الفصل السابع

القانون وجرائم الحاسبات

Chapter seven

Security

جرائم الحاسبات الإلكترونية

هناك عدة طرق تستخدم فيها الحاسبات الإلكترونية بطريقة غير سليمة والهدف منها تحقيق مكاسب شخصية أو لغرض إيذاء الأخرين، من هذه الطرق الاحتيال وانتهاك سرية الأفراد باستخدام الحاسبة الإلكترونية وسرقة الكيانات المنطقية أو برمجيات الحاسب.

الاحتيال وانتهاك سرية الأفراد باستخدام الحاسبة الإلكترونية

يقصد بالاحتيال السرقة باستخدام الحاسبات الإلكترونية ويشمل:

1. **سرقة الأموال:** إن الأشخاص الذين يقومون بالتحايل واستخدام الحاسبة الإلكترونية للسرقة تنقصهم الأمانة حيث يعمدون إلى استخدام الحاسبات العائدة لأصحاب العمل لارتكاب جرائمهم على سبيل المثال قد يقومون بتغيير أرقام سجلات الحسابات بحيث تصبح أقل من المجموع الفعلي للحسابات الموجودة ثم يتم الاستيلاء على المبلغ الذي يتم طرحه من هذه الحسابات، أو استخدام بطاقات مزورة يتم عند استخدامها نقل الأموال من حسابات الزبائن الآخرين إلى حساب سارق الأموال، لا تقتصر عمليات الاحتيال على المصارف أو مؤسسات الأعمال وإنما تشمل أية جهة تعتمد عملها على الحاسبات الاكترونية.

2. **سرقة الوقت:** من الممكن سرقة وقت الحاسبات الإلكترونية، يتم باستخدام مودم وكلمة سر رمزية أو عدد رمزي غير مرخص له يستطيع المجرم أن يتسلل إلى نظام حاسبة يمتلكها شخص آخر أو مؤسسة أخرى لتحقيق أهداف غير شرعية، في الغالب يتسلل السارقون إلى أنظمة رئيسية غالية الثمن، من المعروف أن الشخص الذي يمتلك الحاسبة الإلكترونية يقوم بدفع تكلفة تشغيل هذه الأنظمة.

تظهر حالة سرقة الوقت بصورة جلية في الجامعات، إذ يقوم بعض الطلبة بالاستفادة من المعلومات التي يتعلمونها في كيفية تشغيل واستخدام الحاسبة الإلكترونية إلى استخدام هذه المعلومات بطرق غير مشروعة، على سبيل المثال قد يتسللون إلى حساباتهم لتغيير درجاتهم أو لحسابات غيرهم من الطلبة لإتلاف بياناتهم، قد يشعر الطلبة أن التسلل إلى نظام الحاسبة الإلكترونية الخاص بالجامعة يعد تحدياً مثيراً أو مزاحاً دون أن يدركون أنهم قد يورطون أنفسهم في مشاكل خطيرة جداً.

لا يقتصر الأمر على طلبة الجامعات، إذ يقوم بمثل هذه الأعمال من هم أصغر سناً، على سبيل المثال ألقي القبض على طالب في مرحلة الدراسة الثانوية وهو يتسلل إلى نظام الحاسبة الإلكترونية الخاص بشركة لكي يستطيع أن يمارس بعض الألعاب بواسطة الحاسبة الإلكترونية، أما غيرهم من المجرمين فهم محترفون يستخدمون حاسبات أشخاص آخرين لإنجاز أعمالهم الخاصة.

3. **سرقة المعلومات:** إن أغلب المؤسسات تحتفظ بمعلومات قيمة جداً في الحاسبة الإلكترونية، قد يشعر البعض بالقلق من إمكانية استخدام هذه المعلومات بطريقة غير صحيحة فالملفات الورقية يمكن حفظها في أماكن مقفلة، لكن الملفات المخزونة في الحاسبات الإلكترونية يمكن الوصول إليها عن طريق تخمين كلمة السر أو خوارزميات الدخول فإذا استطاع شخص غير مخول بالوصول ليس لديه الصلاحيات أن ينال معلومات حكومية، قد يلحق ذلك الأذى و الأضرار للمنشأة، قد تحتوي بعض المؤسسات على تقارير يؤدي الاطلاع عليها إلحاق الأذى بحياة ومهن أشخاص عندما تقع هذه المعلومات في أيدي أشخاص ليس لهم حق الاطلاع عليها.

سرقة الكيانات المنطقية أو برمجيات الحاسبة الإلكترونية

يقصد بذلك قيام السارق بنسخ برنامج أو نظام بدون دفع ثمنه للشخص أو للشركة التي تمتلكه قانونياً، إن هذه البرامج تكون غالية الثمن لذلك يقوم السارقون بنسخها بطريقة غير مشروعة والتي تكلف الأشخاص أو الشركات خسائر كبيرة نتيجة لهذا الفعل كما أن هنالك طريقة أخرى للسرقة هي أن يقوم السارق بشراء نسخة من برنامج معين ثم يقوم بنسخه بطريقة غير مشروعة ووضع علامات مزيفة، تسمى هذه الطريقة (البيع تحت علامات مزيفة)، بذلك يستطيع السارق أن يبيع المنتجات البرمجية بسعر منخفض، هذه الطريقة تسبب خسائر كبيرة في الأرباح للناشر تتم حماية برمجيات الحاسبة الإلكترونية بواسطة قوانين حق النشر كما هو الحال مع الكتب والمجلات، هذه القوانين تعطي الأشخاص الذين يطورون البرمجيات وحدهم دون غيرهم حق بيعها وتحقيق الأرباح من ذلك، كما تحول دون استيلاء الأشخاص الذين لا يملكون البرمجيات على حقوق أصحاب البرمجيات الشرعيين، وعندما يتم القبض على سارقي البرمجيات يمكن أن توجه إليهم تهمة خرق قوانين حق النشر مما يعد جريمة خطيرة.

خصائص و طبيعة جرائم الحاسوب الآلي

1- عدم الوضوح والصعوبة في الإثبات، لذلك عادة ما يتردد الذين تقع عليهم الاعتداءات المعلوماتية في الإبلاغ عن تلك الجرائم حتى لا يؤدي ذلك إلى إلحاق المزيد من الضرر، كما أن معظمهم ليس لديه الثقة بالجهات المختصة في التوصل إلى الجناة، و ذلك لصعوبة الأمر من الناحية التقنية.
2- أن الخسارة الاقتصادية التي تسببها الجريمة عادة ما تكون باهظة في أغلبية الجرائم سواء كانت من نوع سرقة المبالغ النقدية من بعض الحسابات أو جريمة سرقة برنامج أو القيام بحذفه أو تدمير بيانات أو ملفات محددة بالإضافة إلى اختراق الشبكات وكشف المعلومات والأسرار، على سبيل المثال قدرت الخسائر الناجمة عن تلك الجرائم في الولايات المتحدة ما بين 300 – 500 مليون دولار سنويا، في حين قدرت تكلفة جريمة الحاسوب الآلي الواحدة في نهاية الثمانينات نحو 600 ألف دولار سنويا، في الوقت الذي تقدر فيه تكلفة السرقة الواحدة تحت تهديد السلاح حوالي ثلاثة ألاف دولار، ذلك تبعا لدراسة أجراها احد مكاتب المحاسبة الأمريكية.

3- انه يمكن حدوثها في زمن قصير كذلك لا يؤدي اكتشاف الخسائر إلى الكشف عن الأساليب المستخدمة إضافة إلى صعوبة إقامة الدعوى في تلك الجرائم التقليدية .
4- يعد من المستحيل تحديد وقت ارتكاب تلك الجرائم، بالتالي يصعب الحصول على دليل مادي في مثل هذه الجرائم، التي تغلب عليها الطبيعة الالكترونية على الدليل المتوفر.

المراحل التي ترتكب فيها جرائم الحاسوب الآلي

1- مرحلة إدخال البيانات

تحدث هذه الجريمة عند قيام المستخدم بتزوير أو تغيير البيانات، على سبيل المثال إذا استطاع الجاني الوصول إلى البيانات المتعلقة بقائمة الهاتف قبل إعدادها بشكلها النهائي من قبل شركة الهواتف، وقيامه بحذف عدد من المكالمات الهاتفية القائمة قبل إرسالها بالبريد، أو عند قيام احد مدخلي البيانات بتغيير المستندات الثبوتية لشخص ما أو القيام بتغيير معلومات شخص مشتبه به من مستخدم الحاسوب غير المحول.

2- مرحلة تشغيل البيانات

يقوم مرتكبو الجرائم في هذه المرحلة بتعديل البرامج الجاهزة والتطبيقات البرمجية التي تعمل على تشغيل البيانات من اجل الوصول إلى نتائج محددة أو مقصودة، في هذه الحالة يكون الجناة على قدر كاف من الدراية والمعرفة بالنظام الذي يعمل عليه الحاسوب.

3- مرحلة اخراج البيانات

تعد هذه المرحلة من أكثر المراحل التي ترتكب فيها جرائم الحاسوب وتتم فيها سرقة المعلومات أو البيانات المتعلقة بالرقابة على المخزون في إحدى المؤسسات أو إفشاء بعض المعلومات الخاصة بالإجراءات الأمنية لمؤسسة هامة، وهي التي تخضع للفحص السري لتأمين وضع معين عند موقف ما لدى السلطات العسكرية أو غيرها كالوزارات والشركات والأفراد، تعد هذه المرحلة من أهم مراحل ارتكاب الجريمة الموجهة للحاسوب الآلي ذلك لان المعلومات تكون هنا مكتملة وجاهزة، هي بذلك في متناول أيدي العابثين والمتسللين مما يتطلب توفير مستلزمات الأمن المعلوماتي بشكل أكثر أمانا وموثوقية في هذه المرحلة تحديدا.

رأي القانون في جرائم الحاسبات الإلكترونية

إن مشكلة العصر هي قلة القوانين التي تحول دون ارتكاب الجرائم بواسطة الحاسبات الإلكترونية فالقوانين المتوفرة تتعلق بجرائم السرقة والسطو والاختطاف والابتزاز، لذلك فإن جرائم الحاسبات الإلكترونية تعد نوعاً جديداً من الجرائم، مع ازدياد انتشارها ظهرت الحاجة إلى وضع قوانين جديدة لمحاربة استخدام الحاسبات الإلكترونية بطريقة غير مشروعة، والواقع أنه لا توجد طريقة معينة تمنع شخص ما من الدخول إلى حاسبة ما وقراءة ملفاتها (في حالة ارتباط الحاسبة بشبكة الانترنت)، إلا أن عليه أولاً إقناع الحاسبة بأنه

مخول بالاطلاع على المعلومات، وذلك بتخمين كلمة المرور المعروفة لدى الحاسبة، حدث ذلك في العالم مرات عديدة حيث استطاع عدة أشخاص التجسس أو التطفل على محتويات ملفات شركات ومؤسسات عديدة، لهذا السبب إن من الصعوبة التصدي لهذا التهديد الصادر من أشخاص تطلق عليهم تسمية (المتطفلين الأذكياء) والذين يمكن تسخيرهم من قبل جهات وحكومات للحصول على ما هو أثمن وأخطر

في السابق كانت بعض المؤسسات تتردد في الإبلاغ عن جرائم الحاسبات الإلكترونية لأنها لم تكن ترغب في أن يعرف أحد أنه تم التسلل إلى نظام الأمان الخاص بها، لكن الآن أصبحت تدرك أهمية الكشف عن السارقين وتقفي آثارهم، أصبحت سرقة المعلومات تعتبر جريمة، إذ أن سرقة معلومات مؤسسة ما واستخدامها غير مسموح به ويعد منافياً للقانون، أن هذه الجرائم تكلف الأشخاص والشركات مبالغ كبيرة وتهدد خصوصياتهم وأمنهم، يجب العمل على تشريع قوانين أكثر صرامة قد تردع بعض ضعيفي النفوس من القيام بأعمال غير نزيهة.

ينقسم الرأي القانوني في معالجة هذه الجرائم إلى اتجاهين:

الاتجاه الأول: يعتقد القانونيين بأن العقوبة يجب أن تتناسب مع تأثير الجريمة، فالعقوبة تكون خفيفة أو في بعض الحالات يكتفي بالتوجيه في الحالات التي تتسم بالتطفل بقصد التسلية والعبث أما في حالات سرقة الأموال أو سرقة المعلومات فإن العقوبة تكون شديدة وقاسية.

الاتجاه الثاني: يعتقد القانونيون المتشددون بأن أي حالة من حالات التجاوز يجب أن يعاقب عليها القانون وبشدة دون النظر إلى تأثيرها ودوافع القائمين بها.

شخصية القائم بجرائم الحاسبات الإلكترونية:

إن اختراق أجهزة الحاسب الالكتروني بنية الإزعاج أو سرقة البيانات أو تشويه المعلومات الموجودة عليه أمر يسبب الأذى للشركات والأفراد.

يصنف القائمين بهذه الجرائم كالآتي:

1. **المتطفلون:** يسمون الهاكرز (Hackers) هم مجموعة من الناس الذين يحاولون التسلل إلى الحاسبات الالكترونية لغرض إثبات مقدرتهم أو لمجرد المزاح ليس لغرض الكسب المادي كهدف أساسي، أغلب القائمين بمثل هذا التطفل هم من فئة الشباب، حيث قام شابان في مرحلة الثانوية بإيقاف الحاسبة الالكترونية في الجامعة عن العمل لمدة يومين عن طريق التحكم عن بعد، بعدها أرسلوا إلى الجامعة رسالة طالبين فيها بنسخة عن برنامج الحاسبة تقدر قيمتها بِـ 500 دولاراً وإلا سيتم

إيقاف الحاسبة عن العمل مرة ثانية، عندما سُئل الشابان عن سبب قيامهما بذلك، أجابا أنه مجرد تحدٍ لما قاله الجميع أنه لا يمكن إنجاز مثل هذا العمل.

2. **محبو المال:** هم مجموعة يحاولون التسلل إلى الحاسبات الالكترونية لغرض سرقة المال أغلبهم من المبرمجين الموهوبين الذين يعرفون كيف يكتبون البرامج بذكاء لمساعدتهم على سرقة المال أو يقومون بالاحتيال بمساعدة الحاسبات لسرقة الأموال من المصارف أو مؤسسات الأعمال، حدث في أحد المصارف أن استخدم رجل بطاقات إيداع مزورة يتم عند استخدامها نقل الأموال من حسابات الزبائن الآخرين إلى حسابه، بدأ زبائن المصرف يشكون بأنه لا يتم تسجيل إبداعاتهم بصورة صحيحة، عند اكتشاف السرقة كان هذا الرجل سرق مبلغ 250 ألف دولار.
3. **المحترفون:** هم مجموعة من الأشخاص الذين يحاولون التسلل إلى الحاسبات الالكترونية لغرض سرقة معلومات قيمة جداً، حساسة وسرية والدوائر الحكومية والعسكرية هي إحدى الجهات الرئيسية التي تحتفظ بملفات سرية مهمة، من الصعوبة في هذا النوع من الجرائم حماية المعلومات إذ أن عملية التسلل إلى الحاسبات الالكترونية لغرض الحصول على المعلومات فقد يسبب الأذى لتلك الدوائر، يعتبر القائمين بهذا النوع من الجرائم من أخطر الفئات.