالحاسب الآلي بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو آثارها، ولذا يقتضي أن تكون جهات التحري والتحقيق على درجة كبيرة من المعرفة بأنظمة الحواسيب الآلية وطريقة تشغيلها، وأساليب ارتكاب الجرائم عليه أو بواسطتها، بالإضافة إلى القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها والتحفظ على البيانات والأجهزة التي استخدمت في ارتكابها أو تلك التي تكون محلاً للجريمة. [1]

وسنتناول بالشرح كل ما سبق ذكره وذلك على هذا النحو:

الفرع الأول

صعوبة اكتشاف الجريمة المعلوماتية

لعل أولى الصعوبات التي تواجه التعامل الأمني مع هذا النوع من الجرائم بعد وقوعها هي صعوبة اكتشافها حتى من قبل الضحايا أنفسهم سواء كانوا أفراداً أو شركات، كما أن الكثير من هذه الجرائم قد تقع دون أن يتم اكتشافها أصلاً أو يتم اكتشافها بعد مرور فترة طويلة على ارتكابها بحيث تكون أدلة الإدانة قد تلاشت أو تعذر استخدامها في الحقيق. [2]

(1) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص60.
(2) محمود أحمد القرعان، مرجع سابق ذكره، ص 233-234.

فالجريمة المعلوماتية تتميز بصعوبة اكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم هي قليلة إذا ما قورنت بما يتم اكتشافه من الجرائم التقليدية. [1]

فقد أشارت الدراسات أن ما يتم اكتشافه من جرائم المعلومات يصل إلى نسبة 10% والذي يتم الإبلاغ عنه من هذه النسبة لا يكاد يصل إلى 5% فقط. [2]

ويمكن اكتشاف جرائم الحاسوب والإنترنت (الجرائم المعلوماتية) بشكل عام بإحدى هذه الطرق:

1. ضبط المجرم وهو في حالة تلبس كضبطه وهو يحاول اقتحام غرفة الحاسوب أو المبنى الخاص به عنوة بغرض سرقة أو إتلاف البيانات الرقمية، أو أن يقوم بالولوج إلى النظام المعلوماتي بطريقة غير مشروعة وبواسطة نوع من أنواع الاتصال الشبكي وباستخدام نفس اسم المستخدم وكلمة المرور الخاصة بمدير النظام (انتحال الشخصية) وأثناء ولوج أو دخوله مدير النظام الحاسوبي إلى نظامه المعلوماتي يجد أن هناك شخصاً آخر متصل بهذا النظام من خارج المنظمة. [3]
2. وجود برمجيات متطورة خاصة بالحماية تقوم باكتشاف الخطر فور حدوثه وذلك مثل أنظمة الجدار الناري أو أنظمة اكتشاف الاختراق وكذلك الأنظمة المضادة للفيروسات، بحيث تقوم وبطريقة آلية بتوجيه إنذار لمدير النظام فور اكتشافها لأية نشاطات مشبوهة على الشبكة المعلوماتية؛ فمثلاً هذه البرمجيات لا غنى عنها في كشف الجريمة بالنظر لضخامة حجم المعلومات الموجودة في شبكة الإنترنت. [4]

---

(1) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص24.

(2) عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة مقدمة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط ، عمان، 2014م، ص 21.

(3) محمود أحمد القرعان، مرجع سابق ذكره، ص 234.

(4) حسين خليل مطر، مرجع سابق ذكره، متاح على نفس الرابط السابق.

3. اكتشاف الجريمة من قبل مدراء النظام وذلك من خلال ملاحظة تلف البيانات، أو تعديل بعض الملفات الحساسة أو ولوج النظام باستخدام بيانات مستخدم مستحدثة قد تم إضافتها بغير علم مدير النظام المعلوماتي. [1]

4. قد يصرح (يعترف) بها الشخص الذي ارتكب الجريمة دون أن يكون لدى الضحية أدنى علم عنها، بحيث إن هذه الجريمة ما كانت ستُكتشف لولا أنه لم يُبلغ هو نفسه عن ارتكابها وذلك على سبيل الابتزاز أو التباهي باختراق الأنظمة المعلوماتية. [2]

ولعل الأسباب وراء صعوبة كشف وإثبات الجرائم المعلوماتية ترجع إلى الأمور الآتية:

1. أنها جريمة لا تترك أثراً مادياً لها بعد ارتكابها، فهي لا تترك أي أثر خارجي أو مرئي لما يجري خلال تنفيذها من عمليات، حيث يتم بالنبضات الإلكترونية نقل المعلومات [3]. وبالتالي اختفاء السلوك المكون لها، كما أن الجاني يمكن أن يرتكب هذه الجريمة في دول وقارات أخرى، ذلك لأن الجريمة المعلوماتية هي جريمة عابرة للدول "دولية" ، وكذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة يشكل عاملاً إضافياً في صعوبة اكتشاف هذا النوع من الجرائم المستحدثة[4].

2. صعوبة الاحتفاظ الفني بآثارها إن وجدت.

3. صعوبة التعامل معها من قبل المحقق التقليدي بسبب الطبيعة الخاصة للجرائم المعلوماتية، ومن ثم ضرورة الاعتماد على الخبرة الفنية لإمكانية كشفها. [5]

---

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص 234.
(2) ذات المرجع السابق، ص 234.
(3) محمد علي العريان، الجرائم المعلوماتية، د. ط. ، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص53.
(4) جميل عبدالباقي الصغير، مرجع سابق ذكره، ص17.
(5) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق ذكره، ص19.

4. تعتمد على الخداع وقمة الذكاء في ارتكابها والتضليل في التعرف على مرتكبيها، مما يجعل الكثير من مجرمي المعلوماتية بمنأى عن العقاب بسبب صعوبة اكتشاف جرمهم. [1]

(1) علي جبار الحسيناوي، مرجع سابق ذكره، ص 136.

الفرع الثاني

تدريب وتطوير الأجهزة المعنية بمواجهة الجرائم المعلوماتية

لكي يتم مواجهة ومكافحة هذا النوع من الإجرام المعلوماتي المستحدث على أكمل وجه لا يكفي سن التشريعات اللازمة لتجريم أشكال هذا الإجرام فقط بل يجب أن تدعمه جهود أخرى تُعنى بإعداد الأجهزة الضبطية المعنية بضبط الجريمة المعلوماتية والتحري عن مرتكبيها وملاحقتهم، وتكون قادرة على التعامل مع هذه الجرائم بشكل جيد وفعال وهي ما يُعرف بشرطة الإنترنت "Internet Police"، فقد قطعت بعض الدول المتقدمة شوطاً كبيراً في هذا المضمار وذلك من خلال قيامها بإنشاء إدارات أو وحدات أو أقسام خاصة بشرطة الإنترنت . [1]

منها دولة مصر حيث أنشأت وزارة الداخلية المصرية عدة أجهزة وهي:

1. إدارة مكافحة جرائم الحاسبات وشبكات المعلومات.
2. قسم مكافحة جرائم الحاسبات وشبكات المعلومات.

حيث أوكلت إليها مهمة تأمين ووقاية نظم شبكات المعلومات لأجهزة وزارة الداخلية لمنع وقوع أية جرائم عليها باستخدام الأساليب والتقنيات العلمية الحديثة، ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات مثل الاختراقات وبث الفيروسات. [2]

وكذلك الولايات المتحدة الأمريكية حيث قامت بإنشاء جهاز شرطة خاصة بجرائم الإنترنت سنة 1987م، ثم تطور هذا الجهاز وتحول إلى شرطة دولية للشبكة المعلوماتية مهمتها السهر على حماية مجتمع تكنولوجيا المعلومات في جميع أنحاء العالم، ومن مهام هذا الجهاز التحري عن

(1) موسى مسعود أرحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 105-106.
(2) خالد ممدوح إبراهيم، مرجع سابق ذكره، ص 169-170.

إساءة استخدام شبكة الإنترنت سواء في الجرائم البسيطة المتمثلة في المضايقات التي تتم من خلال البريد الإلكتروني أو بالنسبة للجرائم الكبيرة أو المعقدة والأكثر خطورة بما في ذلك الاستيلاء على الأموال وتسهيل الأعمال غير المشروعة بأنماطها وصورها كافةً ، والتتبع والقيام بالإدعاء في بعض الأحيان وفض المنازعات، ويمارس هذا الجهاز وظيفته هذه من خلال عدد من المنتسبين إليه والمدربين على أحدث تقنيات وأساليب مكافحة الجريمة المعلوماتية بحيث يمتازون بالتخصص والمعرفة الكافية بكل جوانب الجريمة المعلوماتية والمهارات العالية للقوى البشرية التي تنتمي إليه، بالإضافة إلى الإلمام بالقوانين المُطبقة في هذا المجال[1].

فيجب القيام بإعداد برامج تدريب وتأهيل لهذه الكوادر البشرية من الناحية الفنية على نحو يمكنها من تحقيق المهمة المسندة إليها بالكفاءة المطلوبة، ففي الفترة الأولى لظهور هذا النوع من الجرائم وقعت الشرطة في أخطاء جسيمة أدت إلى الإضرار بالأجهزة والملفات والأدلة الرقمية الخاصة بإثبات الجريمة، وذلك بسبب عدم توافر الكفاءة اللازمة لديهم من أجل مكافحة هذا النوع من الإجرام المعلوماتي. [2]

فمن الضروري الاهتمام بمسألة تأهيل سلطات الملاحقة وتزويد أفرادها بالمعرفة العلمية والتقنية ليكونوا على دراية بكل جوانب الجريمة المعلوماتية، كما دعا المجلس الأوروبي في إحدى توصياته سنة 1999م إلى ضرورة تدريب الشرطة وأجهزة العدالة بما يواكب التطور المتلاحق لتقنية المعلومات، وكذلك عقدت المنظمة الدولية للشرطة الدولية العديد من الدورات التدريبية لمحققي جرائم الحاسب الآلي. [3]

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص 106-107.
(2) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص61.
(3) مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العُليا في الدول العربية، منعقد في 2012/09/25 ، السودان، ص59.

وبالتالي يجب أن يكتسب المحقق في جرائم الحاسب الآلي والإنترنت مهارات خاصة تتسم بالجدة والحداثة وتتوافق مع طبيعة هذا النوع من الإجرام المستحدث ومن هذه المهارات:

1. التعرف على المكونات المادية للحاسب الآلي والتعامل المبدئي معها ومعرفة كيفية تشغيلها.
2. معرفة أساسيات عمل شبكات الحاسب الآلي وأهم مصطلحاتها.
3. التعرف على الصيغ المختلفة للملفات وتطبيقات الحاسب الآلي الرئيسية التي تتعامل معها.
4. إجادة التعامل مع خدمات الإنترنت الرئيسية.
5. معرفة الأدوات والأساليب المستخدمة في ارتكاب الجرائم المعلوماتية. [1]
6. معرفة أهم تقنيات أمن الحاسب الآلي والإنترنت وأدواتها وطريقة عملها ووسائل اختراقها.
7. الإطلاع على بعض الجوانب المتعلقة بالجرائم المعلوماتية ودراسة حالات قد وقعت سلفاً وكيف تم مواجهتها.
8. معرفة أنماط الجرائم المعلوماتية والخصائص التي تتميز بها. [2]

(1) منى كامل تركي، مرجع سابق ذكره، متاح على الرابط السابق.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص 22-26.

الفرع الثالث

صعوبة إثبات الجرائم المعلوماتية والدليل الرقمي

إن الإثبات في المواد الجنائية يخضع لقواعد تختلف عن تلك التي تحكم الإثبات في المواد المدنية، وذلك لاعتبارات عدة منها ما يرجع إلى أهمية الدعوى الجنائية، ومنها ما يرجع إلى اختلاف موضوع الإثبات بين تلك المواد. [1]

فإن طبيعة محل أو موضوع الإثبات المدني يختلف عن موضوع الإثبات الجنائي، ففي حين نجد أن الإثبات المدني ينصب على تصرفات قانونية من السهل في الغالب إثباتها، الإثبات الجنائي يرد على وقائع مادية ونفسية بحيث يكون من الصعب الحصول على أدلة تفيد إثبات الجريمة على مرتكبها، خاصةً إذا تم ارتكابها في الخفاء وفي ظل ظروف غامضة، مع محاولة العبث بالأدلة وطمس آثارها. [2]

وهناك مبدأ أساسي يحكم تقيم وتقدير قيمة الأدلة في قوانين الإجراءات الجنائية وهو "حرية القاضي الجنائي في تكوين عقيدته".

بمعنى أنه له مطلق الحرية في تقدير قيمة أدلة الدعوى، وبالتالي تكوين عقيدته أو قناعته منها، فالقاضي يقبل جميع الأدلة التي يقدمها الخصوم في الدعوى فلا يوجد أدلة يحظر القانون مقدماً قبولها، وبعد ذلك يمارس القاضي السلطة التقديرية الكاملة في تقدير قيمة الأدلة، فله أن يأخذ بها أو أن يطرحها، ومن ثم يحكم في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته

(1) مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، الجزء الثاني، ط1، منشورات الجامعة الليبية، كلية الحقوق، 1971م، لبنان، بيروت، ص 150.

(2) موسى مسعود ارحومة، إشكالية قبول الدليل العلمي أمام القضاء الجنائي، دراسة مقارنة، اطروحة لنيل دكتوراه الدولة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط، 1995-1996م، ص2.

ودون أي التزام عليه بالتقيد بطريق معين من طرق الإثبات إلا إذا أوجب القانون عليه ذلك، وهذا ما تضمنته نص المادة "275" إجراءات جنائية ليبي. [1]

حيث نصت على أن يحكم القاضي في الدعوى بكامل حريته حسب العقيدة التي تكونت لديه، وهذا يعتبر تقريراً لنظام حرية اقتناع القاضي في المسائل الجنائية من حيث طرق إثباتها وتحديد قيمتها التدليلية لوسائل الإثبات المتعلقة بها، حسب ما يتولد في نفسه من قوة اقناعية ناتجة عن تقديره للأدلة المطروحة عليه في الجلسة بعدما يتأكد من مشروعية قبولها في نظام الإثبات الذي ينتمي إليه بالإضافة إلى مشروعية الحصول عليها وطرحها أمام القاضي في الجلسة، وبهذا أطلق على هذا النظام اسم نظام الإثبات الحر، نظراً لما يمنحه للقاضي الجنائي من حرية في تقدير الدليل الذي يطرح عليه في الجلسة.[2]

إذاً نجد أن المشرّع قد خول القاضي سلطة واسعة من حيث قبول الدليل وتقدير قيمته الإثباتية؛ إذ أفسح المجال أمامه لكي يستلهم عقيدته من أية وسيلة أو دليل يطمئن إليه وجدانه ويرتاح إليه ضميره، يستوي أن يكون الدليل الذي بني عليه حكمه واستمد منه قناعته، متحصلاً من إجراءات البحث التمهيدي "جمع الاستدلالات"، أو التحقيق الابتدائي، أو التحقيق النهائي أثناء المحاكمة.[3]

فالإثبات هو الوسيلة الثبوتية التي يتوصل إليها قاضي الموضوع من خلال تكوين قناعته المستمدة من الأدلة المطروحة أمامه في القضية والتي من شأنها إثبات التهمة في حق المتهم وبالتالي إصدار الحكم بالعقوبة المقررة له قانوناً أو نفيها عنه ومن ثم الحكم ببراءته، وبالتالي يُعرف

(1) سالم محمد الأوجلي، مقبولية الدليل الرقمي في المحاكم الجنائية، مجلة دراسات قانونية، جامعة بنغازي، كلية الحقوق ، العدد التاسع عشر، 2016م، ص 23-24..

(2) أحمد الصادق الجهاني، مقدمة في الإثبات الجنائي ، مقرر دراسي لطلبة الدراسات العليا، جامعة بنغازي، للعام الجامعي 2020م، ص1.

(3) موسى مسعود ارحومة، إشكالية قبول الدليل العلمي أمام القضاء الجنائي، مرجع سابق ذكره، ص2-3.

الإثبات بأنه "إقامة الدليل أمام القضاء بالطرق القانونية التي يحددها القانون على وجود واقعة قانونية ترتبت آثارها. [1]

أما الدليل الجنائي فيمكن تعريفه بأنه هو "الواقعة التي يستمد منها القاضي البرهان على إثبات إقتناعه بالحكم الذي ينتهي إليه".[2]

كما يُعرف الدليل في المجال الجنائي بأنه: "الوسيلة التي يستعين بها القاضي للوصول إلى اليقين القضائي الذي يقيم عليه حكمه في ثبوت الإتهام المعروض عليه أو نفيه".[3]

وبجانب مبدأ "حرية القاضي الجنائي في تكوين عقيدته" توجد قاعدة أخرى تحكم الإثبات في المسائل الجنائية وهي:

الدور الإيجابي للقاضي الجنائي في البحث عن الحقيقة: بمعنى أنه عليه التحري عن الحقيقة والكشف عنها، وليس فقط الموازنة بين الأدلة المثبتة للإدانة أو المثبتة للبراءة.[4]

كما أن المعروف في المواد الجنائية إن عبء الإثبات يقع على سلطة الإدعاء من منطلق أن الأصل في الإنسان البراءة وعلى من يدعي عكس ذلك إثباته. [5]

ولاشك في أن كل هذه القواعد التي تحكم الإثبات في المسائل الجنائية بخصوص الجرائم التقليدية هي نفسها المتبعة في شأن الجرائم المعلوماتية، إلا أن الطابع الخاص الذي تتميز به هذه الجرائم يجعل من الصعوبة اكتشاف وقوعها، لأنها لا تترك أثراً مادياً خارجياً "مرئياً"، فالجرائم

(1) عبداللطيف عبداللطيف الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، ط1، دار الحامد للنشر والتوزيع، عمان، 2011، ص 175..
(2) مأمون سلامة، الإجراءات الجنائية في التشريع الليبي، الجزء الثاني، مرجع سابق ذكره، ص 166-167.
(3) سالم محمد الأوجلي، مرجع سابق ذكره، ص 20.
(4) منى كامل تركي، مرجع سابق ذكره، متاح على الرابط السابق.
(5) مفتاح بوبكر المطردي، مرجع سابق ذكره، ص 20.

المعلوماتية لا عنف فيها ولا سفك للدماء ولا آثار اقتحام من أجل سرقة الأموال مثلا، وإنما هي أرقام وبيانات قد تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات الآلية. [1]

ولأن الجرائم المعلوماتية هي جرائم فنية تتطلب تكنيك معين في مجال الحاسبات الآلية وبالتالي فإن أدلة الإدانة الناتجة عنها هي ذات نوعية مختلفة "معنوية" مثل سجلات الكمبيوتر ومعلومات الدخول والاشتراك والبرمجيات والتي دائماً ما تثير أمام القضاء مشكلات جمة من حيث مدى قبولها وحجيتها أمام القضاء الجنائي والمعايير المطلوبة لتكون أدلة خاصةً في ظل قواعد الإثبات التقليدي. [2]

ومن هنا ظهر ما يُعرف "بالدليل الرقمي"، وهذا الدليل يصلح لإثبات الجريمة المعلوماتية سواء كان الاعتداء واقعاً على الكيان المادي للحاسب الآلي أو واقعاً على الكيان المعنوي للحاسب الآلي أو على قاعدة البيانات أو المعلومات التي قد تكون على شبكة المعلومات الدولية مثل انتهاك الملكية الفكرية أو جرائم القرصنة وغيرها. فالدليل الرقمي في مثل هذه الجرائم يُعتبر هو الدليل الأفضل لإثبات وقوعها إن وجد. [3]

وكذلك يصلح الدليل الرقمي لإثبات وقوع الجرائم التقليدية المرتكبة بواسطة الحاسب الآلي والإنترنت وذلك كوسيلة مساعدة لإرتكاب الجريمة مثل استعمال الأدلة الرقمية "حاسوب – هاتف"...الخ، وأيضاً في عمليات الاحتيال أو غش المعلوماتي أو غسل الأموال أو تهريب

(1) محمد علي العريان، الجرائم المعلوماتية، د.ط، دار الجامعة الجديدة للنشر، جامعة الإسكندرية، 2004م، ص25.
(2) يونس عرب، مرجع سابق ذكره، ص 21.
(3) طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، المنعقد في الفترة من 28-2009/10/29م، طرابلس، ص6.

المخدرات ...الخ فبالرغم من عدم اتصال هذه الجرائم بالنظام المعلوماتي فإن الدليل الرقمي يصلح كدليل لإثباتها. [1]

ويُعرف الدليل الرقمي في الجرائم المعلوماتية بأنه: "أي بيانات مخزنة أو منقولة باستخدام الكمبيوتر التي تدعم أو تدحض نظرية كيفية وقوع الجريمة أو توضح عنصراً حاسماً في الجريمة.[2]

كما يُعرف الدليل الرقمي بأنه : "هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهي مكون رقمي لتقديم معلومات في أشكال متنوعة، مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنقاذ وتطبيق القانون[3]. فالأدلة الرقمية هي نتاج لاستخدام التقنية الحديثة من بيانات وأرقام وصور وغيرها في بيئة افتراضية ، وتستخدم في جمعها واستخلاص المعلومات المتعلقة بالجريمة والمجرم برامج خاصة، وتقنية عالية تعتمد على نوع الدليل ونوع الجهاز ونظام التشغيل. [4]

ويتميز الدليل الرقمي بالخصائص الآتية:

1. دليل غير ملموس.
2. دليل من قبيل الأدلة الفنية أو العلمية "الأدلة المستمدة من الآلة".
3. إن فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة تجميع وتحليل فحواه ليكون دليل إثباتها.[5]

(1) طارق محمد الجملي، مرجع سابق ذكره، ص 6.
(2) سالم محمد الأوجلي، مرجع سابق ذكره، ص 20.
(3) طارق محمد الجملي، مرجع سابق ذكره، ص 2-3.
(4) سالم محمد الأوجلي، مرجع سابق ذكره، ص 21.
(5) مفتاح بوبكر المطردي، مرجع سابق ذكره، ص 20

كما أن للدليل الرقمي ثلاثة أنواع:

النوع الأول: مخرجات ذات طبيعة ورقية تسجل فيها المخرجات على الورق ويستخدم في ذلك الطابعات والراسم في طباعة الرسومات بدرجات وضوح مختلفة على الورق.

النوع الثاني: مخرجات ذات طبيعة إلكترونية تستخدم في تخزين المعلومات بدل الوثائق الورقية كالأشرطة المغناطيسية والأوراق المغناطيسية.

النوع الثالث: مخرجات مرئية معروضة بواسطة شاشة الحاسب الآلي ذاته، ويتمثل هذا النوع في عرض البيانات المعالجة آلياً بواسطة الحاسب الآلي على الشاشة الخاصة به. [1]

وأن هذه الجرائم المعلوماتية عادة ما يتم ارتكابها عبر مسافات بعيدة، وذلك باستخدام وحدات طرفية أو باتصال هاتفي يمكن للجاني من خلالها إعطاء تعليمات للحاسب الآلي، فقد حدث أن أحد الهواة في أوروبا تمكن من حل شفرة أحد مراكز المعلومات في البنتاجون وزارة الدفاع الأمريكية وأصبح السبيل أمامه مفتوحاً للعبث ببيانات هذه المراكز. [2]

كما أن الطبيعة الخاصة للجرائم المعلوماتية، بحيث يتم ارتكابها في الغالب في صورة إصدار أوامر إلى جهاز الحاسب الآلي، تجعل الجاني يستطيع تدمير أدلة الإدانة في أقل من ثانية، حالما يشعر بأن أمره سينكشف يُسرع بإلغاء هذه الأوامر بمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسب الآلي، وهذا ما يجعل كشف الجريمة المعلوماتية وتحديد مرتكبها أمراً في غاية الصعوبة. [3]

(1) ذات المرجع السابق، ص 21.

(2) جميل عبدالباقي الصغير، مرجع سابق ذكره، ص 17.

(3) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون بأكاديمية الدراسات العليا طرابلس ، ليبيا، المنعقد خلال الفترة 28-2009/10/29م ، ص 60.

ومع مرور الوقت اكتسب الجناة خبرة واسعة في التلاعب بالبيانات وإتلافها في غضون ثوانٍ معدودة قبل كشف الجريمة ، ويتم ذلك عادة باستخدام برامج معينة تعمل على إتلاف أو تدمير البيانات بصورة تلقائية بعد مضيء فترة من الزمن بحسب رغبة مصمم البرنامج وفي الوقت الذي يشاء، وفي المقابل ومن أجل التصدي لاعتداءات الجناة على النظام المعلوماتي، يجتهد المهندسون في مجال تقنية المعلومات لابتكار برامج معينة لهذا الغرض، تمكن آلية عملها في أنه بمجرد محاولة شخص غير مصرح له ولوج النظام المعلوماتي أو استخدام الحاسب الآلي المزود بهذا البرنامج، فإن هذا الأخير يصدر أمراً للجهاز بحيث يتم إتلاف البيانات المخزنة به ومحوها بصورة تلقائية. (1)

ولعل صعوبة كشف الدليل تزداد بصورة خاصة متى ارتكبت هذه الجرائم في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جرائمهم ودون أن يتركوا أية آثار تدل عليهم، كما قد يصعب الوصول إلى الدليل نتيجة قيام كبرى المواقع العالمية على الإنترنت بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية يمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها أو نسخها أو قد يستخدم المجرم كلمات مرور لتخريب الموقع أو استخدام تقنيات التشفير. (2)

أو قد يلجأ الجناة لوسيلة أخرى يتم بها تدمير وإتلاف البيانات المخزنة بجهاز الحاسب الآلي متمثلة في إغلاق الجهاز بصورة فجائية ودون التقيد بالطريقة الآمنة للإغلاق ، كما قد يلجأ الجاني إلى استخدام حاسب آخر غير حاسبه الشخصي مثل استخدام الحواسيب الآلية الموجودة في مقاهي الإنترنت لإخفاء هويتهم وبالتالي عدم القدرة على كشف جرمهم على اعتبار أن جُل هذه

(1) وليد الزيدي، مرجع سابق ذكره، ص 45-47.

(2) متاح على الرابط: www.djelfa-info>showthread قسم أرشيف منتديات الجامعة – ماهية الجريمة الإلكترونية، تاريخ الزيارة: 2017/02/20م، س: 5:00م.

المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هويتهم، وبالتالي أصبح ذلك عقبة أمام الجهات الضبطية للحيلولة دون الوصول إلى الدليل الرقمي، ولذا فإن الغرض من كل هذه الأعمال هي عرقلة أجهزة الضبط والتحقيق وبالتالي عدم إمكانية ضبط الأدلة الرقمية وصعوبة كشفها أصلاً. [1]

كما استطاعت أجهزة العدالة الجنائية الضبطية مع مرور الوقت وما ترتب عليه من اكتساب مهارة وخبرة واسعة في هذا المجال ، إعادة بناء الدليل الرقمي المشطوب أو المخفي أو المشفر ويعتمد ذلك على نوع الدليل الرقمي ونوع الحاسب الآلي ونظام التشغيل وإعدادات الحاسب، فعندما يتم شطب ملف عادةً ما يبقى موجوداً على القرص ويمكن استرجاعه باستخدام برامج خاصة. [2]

وعند إعادة بناء الدليل الرقمي سيترتب عليه إعادة بناء الجريمة وذلك بإصلاح الأدلة المتلفة واستخدامها لتحديد الأعمال المحيطة بهذه الجريمة، ومن التحديات الأخرى الملفات المشفرة حيث إن 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، وكما يمكن في عدة حالات فك التشفير باستخدام الخبرة والأجهزة المناسبة ولكن محاولة فك التشفير هي محاولة غير عملية في بعض التحقيقات، لأنها تأخذ وقتاً خالياً، فالتشفير هو منطقة تخزينية يمكن استغلالها لتهديد الأمن والقوانين.[3]

وبسبب ازدياد انتشار هذه الأعمال والبرمجيات في الدول المتقدمة وما ينجم عنها من مخاطر، فإن بعضها قد استحدث تشريعات تم بموجبها تجريم اللجوء إلى هذه التقنيات من دون

(1) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مرجع سابق ذكره، ص 1-2.
(2) محمود أحمد القرعان، مرجع سابق ذكره، ص 282..
(3) ذات المرجع السابق، ص 282-283.

ترخيص من الأجهزة المعنية، وكذلك فعلت فرنسا الشيء ذاته، ومن شأن الإقدام على هذا التشفير من دون ترخيص أن يصبح الفعل جريمة يعاقب عليها القانون، وكذلك معاقبة الشخص الذي أعد برنامج التشفير من دون ترخيص. [1]

وهناك عدة نواحٍ لمعالجة وفحص الأدلة الرقمية ومنها:

أ. تمييز الأدلة الرقمية: وهي عملية تتكون من عنصرين:

أولاً: يجب على المحقق أن يميز الأجهزة مثل جهاز الحاسب الآلي والأقراص المرنة وكوابل الشبكات والتي تحتوي على المعلومات الرقمية.

ثانياً: يجب على المحقق أن يميز بين المعلومات غير المهمة والمعلومات المرتبطة بالجريمة. [2]

ب. جمع وحفظ الأدلة الرقمية والأجهزة:

يجب جمع وحفظ جميع الأدلة المتعلقة بالقضية بحالتها الأصلية وعدم تغيرها، لأن القانون يتطلب أو يشترط أصالة الأدلة وعدم تغير الحالة الأصلية لها. [3]

ولكي يكون الدليل الرقمي دليلاً مقبولاً أمام المحاكم يجب بالإضافة إلى مشروعية الدليل، التحقيق من أنه قد استخرج أو تم ضبطه من كمبيوتر أو موقع معين، وهو نسخة مطابقة للبيانات الموجودة بجهاز الكمبيوتر دون أن يلحقه أي تغيير "تلاعب أو تعديل أو تلفيق" منذ ضبطه وتجميعه. [4]

(1) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مرجع سابق ذكره، ص 3.
(2) سالم محمد الأوجلي ، مرجع سابق ذكره، ص 35..
(3) ذات المرجع السابق، ص 35.
(4) ذات المرجع السابق، ص 35.

وبالإمكان التأكد من سلامة الدليل الرقمي من التبديل أو العبث به من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات. [1]

ج. توفير الوقت والجهد وتجنب تعطيل أو مقاطعة عمل فرد أو مؤسسة ما:

فقد يؤدي أخذ الجهاز من المؤسسة إلى توقف عملها مثل أجهزة المستشفيات ، فإن أخذ مثل هذه الأجهزة قد يُعرض حياة الناس للخطر. [2]

د. توثيق الأدلة الرقمية والأجهزة:

إن عملية التوثيق مهمة لعدة أسباب منها أن التوثيق يثبت أن الدليل أصيل ولم يطرأ عليه أي تغيير، وكذلك يستخدم هذا التوثيق للتفريق بين الدليل الأصلي والنسخة المأخوذة منه.

هـ. تصنيف ومقارنة الدليل الرقمي:

وهي مرحلة إيجاد الخصائص التي تصنف الأدلة وتميزها عن غيرها، فمثلاً أكثر الناس يعرفون رسائل البريد الإلكتروني ولكن المحققين المدربين يمكنهم تصنيفها بدقة مثل تحديد نوع التطبيق المستخدم، وكما أن المقارنة مهمة عند فحص الدليل الرقمي باستخدام عينة قياسية Control Specimel بحيث يؤدي ذلك إلى إظهار نواحي فريدة من الدليل الرقمي ويمكن استخدام هذه النواحي لربط القضية مع جهاز معين. [3]

وفي هذا المضمار نتساءل عن **موقف المشرّع الليبي من الدليل الرقمي في مجال الإثبات الجنائي**، فهل اعتد به كدليل إثبات في قانون الإجراءات الجنائية الليبي أم لا؟

أولاً نجد أن المشرّع الليبي قد أخذ بنظام الإثبات المقيد "نظام الأدلة القانونية" ، بمعنى أن المشرّع الليبي قد نص في قانون الإجراءات الجنائية على مجموعة من الأدلة دون سواها ونظم

(1) طارق محمد الجملي، مرجع سابق ذكره، ص 19.
(2) محمود أحمد القرعان، مرجع سابق ذكره، ص 284.
(3) ذات المرجع السابق، ص 284.

طرق الحصول عليها في مجال الإثبات الجنائي، وذلك بجانب تمتع القاضي الجنائي بسلطة واسعة في تقدير الدليل مستنداً في ذلك على نص المادة "275" من قانون الإجراءات الجنائية الليبي. ولكن هذه السلطة في تقدير القيمة الاقناعية للدليل المنصوص عليه، يجب أن تقتصر فقط على الأدلة الوارد ذكرها في قانون الإجراءات الجنائية. [1]

أما بالنسبة لموقف المشرّع الليبي من الدليل الرقمي في مجال الإثبات الجنائي، فمن حيث الأصل لا يوجد نص صريح في قانون الإجراءات الجنائية الليبية يقضي بقبول الدليل الرقمي في مجال الإثبات الجنائي، ومع ذلك نرى أن الأدلة الرقمية إذا ما أخذت شكل النصوص المكتوبة على دعامة فإنها تستمد مشروعيتها كدليل من أدلة الإثبات قياساً على المحررات التي يقبل بها القانون الليبي كدليل إثبات. [2]

وكذلك بالنسبة للأدلة الرقمية إذا ما كانت في شكل صورة وتسجيلات فإنها تستمد مشروعيتها بوصفها قرائن قضائية، وبالرغم من ذلك يجب النص على الأدلة الرقمية كأدلة إثبات وبشكل صريح في قانون الإجراءات الجنائية الليبي، ولكن استثناءً على هذا الأصل يوجد بعض التطبيقات الخاصة تقضي بقبول الدليل الرقمي في مجال الإثبات الجنائي الليبي، فهناك بعض النصوص التي ورد ذكرها في بعض التشريعات الخاصة، اعتد فيها المشرّع الليبي بالدليل الرقمي صراحة كدليل إثبات لبعض الجرائم منها: نص المادة "97/2" من القانون رقم "1 لسنة 1373" و.ر بشأن المصارف حيث نصت على أنه "يعتد بالمستندات والتوقيعات الرقمية التي تتم في إطار

(1) طارق محمد الجملي، مرجع سابق ذكره، ص 9.
(2) ذات المرجع السابق، ص 10.

المعاملات المصرفية وما يتصل بها من معاملات أخرى، وتكون لها الحجية في إثبات ما تتضمنه من بيانات" فهذا النص قد أضفى على المستند الإلكتروني الحجية في الإثبات الجنائي. [1]

وكذلك نصت المادة "6" مكرر من القانون رقم "10 لسنة 1428م" بإضافة مادة للقانون رقم "70 لسنة 1973" بشأن إقامة حد الزنى وتعديل بعض أحكام قانون العقوبات على أنه تثبت جريمة الزنى المنصوص عليها في المادة الأولى من هذا القانون باعتراف الجاني أو بشهادة أربعة شهود أو بأية وسيلة إثبات علمية أخرى" حيث أضفى هذا النص على وسائل الإثبات العلمية القيمة القانونية لإثبات هذه الجريمة. [2]

(1) طارق محمد الجملي، مرجع سابق ذكره، ص 10-11.
(2) ذات المرجع السابق، ص 11.

المبحث الثاني

إجراءات التحقيق الابتدائي في الجريمة المعلوماتية

تمهيد وتقسيم:

التحقيق الابتدائي: هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانوناً بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة. [1]

إذاً للتحقيق الابتدائي ثلاثة عناصر:

الأول: يتعلق بطبيعة الإجراء والغاية منه.

الثاني: يتعلق بالسلطة التي أصدرت هذا الإجراء.

الثالث: يتعلق بالشكل الذي روعي في الإجراء.[2]

أما عن التحقيق الفني في نظم الحاسوب والإنترنت فيعرف بأنه" "البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه، أو الإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسب الآلي أو نظمه أو الإنترنت، للاستدلال بها على صدق نسبة الفعل إلى شخص معين أو كذبه. [3]

فالتحقيق الجنائي في الجريمة المعلوماتية هو عبارة عن فحص جهاز الجاني أو المشتبه به من قبل المحققين، فمثلاً إذا تمت جريمة عن طريق الحاسب الآلي أو الأجهزة الذكية المختلفة،

(1)مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، الجزء الأول، ط1، مطبعة دار الكتب، بيروت، لبنان، 1971ف، ص603.

(2) ذات المرجع السابق، ص 603.

(3) علي جبار الحسيناوي، مرجع سابق ذكره، ص 126-127.

فيأتي المحقق المتخصص ليفحص ما به باستخدام أدوات خاصة ودراسات سابقة وكل ما هو ممكن والهدف منها جمع الأدلة المطلوبة تعطي للنيابة العامة أثناء عملية التحقيق. [1]

وسيتم تقسيم هذا المبحث إلى مطلبين، نتناول في المطلب الأول المعاينة والخبرة الفنية، والتفتيش والضبط في المطلب الثاني على التوالي.

(1) منى كامل التركي، مرجع سابق ذكره، متاح على ذات الرابط السابق.

المطلب الأول

المعاينة والخبرة الفنية

تمهيد وتقسيم:-

تعتبر كل من المعاينة والخبرة الفنية من أهم وسائل جمع الأدلة، التي يلجأ إليها المحقق لإثبات وقوع الجريمة المعلوماتية، كما أنهما من أكبر العقبات التي تواجه الإثبات في الجرائم المعلوماتية.[1]

ومن هنا سيتم تقسيم هذا المطلب إلى فرعين، نتناول في الفرع الأول: المعاينة، وفي الفرع الثاني: الخبرة الفنية وذلك على التوالي.

(1) عبدالله دغش العجمي، مرجع سابق ذكره، ص78.

الفرع الأول

المعـــــاينـــــــة

المعاينة في قانون الإجراءات الجنائية هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة؛ ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة. [1]

كما يقصد بها معاينة مكان أو شيء أو شخص له علاقة بالجريمة المرتكبة وإثبات حالته وضبط ما قد يوجد به من أدلة، والمعاينة قد تكون إجراء من إجراءات التحقيق أو الاستدلال، وذلك بحسب ما قد تكون مشتملة عليه من مساس بحقوق الأفراد، فإذا تمت المعاينة في مكان عام كانت إجراء من إجراءات الاستدلال، وإذا اقتضت دخول مسكن كانت إجراء من إجراءات التحقيق. [2]

إجراءات المعاينة من حيث الأصل قد تتم من قِبل النيابة العامة أو من قِبل قاضي التحقيق أو المحكمة، فإذا كانت الواقعة جناية وفي حالة تلبس، أوجب قانون الإجراءات الجنائية الليبي في المادة "21" منه على النيابة العامة هنا ضرورة الانتقال الفوري إلى محل الواقعة بمجرد إخطارها بارتكاب جناية متلبس بها، وذلك لإثبات حالة الأمكنة ووصفها وصفاً دقيقاً، وبيان حالة الأشياء والأشخاص وكل ما يلزم إثبات حالته، أما فيما يتعلق بالجنايات غير المتلبس بها والجنح عموماً فالانتقال للمعاينة بشأنها متروك لتقدير النيابة العامة وفقاً لظروف التحقيق وما تراه ضرورياً لجمع الأدلة، وفي كل الأحوال إن الأدلة الناتجة من إجراء معاينة مكان الجريمة تخضع كسائر الأدلة الأخرى التي تطرح في الجلسة لتقدير قاضي الموضوع طبقاً لمبدأ حرية الإثبات وتكوين

(1) مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، الجزء الأول، مرجع سابق ذكره، ص 603.
(2) عوض محمد عوض ، قانون الإجراءات الجنائية في التشريع الليبي، د.ط، دار المطبوعات الجامعية، الإسكندرية، 2008م، ص 323.

العقيدة ، فله أن يأخذ بهذا الدليل ويستند إليه في إصدار حكمه إذا اقتنع به وله أن يطرحه جانباً دون معقب أو رقابة عليه من المحكمة العُليا. [1]

ويثور التساؤل هنا عن مدى إمكانية معاينة مسرح الجريمة المعلوماتية، فمثلا المادة "21" من قانون الإجراءات الجنائية الليبي قد نصت على أنه "يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى محل الواقعة ويُعاين الآثار المادية للجريمة ويحافظ عليها ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، ويسمع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبها، ويجب عليه أن يخطر النيابة العامة فوراً بانتقاله ، ويجب على النيابة العامة بمجرد إخطارها بجناية متلبس بها الانتقال فوراً إلى محل الواقعة. [2]

نجد في هذه المادة أن المشرّع الليبي قد سن هذا النص لضبط جريمة لها وجود مادي محسوس في العالم الخارجي، وما يؤكد ذلك هو أن المادة "44" من ذات القانون قد أوجبت على المحقق وضع الأشياء والأوراق التي تضبط في حرز مغلق وتربط كلما أمكن ويختم عليها. [3]

فهذه المواد قد سنها المشرّع الليبي بخصوص الجرائم التقليدية وليس بخصوص أفعال الاعتداء المادي أو المعنوي على نظم المعلومات والتي لم يعتبرها المشرّع الليبي إلى وقتنا الحاضر جرائم معاقب عليها قانوناً، وبالتالي لا يمكن الخوض في تفاصيل هذه الاعتداءات من الناحية الإجرائية لأنها لا تعتبر جرائم أصلاً في نظر قانون العقوبات الليبي، وإلا كان في ذلك انتهاكاً لمبدأ "شرعية الجرائم والعقوبات" .

(1) مفتاح بوبكر المطردي، مرجع سابق ذكره، ص 25.
(2) موسوعة التشريعات الجنائية، ج3، قانون الإجراءات الجنائية والقوانين المكملة له، متاح على ذات الرابط السابق، ص8.
(3) ذات المرجع السابق، متاح على ذات الرابط، ص15..

وهنا نصطدم بالعقبة الأساسية أمام معاينة مسرح الجريمة المعلوماتية التي ترتكب داخل الفضاء الإلكتروني، فالمحقق في هذه الحالة يتعامل مع بيئة مليئة بالنبضات الإلكترومغناطيسية والبيانات المخزنة داخل نظم معلوماتية شديدة الحساسية، ولا يتعامل مع أوراق أو أسلحة أو أشياء قابلة للربط، وهذا ما يؤكد أن القواعد الإجرائية التقليدية قد وضعت لتواجه سلوكاً مادياً يرتكب بواسطة آلات وأدوات قابلة للربط والتحريز. [1]

وإن كان هناك من يقول بصلاحية مسرح الجريمة المعلوماتية للمعاينة من قبل سلطة التحقيق، للضبط والتحفظ على الأشياء التي تُعد أدلة مادية على ارتكاب الجريمة ونسبتها لفاعل معين، كما يمكن وضع الأختام في الأماكن التي ارتكبت فيها الجريمة وضبط كل ما استعمل في ارتكابها، وذلك بالنسبة لمكونات الحاسب الآلي المادية مثل وحدات الإدخال والإخراج والتحكم والذاكرة وشاشة العرض وغيرها، فيمكن في هذه الحالة إخضاعها للنصوص الإجرائية التقليدية. [2]

أما السلوك الإجرامي ذات الطبيعة المعنوية في الجريمة المعلوماتية، فهو عبارة عن بيانات مخزنة في نظام معلوماتي يتطلب إثباته انتقال محقق متخصص، حيث يتم تفتيش عن البيانات عن طريق نقل محتويات الأسطوانة الصلبة الخاصة بالجهاز، ويجب على المحقق أو ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد في التحقيق ، وأن يُطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات، وفحص كل الوثائق المحفوظة، ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية، وفك شفرات الرسائل المشفرة؛ وهذا ما يحدث عندما ترتكب الجريمة عبر شبكة الإنترنت، بالإضافة إلى ضرورة إلمام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الأسطوانة الصلبة للحاسب الآلي، والأوقات التي

(1) عبدالله دغش العجمي، مرجع سابق ذكره، ص 78.
(2) ثنيان ناصر آل ثنيان، مرع سابق ذكره، ص57.

يستخدم فيها برامج استعادة المعلومات التي تم إلغاؤها، لذا يجب على المحقق في البيئة الإلكترونية أن يكون ملماً بمهارات هذه التقنية الحديثة والمتطورة، وفي هذا المجال تظهر الصعوبة في مواجهة مدى فاعلية النصوص التقليدية الخاصة بمعاينة مسرح الجريمة للتطبيق على الجريمة المعلوماتية.[1]

وبالرغم من التسليم بأهمية المعاينة في كشف غموض الكثير من الجرائم التقليدية، إلا أن دورها في مجال كشف غموض الجرائم المعلوماتية وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها قد لا ترقى إلى نفس الدرجة من الأهمية في الجرائم التقليدية ويرجع ذلك لاعتبارين:

1. إن الجرائم المعلوماتية الواقعة على نظم المعلومات والشبكات غالباً لا تخلف عقب ارتكابها أي آثار مادية ملموسة. [2]
2. عادةً ما تطول الفترة الزمنية بين وقت ارتكاب الجريمة ولحظة اكتشافها، مما يفسح المجال أمام الكثير من الأشخاص الذين يترددون على مسرح الجريمة خلال تلك الفترة الزمنية لإحداث أي تغيير في آثار الجريمة المعلوماتية المرتكبة وذلك بإتلافها أو العبث بها أو زوال بعضها، وهذا ما يجعل الدليل المستمد من إجراء المعاينة دليلاً مشكوكاً في مقبوليته أمام القضاء الجنائي. [3]

وحتى يكون للمعاينة في الجرائم المعلوماتية فائدة في كشف الجريمة ومعرفة مرتكبها ينبغي

(1) عبدالله دغش العجمي، مرجع سابق ذكره، ص 79.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص32.
(3) منى كامل تركي، مرجع سابق ذكره، متاح على ذات الرابط السابق.

مراعاة عدة قواعد وإرشادات فنية أهمها ما يلي:

1. تصوير الحاسب الآلي والأجهزة الطرفية المتصلة به، مع مراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة. [1]
2. العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية الخاصة بالتسجيلات الإلكترونية والتي تتزود بها شبكات المعلومات بموافقة موقع الاتصال، وبيان نوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع. [2]
3. إثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء. [3]
4. وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.
5. فصل الكهرباء عن موقع المعاينة، حتى لا يتمكن الجاني من القيام بأي فعل من شأنه التأثير على آثار الجريمة.
6. إبعاد الموظفين عن أجهزة الحاسب الآلي وكذلك عن الأماكن الأخرى التي توجد بها أجهزة الحاسب الآلي. [4]
7. عدم نقل أي معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي لموقع الحاسب الآلي من أي مجال مغناطيسي يمكن أن يتسبب في محو البيانات المسجلة. [5]

---

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 33.
(2) حسين خليل مطر، مرجع سابق ذكره، متاح على ذات الرابط السابق.
(3) ذات المرجع السابق، متاح على ذات الرابط السابق.
(4) علي عدنان الفيل، مرجع سابق ذكره، ص 34.
(5) منى كامل تركي، مرجع سابق ذكره، متاح على ذات الرابط السابق.

8. التحفظ عما قد يوجد بسلة المهملات من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة والأشرطة والأقراص الممغنطة غير السليمة وذلك من أجل فحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة. [1]
9. التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب الآلي ذات العلاقة بالجريمة لرفع ومضاهاة ما قد يوجد بها من بصمات.
10. قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين ؛ وهم من تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسب الآلي والشبكات ونظم المعلومات واسترجاع المعلومات من على الأسطوانات الصلبة أو المرنة، وذلك باستخدام برامج خاصة، بحيث يكونوا قد تلقوا تدريباً كافياً على كيفية التعامل مع نوعية الآثار والأدلة التي يحويها مسرح الجريمة المعلوماتية. [2]
11. فمثلاً في فرنسا يوجد فريقٌ مختصٌ في مجال التقنية الحديثة، يقوم بمرافقة المحققين أثناء التفتيش، وذلك من أجل القيام بفحص كل جهاز ونقل نسخة من الأسطوانات الصلبة وبيانات البريد الإلكتروني، ثم يقوم بإجراء تقرير يُرسل إلى القاضي الذي يتولى التحقيق في القضية. [3]

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص255.
(2) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 56.
(3) علي عدنان الفيل، مرجع سابق ذكره، ص 35.

الفرع الثاني

الخبــرة الفنيـــة

إن معنى الخبرة في قانون الإجراءات الجنائية الليبي هو: إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكانية استخلاص الدليل منه، وهذا ما تضمنته المادة "69" تحت عنوان ندب الخبراء ، حيث نصت على أنه "إذا استلزم إثبات الحالة الاستعانة بطبيب أو غيره من الخبراء، يجب على قاضي التحقيق الحضور وقت العمل وملاحظته. [1]

ولذلك فإنها تفترض وجود واقعة مادية أو شيء يصدر الخبير حكمه بناءً على ما استظهره منه، ومن ثم فإن الخبرة تقوم على حكم الخبير أكثر مما تقوم على جمع الأدلة من قبل المحقق وبحثها. [2]

كما أن الخبرة هي أحد أهم وسائل جمع الأدلة ، يلجأ إليها المحقق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات. [3]

والخبرة هي الاستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدة فنية أو إدارية لا تتوفر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته، والخبرة كدليل في الإثبات تنصرف إلى رأي الخبير الذي يثبته في تقريره، وبما أن تقرير الخبير، يعتبر من الأدلة الفنية فإن إجراء ندب الخبير هو من إجراءات جمع الأدلة، فللمحقق الاستعانة بالخبراء ليستطلع رأيهم في بعض الأمور التي

(1) موسوعة التشريعات الجنائية، الجزء الثالث، قانون الإجراءات الجنائية والقوانين المكملة له، متاح على ذات الرابط السابق، ص21.
(2) عبدالله دغش العجمي، مرجع سابق ذكره، ص 78.
(3) مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، ج1، مرجع سابق ذكره، ص 605.

يتعرض لها أثناء تأدية مهمته في التحقيق الذي ينتهي بإصدار قرار بأن لا وجه لإقامة الدعوى أو بإحالتها إلى محكمة الموضوع، وأما الخبرة في مرحلة المحاكمة فأنها تساعد القاضي في تكوين عقيدته للفصل في القضية المعروضة أمامه. [1]

والخبرة كدليل في الإثبات الجنائي تنصرف إلى رأي الخبير الذي يثبت في تقريره، ولذلك فإن الخبير يأخذ حكم الشاهد ويجوز استدعاؤه لسماع أقواله ومناقشته في التقرير الذي أعده وتقدم به، غير أن الخبير يختلف عن الشاهد من حيث الوقائع التي يشهد بها، فالشاهد يدلي بأقواله عن الواقعة كما حدثت في مادياتها أما الخبير فشهادته فنية أي تنصرف إلى تقيمه الفني للواقعة محل الخبرة ويترتب على ذلك أنه لا يجوز سماع الخبير كشاهد إذا كان إجراء الخبرة قد وقع باطلاً. [2]

وقد أجاز المشرّع لجهات التحقيق ندب الخبراء إذا كانت طبيعة الجريمة محل التحقيق تقتضي الاستعانة بذوي الخبرة لحسم مسألة فنية معينة، والأصل أن المحكمة هي الخبير الأعلى، ولها السلطة التقديرية في أخذ ما ورد في تقرير الخبير أو طرحه كلياً أو الأخذ ببعض ما ورد به، وطرح البعض الآخر وبدون إبداء أسباب لذلك. [3]

وإذا كان لندب الخبراء أهمية فيما يتعلق بالجرائم التقليدية، كاستعانة المحقق الجنائي بالخبراء في العديد من المجالات مثل الأطباء والشرعيين وخبراء الأدلة الجنائية وخبراء التصوير والخبراء البيولوجيين وغيرهم من الخبراء الذين تعتمد الشرطة على خبراتهم المتنوعة في تنفيذها لأعمالها. فإن أهميتها أكثر وضرورتها أشد فيما يتعلق بالجرائم المعلوماتية، خاصة بخصوص إجراءات جمع أدلة المكونات المعنوية في كل وحدات التخزين وتحليلها وكشف أي تلاعب في البرامج والمعلومات، وذلك نظراً لأن التحقيق في الجرائم المعلوماتية يتطلب مهارات فنية معينة

(1) ثنيان ناصر ثنيان، مرجع سابق ذكره، ص78.
(2) مفتاح بوبكر المطردي، مرجع سابق ذكره، ص 40.
(3) ذات المرجع السابق، ص40.

وخبرة سنوات من أعمال الخبرة في هذا المجال، فيجب دائماً الاستعانة بخبير في الحاسب الآلي والشبكات وخبير في تدقيق الحاسبات. [1]

فمنذ بدء ظهور الجرائم ذات الصلة بالحاسب الآلي، والشرطة وسلطات التحقيق أو المحاكمة تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، وذلك بغرض كشف غموض الجريمة، أو تجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق وكشف أي تلاعب في البرامج والمعلومات، وإذا كانت الاستعانة بخير فني أمر جوازي للمحقق أو لجهة التحقيق والحكم، إلا أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأي دون استطلاع رأي أهل الخبرة، ففي هذه الحالة يجب عليه أن يستعين بالخبير، فإذا تصدي للمسألة الفنية وفصل فيها القاضي دون تحقيقها بواسطة خبير كان حكمه معيباً مستوجباً نقضه. [2]

وهذا المبدأ قد استقر عليه قضاء محكمة النقض المصرية، وبناءً عليه فإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق والقاضي فهي أوجب في مجال الجرائم المعلوماتية أو الإلكترونية، حيث تتعلق بمسائل فنية آية في التعقيد، ومحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضها إلا متخصص وعلى درجة كبيرة من التميز في مجال تخصصه، فإجرام الذكاء والفن، لا يكشفه إلا ذكاء وفن مماثلين. [3]

ولذا أرى بأن القاضي الجنائي ولو كان على قدر من الخبرة في مجال المعلوماتية، فإنه لا يستطيع إصدار الحكم في القضية المعروضة أمامه دون الرجوع إلى خبير متخصص في هذا

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص 246-248.
(2) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 62-63.
(3) منى كامل تركي، مرجع سابق ذكره، متاح على ذات الرابط السابق.

المجال، وذلك لضمان الحيادية والموضوعية في إصدار الحكم بخصوص الدعوى الجنائية المعروضة أمامه.

فالقاضي الجنائي لا يستطيع في المسائل التي تخرج عن نطاق ثقافته القانونية مثل المسائل العلمية البحتة، والتي تحتاج إلى أهل الخبرة فيها، أن يخالف الرأي العلمي أو الفني إذا كان المطروح عليه يعتمد كلياً على هذا الرأي، رغم تمتعه بحرية تكوين قناعته، أي أنها ترجع القاضي إلى نظام الإثبات المقيد أو القانوني، وخاصةً إذا كان لا يوجد في ملف الدعوى سوى تقرير فني واحد أو في حالة تعدد التقارير إلا أنها تؤدي جميعها إلى نتيجة واحدة لعدم اختلافها، ولكن لو تعددت التقارير وتعددت النتائج، فالقاضي له أن يختار تقرير الخبير الذي اقتنع به واطمئن إليه أكثر فيصدر حكمه بموجبه ويترك التقرير الآخر، إلا أنه ليس له أن يتجاهل جميع التقارير المعروضة أمامه ويصدر حكمه خلافاً لها، لأنها مساءلة فنية بحتة، يجب الرجوع فيها إلى رأي أهل الخبرة وإلا كان حكمه معيباً كما أوضحنا سابقاً، ففي المسائل الفنية يكون الخبير هو المنشئ للحكم ويقف دور القاضي عند عملية الكشف عنه ووضعه في قالب قضائي. [1]

وإذا كانت قناعة القاضي لا تتفق مع النتيجة التي قدمها الخبير ، فليس أمام القاضي الجنائي إلا القبول بها أو أنه يلجأ لوسائل أخرى للتخلص مما توصل إليه الخبير الفني مثل طلب الاستعانة بخبير آخر غيره. [2]

ولأن البحث عن المعلومات داخل الجهاز الإلكتروني ذاته يُعد أمراً بالغ التعقيد لذا يحتاج إلى وجود خبير، ومن أهم المسائل التي يُستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي:

(1) أحمد الصادق الجهاني، مرجع سابق ذكره، ص 5-7.
(2) ذات المرجع السابق، ص6.

أولاً: الوصف:

أ. تركيب الحاسب الآلي وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور ونظام التشفير...الخ.

ب. طبيعة بيئة الحاسب الآلي أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائل الاتصالات وتردد موجات البث وإمكانية اختراقها. [1]

ج. الموضع المحتمل لأدلة الإثبات والهيئة التي تكون عليها.

د. أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام. [2]

ثانياً: البيان:

أ. كيفية عزل النظام المعلوماتي عند الضرورة دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة. [3]

ب. كيف يمكن عند الاقتضاء نقل أدلة الإثبات إلى أوعية ملائمة بدون أن يلحقها تلف، سواء كانت هذه الأوعية ورقية أو على أقراص ممغنطة، بحيث يتاح للقاضي مطالعتها وفهمها، مع إثبات أن هذه الأدلة هي في حالتها الأصلية وهي نسخة مطابقة للمُسجل على الحاسب الآلي أو النظام المعلوماتي أو الشبكة المعلوماتية أو الدعامة الممغنطة ومن التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم المعلوماتية، القانون البلجيكي الصادر في "2000/11/23م".[4]

---

(1) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص111.

(2) علي عدنان الفيل، مرجع سابق ذكره، ص 29.

(3) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 111.

(4) علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، ط1، عالم الكتب الحديث للنشر والتوزيع، الأردن، 2004م، ص97.

فقد نصت المادة "88" من هذا القانون على أنه "يجوز لقاضي التحقيق وللشرطة القضائية أن يستعين بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المنقولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق. [1]

فإن مهمة الخبير وفقاً للقانون البلجيكي السابق تتمثل من ناحية في تشغيل النظام ومن ناحية أخرى في تقديم البيانات المطلوبة حسب الطريقة التي تُريدها جهة التحقيق، فقد تريد البيانات مسجلة على أقراص ممغنطة أو على ورق. [2]

كما تظهر أهمية الاستعانة بالخبرة الفنية في مجال الجرائم المعلوماتية، في أنها عند غيابها، قد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هي أو جهة التحقيق عن تجميع الأدلة حول الجريمة وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه، فهي تنير الطريق أمام القاضي ليهتدي بها لتحقيق العدالة لاسيما في المجال الجنائي. [3]

ولا يشترط في الخبير كفاءة علمية عالية فحسب في مجال التخصص بل يجب أن يضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه، وعلى وجه الخصوص الجرائم ذات الصلة بالحاسب الآلي، فقد يتعلق الأمر بتزوير المستندات أو بالتلاعب في البيانات أو الغش أثناء نقل أو بث البيانات أو جريمة من جرائم الأموال أو الاعتداء على حرمة الحياة الخاصة، أو عرض صور أو أفلام مخلة بالآداب العامة. [4]

---

(1) علي عدنان الفيل، مرجع سابق ذكره، ص30.
(2) منى كامل تركي، مرجع سابق ذكره، متاح على الرابط السابق.
(3) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 63.
(4) علي عدنان الفيل، مرجع سابق ذكره، ص28.

كما أن التزام الخبير هو التزام ببذل عناية وليس التزام بتحقيق نتيجة، فلا يجب مساءلته إذا لم يصل إلى النتيجة المطلوبة، وذلك بسبب ضعف خبرته الفنية في المجال المعلوماتي، أو بسبب العقبات التي واجهته أثناء مباشرته لمهمته. [1]

ويمكن أن تثور مسؤوليته الجنائية إذا رفض القيام بالمهمة المكلف بها، أو إذا أتلف عمداً البيانات المطلوب منه التعامل معها، أو حفظها. [2]

فضلاً عن التزام الخبير بأداء مهمته التي حددتها له جهة التحقيق، يلتزم كذلك بالمحافظة على سر المهنة، وفي حالة إفشائه السر، يعاقب بالعقوبة المقررة لهذه الجريمة. [3]

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 29-31.
(2) منى كامل تركي، مرجع سابق ذكره، متاح على ذات الرابط السابق.
(3) علي عدنان الفيل، مرجع سابق ذكره، ص 31.

المطلب الثاني

تفتيش وضبط النظم المعلوماتية

تمهيد وتقسيم:-

تسعى أغلب الدول إلى إقامة حالة من التوازن بين حق المجتمع في إيقاع العقاب على من يقومون بجرائم الحاسوب والإنترنت، وبين المحافظة على حقوق الإنسان في مجال الإجراءات الجنائية، وأشد هذه الإجراءات مساساً بالحرية الشخصية هو التفتيش؛ لأنه يتصل بحرية الأفراد ومستودع سرهم وحرمة مساكنهم، فضلاً عن أنه يجمع بين استعمال السلطة وتقييد الحرية، حيث بدأت الأجهزة الأمنية تواجه في هذه الأيام عدداً من الجرائم الواقعة على الحاسوب والإنترنت أو بواسطته، لذا فالضرورة تقتضي الإحاطة بالمشكلات التي تثيرها تقنية المعلومات على المستوى الإجرامي، تمهيداً لمواجهتها بأساليب تتفق مع الطبيعة الخاصة بهذه التقنية الحديثة. [1]

ولأن التفتيش والضبط يُعتبران من أصعب وأخطر الإجراءات الجنائية مساساً بحرية المواطنين، سيتم تناول موضوع تفتيش النظم المعلوماتية في الفرع الأول من هذا المطلب، وضبط النظم المعلوماتية في الفرع الثاني منه على التوالي.

(1) علي حسن محمد الطوالبة، مرجع سابق ذكره، ص46,

الفرع الأول

تفتيش النظم المعلوماتية

أولاً: ماهية التفتيش

التفتيش عن الشيء لغةً: يعني البحث عن مكان وجوده . واصطلاحاً: هو البحث عن الشيء في مستودع السر[1].

وفقهاً: تعددت التعريفات التي أضفاها الفقه على فكرة التفتيش. فعرف جانب من الفقهاء التفتيش بأنه: "الاطلاع على محل له حرمة للبحث عما يفيد التحقيق". ،ويُعرف جانب آخر من الفقه التفتيش بأنه: "إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون، يتم بالبحث في مستودع السر عن أدلة مادية للجناية أو الجنحة التي وقعت، وكل ما يفيد في كشف الحقيقة ويتمثل مستودع السر في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه، وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقاً للإجراءات القانونية المقررة".[2]

كما عرف جانب آخر من الفقهاء تفتيش شخص المتهم بأنه: "هو البحث معه في مستودع سره عن أشياء تفيد في الكشف عن الجريمة ونسبتها إلى المتهم، ولما فيه من اعتداء على الحرية الشخصية فقد حصره المشرّع في حالات معينة نص عليها على سبيل الحصر. [3]

كذلك هناك من يعرفه بأنه "أحد الإجراءات التي يقوم بها موظف مختص طبقاً للإجراءات المقررة قانوناً في محل يتمتع بالحرمة والخصوصية، بهدف الوصول إلى أدلة مادية لجريمة تحقق وقوعها لإثبات نسبتها إلى شخص معين. [1]

(1) طارق إبراهيم عطية الدسوقي، مرجع سابق ذكره، ص 364.
(2) هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ط1، 1997م، ص 47.
(3) مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، الجزء الأول، مرجع سابق ذكره، ص 481.

والتفتيش وفقاً لقواعد قانون الإجراءات الجنائية التقليدية تنقسم من حيث محله إلى قسمين: الأول: تفتيش ينصب على المنازل ، الثاني: تفتيش ينصب على الأشخاص. [2]

وقد عالج المشرّع الليبي موضوع التفتيش بخصوص الجرائم التقليدية في الفصل الرابع من الباب الثاني من قانون الإجراءات الجنائية الليبي في المواد "34" وما بعدها.

أما بالنسبة لتفتيش نظم الحاسب الآلي وشبكة الإنترنت فيمكن تعريفه بأنه: "البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه"، كما يُعرَّف بأنه: "الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسب الآلي أو النظم المعلوماتية أو شبكة الانترنت".[3]

ومن هذه التعاريف يمكن أن نستخلص أهم خصائص تفتيش "النظم المعلوماتية" والتي تميزها عن غيرها من إجراءات التحقيق الأخرى وهذه الخصائص هي:

1. التفتيش يُعد قيداً على حرمة أو حصانة الشخص الذاتية، فهو تعرض قانوني لحرية المتهم الشخصية وحرمة أسراره الخاصة، وذلك بما يحتويه هذا التفتيش في مضمونه على قدر من الجبر والإكراه، وما فيه من مساس بحق السر، حيث يهدف التفتيش هنا إلى كشف أسرار الأشخاص سواء كانت موجودة على جهاز حاسبه الخاص أو على بريده الإلكتروني عبر شبكة الإنترنت.
2. يمتاز التفتيش بأنه وسيلة للبحث عن الأدلة المادية والمعنوية للجريمة وضبطها. [4]
3. إن التفتيش عن ملفات الحاسوب أمر معقد؛ لأن الملفات تتكون من نبضات إلكترونية يمكن تخزينها وتحريكها حول العالم في لحظة. [1]

---

(1) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 64.
(2) علي جبار الحسيناوي، مرجع سابق ذكره، ص 137.
(3) علي محمد حسن الطوالبة، مرجع سابق ذكره، ص 12-13.
(4) ذات المرجع السابق، ص13.

ثانياً: الضمانات القانونية لتفتيش النظم المعلوماتية

إن التفتيش أو البحث في الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدلة المطلوبة ونظراً لما يُمثله التفتيش من تقيدٍ للحرية الفردية واعتداءٍ على حرمة الحياة الخاصة لذا يجب أن تتوافر فيه الضمانات القانونية اللازمة لصحته وهي كالآتي:

1. تفتيش النظم المعلوماتية يتطلب "إذن أو أمر قضائي" يُجيز تفتيش أنظمة الحاسب الآلي، فالأصل أنه يُلزم الحصول على هذا الإذن للتفتيش ، سواء كان التفتيش متعلقاً بشخص المتهم أو أوراقه أو متاعه أو منزله، وذلك من أجل البحث عن الدليل وضبطه. [2]

كما يتعين لإصدار إذن التفتيش أن يحدد القائم به مبرر التفتيش، وبيان محل التفتيش سواء كان مكاناً أو شيئاً أو أشخاصاً، موضحاً ظروف وملابسات الجريمة المرتكبة والدليل المراد ضبطه، وكل ذلك لضمان مشروعية الدليل وسلامة مصدره عند الحصول عليه. [3]

إلا أنه يجوز قبول الدليل الرقمي في حالات معينة من دون الحصول على إذن مسبق للتفتيش وذلك مثل حالة التلبس بالجرم أو الرضا بالتفتيش أو في حالة الضرورة "حادث طارئ" يهدد الحياة وسلامة البدن أو يهدد الدليل الرقمي بالتغيير أو الإتلاف، بحيث يكون من الضروري ضبط جهاز الحاسب الآلي حالاً للتقليل من احتمال تدمير الدليل. [4]

---

(1) عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، ط1، د. ت. ، 2005م، ص 162.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص39.
(3) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص66.
(4) سالم محمد الأوجلي، مرجع سابق ذكره، ص 33.

2. يجب أن تكون مذكرة التفتيش واضحة في تحديد النظام محل التفتيش وإيراد أوسع وصف يغطي كل ما يعرفه المحقق سلفاً عن وجود أدلة متصلة بالجريمة المعلوماتية المراد التحقيق بشأنها. [1]

3. يتعين أن تكون عبارات مذكرة التفتيش عامة بقدر الإمكان، حتى لا يكون نصها قيداً على نطاق التفتيش والضبط ، خاصة في حالة ما يكون النظام المعلوماتي أو مكان وجود الدليل غير معروف في نطاق المكان محل التفتيش، فعلى سبيل المثال يمكن أن تتضمن مذكرة التفتيش إجراء التفتيش أو الضبط لكل سجل أو معلومات توجد بصورة إلكترونية أو مادية أو خطية موجودة في أي جهاز لتخزين المعطيات أو المعلومات سواء كان نظام كمبيوتر أياً كان وصفه أو شبكة معلومات أو وسائط تخزين أو أجهزة اتصال أو أية نظم معالجة وتخزين يمكن أن يوجد فيها الدليل، ولكن مع ملاحظة أن هذه العمومية لمذكرة التفتيش لا تعني عدم وجوب بيان السبب ومبرر التفتيش كما أوضحنا سابقاً، ولا تعني كذلك تجاوز الإجراء بذاته للقواعد القانونية المقررة لحماية الأفراد خاصةً الذين لا صلة مباشرة لهم بالمشتبه به أو بفعله. [2]

4. إن التحري والتفتيش في البيئة المعلوماتية من حيث الأصل يتوقف على مدى دقة مذكرة التفتيش ونطاقها المكاني، فمذكرة التفتيش يمكن أن تغطي أي مكان توجد فه البيانات أو المعلومات الإلكترونية المراد ضبطها، بما أنها قد وجدت في نطاق الاختصاص المكاني وبالنظر إلى الشخص أو الجهة التي يدور التفتيش بشأنها. [3]

(1) محمود أحمد القرعان، مرجع سابق ذكره، ص 109.
(2) يونس عرب، مرجع سابق ذكره، ص 21-22.
(3) محمود أحمد القرعان، مرجع سابق ذكره، ص 109.

ومن هنا تظهر أهم مشكلة في مسائل التفتيش بالنسبة إلى اختراقات الإنترنت أو الاختراقات الخارجية، فقد يتطلب التحري تفتيش أنظمة كمبيوتر عائدة لجهات لا صلة لها بالفعل أو نتيجته، مثل تفتيش نظم مزودي خدمات الإنترنت أو تفتيش أنظمة الخوادم خارج الحدود أو الطلب من مالكيها ومديريها تزويد جهة التحقيق ببيانات معينة، فمن حيث الأصل لا يمكن أن يُقبل قانوناً أن تغطي مذكرات التفتيش مواطن ومواقع وأماكن خارج صلاحية نظام العدالة المكانية ومن هنا نشأت الحاجة إلى تعاون دولي حقيقي في ميدان أنشطة التحري والتحقيق والضبط والتفتيش خارج حدود الدولة. [1]

5. إن الحاجة أصبحت ملحة لوجود تنظيم تشريعي لجوانب الضبط والتفتيش في البيئة المعلوماتية، وكذلك مسائل حماية البيانات الشخصية تجد موجبها في ضرورة توفير معيار مقبول يقيم توازناً بين حقوق وحريات الأفراد حماية خصوصياتهم وبين موجبات المكافحة وحاجتها إلى قواعد استثنائية فرضتها التحديات المتزايدة لهذه النوعية من الجرائم، خاصةً في ظل سرعة إخفاء أو إتلاف الدليل الرقمي واختلاف طبيعة الأدلة المثبتة للجرائم المعلوماتية عن الأدلة التقليدية وما تمتاز به هذه الجرائم من طابع دولي، فإن المكافحة الفعالة قد تنطوي على إهدار لحقوق وحريات الكثيرين والتفريط بضمانات المتهم، وما توجبه قرينة البراءة المقررة له وكل هذا التناقض لا مجال لفضه إلا بإقامة معيار تعكسه القواعد التشريعية. [2]

(1) عبدالله دغش العجمي، مرجع سابق ذكره، ص81.
(2) محمود أحمد القرعان، مرجع سابق ذكره، ص 110-111.

ثالثاً: شروط التفتيش

تنقسم شروط تفتيش نظم الحواسيب الآلية إلى نوعين:

- **شروط موضوعية:** تتعلق بوقوع الجريمة المعلوماتية ومدى توافر أمارات أو قرائن قوية تفيد في كشف الجريمة.
- **شروط شكلية:** تتعلق بالأسلوب الذي يتم به تنفيذ التفتيش في نظم الحاسب الآلي مثل: اقتحام قوات الشرطة للمكان بصورة مفاجئة وسريعة وإبعاد سائر المشتبه فيهم عن كافة الأجهزة الإلكترونية وتشكيل فريق خاص بالتحقيق في هذه الجرائم المعلوماتية. [1]

1. الشروط الموضوعية للتفتيش:

أ. وقوع جريمة معلوماتية:

يجب أن تكون الجريمة قد وقعت بالفعل سواء كان وصفها جناية أو جنحة، فالتحقيق الابتدائي لا يُباشر فيه بصفة عامة إلا بعد وقوع جريمة، سواء كانت جريمة عادية أو جريمة معلوماتية، فلا يجوز إصدار الأمر بالتفتيش من أجل ضبط أدلة في جريمة مستقبلية لم يتحقق وقوعها بعد، ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل، وكذلك فإن التفتيش الذي يقع من أجل فعل لا يُشكِّل جريمة يُعتبر تفتيشاً باطلاً. [2]

وثمة اختلافاً بشأن تعريف الجريمة المعلوماتية أو تحديد مفهومها، وذلك بحسب الزاوية التي ينظر منها لهذه الجرائم أو بالأحرى وفقاً للمعيار أو الأساس الذي يستند إليه كل من حاول

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 38.
(2) علي حسن محمد الطوالبة، مرجع سابق ذكره، ص 62-63.

التصدي لتعريفها، ووفقاً لما تقدم عرفها جانب من الفقه بأنها "الأنشطة غير المشروعة التي يكون فيها الحاسب الآلي والإنترنت موضوعاً للجريمة أو هدفاً لها".[1]

كما تُعرف والجريمة المعلوماتية بأنها هي كل فعل غير مشروع مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة يرتكبه شخص على دراية بتقنية المعلومات. [2]

وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لدولة "بريطانيا" حيث أصدرت قانون إساءة استخدام الحاسب الإلكتروني في "1990م"، وكذلك في "الولايات المتحدة الأمريكية" صدر قانون "الاحتيال وإساءة استخدام الحاسب الإلكتروني" لسنة "1986م". والذي طبق على مستوى الفيدرالي، بالإضافة إلى قوانين بعض الولايات المتحدة الأمريكية مثل "ولاية تكساس" الصادر في "1985م" بشأن الدخول غير المشروع في نظام الحاسب الآلي. [3]

وأيضاً في دولة فرنسا قد صدر قانون رقم "19-88" في عام "1988م" وهو القانون الخاص بالغش المعلوماتي، كما أدرج المشرّع " الإماراتي" جرائم الحاسب الآلي والإنترنت في القانون رقم "5" لسنة "2006" . [4]

وكذلك المشرّع المصري، فقد أضفى الحماية الجنائية على مجالين من مجالات الحاسب الآلي وهي:

1. البرامج وقواعد البيانات التي اعتبرها من ضمن المصنفات المشمولة بحماية حق المؤلف.

(1) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق ذكره، ص84.
(2) محمد علي العريان، مرجع سابق ذكره، ص 11- 12.
(3) علي عدنان الفيل، مرجع سابق ذكره، ص 49.
(4) هلالي عبداللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق ذكره، ص 115..

2. البيانات الفردية التي تقتضي إجراء إحصاء للسكان وكذلك البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين. [1]

أما في غير هذه الحالات من الصور الإجرامية التي لم يبسط بعد قانون العقوبات مظلته عليها، فإن هذا الشرط لا يتوافر بالنسبة لها. [2]

ومن الأهمية أن نؤكّد على أن إجراء التفتيش للنظم المعلوماتية لا يتخذ إلا بصدد جريمة قد ارتكبت بالفعل، فلا يصح القيام به لضبط جريمة مستقبلية ولو كان مُثبت وقوعها، فلو فرضنا مثلاً أن التحريات قد أثبتت أن شخصاً معيناً سوف يتاجر في برامج نظم معلومات مقلدة أو منسوخة، مما يُعد اعتداء على حق المؤلف وأنه سيستلم كمية من هذه البرامج في يوم معين، فصدر أمر من النيابة العامة لضبطه وتفتيش ما يحوزه عند تسلمه هذه البرامج، فإن هذا الأمر يقع باطلاً لأنه صدر من أجل جريمة مستقبلية وليس بصدد جريمة قد وقعت بالفعل، ولكن إذا كان مأمور الضبط القضائي لم يقم بتفتيش ما يحوزه المتهم المعلوماتي إلا بعد أن شاهده وهو يتسلم هذه البرامج المنسوخة، فإنه يكون قد شاهد الجريمة وهي في حالة تلبس مما يبرر له تفتيش ما يحوزه بناءً على هذه الحالة وحدها. [3]

ب. اتهام شخص أو عدة أشخاص معينين بارتكاب الجريمة لمعلوماتية أو المشاركة فيها:

ينبغي أن تتوافر في حق الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية تدعو للاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية سواء بوصفه فاعلاً أو شريكاً مما يستوجب

(1) ذات المرجع السابق، ص115.
(2) هلالي عبداللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق ذكره، ص 115.
(3) سعد سالم العسبلي، قانون الإجراءات الجنائية في الفقه والقضاء المقارن، ج1، ط1، الفضيل للطباعة والنشر والتوزيع، ليبيا، بنغازي، 2013، ص 161

اتهامه بها، بحيث إذا لم تتوافر هذه الدلائل يكون على قاضي التحقيق أن يصدر أمراً بأن لا وجه لإقامة الدعوى الجنائية، فهو شرطٌ عامٌ في جميع أحوال التفتيش. [1]

وفي مجال الجريمة المعلوماتية... يمكن القول بأن تعبير الدلائل الكافية يقصد بها مجموعة من المظاهر أو الأمارات المعينة التي تنهض على السياق العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة المعلوماتية إلى شخص معين، سواء بوصفه فاعلاً أو شريكاً. [2]

كما تُعرف الدلائل الكافية بأنها عبارة عن أمارات معينة تستند إلى العقل وتبدأ من ظروف أو وقائع يستنتج منها الفعل، توحي للوهلة الأولى بأن جريمة ما قد وقعت وأن شخصاً معيناً هو مرتكبها. [3]

ج. توافر أمارات قوية أو قرائن تفيد في كشف الحقيقة:

لا يكفي لجعل سلطة التحقيق تصدر قراراً بالتفتيش ومباشرته مجرد وقوع جناية أو جنحة واتهام شخص معين بارتكابها أو المشاركة فيها، بل يجب بالإضافة إلى ذلك أن تتوافر أمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره. [4]

(1) ذات المرجع السابق، ص 161.
(2) طارق إبراهيم عطية الدسوقي، مرجع سابق ذكره، ص 404-405.
(3) هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق ذكره، ص 116.
(4) ذات المرجع السابق، ص 122.

كما يجب أن تكون هذه الأجهزة المعدات الجائز تفتيشها قد استعملت في الجريمة المعلوماتية أو أشياء متحصلة منها أو أية أشياء أو مستندات إلكترونية يحتمل أن يكون لها نفعٌ في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره. [1]

ويستوي أن تكون هذه الأشياء أو الأجهزة المعلوماتية في حيازة الشخص أو في منزله أو أن يكون هذا الشخص متهماً أو ليس كذلك، وكل ما هنالك أنه إذا كان الشخص غير متهم فإن تفتيشه هو أو منزله يخضع لأحكام خاصة. [2]

إذاً متى توافرت كل هذه الشروط فإنه يجوز لسلطة التحقيق تفتيش الجهاز الإلكتروني وملحقاته المكونة له المادية والمعنوية، وذلك من أجل ضبط أدلة الجريمة وكل ما من شأنه أن يكشف الجريمة المعلوماتية. [3]

رابعاً: محل التفتيش:

يشمل محل التفتيش للحاسب الآلي "المكونات المادية" والمكونات "المنطقية أو المعنوية" له.

1. تفتيش المكونات المادية للحاسب الآلي:

لا يوجد خلاف في أن الولوج إلى المكونات المادية للحاسب الآلي بحثاً عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة المضيئة. [4]

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 50.
(2) هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، مرجع سابق ذكره، ص 122.
(3) علي حسن الطوالبة، مرجع سابق ذكره، ص 72.
(4) هلالي عبداللاه، مرجع سابق ذكره، ص 73.

وإن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجود فيه تلك المكونات، وهل هو من الأماكن العامة أو من الأماكن الخاصة فإذا كانت موجودة في مكان خاص كمنزل المتهم أو أحد ملحقاته كان لها حكمة، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه أو منزله وبنفس الضمانات والإجراءات المقررة قانوناً في التشريعات المختلفة، مع مراعاة التمييز بين ما إذا كانت مكونات الحاسب المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصلة بحاسب آلي آخر، أو بنهاية طرفية في مكان آخر كمسكن غير المتهم مثلاً، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة، تَعيَّن مراعاة القيود والضمانات التي يستلزمها المشرّع لتفتيش هذه الأماكن. [1]

أما إذا كانت هذه المكونات المادية موجودة أو حائزاً لها في مكان عام، سواء كانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أو كانت من الأماكن العامة بالتخصيص، كالمقاهي والمطاعم والسيارات العامة فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال. [2]

وهناك بعض التشريعات المقارنة التي تنص صراحة على تفتيش مكونات الحاسب الآلي ومن ذلك القانون الإنجليزي الصادر في "29 يونيو سنة 1990م" "قانون إساءة استخدام الحاسب الآلي" فبالنسبة للجرائم المدرجة في القسم الثاني والقسم الثالث من هذا القانون والمعاقب عليها بعقوبة السجن لمدة لا تتجاوز خمس سنوات، فإن هذه النوعية من الجرائم تجيز القبض على المتهم دون حاجة لإذن قضائي كما تجيز تفتيش محل إقامة المتهم بحثاً عن أدلة مادية ذات قيمة تتعلق

(1) حسين خليل مطر، مرجع سابق ذكره، متاح على ذات الرابط السابق.
(2) عبدالله حسين علي محمود، مرجع سابق ذكره، ص 37-38

بالجريمة محل القبض، أما بالنسبة للجرائم المدرجة في القسم الأول والمعاقب عليها بالحبس لمدة لا تتجاوز ستة أشهر فإن التفتيش لا يكون إلا بناءً على إذن قضائي يستند على أسباب منطقية. [1]

2. تفتيش المكونات المنطقية للحاسب الآلي:

إن المكونات المنطقية "المعنوية" للحاسب الآلي من بيانات وبرامج ومعلومات قد تكون محلاً لارتكاب جريمة ما أو وسيلة لارتكابها وبناءً عليه يتم إصدار إذن قضائي بتفتيش الحاسب الآلي من أجل البحث عن أدلة تفيد في كشف الحقيقة. [2]

ويمكن تعريف الكيان المنطقي بأنه "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات".[3]

وقد ثار جدل فقهي بين فقهاء القانون الجنائي حول مدى إمكانية تفتيش وضبط البيانات المخزنة أو المعالجة إلكترونياً بصورها وأشكالها المختلفة كالأقراص والأشرطة الممغنطة، بما في ذلك ذاكرة الحاسب الآلي وقد انقسموا في ذلك إلى اتجاهين:

الاتجاه الأول:

ذهب أنصاره إلى القول بعدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب الآلي باعتباره وسيلة لإثبات المادي يهدف إلى ضبط أدلة مادية تتعلق بالجريمة وتفيد في كشف الحقيقة وهذا ما يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي، ويمثل هذا الرأي

(1) طارق إبراهيم عطية الدسوقي، مرجع سابق ذكره، ص 382-383
(2) علي جبار الحسيناوي، مرجع سابق ذكره، ص 139.
(3) علي حسن الطوالبة، مرجع سابق ذكره، ص 24.

جانب من الفقه الفرنسي الذي يرى أن النبضات والإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المادية المحسوسة التي يمكن تفتيشها وضبطها. [1]

الاتجاه الثاني:

يرى أنصاره أن المعلومات التي لا تُعد شيئاً مادياً وإنما ذات طبيعة معنوية وهي مجرد نبضات إلكترونية أو إشارات أو موجات كهرومغناطيسية إلا أنها قابلة بأن تُخزن في أوعية ووسائط مادية كالأقراص والأشرطة الممغنطة، وبالتالي فهي ليست شيئاً معنوياً كالحقوق والآراء والأفكار بل أصبحت بعد تخزينها في أوعية ووسائط مادية، أشياء مادية محسوسة لها وجود ملموس في العالم الخارجي ومن ثم يجوز أن يرد عليها التفتيش والضبط. [2]

ومن جانبي أرى أن الاتجاه الأول هو الأكثر قبولاً من الناحية المنطقية، ذلك لأن القواعد التي تحكم التفتيش والضبط قد وضعت في زمن مبكر وقبل ظهور الحاسب الآلي وتطبيقاته، كما أن طبيعة البيانات والمعلومات تتطلب إدراج قواعد خاصة تحكمها وليس القيام بتطويع القواعد التقليدية وتوسيع نطاقها ليشملها، وذلك حتى لا يحدث تصادم مع مبدأ الشرعية الإجرائية.

وبالنسبة لموقف التشريعات الحديثة نجد أن "التشريع الأمريكي" قد ذهب إلى التأكيد على هذا الاتجاه، فالمادة "34" من القواعد الفيدرالية الخاصة بالإجراءات الجنائية الصادرة سنة "1970م" بعد تعديلها يوسع نطاق التفتيش ليشمل أوعية التخزين والبريد الإلكتروني والصوتي المنقول عن طريق الفاكس، فضلاً عن أن الاتفاقية الأوروبية للجريمة الافتراضية "اتفاقية بودابست" تقضي في المادة "19" منها بإلزام الدول الأطراف في هذه الاتفاقية بضرورة تبني التدابير والإجراءات

(1) علي عدنان الفيل ، مرجع سابق ذكره، ص 42.
(2) مفتاح بوبكر المطردي، مرجع سابق ذكره، ص 53.

التشريعية التي تخول السلطات المختصة ولوج البيئة المعلوماتية وذلك من أجل تيسير إثبات هذه الجرائم.[1]

3. مدى خضوع شبكات الحاسب الآلي للتفتيش:

إن طبيعة التقنية الرقمية للجريمة المعلوماتية قد خلقت العديد من التعقيدات أمام أعمال التفتيش والضبط، فالبيانات التي تحتوي على أدلة والمراد ضبطها قد تتوزع عبر الشبكة المعلوماتية في أماكن مجهولة بعيدة تماماً عن الموقع المادي للتفتيش وإن ظل من الممكن الوصول إليها من خلال حاسب آلي يقع في الأبنية الجاري تفتيشها ، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، مما قد يسبب الانزعاج للسلطات القضائية في ذاك البلد، لاعتبار هذا الإجراء خارق للسيادة الوطنية لها. [2]

وتعتبر امتداد نطاق التفتيش إلى نظام غير النظام محل الاشتباه محل أو موضع تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش. [3]

وهذا بقدر ما يزيد تعقيد مشاكل الجريمة المعلوماتية العابرة للحدود، يزيد من أهمية تبادل المساعدة القانونية بين الدول. [4]

(1) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مرجع سابق ذكره، ص 8.
(2) علي عدنان الفيل ، مرجع سابق ذكره، ص 44.
(3) عبد الله دغش العجمي، مرجع سابق ذكره، ص81.
(4) علي عدنان الفيل، مرجع سابق ذكره، ص 44.

وفي هذا المضمار يجب أن نميز بين الحالات الآتية:

أ. في حالة اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل إقليم الدولة:

يثير هذا الفرض تساؤلاً هاماً حول مدى إمكانية امتداد نطاق التفتيش إذا تبين أن الحاسب الآلي أو النهاية الطرفية في منزل المتهم متصل بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم؟.[1]

نجد أن القواعد العامة للتفتيش في قانون الإجراءات الجنائية الليبي تقضي بأن تفتيش غير المتهمين أو تفتيش منازل غير المتهمين لا يجوز إجراؤه من النيابة العامة إلا بعد الحصول على إذن من القاضي الجزئي هذا إذا كان التحقيق يباشر من قبلها، أما إذا كان يباشره قاضي التحقيق نفسه فلا يستلزم حصول هذا الإذن ومن ثم إذا كان مثلاً الحاسب الآلي موجوداً بمنزل غير المتهم فلا يجوز تفتيشه من قبل النيابة العامة إلا بعد استصدار إذن من القاضي الجزئي قبل ولوجه، وإلا كان الإجراء باطلاً. [2]

والجدير بالذكر هنا أن الجريمة التي وقعت والمراد إجراء التفتيش بشأنها، لابد أن تكون من ضمن الجرائم التقليدية التي نص قانون العقوبات الليبي على تجريمها، والحاسب الآلي أو شبكة المعلوماتية الدولية لم تكن إلا وسيلة لارتكاب هذه الجرائم التقليدية وليس موضوع الجريمة، ففي هذه الحالة فقط من الممكن إعمال القواعد التقليدية الموجودة في قانون الإجراءات الجنائية الليبي الخاصة بالتفتيش، فلا يجوز تطبيق قواعد التفتيش التقليدية بشأن الجريمة المعلوماتية، لأن المشرّع الليبي لم ينص على تجريمها بعد كما سبق القول، فلا مجال للخوض في مدى إمكانية تطبيق القواعد الإجرائية التقليدية من معاينة وخبرة وتفتيش وضبط بخصوصها.

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 44.
(2) مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، الجزء الأول، مرجع سابق ذكره، ص 619.

غير أن صدور الإذن قد يستغرق بعض الوقت، مما قد يؤدي إلى تلاشي الدليل واندثاره بالمحو أو الإتلاف لأن الجاني قد يحاول العبث بالدليل لكي لا ينكشف أمره قبل صدور الإذن بالتفتيش. [1]

ولذا كان من الضروري معالجة هذه المشكلة بنص خاص يقضي بتوسيع سلطات الجهة المعنية بإجراء التفتيش ولو استلزم الأمر ولوج النظام المعلوماتي دون الحصول على إذن عند الضرورة، ومتى كان من شأن انتظار صدور الإذن أن يفوت فرصة الحصول على الدليل ومن ثم كشف الحقيقة. [2]

وقد أقرت "الاتفاقية الأوروبية" للجرائم المعلوماتية ذلك متى كانت المعلومات المخزنة بحاسوب غير المتهم يتم الدخول إليها من خلال الحاسب الأصلي محل التفتيش. [3]

كما تبنت بعض التشريعات المقارنة هذا الاتجاه منها "قانون تحقيق الجنايات البلجيكي" الصادر في "23 نوفمبر عام 2000" والذي ينص على أنه "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقاً لضابطين:

1. إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث .
2. إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث. [4]

(1) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 66.
(2) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مرجع سابق ذكره، ص 10.
(3) هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، مرجع سابق ذكره، ص 68.
(4) علي عدنان الفيل، مرجع سابق ذكره، ص 45.

فنلاحظ بأنه قد أجاز امتداد التفتيش ولكن ليست بصورة مطلقة بل بقيود وضوابط معينة كما سبق بيانها.

كما أنه كذلك في الولايات المتحدة الأمريكية تجيز المادة "41" من قانون الإجراءات الجنائية الفيدرالي الأمريكي لقاضي التحقيق إصدار إذن تفتيش ملكية داخل منطقة أو خارجها متى كانت الملكية عند طلب الإذن موجودة داخل المنطقة ، ولكن يخشى أو يتوقع تحركها خارج المنطقة قبل تنفيذ الإذن. [1]

كما نص مشروع قانون جريمة الحاسب الآلي في القسم الخامس المادة "125" الهولندي على إمكانية أن يمتد التفتيش إلى الأجهزة المعلوماتية الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة وأن يكون التدخل مؤقتاً. [2]

وكذلك فأنه عند تفتيش حاسب متصل مع حواسيب أخرى داخل الدولة تملك جهة المفتش البحث عن الأدلة الجرمية على طول شبكات الاتصال المحلية وخارج الحيز المكاني المحدد في إذن التفتيش بشرطين:

- احتمال وجود أدلة جرمية تساعد في ظهور الحقيقة.
- مراعاة ضوابط وشروط التفتيش المقررة قانوناً بالنسبة للمكان أو الشخص كتمتعه بالحصانة وغيره... [3]

(1) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مرجع سابق ذكره، ص 10-11.
(2) طارق إبراهيم الدسوقي، مرجع سابق ذكره، ص 387.
(3) علي جبار الحسنياوي، مرجع سابق ذكره، ص 139-140.

ب. في حالة اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج إقليم الدولة:

من المشاكل التي تواجه سلطات الإدعاء في جمع الأدلة هي قيام مرتكب الجرائم المعلوماتية بتخزين بياناتهم في أنظمة تقنية خارج إقليم الدولة مستخدمين في ذلك شبكة الاتصالات الدولية، والهدف من وراء ذلك هو عرقلة سلطات التحقيق في إجراءات جمع الأدلة والتحقيق، وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي لدولة أخرى وهو ما يسمى بالولوج أو التفتيش عبر الحدود ويتعذر القيام به بسبب تمسك كل دولة بمبدأ السيادة الوطنية. [1]

فإن التفتيش الإلكتروني العابر للحدود مرفوض لما ينطوي عليه من انتهاك لسيادة دولة أخرى، وإن كان من الضروري القيام لهذا الإجراء فيجب أن يتم في إطار اتفاقيات ثنائية أو متعددة الأطراف تُجيز هذا الامتداد تُعقد بين الدول المعنية، أو على الأقل يجب الحصول على إذن الدولة الأخرى. [2]

فعند تفتيش حاسب آلي موجود خارج الدولة لا تملكك من حيث الأصل الجهة المختصة بالتفتيش تجاوز حدود الدولة، وإلا أصبحت أن تجاوزت حدودها غير مختصة مكانياً دون صلاحيات للتفتيش وفي ذلك انتهاك للسيادة الوطنية للدول الأخرى، إلا أنه وبالرغم من ذلك يمكن اللجوء إلى المساعدة القانونية المتبادلة والإنابة القضائية، وهذا ما يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني. [3]

ومن كل ذلك نفهم بأنه إذا ما وُجِدَ دليلٌ بشأن الجريمة المعلوماتية في الوسط الافتراضي في جهاز ما في دولة أخرى، فإن سلطات التحقق لن تتمكن من الحصول عليه، إلا عن طريق اتفاقيات الإنابة القضائية فهي السبيل لتحصيل هذا الدليل، بحيث تفوّض الدولة الأخرى في جمع

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 46.
(2) ذات المرجع السابق، ص 46.
(3) علي جبار الحسنياوي، مرجع سابق ذكره، ص 140.

هذا الدليل وإرساله لدولة التحقيق، وهذا ما نصت عليه المادة "25 / أ" من قانون الحاسوب الهولندي فقد اعتدت بالدليل المتحصل عليه في إقليم دولة أخرى إذا تم ذلك تنفيذاً لاتفاقيات التعاون الأمني والقضائي. [1]

كما يؤيد هذا الرأي التطبيق القضائي في ألمانيا ففي إحدى قضايا الغش المعلوماتي، قد تبين وجود اتصال بين الحاسب الإلكتروني المتواجد في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات مشروعات فيها، وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، فلم تتمكن من ذلك إلا عن طريق التماس المساعدة القانونية والتي تتم بالتبادل بين الدولتين. [2]

وفي المقابل هناك جانب آخر من الفقه يؤيد أمر إمكانية امتداد التفتيش إلى الحواسيب الموجودة خارج إقليم الدولة، وهذا الاتجاه أخذت به الاتفاقية الأوروبية بشأن الجرائم المعلوماتية سنة "2001م" في المادة "32" فنصت على إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى من دون إذنها في حالتين:

الأولى: إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور.

الثانية: إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

فلابد من اللجوء إلى صور التعاون الدولي في هذا المجال وذلك بمقتضى اتفاقية ثنائية أو متعددة الأطراف. [3]

(1) طارق محمد الجملي، مرجع سابق ذكره، ص 15.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص 15.
(3) هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، مرجع سابق ذكره، ص 93.

أو على الأقل الحصول على إذن الدولة التي يتم التفتيش في مجالها الإقليمي وهذا ما قامت به الشرطة اليابانية حيث ساورها الاعتقاد بأن مجموعة من المخربين قد استخدمت أجهزة الحاسب الآلي في الصين والولايات المتحدة الأمريكية في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة، وقد طالبت الشرطة اليابانية كل من بكين و واشنطن بتسليم بيانات الدخول المسجلة على أجهزة الحاسب الآلي في كل هاتين الدولتين ، حتى تتمكن من الوصول إلى جذور هذه العملية الإرهابية. (1)

كما أخذ كذلك بهذا الاتجاه "القانون الفرنسي" في المادة "17" من قانون الأمن الداخلي الفرنسي، وقد برر الفقه الفرنسي هذا الاتجاه بأن العالم الافتراضي لا يعرف الحدود، كما يسمح قانون "التحقيق البلجيكي" في المادة "88" القاضي التحقيق الحصول على نسخة من البيانات التي هو في حاجة إليها دون انتظار صدور إذن من سلطات الدولة الأخرى. (2)

أما في الولايات المتحدة الأمريكية فإن الأمر يتوقف على وضع الشخص الذي ينفذ التفتيش، فإذا كان قبل مباشرته يعلم بأن البيانات والمعلومات المراد بحثها مخزنة بعيداً في نطاق دولة أخرى، فعندئذ يستلزم التماس طلب مساعدة يتم توجيهه إلى سلطات الدولة الأخرى، أما إذا كان القائم بالتفتيش يجهل أو ليس في وسعه معرفة أن البيانات المراد تفتيشها خارج حدود دولته فإن ما يسفر عنه التفتيش من ضبط لا يهدر ويمكن قبوله والاستناد إليه في الإثبات بوصفه دليلاً مشروعاً متى أطمأنت إليه المحكمة. (3)

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 47.
(2) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مرجع سابق ذكره، ص 29.
(3) ذات المرجع السابق، ص 29.

ج. ضبط الاتصالات والمراسلات "المراقبة الإلكترونية" عبر شبكات الحاسب الآلي:

إن وسائل الاتصالات الحديثة تعتمد إلى حد كبير على هذه التقنية الحديثة والمتطورة ذاتها كاعتمادها على خطوط الهاتف مثلاً، هذا ما يساعد على مد صلاحية التنصت والمراقبة للمراسلات الإلكترونية مع الاحتفاظ بالضوابط القانونية وهي أن تكون دعوى الحق العام محركة، وأن تكون الصلاحية مقتصرة حصراً على المدعي العام، وأن يكون للتنصت والمراقبة فائدة في إظهار الحقيقة. (1)

وطبقاً للمادة "180" من قانون الإجراءات الجنائية الليبي يجوز للنيابة العامة مراقبة المكالمات الهاتفية والرسائل البريدية والبرقيات وما في حكمها بعد الحصول على إذن من القاضي الجزئي ولا يجوز مباشرته من دون إذن؛ نظراً لخطورة الإجراء المذكور باعتباره يمس حرمة الحياة الخاصة، وهذا النص جائزاً ومشمولاً بالنص المشار إليه بصورة ضمنية، حيث يتسع مفهوم الرسائل إلى أبعد من المفهوم التقليدي لها. (2)

كما أن التنصت والأشكال الأخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريباً، فالقانون "الفرنسي" الصادر في "1991م" يجيز اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات. (3)

وكما في هولندا أجاز المشرّع لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة ضالع فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات، وكذلك في الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الإلكترونية بما في ذلك شبكات الحاسب الآلي بشرط الحصول على إذن تفتيش صادر من القاضي، أما في اليابان فقد أقرت كذلك

(1) علي جبار الحسيناوي، مرجع سابق ذكره، ص 140.
(2) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مرجع سابق ذكره، ص 144.
(3) طارق إبراهيم الدسوقي عطية، مرجع سابق ذكره، ص 390.

محكمة مقاطعة "Kofa" عام "1991م" شرعية التنصت على شبكات الحاسب الآلي للبحث عن الدليل. [1]

ويمكن تعريف المراقبة الإلكترونية بأنها هي الاكتساب السمعي أو أي اكتساب لمحتويات أي اتصال سلكي أو إلكتروني أو شفوي باستخدام أي جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر. [2]

وكذلك نصت المادة "88" من قانون أصول المحاكمات الجزائية الأردني على أنه "للمدعي العام أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق كافة البرقيات ويجوز له مراقبة المحادثات الهاتفية متى كان لذلك فائدة في إظهار الحقيقة". [3]

كما أن تفتيش نظم الحاسب الآلي يمكن أن يتم بطرق عدة مثلاً المرشد الفيدرالي الأمريكي جاء بأربع طرق أساسية للتفتيش ممكنة التحقيق هي:

1. تفتيش الحاسب الآلي ، وطبع نسخة ورقية من ملفات معينة في ذات الوقت.
2. تفتيش الحاسب الآلي ، وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت. [4]
3. عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.
4. ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع. [5]

---

(1) علي عدنان الفيل، مرجع سابق ذكره، ص 48.
(2) عمر محمد بن يونس، مرجع سابق ذكره، ص 367.
(3) علي جبار الحسيناوي، مرجع سابق ذكره، ص 140.
(4) علي عدنان الفيل، مرجع سابق ذكره، ص 49.
(5) ذات المرجع السابق ، ص 49.

الفرع الثاني

ضبط النظم المعلوماتية

إن الهدف أو الغاية من وراء إجراء التفتيش، سواء كان التفتيش واقعاً على الأشخاص أو المساكن أو الأجهزة الإلكترونية هو ضبط الأدلة التي تفيد في كشف الحقيقة، أي ضبط الأشياء التي تعد في ذاتها الدليل على الجريمة، أو يمكن أن نستخلص منها هذا الدليل وقد تكون هذه الأشياء هي ما تم استعمالها في ارتكاب الجريمة. [1]

وقد نصت على ذلك المادة "75 / 2" من قانون الإجراءات الجنائية الليبي "للمحقق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة والآلات وكل ما يحتمل إنه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليه وكل ما يفيد في كشف الجريمة والضبط هو وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة".[2]

ولما كان الضبط هو الأثر المباشر للتفتيش وباعتباره أحد إجراءات التحقيق، فتطبق عليه القواعد التي تنطبق على التفتيش، فالعلاقة وثيقة بين التفتيش والضبط فإذا ما بطل إجراء التفتيش بُطل إجراء الضبط كذلك، وبناءً على ذلك فإن القاعدة هي أن الضبط لا يرد إلا على الأشياء المادية سواء كانت منقولات أو عقارات بوصفها أدلة مادية للجريمة والتي يجري التفتيش بشأنها. أما الأشياء المعنوية فلا تصلح بطبيعتها محلاً للضبط ، والشرط اللازم توافره لصحة إجراء الضبط هو أن يكون الشيء مفيداً في كشف الحقيقة، فكل ما يحقق هذه الغاية يصح ضبطه. [3]

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط3، دار النهضة العربية، القاهرة، 1996م، ص 481.
(2) عوض محمد ، الوجيز في قانون الإجراءات الجنائية، الجزء الأول، د. ط، دار المطبوعات الجامعية، الإسكندرية، د.ت، ص 603..
(3) علي حسن الطوالبة، مرجع سابق ذكره، ص 135.

أما إجراء الضبط في "الجرائم المعلوماتية" فقد يكون محله "شيئاً مادياً" أو بيانات معالجة إلكترونياً "شيئاً معنوياً"، فإن الضبط لا يتوقف على تحريز جهاز الكمبيوتر فقط بل يمتد إلى ضبط المكونات المادية لمختلف أجزاء النظام التي تزداد يوماً بعد يوم، وقد ينصب إجراء الضبط على المكونات المنطقية "المعنوية" مثل المعطيات والبرامج والبيانات المخزنة في النظام المعلوماتي أو في النظم المرتبطة بالنظام محل الاشتباه ذات الطبيعة المعنوية والمعرضة للتغيير والإتلاف بكل سهولة. [1]

أولاً: ضبط المكونات المادية للحاسب الآلي:

الأصل في إجراء الضبط أنه يرد على الأشياء المادية التي تصلح بطبيعتها لوضع اليد عليها، ولذا لا يثير ضبط المكونات المادية للحاسب الآلي وملحقاته أية إشكالية باعتبارها أشياء مادية وبالتالي يجوز وقوع إجراء الضبط عليها. [2]

ومن الأشياء المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات جرائم الحاسب الآلي ونسبتها للمتهم هي:

1. وحدة الإدخال: وتشمل عدة أشياء تتمثل بلوحة المفاتيح ونظام الفأرة ونظام القلم الضوئي ونظام القراءة الضوئية للحروف ونظام قراءة الحروف المغناطيسية ونظام إدخال الأشكال والرسومات.
2. وحدة الحساب والمنطق: وتشمل مجموعة من الدوائر الإلكترونية والمسجلات.
3. وحدة التحكم: وما تستعين به من مسجلات وسماعات منطقية.
4. وحدة المخرجات: وما تشمله من وسائط كالشاشة والطابعة والرسم. [1]

(1) علي جبار الحسيناوي، مرجع سابق ذكره، ص 132.
(2) مفتاح بوبكر المطردي، مرجع سابق ذكره، ص 57.

5. وحدة التخزين الثانوية: بما تشمله من أقراص مغناطيسية بنوعيها المرن والصلب والأشرطة المغناطيسية.

6. الأجهزة والوحدات الملحقة بالحاسوب لاستخدام شبكة الإنترنت، مثل جهاز المودم. [2]

وأجهزة اختراق الاتصالات وتحليل الشيفرات وكلمات المرور، وهذه الأجهزة وظيفيتها استقبال البيانات المدخلة إلى الحاسوب وتمريرها إلى داخل الجهاز وهي عادةً تمرر إلى وحدة الذاكرة للتخزين. [3]

وهناك بعض التشريعات التي أجازت القيام بإجراء الضبط على المكونات المادية منها المادة "487" من "قانون الإجراءات الجنائية الكندي" والمادة "251" من قانون "الإجراءات الجنائية اليوناني" وكذلك قانون إساءة استخدام الحاسب الآلي في "انجلترا" الصادر في عام "1990م" حيث أجاز صراحة تفتيش وضبط مكونات الحاسب الآلي المادية، وكذلك قانون المنافسة في كندا. [4]

كما أجاز "المشرّع الأردني" ضبط الأشياء المادية، وهذا ما نصت عليه المادة "33" من قانون "الإجراءات الجنائية الأردني" بقولها: "إذا تبين من ماهية الجريمة أن الأوراق أو الأشياء الموجودة لدى المشتكي عليه يمكن أن تكون مدار استدلال على ارتكابه الجريمة فللمدعي العام أو من يُنيبه أن ينتقل حالاً إلى مسكن المشتكي عليه للتفتيش عن الأشياء التي يراها مؤدية إلى إظهار الحقيقة". كما نصت المادة "34" على أنه " إذا وجد في مسكن المشتكي عليه أوراق أو أشياء تؤيد التهمة أو البراءة فعلى المدعي العام أن يضبطها وينظم بها محضراً"، فنجد أن القانون الأردني قد أباح لسلطة التحقيق ضبط جميع الأشياء التي تفيد في كشف الحقيقة، بما في ذلك الأوراق

---

(1) علي حسن محمد الطوالبة، مرجع سابق ذكره، ص 21-23.

(2) المودم: هو الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال مع بعضها البعض عبر خطوط الهاتف، وقد تطور المودم إلى أجهزة إرسال الفاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها، وللمودم أشكال وهياكل تتطور مع تطور تقنية الحواسيب الآلية.

(3) علي حسن الطوالبة، مرجع سابق ذكره، ص 140.

(4) ذات المرجع السابق، ص 141.

أو أسلحة الجريمة، وقد تكون فيما استعمل في ارتكاب الجريمة أو أثنائها، وبالتالي يمكن أن تنطبق على أجهزة الحاسب الآلي ومكوناته المادية سواء أوجدت عند المشتكي عليه أم عند غيره. [1]

فالأشياء يمكن أن تمتد لتشمل مدخلات الحاسوب مثل: لوحة المفاتيح وشاشات اللمس أو نظام الفأرة أو قد تكون مما استعمل في ارتكاب الجريمة المعلوماتية كالماسح الضوئي أو الطابعة وقد تكون مما نتج عن الجريمة المعلوماتية، فمثلاً: في الأردن قامت السلطة المختصة بالتحقيق في جريمة قتل الدكتور عوني سعد، بضبط جهاز الحاسب الآلي الخاص بعيادة المغدور ونوعه 486×4 وأقراص مرنة عددها 68 قياس خمسة وربع أنش، وأقراص مرنة ديسكات عددها 12 قياس ثلاثة ونصف أنش، بالإضافة إلى ضبط محتويات الحاسب الآلي. [2]

ثانياً: ضبط المكونات المعنوية للحاسب الآلي "البيانات والمعلومات الإلكترونية":

يستخلص من صياغة التشريعات الجنائية لمفهوم الضبط أنه يقتصر على الأشياء المادية فقط، ولذا فقد اختلفت التشريعات الإجرائية والاتجاهات الفقهية في مسألة ضبط الأشياء المعنوية أو الكيانات المنطقية والتي لا تصلح بطبيعتها أن تكون محلاً لوضع اليد، فأصبحت مثَار جدل حول مدى جواز ضبط المكونات المعنوية للحاسب الآلي من معلومات وبرامج وما تحتويه صناديق البريد الإلكترونية من رسائل وصور وبيانات، وأي أدوات دفع إلكتروني أو أي أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف. [3]

(1) علي حسن الطوالبة، مرجع سابق ذكره، ص 141.
(2) علي حسن محمد الطوالبة، مرجع سابق ذكره، ص 140-142.
(3) عبدالله دغش العجمي، مرجع سابق ذكره، ص 81-82.

فقد انقسمت التشريعات والاتجاهات إلى اتجاهين رئيسيين:

الاتجاه الأول: يرى أصحاب هذا الاتجاه بأنه من غير الممكن ضبط البيانات الإلكترونية لانتفاء الطابع المادي لهذه البيانات، ذلك لأن بيانات الحاسب الآلي ليست مثل الأشياء المحسوسة والملموسة، وبالتالي لا تصلح لأن يرد عليها إجراء الضبط. [1]

وقد أخذت بعض تشريعات الدول بهذا الاتجاه منها قانون "الإجراءات الجنائية الألماني، فقد قصرت المادة "94" منه محل الضبط على الأشياء المادية المحسوسة أو الملموسة ، ويفسر الفقه الألماني نص هذه المادة بأن البيانات المعالجة آلياً لا يمكن ضبطها مجردة ذلك لأنها تفتقر إلى الكيان المادي ولكن عند تحويلها أو صبها في كيان مادي يمكن ضبطها حينها مثل طباعة هذه البيانات على الأوراق أو بتصوير الشاشة أو نقلها على حافظة البيانات ومن ثم التعامل معها، وهذا ما يؤيده كذلك جانب من الفقه الفرنسي، كما أقره التشريع الروماني بحيث أجاز إجراء الضبط إذا ما كان واقعاً على الدعامة المادية المدون عليها بيانات الحاسب الآلي كالأشرطة المغناطيسية أو الأقراص وليس واقعاً على كيان غير مادي وقد اتبعت كذلك دولة اليابان نفس النهج. [2]

وبالرغم من ذلك يرى أصحاب هذا الرأي أو الاتجاه ضرورة التدخل التشريعي وذلك من أجل توسيع دائرة الأشياء التي يمكن أن يرد عليها إجراء الضبط بشكل صريح ليشمل بالإضافة إلى الأشياء المادية، كذلك البيانات الإلكترونية بكافة أنواعها وأنماطها المحسوبة وليس فقط الاكتفاء بالنص التشريعي كما ورد ذكره في التشريعات الإلكترونية مثل تدوين هذه البيانات أو المعلومات في أوراق أو تصوير الشاشة...الخ، فهذا فيه تحميل للنص أكثر مما يحتمل، وهذا ما أرى ضرورة

(1) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 66.
(2) علي حسن محمد الطوالبة، مرجع سابق ذكره، ص 145.

القيام به من جانب جميع الدول التي لم تقم بعد بتوسيع دائرة الأشياء الواقع عليها إجراء الضبط في تشريعاتها الإجرائية الجنائية. [1]

ولذا فقد اقترح أتباع هذا الاتجاه إضافة عبارة المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي إلى النص القانوني الذي ينص على التفتيش والضبط ليشمل هذا التطور التكنولوجي الحاصل في بيئة المعلومات. [2]

الاتجاه الثاني: يرى أنصاره أنه لا يوجد ما يمنع من أن يرد الضبط على البيانات الإلكترونية مستندين في ذلك على أن الغاية من التفتيش هو ضبط جميع الأدلة التي تفيد في كشف الحقيقة. [3]

كما يرى أن البيانات المعالجة إلكترونياً ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره. [4]

كما يجد هذا الاتجاه تجسيده التشريعي في قوانين بعض الدول مثل "الولايات المتحدة الأمريكية" التي قضت بإعطاء سلطات التحقيق مُكنة القيام بأي شيء يكون ضرورياً لجمع الأدلة وحمايتها بما في ذلك المكونات المعنوية للحاسب الآلي وإن كان لا يتصور ضبطها باعتبارها أشياء غير محسوسة وغير مادية، فإنه من الممكن ضبطها إذا أصبح لها كيان مادي، مثل تسجيل المعلومات والبيانات الإلكترونية المراد ضبطها على ورق أو تسجيلها في أشرطة أو أقراص أو نسخها في ملفات إذ في هذه الحالة تتحول المكونات المعنوية للحاسب الآلي إلى أشياء مادية

(1) مفتاح بوبكر المطردي، مرجع سابق ذكره، ص 57
(2) ذات المرجع السابق، ص 57.
(3) ذات المرجع السابق، ض 57.
(4) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 67.

مرئية ومقروءة وتكتسب بالتالي كياناً مادياً يمكن بواسطتها ضبطها ونقلها من مكان لآخر والقول نفسه ينطبق بشأن الرسائل الإلكترونية، فيجوز للمحقق أن يضبط الرسائل المخزنة بالبريد الإلكتروني عن طريق طباعة الرسالة المراد ضبطها أو تسجيلها في ملف أو قرص. [1]

وكذلك سار على نفس هذا النهج قانون "الإجراءات الجنائية اليوناني" في المادة "251" والتي تعطي سلطة التحقيق إجازة القيام بأي شيء وهذا يعني أن التحقيق يشمل ضبط البيانات المخزنة أو المعالجة إلكترونياً، وهذا ما نصت عليه كذلك المادة "29 / 7" من قانون "الإثبات الكندي" بقولها أن "تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة، يستوي في ذلك أن تكون السجلات مكتوبة أم في شكل إلكتروني".[2]

وأيضاً المادة "39" من قانون "تحقيق الجنايات البلجيكي" المدخلة في التفتيش بمقتضى القانون الصادر في 2000/11/23م حيث وسعت من نطاق التفتيش والضبط فقد شمل الحجز أو الضبط وفقاً لهذه المادة الأشياء المادية وكذلك البيانات المعالجة إلكترونياً. [3]

وخشية من محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها بطريق التفتيش ، للمحقق التحفظ على هذه الأدلة ، ويتم التحفظ على البيانات محل الجريمة، وكذلك الأدوات التي استخدمت في ارتكابها، أو الآثار المتخلفة عنها وتفيد في كشف الحقيقة، ويتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، وتبقى تحت

(1) مفتاح بوبكر المطردي، مرجع سابق ذكره، ص 58.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص 58.
(3) ذات المرجع السابق، ص 58 – 59..

تصرفها إلى حين انتهاء المحاكمة، ويرى البعض ضرورة حفظ نسخة أخرى، خوفاً من تلف أو ضياع النسخة الوحيدة الموجودة تحت تصرف جهة التحقيق أو المحكمة. [1]

والمثال على ذلك المادة "88" من قانون "تحقيق الجنايات البلجيكي" لقاضي التحقيق سلطة الأمر بالتحفظ عليها، إن وجدت على الأرض البلجيكية أو أن يطلب من السلطات الأجنبية نسخة من هذه البيانات محل الجريمة، إن وجدت لدى دولة أجنبية. [2]

والجدير بالذكر في الختام القول بأن إجراء الضبط للبيانات المعالجة إلكترونياً يُواجه صعوبات كثيرة منها:

أ. حجم الشبكة التي تحتوي على المعلومات المعالجة إلكترونياً والمطلوب ضبطها.

ب. وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع الجهات المختصة بالتحقيق في عملية التفتيش والضبط والتحفظ على الأدلة.

ت. يُمثل التفتيش والضبط في بعض الأحيان اعتداءً على حقوق غيرنا أو على حرمة الحياة الخاصة ولذا يجب اتخاذ جميع الضمانات القانونية اللازمة لحماية هذه الحقوق والحريات كما اوضحناها سالفاً. [3]

(1) ثنيان ناصر آل ثنيان، مرجع سابق ذكره، ص 67.
(2) علي عدنان الفيل، مرجع سابق ذكره، ص 59.
(3) ذات المرجع السابق، ص 59.

الخاتمة

الخاتمة

الحمد لله الذي يسر لنا إتمام هذا العمل المتواضع والذي حاولنا فيه الوقوف على ملامح السياسة الجنائية في شأن مواجهة القرصنة المعلوماتية، سواء من الناحية الموضوعية أم من الناحية الإجرائية فأوضحنا الجهود المبذولة للتصدي لها من الجانب التشريعي لعدد من الدول العربية والدول الغربية.

كما قمنا بدراسة الجانب الإجرائي للجريمة المعلوماتية، سواء من ناحية إجراءات جمع الأدلة والاستدلال أو إجراءات التحقيق الابتدائي، ومن خلال هذه الدراسة قد توصلنا إلى مجموعة من النتائج وإبداء بعض التوصيات أو المقترحات وهي كما يلي:

أولاً: النتائج

1. إن صور القرصنة المعلوماتية هي ذات طبيعة خاصة متميزة، تتسم بعدد من الخصائص التي تنفرد بها عن غيرها من الجرائم التقليدية سواء من حيث أسلوب ارتكابها أو دوافعها، وذلك راجع إلى عدة عوامل منها الطبيعة المعنوية لهذه الظاهرة الحديثة، فهي غالباً ما تقع على بيانات وبرامج مخزنة في الحاسب الآلي، كما برز ما يُعرف بالمجرم المعلوماتي ذو المهارات التقنية الخاصة في مجال المعلوماتية.
2. إن النصوص العقابية التقليدية في قانون العقوبات الخاص بأي دولة ما ستبقى دائماً قاصرة من مواجهة الجريمة المعلوماتية يكون محلها أو موضوعها متمثل في المعلومات أو البيانات المعالجة آلياً سواء أكانت موجودة على الحاسب الآلي أو على شبكة المعلومات الدولية، وليس بالنسبة للجرائم التي يكون الحاسب الآلي أو شبكة المعلومات الدولية، وليس بالنسبة للجرائم التي يكون الحاسب الآلي أو شبكة المعلومات الدولية مجرد وسيلة لارتكابها فقط مثل جرائم

السب والقذف بواسطة الآلة الرقمية "حاسب آلي – هاتف محمول...الخ"، لأن هذه النصوص التقليدية قد وضعت في زمن سابق على ظهور الحاسب الآلي والشبكة المعلوماتية، وما أفرزته هذه التكنولوجيا الحديثة من مظاهر إجرامية مختلفة.

إضافة إلى أن محاولة تطبيق النصوص المتعلقة بالجرائم التقليدية على الاعتداءات الواقعة على الأنظمة المعلوماتية عن طريق القياس، هو قياسٌ مع الفارق، وبالتالي سيترتب على ذلك مخالفة أو تصادم مع المبادئ العامة المستقرة والتي تقوم عليها جُل القوانين العقابية مثل مبدأ "شرعية الجرائم والعقوبات".

3. إن هناك فراغاً تشريعاً في مجال الجرائم المعلوماتية، حيث عجزت الكثير من التشريعات العقابية النافذة في كثير من الدول وخاصة الدول العربية عن مواجهة أو مكافحة هذه الظاهرة الإجرامية والوقاية منها، إذ لم تقم بإجراء أي تعديل على قوانينها بما يكفل التصدي لهذه الظاهرة الإجرامية المستحدثة، أو لم تقم أصلاً بتجريم هذه الاعتداءات الواقعة على النظم المعلوماتية، بوضع نموذجاً تجريمياً لها سواء في التشريعات النافذة أو في تشريعات خاصة لمعالجة هذا النوع من الإجرام المعلوماتي، وهذا هو الحاصل في دولة ليبيا، حيث لم يقم المشرّع الليبي إلى يومنا هذا بإصدار تشريع خاص يعالج هذه الظاهرة الإجرامية الخطيرة.

إلا أن هناك بعض الدول الأخرى التي خطت خطوات متقدمة عن غيرها في هذا المجال فقامت بإصدار تشريعات خاصة بهذا النوع من الإجرام مثل دولة الإمارات العربية ودولة عمان ودولة مصر.

أما الدول الغربية فكانت هي السباقة في مجال مكافحة الجريمة المعلوماتية، فقامت بإصدار تشريعات خاصة تعالج هذا النوع من الإجرام المستحدث مثل التشريع الفرنسي والتشريع الأمريكي والتشريع الإنجليزي.

4. لقد عملت بعض الدول مثل دولة مصر والإمارات العربية المتحدة والولايات المتحدة الأمريكية على استحداث أجهزة خاصة يناط بها مهمة مكافحة الإجرام المعلوماتي المستحدث ، بحيث يكون عناصر هذه الأجهزة ذات تأهيل وتدريب عالي في مجال التقنية المعلوماتية وعلى معرفة بكيفية التعامل مع الجريمة المعلوماتية على أكمل وجه وذلك فيما يتعلق بكشف هذه الجرائم وتعقب مرتكبيها وتفتيش النظم المعلوماتية وضبط الأدلة الرقمية والتحفظ عليها خوفاً من اتلافها أو ضياعها ، وذلك من أجل كشف الحقيقة.
5. هناك العديد من التحديات في مجال إثبات الجريمة المعلوماتية ، أهمها صعوبة اكتشافها وذلك إما بسبب أحجام المجني عليهم عن تقديم شكوى بخصوص الجرائم المعلوماتية لخوفهم على سمعتهم وأعمالهم التجارية أو لغياب النص التجريمي لما وقع عليهم من سلوكيات أو لجهلهم أصلاً لما حدث من جرائم التقنية إما بسبب الطبيعة المعنوية لهذه الجريمة، فهي لا تترك أثراً مادياً ملموساً لها بعد ارتكابها ولا دلائل مادية مما يجعل الأدلة التقليدية غير ملائمة لإثبات تلك الجرائم، وهذا ما يدفع بالمحققين للبحث عن الأدلة الرقمية في البيئة المعلوماتية لإثبات الجريمة المعلوماتية، ومواجهة ما يترتب على ذلك من صعوبات سواء في مرحلة التفتيش والضبط وذلك فيما يتعلق بصحة تفتيش الوسط الافتراضي وبصفة القائم بالتفتيش وغيرها. أو في مرحلة المحاكمة فيما يتعلق بتحديد القيمة القانونية للدليل الرقمي من حيث مشروعيته وحجيته أمام القضاء الجنائي.
6. تثير هذه الطائفة من الجرائم العديد من الإشكاليات في الجانب الإجرائي، فضلاً عن صعوبة كشفها وإثباتها وذلك فيما يخص إجراء التفتيش والضبط، فإن التفتيش الواقع على مكونات الحاسب المادية لا يواجه أي مشكلة عند تنفيذ إجراء التفتيش لإمكانية وسهولة ذلك، لأن التفتيش من حيث الأصل يقع على أشياء مادية وهذا ما نصت عليه أغلب القوانين الإجرائية.

ولكن المشكلة تكمن في تفتيش أو ضبط مكونات الحاسب الآلي المنطقية أو المعنوية، حيث اختلفت الآراء الفقهية والاتجاهات التشريعية في خصوص مدى جواز إمكانية خضوع هذه المكونات المعنوية للحاسب الآلي للتفتيش والضبط.

7. إن الخبرة والمعاينة في الجرائم المعلوماتية اليوم تحتاج إلى إدارة خاصة يعمل بها متخصصون في أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية، وذلك بسبب الطبيعة الفنية والمعقدة للجرائم المعلوماتية، بحيث لا يمكن الفصل فيها دون الرجوع لأهل الخبرة في هذا المجال.
8. إن الطابع التقني والعابر للحدود للجريمة المعلوماتية، قد خلق العديد من التعقيدات أمام الجهات المختصة بالتحقيق عند القيام بأعمال التفتيش والضبط للبيانات التي تحتوي على أدلة، بحيث قد تتوزع هذه البيانات عبر الشبكة المعلوماتية لتقع أو تدخل في نطاق دولة أخرى، مما يستدعي اللجوء إلى المساعدة القانونية المتبادلة وغيرها من صور التعاون الدولي في خصوص هذا المجال، وإلا كان هناك اعتداءً على مبدأ السيادة الوطنية للدول.

ثانياً: التوصيات "المقترحات":

إن خطورة هذه الظاهرة الإجرامية والتي تزداد يوماً بعد يوم بسبب التطور السريع الحاصل في مجال تكنولوجيا المعلومات، جعل من الضروري تضمين هذه الدراسة ببعض المقترحات أو التوصيات والتي قد تساعد ولو بقدر بسيط في الحد من هذه الظاهرة الإجرامية المستحدثة والخطيرة في آن واحد ومنها:

1. فيما يتعلق بالناحية الموضوعية ، فمن الضروري إصدار قوانين عقابية خاصة ومستقلة تحتوي على نصوص موضوعية تجرم كل الصور المختلفة للجريمة المعلوماتية، وقادرة على مواجهة ومكافحة هذا النوع من الإجرام المستحدث من قبل جميع الدول في العالم أجمع، أو على الأقل العمل على تعديل قوانينها الحالية النافذة بما يتسع لتجريم هذا النوع من الإجرام بدلاً من اللجوء إلى النصوص والقواعد التقليدية وغير الملائمة أصلاً للطبيعة الخاصة للجريمة المعلوماتية لتطبيقها عليها.

لذا يجب حث جميع الدول التي لم تقم بعد بإصدار تشريع خاص بالجريمة المعلوماتية على القيام بذلك، منها دولة ليبيا، فيجب على المشرّع الليبي أن يستفيق من غيبوبته الطويلة خاصة في ظل استفحال هذا الإجرام المعلوماتي في وقتنا هذا، وبالتالي ضرورة العمل على سن تشريع جنائي خاص يعالج الجريمة المعلوماتية من مختلف جوانبها وأبعادها.

2. ضرورة إجراء تعديل على القوانين الإجرائية القائمة بما يكفل تفعيل مكافحة هذه الجرائم وتعقب الجناة والتحقيق معهم، بحيث تتسم النصوص الإجرائية بنوع من المرونة مثل التسامح للمحقق بتفتيش الحواسيب الشخصية والشبكة المعلوماتية واعتراض الاتصالات التي تتم عبر شبكة المعلومات في أسرع وقت ممكن وذلك لضمان عدم ضياع الدليل الرقمي والذي يجب النص عليه صراحة كدليل من أدلة الإثبات في المجال الجنائي، ودون الانتظار للحصول على إذن

مسبق للتفتيش ليس فقط في حالة التلبس بالجريمة، بل يجب إضافة حالات أخرى مثلاً في حالة وصول معلومات مؤكدة على القيام بهذه الاعتداءات الخطيرة على النظم المعلوماتية ومن مصدر موثوق به، كما يجب النص صراحة على جواز تفتيش الوسط الافتراضي وضبط محتوياته.

3. ضرورة إعداد كوادر فنية خاصة يُعهد إليها مهمة التعامل مع هذه الطائفة من الجرائم، وبالتالي تختص بالتحقيق في الجريمة المعلوماتية وتفتيش الوسط الافتراضي وضبط الأدلة الناتجة عنه وملاحقة مرتكبيها وتعقبهم، ومن ثم مكافحة الجريمة المعلوماتية على أكمل وجه، ولذا يجب تدريب هذه الكوادر من خلال إجراء دورات تدريبية وتثقيفية في هذا المجال يتم فيها التوعية بهذا النوع من الإجرام المعلوماتي المستحدث ومعرفة خصائصه وسماته وأساليب ارتكابه.
4. ضرورة تأهيل قضاة متخصصين للنظر في قضايا الجريمة المعلوماتية والرفع من كفاءة رجال القضاء ليصبحوا مهيئين ومستعدين للتعامل مع هذا النوع من الإجرام المعلوماتي، سواء في مجال التحقيق أو المحاكمة، وذلك من خلال تدريبهم أثناء الخدمة عن طريق معاهد القضاء من أجل تنمية الوعي لديهم بأبعاد الجريمة المعلوماتية وأساليب ارتكابها، وكذلك يجب المتابعة المستمرة لآخر ما يتوصل إليه خبراء أمن المعلومات من الوسائل الفنية الكفيلة بحماية المال المعلوماتي.
5. ضرورة إنشاء إدارة خاصة للخبرة والمعاينة في الجرائم المعلوماتية، وتدريب القائمين على إدارة الخبرة الجنائية وكذلك تدريب رجال النيابة العامة والضبطية القضائية على استخدام مهارات الحاسب الآلي، وذلك لتمكينهم من التعامل مع الجريمة المعلوماتية بالطريقة الصحيحة.
6. التوجه إلى عقد الاتفاقيات الدولية بشكل موسع، للاستفادة من نظام الإنابة القضائية وتبادل المساعدة القانونية في المجال المعلوماتي في حالة عبور آثار الجريمة المعلوماتية لحدود الدولة

الواحدة، وذلك لتسهيل مهمة المحققين ورجال الضبط القضائي، ومن ثم تفادي مشكلة البحث عن الدليل الرقمي خارج حدود الدولة، وعدم التصادم مع مبدأ السيادة الوطنية للدول.

7. ضرورة تدريس الجريمة المعلوماتية كمقرر علمي لطلاب كليات الحقوق والشرطة ومعاهد القضاء بما يمكنهم من تكوين خلفية معرفية جيدة عن هذه الجريمة المعلوماتية وأبعادها ومخاطرها ووسائل مكافحتها.
8. ضرورة تسليط الضوء على موضوع الجريمة المعلوماتية من قبل وسائل الإعلام المختلفة وذلك عن طريق عرض برامج تثقيفية من حين لآخر من أجل توعية مستخدمي شبكة الإنترنت بمخاطرها وما قد ينجم عنها من أضرار فادحة وكذلك بيان أساليب الوقاية من هذه الاعتداءات الخطيرة من قبل الهاكرز وبالتالي الحيلولة دون وقوعهم ضحايا لهذا الإجرام المعلوماتي المستحدث.

ثبت المراجع

ثبت المراجع

أولاً: الكتب العامة والمتخصصة:

أ. الكتب العامة:

1. جلال ثروت، نظم القسم العام في قانون العقوبات ، نظرية الجريمة، د. ط ، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2010م.
2. سعد سالم العسبلي، قانون الإجراءات الجنائية في الفقه والقضاء المقارن، ج1، ط1، الفضيل للطباعة والنشر والتوزيع، ليبيا، بنغازي، 2013م.
3. عوض محمد عوض، الوجيز في قانون الإجراءات الجنائية ، الجزء الأول، د. ط، دار المطبوعات الجامعية، الإسكندرية، د.ت.
4. عوض محمد عوض، قانون الإجراءات الجنائية في التشريع الليبي، د.ط، دار المطبوعات الجامعية، الإسكندرية، 2008م.
5. مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، الجزء الأول، ط1، مطبعة دار الكتب، بيروت، لبنان، 1971م.
6. محمد رمضان باره، شرح الأحكام العامة للجريمة والجزاء، الجزء الأول، "الجريمة"، الطبعة الثالثة، 2000م.
7. محمد رمضان بارة، شرح قانون العقوبات الليبي، القسم الخاص، الجزء الثاني، جرائم الاعتداء على الأموال، د.ط، 2013م.
8. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1996م.

9. موسى مسعود ارحومة، الأحكام العامة لقانون العقوبات الليبي، الجزء الأول، النظرية العامة للجريمة، الطبعة الأولى، بدون ناشر، 2005م.

ب. الكتب المتخصصة:

1. أحمد خليفة الملط، الجرائم المعلوماتية، د. ط.، جامعة الإسكندرية، 2005م.
2. أيمن عبدالحفيظ عبدالحميد سليمان، إستراتيجية مُكافحة جرائم استخدام الحاسب الآلي، د.ط، بدون ناشر، 2003م.
3. أورين كير، "مؤلف"، نطاق الجريمة الافتراضية، عمر محمد بن يونس، "مترجم"، د.ط، جامعة الإسكندرية، د.ت، 2004م.
4. جميل عبدالباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية للنشر، القاهرة، 1992م.
5. حمزة محمد أبوعيسى، جرائم تقنية المعلومات، ط1، دار وائل للنشر والتوزيع، عمان، 2017م.
6. خالد ممدوح إبراهيم، أمن الحكومة الإلكترونية، د.ط.، الدار الجامعية – الإسكندرية، 2010م.
7. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني لحماية المعلومات"، د. ط. دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2009م.
8. عبدالفتاح عبداللطيف الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، ط1، دار الحامد للنشر والتوزيع، عمان، 2010م.
9. عبدالفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، د. ط.، 2009م.

10. علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004م.

11. عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002م.

12. علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، د.ط، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009م.

13. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، د.ط، دار الكتب والوثائق القومية، المكتب الجامعي الحديث، الموصل، 2012م.

14. علي عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، د. ط.، الدار الجامعية للطباعة والنشر، الإسكندرية، 1999م.

15. عصام عبدالفتاح مطر، التشريعات الإلكترونية الدولية والعربية، د.ط. المكتب الجامعي الحديث، 2010م.

16. عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية"، الطبعة الأولى، بدون ناشر، 2005م.

17. فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، د.ط.، كلية الحقوق، جامعة الإسكندرية، د.ت.

18. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، د.ط.، دار النهضة العربية، القاهرة، د.ت.

19. محمد علي العريان، الجرائم المعلوماتية، د.ط، دار الجامعة الجديدة للنشر، جامعة الإسكندرية، 2004م.

20. محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، د.ط. الإسكندرية، دار الجمهورية للصحافة، أكتوبر، 2010م.

21. محمد فتحي عيد، الإجرام المعاصر، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1999م.

22. محمود أحمد القرعان، الجرائم الإلكترونية، ط1، دار وائل للنشر والتوزيع، 2017م.

23. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم.الإنترنت والحاسب الآلي ووسائل مكافحتها، د. ط.، دار الفكر الجامعي، الإسكندرية، 2006م.

24. نسرين عبدالحميد نبيه، الإجرام المعقد، د.ط، منشأة المعارف، الإسكندرية، 2007م.

25. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، د.ط، دار النهضة العربية، القاهرة، 1992م.

26. هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم لمعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003م.

27. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ط1، 1997م.

28. وليد الزيدي، القرصنة على الإنترنت والحاسوب، ط1، دار أسامة للنشر والتوزيع، الأردن، عمان، 2003م.

ثانياً: الرسائل العلمية:

1. أيمن عبدالحفيظ عبدالحميد سليمان، إستراتيجية مُكافحة الجرائم الناشئةة عن استخدام الحاسب الآلي "دراسة مقارنة"، رسالة مقدمة للحصول على درجة الدكتوراه في علوم الشرطة، أكاديمية الشرطة، كلية الدراسات العليا، 2003م.
2. أيمن عبدالله فكري، جرائم نظم المعلومات، رسالة مقدمة لاستكمال الحصول على درجة الدكتوراه، جامعة المنصورة، 2005-2006م.
3. ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، دراسة تآصلية تطبيقية، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2012م.
4. رحاب علي عميش، الجرائم المرتكبة بواسطة الحاسب الآلي ، بحث مقدم استكمالاً لمتطلبات التخصص الدقيق "الدكتوراه"، كلية الحقوق ، جامعة قاريونس، 2006-2007م.
5. عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة مقدمة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط ، عمان الأردن، 2014م.
6. موسى مسعود ارحومة، إشكالية قبول الدليل العلمي أمام القضاء الجنائي "دراسة مقارنة" ، أطروحة لنيل دكتوراه الدولة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط، تصفيف وإخراج الشركة المغربية للطباعة والنشر، 1995-1996م.

ثالثاً: البحوث:

1. أحمد الصادق الجهاني، مقدمة في الإثبات الجنائي، مقرر دراسي لطلبة الدراسات العليا "دروس ألقيت عليهم"، جامعة بنغازي، كلية القانون، للعام الجامعي، 2020م.
2. سالم محمد الأوجلي، مقبولية الدليل الرقمي في المحاكم الجنائية، مجلة دراسات قانونية، تصدرها كلية الحقوق، جامعة بنغازي، العدد التاسع عشر، منشورات جامعة قاريونس، 2016م.
3. سناء خليل، الجريمة المنظمة والعبر الوطنية "الجهود الدولية ومشكلات الملاحقة القضائية"، المجلة الجنائية القومية، العدد الثاني، المجلد التاسع والثلاثون، يوليو، 1996م.
4. طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون ، المنعقد في الفترة من 28-2009/10/29م ، تنظمه أكاديمية الدراسات العليا – طرابلس.
5. فائزة الباشا، سياسة التجريم في مواجهة الجرائم المعلوماتية، ورقة عمل مقدمة إلى المؤتمر الذي عقد في لبنان- منعقد في الفترة 25-2009/02/27م.
6. مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العُليا في الدول العربية، منعقد في 2012/09/25م، السودان.
7. موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، بأكاديمية الدراسات العليا، طرابلس، ليبيا، المنعقد خلال الفترة 28-2009/10/29م.

8. موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مجلة دراسات قانونية، مجلة علمية تصدرها كلية القانون، جامعة قاريونس، العدد السابع عشر، منشورات جامعة قاريونس ، بنغازي ، أكتوبر، 2008م.

9. يونس عرب، جرائم الكمبيوتر والإنترنت، "ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية والملاحقة والإثبات ، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10-2002/02/12م.

10. يونس عرب، الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وسلطنة عمان، هيئة تنظم الاتصالات ، مسقط، سلطنة عمان، الأردن، 2-4 / أبريل/ 2006م.

رابعاً: الشبكة المعلوماتية:

1. جمال الدين كرابيج، الجريمة المعلوماتية، "بحث بعنوان الجريمة المعلوماتية الصحيفة القانونية الإلكترونية، سوريا، 2010-2011م، متاح على الرابط: jle-gov.sy.index.php تاريخ الزيارة: 2017/01/17م.
2. ماهية الجريمة الإلكترونية، قسم أرشيف منتديات الجامعة ، متاح على الرابط: www.djelfa-info>showthread ، تاريخ الزيارة: 2017/02/20م.
3. متاح على الرابط: tecbytec.ahlamontada.com، تاريخ الزيارة 2016/11/05م
4. متاح على الرابط: allthelec82013o4debjimohamed.blogspot.com تاريخ الزيارة:2016/11/05م.
5. متاح على الرابط: www.cunotic.com تاريخ الزيارة: 2016/11/05م
6. متاح على الرابط : www.startimes.com، تاريخ الزيارة 2016/11/05م.
7. متاح على الرابط: tecbytec.ahlamontada.com، تاريخ الزيارة: 2016/11/06م.
8. منتديات جيوش الهاكرز: متاح على الرابط: www.aliy.yosh.comishowthread، تاريخ الزيارة: 2016/11/18م.
9. طرق وكيفية اختراق المواقع الاكترونية، متاح على الرابط: lefafta.blogspot.com blog.spot29 تاريخ الزيارة: 2016/04/29م.
10. القرصنة الإلكترونية، سلاح العصر الرقمي، متاح على الرابط: www.aljazeera.net تاريخ الزيارة: 2016/05/25م.
11. مشروع قانون مكافحة جرائم تقنية المعلومات، متاح على الرابط: aitmagahram.or.eg.com تاريخ الزيارة:2017/01/01م.

12. نشر نص قانون مكافحة جرائم الإنترنت "الحق والضلال" متاح على الرابط: www.christian..dogma.com تاريخ الزيارة : 2017/01/01م.
13. ثقافة قانونية، جهود سلطنة عمان في مكافحة جرائم تقنية المعلومات، متاح على الرابط: hussain-alghafri-blogspot.com ، تاريخ الزيارة: 2017/01/03م.
14. حسين بن سعيد بن سيف الغافري، منتدى القانون العماني، نتاح على الرابط: www.omanLegal.net.work تاريخ الزيارة: 2017/01/04م.
15. قانون جرائم تقنية المعلومات، قوانين وإجراءات سلطنة عمان موافدين، المرسوم السلطاتي رقم 2001/12. متاح على الرابط: https://m.facebook.com>permalink تاريخ الزيارة: 2017/01/08م.
16. مصطفى السيد علي بلاس، ملامح قانون مكافحة جرائم تقنية المعلومات، متاح على الرابط، 2015.omandaily.om ، تاريخ الزيارة: 2017/01/10م
17. دولة الإمارات العربية المتحدة قانون مكافحة جرائم تقنية المعلومات، شبكة المعلومات الدولية، متاح على الرابط، www.gcc-legal-org>LawAsppf>Law تاريخ الزيارة: 2017/01/10م.
18. متاح على الرابط: www.albayanae/across.the-uae/assident تاريخ الزيارة: 2017/01/17م.
19. تعديل تشريعي يشدد جرائم الإنترنت من جنحة إلى جناية، الإمارات اليوم، متاح على الرابط: www.emarataNoum.com>other تاريخ الزيارة: 2017/01/19م.
20. يونس عرب، ورقة عمل، الاتجاهات التشريعية للجرائم الإلكترونية، متاح على الرابط: www.arablaw.orglowoff@hd.com

21. متـــاح علـــى الـــرابط: www.ituarubic.org>EcrimesDoC6 تـــاريخ الزيـــارة: 2017/01/29م.

22. متاح على الرابط: Cybercrime<pdf<eipr.org تاريخ الزيارة: 2020/10/03م.

23. مرسوم سلطاني رقم 2011/12 بإصدار قانون مكافحة جرائم تقنية المعلومات متاح على الرابط: www.qanoon.om تاريخ الزيارة: 2020/10/04م.

24. متاح على الرابط: polickwww.mone.gor.om تاريخ الزيارة: 2020/10/04م.

25. متاح على الرابط: www.emaratayoum.com تاريخ الزيارة: 2020/10/05م.

26. متاح على الرابط: news<www.hrw.org تاريخ الزيارة: 2020/10/05م.

27. بشأن تعديل المرسوم بقانون اتحادي رقم (5) لسنة 2010م في شأن مكافحة جرائم تقنية المعلومات متاح على الرابط: ArticlsTDetails<site.eastLaws.com

28. قانون إساءة استخدام الكمبيوتر البريطاني COMPUTER MISUSE ACT متاح على الرابط: commencement29August1990<galan.2184445.com

29. الجريمة عبر الإنترنت (3) تشريعات ضد الجرائم الإلكترونية على مستوى العالم، مجلة جيـــوش الأمـــة، رئـــيس التحريـــر : يوســـف أيـــوب متـــاح علـــى الـــرابط: Article<www.soualomma.com, تاريخ الزيارة: 2020/10/06م.

30. منـى كامـل تركـي، التحقيـق الجنـائي فـي الجـرائم الإلكترونيـة، بحـث منشـور فـي المدونـة الإلكترونية، متاح على الرابط: blog-page..<amdayss.blogspot.com تاريخ الزيارة: 2020/10/05م.

31. حسين خليل مطر، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، بحث مقدم إلى مؤتمر "الإصلاح التشريعي طريق نحو الحكومة الرشيدة ومكافحة الفساد" الذي أقامته مؤسسة النبأ للثقافة والإعلام ، جامعة الكوفة ، كلية القانون 25 – 26 نيسان، 2018م، متاح على الرابط annabaa.org.com.

32. موسوعة التشريعات الجنائية، الجزء الثالث، قانون الإجراءات الجنائية والقوانين المكملة له، متاح على الرابط: <2016/01<iteadel.gov.ly

33. شبكة قوانين الشرق EASTLWS.COM.، متاح على الرابط: http://security-Legislation.ly/sites تاريخ الزيارة: 2020/11/1م.

Criminal Policy in the Face of Information Piracy

By
Faezah Sulayman Omar

Supervisor
Dr. Mossa Massoud Irhouma

ABSTRACT

The computer and the international information network are the most important requirements of modern times. The importance of this study is that any modern invention has its advantages and disadvantages represented in misuse of this recent technology.

This study aims to shed light on the images of information piracy and show what it is and the possibility of addressing this criminal phenomenon objectively and procedurally.

To implement this study, a "descriptive analytical" approach has been adopted. The most important of these findings are as follows:

1. The image of the information piracy is with special nature, marked with distinct characteristics from the conventional crimes.
2. There is a legislative vacuum in the field of cybercrime that states, especially Arab countries, are confronted with as they have not criminalized such attacks on information systems, such as what is occurring in Libya, or it did not make any adjustment in its

legislations, enough to guarantees confronting it with good and integrated manner.

3. Creation of special tools to combat information criminality, consisting of highly qualified personnel in the field of information technology.
4. There are many challenges in its procedural aspect, the most important in the field of evidencing the information crime, where it is difficult to discover due to its moral nature , which led to the emergence of what is known as digital evidence, as well as in the field of conducting inspection and control of the components of the moral computer "logical", contrary to the original inspection, where it fall on things with materialistic nature.

Criminal Policy in the Face of Information Piracy

By

Faezah Sulayman Omar

Supervisor

Prof. Mossa Massoud Irhouma

This Thesis was submitted in Partial Fulfillment of the Requirements for Master's Degree of Criminal Low.

University of Benghazi

Faculty of Low

June 2020