المحاضرة الخامسة: تابع أنواع الجرائم الالكترونية

ب- جرائم الاعتداء على حرمة الحياة الخاصة عبر الانترنت: حظيت الحياة الخاصة بحماية دستورية وقانونية في مختلف تشريعات الدول المتقدمة ، لما لخصوصية الافراد من أهمية قصوى على كيان الفرد والمجتمع معا.

والحق في الخصوصية هو أحد الحقوق التي تثبت للإنسان، والتي غالبا ما يصعب حصر الجوانب المختلفة لها، والتمييز بحدود واضحة بين ما يعد من الحياة الخاصة للإنسان، وما يعد من الحياة العامة له. (الشوابكة، 2009، صفحة 58)

من المبادئ الأساسية، أن تخزين المعلومات لا يعني أن هذه المعلومات قد انتقلت من الخصوصية إلى العلانية، كما أتن الرضا بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى الكافة.

وبالرغم من أن وسائل الاتصال الحديثة ممثلة بشبكة الانترنت ساعدت على سهولة وسرعة التبادل الالكتروني للبيانات فإن ذلك لا يرنو إلى ترك البيانات الشخصية المعطاة عرضة للمتطفلين الهواة الهاكرز أو حتى المخربين الكراكرز دون رقيب أو عتيد، وذلك لأهمية هذه البيانات بالنسبة لأشخاصها المتعلقة بهم وسريتها، وكذلك لوثوقهم في الجهة التي تطلب منهم معرفة بعض البيانات الاسمية للدخول أو الولوج إلى مواقع معينة. فشبكة الانترنت لا تتوافر فيها السرية الكاملة والأمان لما ينقل عبرها من معلومات أو بيانات، مما يسهل الحصول – من خلالها-على المعلومات والبيانات بطريقة غير مشروعة. (الشوابكة، 2009، صفحة 62)

- موضوع حماية الحياة الخاصة: ان موضوع البيانات الاسمية المتعلقة بالحياة الخاصة ليست المعلومات المختزنة بحد ذاتها، إنما تتمثل في المصالح التي تهددها هذه المعلومات غير الصحيحة أو المشوهة.

وبما ان الانترنت يتمتع ببنية شبكية عالمية، فإنه يمكن الربط بسهولة بين المعلومات الشخصية التي تجمع عن المستخدم ، سواء تم الحصول على هذه البيانات من خلال الاستمارات الالكترونية التي تعبأ من قبل المستخدم أو من خلال استخدام برمجيات خاصة بالتجسس سباي واي تجمع مختصرة عن طريق استخدام الانترنت، متضمنة معلومات

حساسة مثل ارقام بطاقات الائتمان الخاصة، أو تستخدم مثل تلك البيانات لانتحال شخصية صاحب الحق في هذه البيانات واستخدامها بشكل غير مشروع.

وكون الحق في المعلومات يصلح لان يكون محلا للحقوق الشخصية والمالية، فإنه يجب أن تحمى خصوصية الافراد بقوانيين حديثة، وذلك بالتخلي عن حرفية النص الجنائي فيما يتعلق بالحماية الجنائية للحق في الخصوصية وعن العناصر المبهمة المكونة للجريمة، للحفاظ قدر الإمكان على خصوصية المعلومات الخاصة بالافراد من مخاطر الانترنت واستخداماته والتي غدت تقدما للوسائل القامعة للحرية الفردية إذا ما أسيء استخدامها. وهذا المساس بالمعلومات الشخصية للافراد، قد يكون مصدره هواة متطفلون الهاكرز لا يلحقون أي أذى بصاحب البيانات ولا يتسببون عادة بأية أضرار، إنما يكون هدفهم إثبات مقدرتهم على التفوق التقني واختراق حواجز الامن وجدران النار فاير وايل ، أو للتسلية باستخدام هذه المعلومات بإزعاج الآخرين ، أو حتى صاحب المعلومات برسائل البريد الالكتروني غير مرغوب فيه (المتطفل) سبام مايل .

وقد يكون مصدر هذه المساس اشخاص مخربيون الكراكرز يجدون بيئة الانترنت المكان الأنسب لممارسة هواياتهم الاجرامية بخفاء. وذلك بالاعتداء على البيانات الشخصية للآخرين وانتهاكها بشتى الصور. (الشوابكة، 2009، صفحة 64)

ج- جرائم الاستغلال الجنسي للأطفال عبر الانترنت: لا شك ان عالمية نطاق الانترنت أدى إلى تحولها إلى ساحة مفتوحة لممارسة جميع أنواع الاجرام الممكنة والمحتملة، ومن ضمنها الاعمال المخلة بالآداب العامة والأخلاق ، والتي تتباين من بلد لآخر، ولا سيما أن كل مستخدم أو مشترك في شبكة الانترنت يمكنه الحصول على بيانات محظورة في قوانين بلده، وفي ذات الوقت ، ولا تكون محظورة في قوانين مصدر هذه البيانات. (الشوابكة، 2009، صفحة 105)

يندرج تحت هذا البند جرائم ارتياد المواقع الإباحية؟ الشراء منها أو إنشائها وقد اصبح الانتشار الواسع للصور والأفلام الإباحية على شبكة الانترنت بشكل قضية ذات اهتمام عالمي في الوقت الراهن، بسبب الازدياد الهائل في أعداد مستخدمي الانترنت حول العالم. وتختلف المواقع الإباحية عن القوائم البريدية – التي تخصص لتبادل الصور والأفلام الجنسية- في أن المواقع الإباحية غالبا ما يكون الهدف منها الربح المادي حيث يستوجب على متصفح هذه المواقع

دفع مبلغ مقطوع مقابل مشاهدة فيلم لوقت محدد أو دفع اشتراك شهري أو سنوي مقابل الاستفادة من خدمات هذه المواقع ، وإن كانت بعض هذه المواقع تحاول استدراج مرتديها بتقديم خدمة ارسال صور جنسية مجانية يومية على عناوينهم البريدية كما أن تصفح الموقع يتطلب في الغالب الاتصال المباشر بشبكة الانترنت .

أما القوائم البريدية فهي اسهل إنشاء وغالبا مجانية ويقوم أعضائها من المشتركين بتبادل الصور والأفلام على عناوينهم البريدية وربما القوائم البريدية ابعد عن إمكانية المتابعة الأمنية حيث يركز نشاطها على الرسائل البريدية والتي تكون من الصعوبة بمكان منعها عن أعضاء أي مجموعة حتى وان تم الانتباه إلى تلك القائمة لاحقا وتم حجبها فان الحجب يكون قاصرا على المشتركين الجدد والذين لا يتوفر لديهم وسائل تجاوز المرشحات أما الأعضاء السابقين فلا حاجة لهم إلى الدخول إلى موقع القائمة حيث يصل إلى بريدهم ما يريدونه دون أن تستطيع وسائل الحجب التدخل. ويشترك في القوائم الإباحية آلاف الأشخاص التي تصل أي رسالة يرسلها مشترك منهم إلى جميع المشتركين مما يعنى كم هائل من الرسائل الجنسية التي يتبادلها مشتركي القائمة بشكل يومي.

واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة والمزايا الأخرى التي تقدمها حيث "" تتيح الانترنت أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم الجميع بيوتهم ومكاتبهم؟

فهناك على الشبكة طوفان هائل من الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيل في التاريخ. فكل مستخدم للأنترنت معرض للتأثر بما يتم عرضه على الانترنت الذي لا يعرف بأي حدود دولية أو جغرافية فهو يشكل خطرا حقيقيا للأطفال فضلا عن الكبار نتيجة تأثيراته المؤذية وغير المرغوبة . (عياد، 2006، صفحة 76، 77)

واذا كانت هذه الصور الخلاعية موجهة إلى شريحة كبيرة من المستهلكين بصرف النظر عن أعمارهم أو جنسهم ، فإن الحاجة ملحة لحماية الأطفال من أن يكونوا عرضة لهذه المواد الإباحية، أو من أن يكونوا لها مما يشكل أذى ماديا ومعنويا لهؤلاء الأطفال.

وتصوير الأطفال في أوضاع جنسية مخلة قد يقع على أطفال حقيقيين أو يقع على أطفال افتراضيين، وفق ما يعرف بالصور الزائفة ، حيث يتم تركيب صور أطفال على أجساد عارية وفي أوضاع جنسية مخلة ، مما يشكل اعتداء على الطفولة وإعتداء عل الآداب والأخلاق العامة ، وكذلك يعتبر اعتداء على ملكية الشخص لصورته والاستغلال المالي لها.

(الشوابكة، 2009، صفحة 105)

ثانيا: جرائم الاعتداء على الأموال عبر الانترنت : لم تعد المعلوماتية مجرد وسيلة لإلحاق الضرر بالغير، بل إن قدرتها على معالجة الابيانات ونقلها ، سواء في شكل منتجات أو خدمات مستحدثة ، اكسبها قيمة تجارية ذات طابع مالي وهو ما هيأ الفرصة لظهور قيم اقتصادية مستحدثة.

ولم تقتصر أساليب إساءة استخدام الثورة التقنية على الاعتداء على الأشخاص ، بل تعدنها لتطال الذمة المالية للغير، مما يشكل اعتداء على أموالهم المادية ، التي كفلت النصوص التقليدية حمايتها ، وكذلك الأموال المعنوية (اللامادية)وهي مثار جدل تباين التشريعات في حمايتها وفقا للمفهوم المادي والمنقول للأموال...

وتثير جرائم الاعتداء على الأموال الناجمة عن استخدام الحواسيب المرتبطة بشبكة الانترنت تساؤلات عدة حول طبيعة الاعتداءات.

فإذا كان موضوع الاعتداء على الأموال في نطاق المعالجة الآلية للمعلومات ينصب على الحاسب الآلي ذاته وما يرتبط به من اسلاك وما يتصل به من ملحقات، فإنه هنا لا يثير أية صعوبة في تطبيق النصوص الجزائية التقليدية، كون الامر يتعلق بمال مادي منقول وفقا لمفهوم الدارج. أما إذا وقع الاعتداء على ما يتعلق "" بفن الحاسب الآلي"" من برمجيات سوفت واير ونظم ، فإن النصوص التقليدية تأتي قاصرة عن حمايتها لما لهذا المال من طابع خاص غير تقليدي.

وفي نطاق شبكة الانترنت ، يعتبر الحاسب الآلي أداة سلبية لارتكاب الجريمة ضد الفرد ، إذ تستخدم الحواسيب المرتبطة بشبكة الانترنت كوسيلة لتنفيذ الجرائم والاعتداء على أموال الغير والتي اتخذت صور مستحدثة. لذا برزت الدعوى إلى فرض الحماية عبرها. **(الشوابكة، 2009، صفحة 136، 167)**

وبناء على ما سبق وترتيبا عليه ، ارتأينا لعرض نوعية جرائم الاعتداء على الأموال عبر شبكة الانترنت :

أ–سرقة المال المعلوماتي المعنوي:

ان الصورة الاغلبية لسرقة المال المعلوماتي المعنوي –ان امكن الوصف– تأخذ صورة اختلاس البيانات والإفادة منها باستخدام السارق للمعلومات الشخصية– مثل الاسم ، العنوان، الأرقام السرية– الخاصة بالمجنى عليه، والاستخدام

غير المشروع لشخصية المجني عليه ليبدأ بها عمليات السرقة المتخفية عبر الانترنت بحيث تؤدي بالغير إلى تقديم الأموال –الالكترونية أو المادية– –إلى الجاني– عن طريق التحويل البنكي.

*أنماط سرقة المال المعلوماتي المعنوي: اذا كان المال المعلوماتي المخزن في قواعد البيانات والمتبادل عبر خطوط شبكة الانترنت يتمثل في البيانات والمعلومات اللامادية ، فإن تلك البيانات هي هدف الجاني وغايته، فإذا ما اختلست تلم المعلومات بطريقة أو بأخرى فإن ذلك يمثل اعتداء على البيانات وسببا موجبا لقيام وصف السرقة أو الاحتيال أو إساءة الائتمان وذلك حسب طبيعة الاختلاس ونية الجاني.

ويتم اعتراض وجمع وتحليل المعلومات المنقولة عبر شبكة الانترنت باعتراض الرسائل الالكترونية والمعلومات المنقولة بواسطة محطات الالتقاط المنتشرة على الشبكة، ومن ثم سحب نسخة من الجهاز ليتم ايداعها في بنوك عملاقة للمعلومات بعد تصنيفها حسب اللغة التي كتبت بها، وبعد ذلك يتم فحص المحتويات وباستخدام تقنية التقاط للكلمات الحساسة مما يتيح المجال في بناء مرجع الكتروني للكلمات الخطيرة والمثيرة للشبهة، ومن ثم تستخدم هذه المعلومات في مجالات مختلفة إيجابية– كتلك المتعلقة بمكافحة الجريمة– أو سلبية ، وذلك بإساءة استخدام هذه المعلومات المعترضة في ارتكاب الجرائم عبر خطوط الشبكة.

وكذلك قد يقوم الجاني باستخدام واستغلال جهد ووقت الحاسب الآلي في غير الأحوال المصرح بها، ليقوم بتحقيق منفعة شخصية ، أو بغرض التسلية مما يثر التساؤل حول طبيعة استغلال الشخص للحاسب الآلي، ومنه يمكن عرض أنماط سرقة المال المعلوماتي المعنوي في :

– الالتقاط غير المشروع للبيانات : ان الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن ، يتيح للمجرم المعلوماتي ممارسة نشاطاته الاجرامية من اجل تحقيق مكاسب شخصية متباينة ومتعلقة بذات المجرم .بحيث تمكنه من التقاط البيانات المخزنة في قواعد البيانات أو المتبادلة عبر قنوات الانترنت واستخدامها بطرق غير مشروعة.

ويتمكن المجرم المعلوماتي من التقاط البيانات – بعد الدخول غير المشروع إلى النظام أو البقاء فيه– إما عن طريق التجسس المعلوماتي أو عن طريق الاحتيال (الخداع) أو عن طريق تفجير الموقع المستهدف، ونعرض لذلك تباعا:

* أسلوب التجسس المعلوماتي: يتمثل هذا الأسلوب في قيام قراصنة الانترنت باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالمتعاملين على شبكة الانترنت – كالمؤسسات والشركات التجارية – ومن ثم استخدام هذه البيانات والمعلومات في ممارسة الأنشطة الجنائية.

وتتراوح خطورة التجسس بحسب أهمية المعلومات الملتقطة، والتي قد تكون: معلومات سرية تجارية (اقتصادية) أو معلومات عسكرية أو معلومات خاصة ببيانات بطاقة ائتمان أو غير ذلك من المعلومات.

ويتمكن مجرموا الانترنت من التقاط البيانات والمعلومات بصورة غير مشروعة باستخدام أساليب فعالة في قرصنة كلمات المرور، عن طريق التعقب والتسلل للبرامج التي تتجه أليها أكثر أسماء المستخدمين، ومن ثم سرقة كلمات المرور التي تدون في قوائم ملفات كلمات المرور، حيث تقارن البرامج المتعقبة كلمات المرور المشفرة مع قاموس للكلمات العامة، فإذا تقاربت كلمة المرور الملتقطة مع الكلمة في القاموس، فإن المجرم المعلوماتي يحصل على اسم مستخدم جديد وكلمة مرور جديدة كاجراء التحويلات الالكترونية بحساب المجني عليه وادخالها إلى حساب الجناة أو لحساب أشخاص آخرين. (الشوابكة، 2009، صفحة 166، 167)

*أسلوب الخداع : يتمثل هذا الأسلوب في قيام قرصنة الانترنت بإنشاء مواقع وهمية خاصة بهم، مشابهة للمواقع الاصلية للشركات والمؤسسات التجارية المتعاملة بالتسويق عبر الانترنت وغيرها من المواقع سيتس على شبكة الويب .

ويتم من خلال هذه المواقع الوهمية على شبكة الانترنت استقبال جميع المعاملات التجارية والمالية، ومن بينها البيانات والمعلومات الخاصة والسرية– كالبيانات الخاصة ببطاقة الدفع الالكتروني – والرسائل الالكترونية المتعلقة بالموقع الأصلي، حيث يظهر الموقع الوهمي بمظهره.

والحقيقة ان أسلوب الخداع من قبل قراصنة الكمبيوتر للحصول على البيانات والمعلومات اقرب بانطباق وصف الاحتيال عليه، أكثر من أي وصف قانوني آخر، إذ يتم إيهام المجني عليهم بوجود مشروع كاذب (الموقع الوهمي) بغرض الحصول على البيانات و المعلومات واستغلالها بصورة غير مشروعة بغية تحقيق منفعة التحويل الالكتروني من ارصدة المجني عليهم إلى ارصدة الجناة. (الشوابكة، 2009، صفحة 169)

* تقنية تفجير الموقع المستهدف: ويقوم هذا الأسلوب بضخ كميات كبيرة من الرسائل الالكترونية من جهاز الحاسب الآلي للجاني إلى الجهاز المستهدف ، بقصد التأثير على ما يعرف (بالسعة التخزينية) بحيث يشكل

هذا الكم الهائل من الرسائل الالكترونية ضغطا يؤدي في المحصلة إلى تفجير الموقع العامل على الشبكة لتتشتت المعلومات والبيانات المخزنة فيه لتنتقل بعد ذلك إلى الجهاز الخاص بالمجرم أو تمكن هذا الأخير من حرية التجول في الموضع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه الجاني من ارقام ومعلومات وبيانات مملوكة للغير. (الشوابكة، 2009، صفحة 169، 170)

-سرقة منفعة الحاسب الآلي: يقصد بسرقة منفعة الحاسب الآلي استخدامه لأغراض شخصية أو تجارية بدون علم مالكه أو حائزه القانوني وهي تستتبع بالضرورة استخدام وقت الحاسب الآلي أو ورق الآلة من اجل أغراض شخصية مما يخلق طائفة جديدة من الجرائم المعلوماتية تتمثل بسرقة وقت الحاسب الآلي، حيث يتم الولوج إلى أنظمة المعلوماتية لتحقيق أهداف ذاتية.

والصورة الغالبة لحالات سرقة منفعة الحاسب الآلي لا تهدف إلى تحقيق غرض إجرامي – أي بدون ربح أو استفادة- بل قد يلجأ إليها بعض الأشخاص –على سبيل المثال- لتحرير بطاقات مخصصة لأعمال الخير أو لنسخ ألعاب الفيديو لاستعمالهم الشخصي.

وتتم سرقة منفعة الحاسب الآلي، بالاستخدام غير المشروع لأنظمة المعلوماتية لسرقة الخدمات المعلوماتية أو سرقة الوقت وهي واسعة الانتشار في مجال المعلوماتية كاستخدام ارقام حسابات الشركة أو التلاعب ببيانات الحاسب الآلي لمعرفة – على سبيل المثال- الوقت الفعلي لدفع الأجرة، أو لمعرفة زبائن الشركة أو الخدمات التي تقدمها. (الشوابكة، 2009، صفحة 171)

ب-التحويل الالكتروني غير المشروع للأموال: اكتسب التعامل بالأموال في عصر المعلوماتية صفة البيانات الالكترونية المخزنة في ذاكرة الحاسب الآلي، وأدت الثورة الرقمية إلى إمكانية إجراء تحويلات ومبادلات لهذه الأموال من أي مكان العالم. وتكمن خطورة الامر في إمكانية تلاعب الجاني في هذه البيانات المختزنة في ذاكرة الحاسب الآلي أو في برامجه وإجراءات واجراء تحويلات في كل أو بعض أرصدة الغير أو الغير أو فوائدها وادخالها في حسابه.

وغالبا ما يتم ولوج محترفي في شبكات الانترنت إلى بيانات حساب الآخرين من خلال الحصول على كلمة مدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجنى عليه، فإذا ما تم الاستلاء على كلمة المرور وادخالها في أنظمة الحاسب

الآلي فإنها – إذا ما كانت مدرجة وملائمة –سوف تنسجم وتقترن بالملف ومن ثم تسمح للمستخدم بالولوج إلى النظام المعلوماتي، وبعكس ذلك فإن المستخدم يمنع من الولوج.

ويحصل مجرموا المعلوماتية على كلمات المرور الخاصة بالغير إما بالغير إما بالتقاطها أثناء تواجدهم في النظام المعلوماتي، أو من خلال بث برامج تتعقب الأنظمة المعلوماتية التي يتجه إليها أكثر المستخدمين وسرقة كلمات المرور الخاصة بهم، والحصول على البيانات الخاصة بالجاني واستخدام المفيد منها في اجراء التحويلات المالية الالكترونية من حساب المجني عليه وإدخالها في ارصدتهم وفي النظام المعلوماتي الخاص بهم.

والحصول على المعلومات والبيانات المتعلقة بالمستخدمين قد يتم من قبل العاملين على ادخال البيانات في ذاكرة الحاسوب أو من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات، وذلك بفعل الالتقاط أو بالتحايل أثناء عملية تبادل البيانات من قبل المخادعين الخارجين ، ويكون ذلك باستخدام طريقتين:

* الطريقة الأولى : يطلق عليها اسم بروكو وتكمن آلية عملها في استقطاع بعض السنتيمات من الايداعات الدورية ، وقد قام بالفعل أحد المستخدمين في شركة تأمين ببرمجة الحاسوب لاستقطاع الكسور الخاصة بالسنتيمات في كل عمليات الشركة وتحويلها إلى حسابه السري.

* الطريقة فتعرف باسم سلامي وتكمن في تقنية استقطاع مبالغ مالية صغيرة من حسابات مالية ضخمة ، وتحويلها آليا عبر الفضاء الالكتروني إلى حساب الجاني الشخصي ليستخدمها فيما بعد .

وقد قام بالفعل مبرمج في أحد البنوك منوط به اعداد البرامج المتعلقة بإعادة المال الزائد من مالكي بطاقات الفيزا باستخدام طريقة سلامي باستقطاع 25 سنت من حاملي البطاقة وبطريقة عشوائية وادخالها في حساب الفيزا الخاص به، ولم يكتشف هذا المستخدم إلا بعد اكتشاف تغير نمط حياته ، وقد وجه إليه تهمة الاحتيال على البنك.

(الشوابكة، 2009، صفحة 178، 179)

ويتم الاحتيال بطرق منها:

* الاحتيال (النصب) في نطاق المعلوماتية: يرى البعض أن الاحتيال المعلوماتي هو كل سلوك احتيالي يرتبط بعملية التحسيب الالكتروني بهدف كسب فائدة أو مصلحة مالية.

والحقيقة أن هذا التعريف يشمل كل ضروب غش الحاسوب، والمتمثلة بالاعتداء على المعطيات المخزنة في النظام المعلوماتي والمتبادلة عبر قنوات النظام ، بما تمثلها من أموال وخدمات بغرض الحصول على منفعة مادية.

(الشوابكة، 2009، صفحة 180)

ان الطرق الاحتيالية المستخدمة في الحصول على الأموال المعلوماتية ممثلة بالمعلومات تتم في حالتين:

الحالة الأولى: وتتمثل في الحصول على المعلومات في حالة نقلها عبر شبكة الانترنت بوسائل احتيالية من شأنها الحصول على المعلومة من جراء استخدامها. ولعل استخدام البريد الالكتروني من أكثر الطرق استخداما من قبل المحتالين للحصول على مكاسب مالية متنوعة، ومن أشهر هذه الطرق ما يعرف باسم الرسائل المتسلسلة أو طرقة الهرم.

ومن الأمثلة على الطريقة الأولى ارسال بريد الكتروني إلى الغير يتضمن أسماء عدد قليل من الأشخاص واحدا تلو الآخر، وعلى الشخص الوارد اسمه في اعلى القائمة، وتتمثل الخطوة التالية في أن يرسل المجنى عليه الرسالة المتلقية عبر البريد الالكتروني أو العادي إلى عدد آخر من الأشخاص الذين يتعين عليهم إتباع الخطوة ذاتها، وهكذا عندما يصل اسم المجنى عليه إلى أعلى القائمة – بعد فترة معينة– ستتدفق عليه الأموال.

الحالة الثانية: وتتمثل في اختلاس الأموال بمداولات معلوماتية، وتتم من خلال ادخال معلومات أو تعديل معلومات أو تعطيلها أو انشاء نظام معلوماتي جديد.

ويرى البعض أن ادخال معلومات وهمية في شبكة الكمبيوتر وانتقالها تبعا لذلك لشبكة الانترنت، باستعمال اسم كاذب أو صفة غير صحيحة والحصول على أموال نتيجة هذا التلاعب تقوم به جريمة النصب.

وقد أصبحت مواقع الانترنت ممتلئة بالمواقع الوهمية المشابهة للمواقع الحقيقية، والتي يقوم الجناة بوضعها على الشبكة بعد أن يتم حجب المواقع الاصلية، وذلك بغية الحصول على الأموال من جراء التعامل مع هذه المواقع.

فالمتاجر الافتراضية والبنوك الافتراضية هي ما تتيح لمخترقي شبكات الانترنت من استغلال المواقع الوهمية وخداع مستخدمي الشبكة عن طريق التلاعب بالبيانات من ادخال أو تعديل أو تعطيل أو حتى انشاء نظام معلوماتي جديد ،ولإذا كانت عملية الخداع، وهي محور جريمة الاحتيال، تتطلب من المجنى عليه عقلا يفكر فيما يعرض عليه من أمور

قد تفوت عليه وجه الحقيقة أو الصواب وتقوده إلى الوقوع في الغلط ، ويتصرف في المال تبعا لذلك. (الشوابكة، 2009، صفحة 182، 183، 184)

* الاحتيال باستخدام بطاقات الدفع الالكتروني عبر الانترنت :

يعتمد نظام بطاقة الدفع الالكتروني على عمليات التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر بالبنك الذي يوجد به حسابه، وذلك من خلال شبكة التسوية الالكترونية للهيئات الدولية (هيئة الفيزا كارد – هيئة الماستر كارد) .

وتعطى بطاقة الدفع الالكتروني الحق للعميل في الحصول على السلع والخدمات عبر شبكة الانترنت عن طريق تصريح كتابي أو تلفوني بخصم القيمة على حساب بطاقة الدفع الالكتروني الخاصة به، وهو ما يطلق عليه مايل فون اوردرفيكفي لاجراء العملية أن يدخل العميل إلى موقع التاجر على الشبكة المعلوماتية، ثم يختار السلع المراد شرائها، حيث تتم عمليات التعاقد بعد ملء النموذج الالكتروني- الذي يظهر على شاشة الحاسب – بينات بطاقة الائتمان الخاصة بالمشتري وعنوانه، ثم يقوم بعد ذلك التاجر بخصم قيمة السلع من بطاقة الدفع الالكتروني وارسالها إلى عنوان المشتري.

وقد اتاحت الثورة الرقمية لقراصنة المعلوماتية إمكانية تخليق ارقام البطاقات الائتمانية بواسطة برامج تشغيل، تتيح إمكانية تخليق ارقام بطاقات بنك معين من خلال تزويد الحاسب بالرقم الخاص بالبنك مصدر البطاقة، علاوة على إمكانية التقاط هذه الأرقام عبر قنوات الانترنت المفتوحة واستخدامها بطريقة غير مشروعة في عمليات التسوق عبر الشبكة، بحيث يتم خصم قيمة السلع من العملاء الشرعيين لهذه البطاقات. (الشوابكة، 2009، صفحة 193، 194)

* جريمة إساءة الائتمان في نطاق المعلوماتية: موضوع جريمة إساءة الائتمان هو مال سلمه المجني عليه على سبيل الأمانة بمقتضى عقد من عقود الأمانة المحددة حصرا بنص القانون، لكن الجاني خان ثقة المجني عليه واستولى على المال، أو قام بتبديده، أو استعمله على وجه غير متفق عليه.

ولذلك فإن محل جريمة الائتمان ينطوي على مال منقول مملوك لغير الجاني، بالإضافة إلى كون هذا المال قد سلم إلى الجاني على سبيل الأمانة تسليما ناقلا للحيازة الناقصة بناء على عقد من عقود الأمانة الواردة حصرا في القانون.

ونعرض فيما يلي لمحل جريمة إساءة الائتمان :

- يتطلب المشرع الجزائي لقيام الجريمة أن يقع الاعتداء على مال ذي طبيعة مادية ملموسة فضلا عن كونه منقولا ومملوكا للغير.

وإذا كانت الأموال المعلوماتية كالبيانات والمعلومات والبرامج تتمتع بطبيعة ذاتية غير ملموسة(معنوية) فإن النصوص الجزائية تأتي قاصرة عن حماية الأموال المعلوماتية اللامادية من الاستلاء عليها.

- ان يكون المال منقولا: يثير مفهوم المال المنقول صعوبات جمة في نطاق المعلوماتية بما يتعلق بالبيانات والبرامج والمعلومات فيما إذا امكن اعتبارها من المنقولات، وبالتالي تصلح لانطباق النصوص المتعلقة بإساءة الائتمان عليها، أم أنها لا تعد كذلك وبالتالي لا تصلح محلا للجريمة. (الشوابكة، 2009، صفحة 204، 205)

ج- جريمة إتلاف نظام المعلوماتية عبر الانترنت: تقع جريمة الاتلاف في نطاق المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج

Logicial

والبيانات

Data

المخزنة والمتبادلة بين الحواسيب وشبكاته- الداخلية(المحلية) أو العالمية(الانترنت)- ويكون ذلك بطريق التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو إتلاف المعلومات المخزنة بالحواسيب والمتبادلة عبر الشبكة العالمية

Global Net

بمحوها أو تعديلها أو تغيير نتائجها أو بطريق التشويش على النظام المعلوماتي، بما يؤدي إلى إعاقة سير عمل النظام الآلي بصورة المختلفة.

ويكون الاتلاف العمدي للبرامج والبيانات بمحوها كلية أو تدميرها إلكترونيا، أو تشويهها على نحو إتلاف بما يجعلها غير صالحة للاستعمال.

وتأخذ جريمة الاتلاف في نطاق المعلوماتية إما صورة الاتلاف المادي، وذلك بالاعتداء على المكونات المادية للحاسب الآلي

Hard Ware

من أجهزة ودعامات، وشرائط، وأقراص ممغنطة (وما تحتوي من معلومات) وشاشات، وكوابل ...الخ ، وهنا لا تثار أية عقبة قانونية في تطبيق النصوص التقليدية الخاصة بجريمة الاتلاف على مثل هذه الاعتداءات إذ ينصب الاعتداء في هذا الاطار على مال مادي مملوك للغير.

وكذلك يتخذ الاتلاف صورة الاعتداء على البرامج أو البيانات والمعلومات المخزنة في قواعد الحاسب الآلي والمتبادلة بين الحواسيب عبر قنوات الاتصال في شبكة الانترنت سواء تم ذلك بمحوها أو تعديلها ، أو تغيير نتائجها.

(الشوابكة، 2009، صفحة 216، 217)

وهذا صور الاعتداء على سير نظام المعالجة الآلية للبيانات (إتلاف المال المعلوماتي المعنوي)

* الاعتداء على البيانات داخل نظام المعالجة الآلية للبيانات : ان الاعتداء على البيانات والبرامج داخل النظام المعلوماتي بإتلافها يتخذ إحدى صورتين:

الصورة الأولى: أن يتم محو البيانات والمعلومات كلية وتدميرها إلكترونيا

الصورة الثانية: أن يتم تشويه المعلومة أو البرامج عن طريق تعديل البيانات أو تعديل طرق معالجتها أو وسائل انتقالها.

وتتنوع أساليب الاتلاف التي قد تكون نتيجة فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن أو قد تكون نتيجة استخدام الطرق التقنية والفنية كاستخدام فيروسات الحاسب الآلي.

صور الاعتداء على البيانات والبرامج ذاخل نظام المعالجة الآلية للبيانات: ان اتلاف البيانات والأموال اللامادية سواء بمحوها وتدميرها الكترونيا أو بتشويهها أو تعديل طرق معالجتها ووسائل انتقالها يثير تكييفها جنائيا اختلاف ملموسا بحسب الغاية التي هدف إليها المجرم المعلوماتي من واقعة الاتلاف. (الشوابكة، 2009، صفحة 229، 230)

وتنوع صور اتلاف البيانات والبرامج بحسب ما إذا اتخذت صورة التدخل في المعطيات أو إذا اتخذت صورة التدخل في الكيان المنطقي:

أولا- التدخل في المعطيات: ان المعطيات أو البيانات تمثل المعلومات المدخلة في النظام الآلي للحاسب بغرض معالجتها ، ويكون التدخل فيها إما بإدخال معلومات وهمية في النظام المعلوماتي أو بتزوير المعطيات الموجودة.

- ادخال معلومات وهمية: ويقصد بذلك إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة من قبل وقد يتم إدخال هذه البيانات بقصد التشويش على صفحة البيانات القائمة.

- ادخال معلومات مزورة: وتعني تزوير المستندات والبيانات المختزنة على الكمبيوتر، وتزوير المعلومات بحيث يتم وضع معلومات بديلة للمعلومات الحقيقية، وتزييف المخرجات، وتستهدف جريمة تزوير المستندات والبيانات بشكل واسع البيانات الممثلة للمستحقات المالية والايداعات المصرفية وحسابات ونتائج الميزانيات وأوامر الدفع وقوائم المبيعات وأنظمة التحويل الالكترونية للأموال والودائع المصرفية.

ويتم التزوير في هذه الحالة إما عن طريق الحالة عن طريق استبدال المعطيات أو عن طريق المحو المنتقى للمعطيات، وإذا كان التلاعب في المعطيات يؤدي إلى قيام جريمة التزوير- بالإضافة للإتلاف- . (الشوابكة، 2009، صفحة 231، 232)

ثانيا- التدخل في الكيان المنطقي: يمثل الكيان المنطقي مجموعة البرامج المخصصة للقيام بالمعالجة عن طريق الحاسب الآلي، ويكون ذلك إما بتعديل البرنامج أو بخلق برنامج جديد(وهمي) . (الشوابكة، 2009، صفحة 235)

الطرق الفنية لإتلاف المال المعلوماتي المعنوي:

تتنوع الطرق الفنية والتقنية المستخدمة لإتلاف البيانات والبرامج بدءا من فيروسات الحاسب الآلي

Programmes Virus

ومرورا ببرامج الدودة

Worm Software

وانتهاء بالقنبلة المنطقية أو الزمنية

Logic bomb

ويتفق الفقهاء في كل من إنجلترا والولايات المتحدة على أن المشكلات القانونية التي تنشأ عن جميع الفيروسات تكاد تكون واحدة فلا وجه للتفرقة بين الفيروس والدودة وحصان طروادة. فهي نفس الفيروسات ويترتب عليها نفس المشكلات القانونية.

*** فيروسات الحاسب الآلي: وهي عبارة عن برامج خبيثة

Amalicious program

تتسلل إلى البرمجيات بحيث تدخل إليها وتنسخ نفسها على برامج أخرى في الحاسب الآلي.

وتستخدم الفيروسات في أحد غرضين: حمائي أو تخريبي.

الغرض الحمائي: ويكون ذلك لحماية البيانات والبرامج من خطر النسخ غير المشروع (المرخص به)، إذ ينشط الفيروس بمجرد النسخ ويدمر نظام الحاسب الذي يعمل عليه.

الغرض التخريبي: ويكون ذلك بهدف الدعاية أو الابتزاز، حيث يرمي واضع الفيروس للتخريب بهدف التخريب ذاته أو بهدف الحصول على منافع شخصية.

وتكون هذه الفيروسات مرافقة ومخزنة على البرامج التطبيقية وبرامج التشغيل وتنشط في حالة نسخ البرامج من جهاز لآخر.

أو عن طريق نقل المعلومات المباشر من شبكة لأخرى وخاصة عبر الانترنت، بحيث تكون مختبئة داخل رسائل البريد الالكتروني، والوثائق والمعلومات التجارية والمالية عبر الشبكة، مما يشكل اعتداء على نظمها.

وتنتقل هذه الفيروسات في حالة نسخ البرامج الحاملة لها، أو بتحميل البيانات والمعلومات بحيث تنسخ نفسها على

Zerosector

وهو المسار الأول الموجود على وحدة التخزين الرئيسية الصلبة داخل الجهاز

HD

وتقوم بالسيطرة على نظام التشغيل حتى تتمكن من تعطيل الجهاز كلية، وقد تنسخ نفسها تكرارا بحيث لا يمكن تنزيلها على الذاكرة العشوائية

RAM

مما يؤدي إلى عدم إمكانية تشغيل البرامج.

وتقسم أنواع فيروسات الحاسب الآلي من حيث تكوينها وأهدافها إلى:

– فيروس عام العدوى: وهو يستهدف نوعا معينا من النظم لمهاجمته ويتميز بالبطء في الانتشار، علاوة على صعوبة اكتشافه.

– فيروس عام الهدف: ويتميز بسهولة إعداده واتساع مدى تدميره وتندرج تحته الغالبية العظمى من الفيروسات.

– فيروس محدد الهدف: ويقوم بتغيير الهدف من عمل البرامج دون تعطيلها، وهو يحتاج إلى مهارة عالية بالتطبيق المستهدف، كأن يحدث تلاعبا ماليا أو تعديل معين في تطبيق عسكري كفيروس حصان طراودة

Trojan Horse

والتي سهلت مواقع الانترنت انتشاره.

*** برامج الدودة

Worm Software

أطلق في عام 1988 عبر شبكة الانترنت في الولايات المتحدة برنامج يعرف بالدودة والذي سبب لأجهزة الحاسب الآلي – خلال الشبكة– انهيار في قيادة وتوجيه الجامعات، والمعدات العسكرية ومنشآت الأبحاث الطبية.

ويقوم برنامج الدودة باستغلال أية فجوة في نظم التشغيل كي ينتقل من حاسب إلى آخر، أو من شبكة إلى أخرى عبر الوصلات التي تربط بينهما، وتتكاثر "أثناء عملية انتقالها بإنتاج نسخ منها، وتهدف هذه البرامج إلى العمل على تقليل

خفض كفاءة الشبكة، أو إلى التخريب الفعلي للملفات والبرامج ونظم التشغيل، وذلك بإشغال أي حيز ممكن من سعة الشبكة.

وقد أطلقت دودة الانترنت عن طريق طالب امريكي يدعى روبرت موريس وهو طالب في قسم علوم الكمبيوتر بجامعة كورنيل بولاية نيويورك، تعمد بث برنامج دودة الانترنت لكي يثبت عدم ملائمة أساليب وسائل الأمان في شبكات الكمبيوتر، ولكنه تسبب في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة، بالإضافة إلى إعاقة طريق ومسلك الشبكات، بالإضافة إلى خسائر مالية كبيرة في مواجهة دودة الانترنت.

وقد أدين موريس بانتهاك قانون الاحتيال وإساءة استخدام الكمبيوتر، وحكم عليه بالحبس لمدة ثلاث سنوات، وبالعمل أربعمائة ساعة في الخدمة الاجتماعية وغرامة قدرها (10.500) دولار، بالإضافة إلى تكاليف المراقبة.

(الشوابكة، 2009، صفحة 238، 239، 240)

*** القنبلة المعلوماتية: وهي بدورها تنقسم إلى قسمين:

– القنبلة المنطقية: وهي عبارة عن برامج صغيرة يتم إدخالها بطرق غير مشروعة ومخفية مع برامج أخرى، وتهدف إلى تدمير وتغيير برامج ومعلومات النظام في لحظة محددة أو في فترة زمنية منتظمة، بحيث تعمل على مبدأ التوقيت فتحدث تدميرا وتغيرا في المعلومات والبرامج عند إنجاز أمر معين في الحاسب الآلي، أو برنامج معين.

ومن الأمثلة على ذلك زرع القنبلة المنطقية لتعمل لدى سجل موظف بحيث تنفجر لتنمو سجلات الموظفين الموجودة أصلا في المنشأة، ففي الولايات المتحدة الامريكية في ولاية لوس انجلس تمكن أحد العاملين بإدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها، مما أدى إلى تخريب هذه النظام عدة مرات.

– القنبلة الزمنية: وسميت كذلك لقيامها بالعمل التخريب في وقت يحدد سلفا، فعلى سبيل المثال:

يمكن للمخرب كتابة برنامج وظيفته مسح الكشوفات التي تحمل أسماء الموظفين وبياناتهم اللازمة لدفع وارباك أعمال الشركة وإساءة سمعتها، والقنبلة الزمنية على نقيض من المنطقية تثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة والوقت اللازم.

ومن الأمثلة الواقعية، قيام محاسب خبير في نظم المعلومات، بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة وذلك بدافع الانتقام من المنشأة التي يعمل بها لفصله منها، حيث انفجرت بعد مضي ستة أشهر من رحيله عن المنشأة، وترتب على ذلك أتلاف كل البيانات المتعلقة بها.

ويثار بشأن الاتلاف الذي يقع على نظم شبكة الانترنت ويضر بالمستخدمين مسألة مسؤولية الشبكة، التي تنحصر في توفير اتصال أمثل للمستخدم المتعاقد معها.

وإذا كان الاتصال الأمثل يقصد به الاتصال الميسور والمستمر والمتاح في كل الأوقات، فإن مضمون هذا الاتصال أو فحواه والاضرار التي تترتب عليه ليست من مسؤولية الشبكة، إنما مسؤولية مرسل البرنامج المصاب بالفيروس. وتسأل الشبكة عن مراقبة الاتصال ومضمونه، إذا كلفت رسميا بذلك من قبل السلطات المختصة بتعقب جرائم المعلوماتية، وإلا أصبحت مسؤولة عن جريمة الاعتداء على الحق في الخصوصية. (الشوابكة، 2009، صفحة 240، 241، 242)