جريمة الإتلاف المعلوماتي

د. أسامة بن غانم العبيدي
أستاذ القانون المشارك
معهد الإدارة العامة – الرياض

المستخلص:

مع التقدم السريع الذي يشهده العالم في استخدام الحاسب الآلي والإنترنت ظهرت العديد من السلبيات التي تطول المجتمعات كافة . ومن أهم تلك السلبيات ظهور أنواع جديدة من الجرائم ، حيث أصبح الجاني يستطيع ارتكاب جرائمه باستخدام هذه التقنيات الحديثة .

ويتناول هذا البحث جريمة إتلاف البيانات والمعلومات التي تعد من الجرائم الهامة والتي يترتب على ارتكابها خسائر مادية جسيمة تؤثر سلباً في الاقتصاد والأمن العالمي .

وقد بين الباحث في المبحث الأول ماهية جريمة الإتلاف المعلوماتي وأركانها ووسائل ارتكابها ، كما أوضح في المبحث الثاني صور جريمة الإتلاف المعلوماتي، وفي المبحث الثالث موقف التشريعات الوطنية من جريمة الإتلاف المعلوماتي .

الكلمات المفتاحية :

المعلومات، الجرائم الإلكترونية، القانون ، الإتلاف المعلوماتي

المقدمة :

شهد عصرنا هذا تقدماً كبيراً في تقنية الاتصالات والمعلومات وخاصة مع تطور الحاسبات الآلية وشبكة الإنترنت ، وصاحَب هذا التطور الهائل والمتسارع في تقنية الحاسبات الآلية وشبكة الإنترنت تطور مماثل في أساليب وصور ارتكاب الجرائم بواسطة الحاسب الآلي وشبكة الإنترنت .

ومن هذه الجرائم جريمة الإتلاف المعلوماتي والتي تؤدي إلى خسائر كبيرة تؤثر سلباً في الاقتصاد والأمن العالمي ، مما يستدعي من دول العالم كافة مكافحتها ، وتقتضي أيضاً تحديث النصوص القانونية والتشريعات لمكافحة هذه الجريمة .

ويناقش هذا البحث جريمة الإتلاف المعلوماتي وموقف التشريعات المقارنة من هذه الجريمة .

الدراسات السابقة :

لم تركز الدراسات السابقة التي تناولت جرائم الحاسب الآلي والإنترنت بشكل كبير على جريمة الإتلاف المعلوماتي ، وإنما تطرقت إلى هذه الجريمة بشكل موجز ومختصر ، وقد ذكرنا في قائمة المراجع لهذا البحث العديد من المراجع ذات العلاقة التي يمكن الرجوع إليها في مجال هذه الجريمة .

هدف البحث :

يهدف هذا البحث إلى دراسة موضوع جريمة الإتلاف المعلوماتي وموقف القوانين والتشريعات المقارنة من هذه الجريمة بغية الحد من ارتكاب هذه الجريمة ومعاقبة مرتكبيها .

منهج البحث :

يعتمد هذا البحث على منهج الدراسة التحليلية للنصوص القانونية والأنظمة المقارنة مع الاستناد إلى المراجع العلمية القانونية ذات العلاقة .

خطة البحث :

سوف يقسم هذا البحث إلى :

المبحث الأول : ماهية جريمة الإتلاف المعلوماتي وأركانها ووسائل ارتكابها .

المبحث الثاني : صور جريمة الإتلاف المعلوماتي .

المبحث الثالث : موقف التشريعات الوطنية من جريمة الإتلاف المعلوماتي .

وسوف نستعرض النتائج والتوصيات والخاتمة في نهاية البحث .

المبحث الأول – ماهية جريمة الإتلاف وأركانها ووسائل إتلاف المال المعلوماتي

الإتلاف هو تخريب الشيء موضوع الجريمة ، وذلك بإتلافه أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله ، ولا نجد أية مشكلة في تطبيق الإحكام المتعلقة بجريمة الإتلاف في حالة إتلاف العناصر المادية لنظام المعالجة الآلية للمعلومات كشاشات العرض (Monitors) والأسطوانات والأشرطة والأقراص المغنطة ومعدات الإدخال والإخراج . ذلك أن جميع النصوص القانونية التي تتناول بيان أحكام هذه الجريمة ، تجرم إتلاف المنقولات . وتتنوع وسائل إتلاف هذه العناصر المادية ، سواء من خلال إحداث تغييرات في قوة التيار الكهربائي ، أو بواسطة إحداث حريق أو استعمال قوى مغناطيسية وغير ذلك من الوسائل [1].

وقد تناول المشرع المصري هذه الجريمة في المادة (361) من قانون العقوبات بالقانون رقم (97) لعام 1992م والتي تنص على أنه " كل من خرب أو أتلف عمداً أموالاً ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تتجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين .

فإذا ترتب على الفعل ضرر مالي قيمته خمسون جنيهاً أو أكثر كانت عقوبة الحبس مدة لا تتجاوز سنتين وغرامة لا تتجاوز خمسمائة جنية أو بإحدى هاتين العقوبتين .

وتكون العقوبة الحبس مدة لا تزيد على خمس سنوات وغرامة لا تقل عن مائة جنيه ولا تتجاوز ألف جنيه إذا نشأ عن الفعل تعطيل أو توقف أعمال مصلحة ذات منفعة عامة أو إذا ترتب عليه جعل حياة الناس أو صحتهم أو أمنهم في خطر. ويضاعف الحد الأقصى للعقوبة المقررة لهذه الجريمة إذا ارتكبت تنفيذاً لغرض إرهابي " .

ويتبين لنا أن المشرع المصري لم يقم بوضع تعريف لهذه الجريمة وإنما اكتفى بذكر الصور التي يمكن أن يتخذها الركن المادي المكون لها . الأمر الذي حدا بالفقه للقيام بتعريفه .

والإتلاف لا يخرج عن كونه فناء الشيء أو جعله بحالة غير الحالة التي هو عليها بحيث لا يمكن الاستفادة منه وفقاً للغرض الذي وجد من أجله ، مما يعني أن جوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي وجد أو أعد من أجله . أو هو التأثير على مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الانتقاص من كفاءته لأوجه الاستعمال المعد لها [2].

([1]) ويجدر بالذكر أن هناك بواعث متعددة تدفع الأشخاص لإتلاف المكونات المادية لأنظمة المعالجة الآلية للمعلومات ، ومن هذه البواعث رغبة الموظف المفصول في الانتقام من رئيسه أو رب عمله . وهناك حالات تقوم بها جماعة إرهابية بتدمير حاسبات آلية كما حصل في إيطاليا وفرنسا حيث قامت إحدى الجماعات الإرهابية بتدمير وإتلاف عدد كبير من الحاسبات الآلية في مركز للحاسبات الآلية ، وقدرت الخسائر في إيطاليا ما يعادل عشرة ملايين دولار أمريكي ، وهي إجمالي الخسائر الناتجة عن الاعتداءات على عشر مراكز متفرقة منذ عام 1976م وحتى 1978م . وفي فرنسا فقد قامت جماعة إرهابية أطلقت على نفسها اسم (كلودو) (Clodo) بإتلاف عدد كبير من أجهزة الحاسبات الآلية في عدد من المؤسسات في عامي 1980 و 1981م ، وقد قدرت الخسائر المترتبة عن كل هجوم بنحو مليون ونصف مليون فرنك فرنسي . كما قام عدد من المتظاهرين ضد حرب فيتنام في الولايات المتحدة بتدمير عدد كبير من أجهزة الحاسب الآلي .

انظر نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، الطبعة الأولى ، بيروت، 2005م ، ص 182 وما بعدها .

انظر أيضاً أسامة بن غانم العبيدي ، جرائم الحاسب الآلي والإنترنت : الصعوبات التي تعترض المكافحة، دورية الإدارة العامة ، معهد الإدارة العامة ، المجلد الثامن والأربعون ، العدد الأول ، يناير 2008م . ص 87 وما بعدها .

([2]) محمود مصطفى ، شرح قانون العقوبات ، القسم الخاص ، الطبعة الثامنة ، دار النهضة العربية ، القاهرة ، 1984 ، ص 645 .

أما المشرع الأردني فقد نص في المادة (445) من قانون العقوبات الأردني على أن " كل من ألحق باختياره ضرراً بمال الغير المنقول ، يعاقب بناء على شكوى المتضرر بالحبس مدة لا تتجاوز سنة أو بغرامة لا تتجاوز خمسين ديناراً أو بكلتا العقوبتين " .

وبناء على ما سبق فإن الإتلاف لا يتحقق فقط في التأثير على مادة الشيء، وإنما يتحقق أيضاً في حالة الانتقاص من القيمة الاقتصادية للشيء ، أي أنه إذا لم يترتب على فعل الشخص التأثير على مادة الشيء إنما استمرت مادة الشيء باقية كما كانت عليه قبل ذلك ، متكاملة من حيث الحجم والوزن والتماسك ، ولكن ما أصابها من انتقاص نال من قيمتها ، أي أن قيمتها قد زالت وانتقصت فإن الفعل يتعين أن يعتبر إتلافاً على الرغم من أن مادة الشيء لا زالت متكاملة ، مما يعني أن العبرة في تحقق الإتلاف هو ليس التعرض لمادة الشيء ، إنما العبرة بمدى مساس الفعل بقيمته المادية ، فالفعل الذي يؤدي إلى فقدان الشيء قيمته المادية أو الانتقاص منها فإنه يحقق التعدي الذي يعاقب عليه القانون على أساس أنه قد ذهب بأهمية الشيء بالنسبة لمالكه [3]. مما يفيد بأن محل الحماية الحقيقي هو قيمة الشيء وما حمايته من الناحية المادية إلا وسيلة لحماية قيمته ، كون الشيء يفقد قيمته أيضاً بفناء مادته إما بشكل كلي أو جزئي [4].

ونلاحظ مما سبق أيضاً انطباق نص المادة (361) من قانون العقوبات المصري مع نص المادة (445) من قانون العقوبات الأردني ، على إتلاف المال المعلوماتي المادي ، وإن كانت في بعض الأحيان تثار مسألة إتلاف بعض أدوات الحاسب الآلي وشبكات الحاسب الآلي مما يؤثر في برامجه وبياناته وكذلك على سير عمل النظام المعلوماتي بشكل عام ، ونرى أن هذا النمط من الأفعال يخرج عن إطار الجرائم المعلوماتية على اعتبار أن الجرائم المعلوماتية إنما تقوم بالأعمال التي تشكل اعتداء على المعلومات المبرمجة ونظم معالجتها ، وإنما يكون ذلك عن طريق استخدام وسائل تقنية مرتبطة ببرامج معلومات ، وبالتالي لا نرى الحاجة إلى وضع نصوص قانونية خاصة بإتلاف المكونات المادية لنظم معالجة المعلومات ، حيث يمكن تطبيق النصوص القانونية التقليدية بشأنها ، ومع ذلك فإن قانون العقوبات في ولاية كاليفورنيا في الولايات المتحدة الأمريكية في القسم (502) منه جرم إتلاف وتخريب أنظمة المعالجة الآلية للمعلومات بمكوناتها المادية والمعنوية [5].

وقد عالج المشرع الإماراتي هذه المسألة إذ نص في المادة (424) من قانون العقوبات بأنه "يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تتجاوز عشرة آلاف درهم أو بإحدى هاتين العقوبتين كل من هدم أو أتلف مالاً مملوكاً للغير ثابتاً كان أو منقولاً جعله غير صالح للاستعمال أو عطله بأية طريقة .

وتكون العقوبة الحبس إذا نشأ عن الجريمة تعطيل مرفق عام أو منشأة ذات نفع عام أو إذا ترتب عليها جعل حياة الناس أو أمنهم أو صحتهم في خطر .

([3]) محمود نجيب حسني ، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية ، القاهرة ، 1986م ، ص 21 .

([4]) محمد حماد مرهج الهيتي ، جرائم الحاسوب ، دار المناهج للنشر والتوزيع ، الطبعة الأولى ، عمان، 2006م ، ص 197 وما بعدها .

([5]) أسامة بن غانم العبيدي ، جرائم الحاسب الآلي والإنترنت ، الصعوبات التي تعترض المكافحة ، مرجع سابق ، ص 87 . انظر أيضاً نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ، مرجع سابق ، ص 188 وما بعدها . انظر أيضاً سليمان أحمد فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية ، دار النهضة العربية ، القاهرة ، 2007م ، ص 93 .

وتكون العقوبة السجن مدة لا تزيد على خمس سنوات إذا وقعت الجريمة من عصابة مؤلفة من ثلاثة أشخاص على الأقل .

ويتبين لنا من النص السابق أن المشرع الإماراتي لم يعرِف جريمة الإتلاف وإنما اكتفى بذكر صور تحقيق الجريمة وركنها المادي . وقد تناول المشرع الأردني مسألة الإتلاف المادي لمنشآت الاتصالات وما تحتوي عليها من أجهزة مادية بشكل عام في المادة (72) من قانون الاتصالات رقم (13) لعام 1995م وذلك بالنص على أن :

أ- كل من أقدم قصداً على تخريب منشآت الاتصالات أو ألحق بها ضرراً عن قصد يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل عن 200 دينار ولا تزيد على 5000 دينار أو بكلتا العقوبتين ، وتضاعف العقوبة إذا تسبب فعله بتعطيل حركة الاتصالات

ب - كل من تسبب إهمالاً في تخريب منشآت الاتصالات أو إلحاق الضرر بها ، يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على 100 دينار أو بكلتا العقوبتين " .

ويلاحظ من النص السابق أن المشرع الأردني كفل حماية منشآت الاتصالات ومن ضمنها منشآت الإنترنت من الاعتداء بإتلافها أو إلحاق الضرر بها ، إضافة إلى حماية المشرع للأموال المعنوية من الإتلاف في المواد من (76) إلى (80) من قانون الاتصالات الأردني لعام 1995م . أما المنظم السعودي فقد نص في الفقرة (11) من المادة (37) من نظام الاتصالات السعودي لعام 1422هـ على أنه " يعد مرتكباً لمخالفة كل مشغل أو شخص طبيعي ، أو معنوي يقوم بأحد الأعمال الآتية :

إساءة استخدام خدمات الاتصالات مثل إلحاق الضرر بشبكات الاتصالات العامة ، أو تعمد إجراء اتصال يخالف قواعد الآداب العامة ، أو له طابع تهديدي أو يؤدي إلى إحداث فزع أو إزعاج " . وسنستعرض في هذا المبحث ماهية جريمة الإتلاف المعلوماتي وأركانها ووسائل إتلاف المال المعلوماتي .

المطلب الأول - المقصود بإتلاف معلومات وبرامج الحاسب الآلي :

يقصد بإتلاف برامج الحاسب الآلي ومعلوماته إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ويطلق عليه مصطلح تدمير نظم المعلومات (Information Sabotage) وعادة لا يستهدف مرتكب هذا الاعتداء فائدة مالية لنفسه ، بل يسعى للإعاقة وتعطيل نظم المعلومات عن أداء وظائفها وإحداث أضرار بها [6].

والمقصود من الإتلاف هنا هو ذلك الذي يوجه إلى الجانب المنطقي والمعنوي في الحاسب الآلي والذي أصبح يشكل قيمة مالية مرتفعة ، فإتلاف برامج ومعلومات الحاسب الآلي فيه إفقاد لمنفعة هذه البرامج والمعلومات .

([6]) المقصود من الإتلاف هنا هو ليس الإتلاف المادي ، الذي حصل عندما قامت إحدى المنظمات الإرهابية في فرنسا عام 1980م بإتلاف برامج وملفات أحد مراكز الحاسب الآلي المتخصصة في بيع الحاسبات الآلية حيث أن هذا لا يعد من قبيل جرائم الحاسب الآلي حيث تركز الاعتداء فيه على أموال مملوكة للغير ، وباستطاعة قانون العقوبات التقليدي تقديم الحماية ضد هذا النوع من الاعتداءات .

انظر: محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع، عمان، 2005م . ص 99 وما بعدها انظر أيضاً :

Walter Gary Sharp, Redefining National Security in Today's World of information technology and Emergent Threats, 9 Doke J Comp and Int'l 383-384 (1999)

وقد استخدام المشرع في ولاية كاليفورنيا بالولايات المتحدة الأمريكية تعابير عدة للإشارة على الإتلاف ، فاستخدم عبارات (عدل ، أفسد ، محى ، دمر) ويبدو لنا أن جميع هذه العبارات تندرج تحت مفهوم الإتلاف لأن المقصود منها هو حصول ذلك [7].

أما المشرع المصري فقد استخدم في المادة (361) من قانون العقوبات المصري عبارتي " خرب أو أتلف " .

أما المشرع الفرنسي فقد استخدم تعابير مثل أفسد ، وعطل ومحى وعدل ، وهذه التعبيرات أيضاً تندرج تحت مفهوم الإتلاف . ويظهر لنا أن السبب في استخدام المشرع لتعبيرات مختلفة هو طبيعة برامج الحاسب الآلي وسعي المشرع إلى الإحاطة بجميع الأفعال الجرمية المتصور حدوثها والتي تؤدي إلى الإتلاف سواء من ناحية تشغيلها أو من ناحية الاستفادة منها أو التقليل من قيمتها المالية .

وإفساد البرنامج يتمثل في إفقاد صلاحيته للاستعمال وفقاً للغرض الذي وضع من أجله ، وذلك بإدخال تعديلات جوهرية عليه أو حذف معلومات أساسية منه تدخل فيه ، أو في تكوينه ، بحيث لا يمكن نتيجة لذلك أن يؤدي الوظائف التي كان يؤديها ، أما التعطيل فإنه إعاقة لتشغيل النظام الآلي أو منع تشغيله بإدخال معطيات جديدة أو محو أو تعديل المعطيات المختزنة بالجهاز والتي يعمل بموجبها الحاسب الآلي [8].

المطلب الثاني - الركن المادي لجريمة الإتلاف :

يتمثل الركن المادي في جريمة الإتلاف بإحداث ضرر في مال الغير وفي الحاسب الآلي في شقه المادي يمكن أن يكون الإتلاف بتخريب الجهاز أو تكسيره، وغيرها من الأضرار التي يمكن أن يتعرض لها أي جهاز آخر . وقد تناول المشرعون في دول العالم المختلفة الإتلاف إذا ما وقع على مال ثابت أو منقول مملوك للغير ، فإذا كان محل الإتلاف جهاز الحاسب الآلي أو أدواته أو الأجهزة المتصلة به أو الأقراص المغنطة أو الأشرطة أو الدعامات أو غيرها مما يختص بالمعلومات وله كيان مادي فإنه لا تثار أي عقبة قانونية في تطبيق النصوص التقليدية الخاصة بجريمة الإتلاف على اعتبار أن محل الجريمة مال مادي مملوك للغير. أما بالنسبة للبرامج (الشق المعنوي) في الحاسب الآلي ، فيمكن أيضاً أن تتعرض للإتلاف بالتخريب والتغيير بهذه البرامج

---

(7) " Knowingly accesses and without permission alters, damages deletes, destroys , or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme of artifice to defraud , deceive or extort , or (B) wrongfully control or obtain money , property , or data , S502 (C) (1) , 1998 Main volume text , California Code.

انظر أيضاً :

Eric J. Sinrod, and William P Reilly, "Cyber-Crimes: A practical approach to the Application of Federal Computer Crimes Laws, 16 Santa Clara computer and High Tech L.J 177, 181-90 (2000)

(8) فالإتلاف إذا نتج عن إدخال تغييرات شاملة على البرنامج بحيث يصبح غير صالح للاستعمال في الغرض الذي أعد من أجله فإنه يمكن القول نتيجة لذلك بأنه تم إفناء البرنامج أو صورة كاملة ، أما التعطيل فيتحقق بإدخال تغييرات تؤدي إلى إتلاف جزئي في البرنامج من شأنه أن يؤدي إلى عدم إمكانية استخدام الحاسب الآلي في الغرض الذي أعد من أجله أو أن يؤدي إلى تقليص كفاءته في الاستخدام ، أو أن يؤدي إلى عدم إمكانية استخدامه بصورة نهائية وكاملة لتلف البرامج التي يعمل بها .انظر محمد حماد مرهج الهيتي ، جرائم الحاسوب ، دار المناهج للنشر والتوزيع ، عمان ، 2006م ، ص 197 وما بعدها .

أنظر أيضاً :

Edward Wise, Computer Crimes and Other Against Information Technology in the United States, RI S.P. 1993, at 652-654

والبيانات والمعلومات ولعل أكثر السلوكيات الإجرامية انتشاراً في إتلاف برامج الحاسب الآلي هو ما تقوم به الفيروسات والديدان التي تهاجم برامج الحساب الآلي وتقوم بإتلافها .

إذن يتمثل جوهر الإتلاف في تخريب الشيء محل الإتلاف أو الانتقاص من منفعته بجعله غير صالح للاستعمال أو تعطيله[9] ، ويتحقق الركن المادي لإتلاف المال المعلوماتي بإتلافه أو تخريبه أو تعطيله أو بجعله غير صالح للاستعمال. ويقصد بالإتلاف إفناء الشيء أو هلاكه كلياً ، ويقصد بالتخريب توقف الشيء تماماً عن أداء منفعته حتى مع عدم فناء مادته ، سواء كان هذا التوقف كلياً أو جزئياً. ويكون الشيء غير صالح للاستعمال بجعله لا يؤدي وظيفته على النحو المطلوب ، أما التعطيل فيكون بتوقف الشيء عن القيام بوظيفته لفترة مؤقتة ، وتتحقق جريمة الإتلاف بتحقق إحدى هذه النتائج [10].

ويتمثل الركن المادي في نشاط إجرامي وهو فعل الإتلاف ، ومحل يتمثل في مال ثابت أو منقول مملوك للغير .

والإتلاف وفقاً لما سبق وأن ذكرنا قد يرد على كل المال أو على جزء منه ولكن إن حصل الإتلاف على جزء من المال فيشترط لحصول الإتلاف أن يجعل المال غير صالح للاستعمال كما أنه لا يشترط أن يتم بوسيلة معينة بشرط ألا تكون هذه الوسيلة مما يخضع لنص عقابي آخر [11].

ويمكن تناول الركن المادي لجريمة الإتلاف كما هو منصوص عليها في المادة (361) من قانون العقوبات المصري بخصوص حالات الاعتداء على برامج وبيانات الحاسب الآلي إذا أخذنا بإمكانية مباشرة أفعال الإتلاف عليها بالصورة الواردة في النصوص التشريعية باعتبارها صور للنشاط الإجرامي .

أولاً - النشاط الإجرامي :

يتخذ النشاط الإجرامي في جريمة الإتلاف أربع صور كما هو منصوص عليه في المادة (361) من قانون العقوبات المصري وهي على النحو التالي :

1- التخريب : ويقصد به أن المال أصبح غير قابل للإصلاح لما أعد له مع بقاء أصله .
2- الإتلاف : ويقصد به تعييب الشيء بما يجعله غير صالح لما أعد له مع بقاء أصله .

---

[9]) هدى حامد قشقوش ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد بالقاهرة في الفترة من 25- 28 أكتوبر 1993م. ص 564 .

[10]) عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ، بدون ناشر ، بدون تاريخ . ص183 . انظر أيضاً : محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، دار الثقافة للنشر والتوزيع، عمان ، 2004م . ص 218 وما بعدها .

[11]) وتدخل جريمة الإتلاف في عداد الجرائم التي يطلق عليها (الجرائم ذات الطابع الحر) حيث لا تتقيد بالوسيلة التي يقع بها إتلاف الأجهزة سواء بتكسيرها أو إحراقها أو تعطيلها . والاعتداء على الأموال المعلوماتية المادية يقع على أجهزة الحاسب الآلي ومعداته وملحقاته ، كالدعامات والبرامج المنسوخ عليها المعلومات والأوراق المستعملة في عمله والشرائط الممغنطة ، ويمكن في هذه الحالة تطبيق نصوص قانون العقوبات المتعلقة بالإتلاف . انظر هدى قشقوش ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، المرجع السابق . ص 153 . انظر أيضاً : محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، المرجع السابق ، ص 218 وما بعدها . انظر أيضاً: عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والإنترنت ، الجرائم الإلكترونية ، منشورات الحلبي الحقوقية ، بيروت ، 2007م . ص 72 وما بعدها . انظر أيضاً : محمد الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات ، ط 2 ، دار النهضة العربية، القاهرة ، 198م . ص 33 وما بعدها .

3- جعل الشيء غير صالح للاستعمال أي إعدام صلاحيته ويلحق بالتخريب .

4- تعطيل الشيء، أي إعاقته عن العمل كلياً أو جزئياً [12].

وتبعاً لذلك تتحقق جريمة الإتلاف طالما وقع إتلاف أو تخريب على المال على نحو يذهب بقيمته كلها أو بعضاً منها مما يجعل الشيء غير صالح للاستعمال أو تعطيله أياً كانت الوسيلة المستخدمة لتحقيق ذلك [13].

أما المشرع الإماراتي فقد حدد النشاط الإجرامي الممثل للركن المادي في المادة (424) من قانون العقوبات الإماراتي وحددها بأربع صور للفعل الذي يتحقق به الركن المادي لجريمة الإتلاف وهذه الصور هي :

1- هدم المال - إتلاف المال 3 جعل المال غير صالح للاستعمال 4- تعطيل المال.

وقد يقع الإتلاف على جزء من المال وتقوم الجريمة شريطة أن يكون من شأن هذا الإتلاف جعل المال غير صالح للاستعمال أو تعطيله ، والعبرة في إتلاف الشيء هنا هو في الانتقاص الحاصل في قيمته ، لذلك فإن محل الحماية الحقيقي هو قيمة الشيء وليس حماية مادته إلا وسيلة إلى حماية قيمته فإذا كان الفعل قد أفقد الشيء قيمته إذا نقص منها فقد تحقق الاعتداء الذي يعاقب عليه القانون على اعتبار أنه قد أزال أهمية الشيء بالنسبة لمالكه [14].

ثانياً : محل الجريمة :

نفرق في دراستنا لمحل الجريمة بين حالتين :

1- إذا كان محل الجريمة هو المكونات المادية للحاسب الآلي مثل شاشات العرض (Monitors) والأشرطة المغنطة والأسطوانات والمفاتيح وغيرها من المكونات المادية سواء أكانت تحوي برامج أو بيانات أو مجرد أوعية خالية شريطة أن يؤدي الإتلاف أو التخريب إلى الإقلال من قيمتها الاقتصادية أو يؤدي إلى تعطيلها أو جعلها غير صالحة للاستعمال ، ومن الأمثلة على ذلك قيام مجموعة إرهابية ألمانية بالهجوم على أحد مراكز الحاسب الآلية في المانيا وتدمير هذا المركز بما فيه من حاسبات آلية مما تسبب في أضرار مادية جسيمة تقدر بمليوني مارك ألماني [15].

---

[12]) هشام فريد ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتب الآلات الحديثة ، أسيوط ، 2000م ، ص 309 ، وما بعدها .

[13]) هدى حامد قشقوش ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، المرجع السابق ، ص 568 . انظر أيضاً: عبدالفتاح حجازي ، مكافحة جرائم الكمبيوتر والإنترنت ، دراسة معمقة في القانون المعلوماتي ، دار الفكر الجامعي ، الإسكندرية ، 2006م ، ص 13 .

[14]) ولم يحدد المشرع الإماراتي هنا وسيلة محددة لفعل الإتلاف وبالتالي تقع الجريمة بأي فعل من شأنه تعطيل المال محل الجريمة أو تعييبه وجعله غير صالح للاستعمال بعد ذلك .انظر الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، محمد عبيد الكعبي ، دار النهضة العربية، القاهرة ، بدون تاريخ ، ص 212 وما بعدها ، القاهرة ، بدون تاريخ ص 212 وما بعدها . انظر أيضاً محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، مرجع سابق ص 219 ، وما بعدها ، محمد البشرى ، التحقيق في جرائم الحاسب الآلي والإنترنت ، مرجع سابق ص 219 وما بعدها . محمد البشرى ، التحقيق في جرائم الحاسب الآلي والإنترنت ، المجلة العربية للدراسات الأمنية والتدريب ، المجلد 15 ، العدد 30، أكاديمية نايف العربية للعلوم الأمنية ، نوفمبر 2000م . ص 124 .

[15]) وكذلك قيام مجموعة إرهابية إيطالية تسمى بالألوية الحمراء (The Red Brigades) بارتكاب العديد من الهجمات بإلقاء قنابل وإشعال النار في عدد من مراكز الحاسبات الآلية عامي 1976 و 1978 م . وكذلك قيام منظمة العمل اليسارية الفرنسية بالهجوم على مقار شركة فليبس (Philips) وتدمير برامج معلوماتية وبيانات زعمت أنها تستخدم لأغراض عسكرية وتجسس . انظر هشام محمد فريد رستم ، الجرائم المعلوماتية . مجلة الأمن والقانون ، دبي ، العدد (2) 1999م . ص 153 وما بعدها .

2- إذا كان محل الجريمة المكونات غير المادية ويطلق على هذه الحالة للإتلاف (تدمير نظم المعلومات) ويقصد به إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ، ولا يهدف التدمير هنا إلى الحصول على منفعة الحاسب الآلي أياً كان نوعها (من استيلاء على أموال أو الحصول على معلومات) وإنما يكون هدفه وباعثه هو تدمير هذه البرامج والبيانات أو محوها كلها أو بعضها لغرض الانتقام أو المنافسة أو العبث أو غير ذلك من البواعث . ونرى أنه في الحالة الأولى التي ينصب فيها الإتلاف على المكونات المادية فلا توجد صعوبة في تطبيق النصوص التقليدية للإتلاف حسبما هو وارد في نص المادة (361) من قانون العقوبات المصري ، ولكن تثور الصعوبة في مدى انطباق هذه النصوص على الأموال المعنوية للحاسب[16].

وقد انقسم الفقه في ذلك إلى اتجاهين :

الاتجاه الأول :

يرى أنصار هذا الاتجاه أنه إذا اقتصر الإتلاف على البرامج والبيانات دون الدعامات المالية التي تم تسجيلها وتخزينها عليها لا تقوم جريمة الإتلاف على اعتبار أن المادة (361) من قانون العقوبات المصري تقصر حمايتها على الأشياء ذات الطبيعة المادية ويستدلون على صحة هذا الرأي بالأسباب الآتية:

1- القانون أو النظام لا يحمي في الأصل إلا مادة الشيء وذلك توصلاً إلى توفير الحماية القانونية لقيمته الاقتصادية التي تعتمد على بقاء مادته صالحة وفقاً للغرض منها .[17]

2- لا تعد البيانات والبرامج مالاً في حد ذاتها ،وبالتالي لا يمكن أن يتم تملكها ، حيث أن حق الملكية لا ينصب إلا على الأشياء المادية التي لها قيمة اقتصادية وقيمة مادية وهو ما لا ينطبق على البرامج والبيانات باعتبارها قيم غير مادية .

3- بما أن محو هذه البرامج والبيانات يتم عن طريق التدخل في وظائف الحاسب الآلي فإن هذا النشاط لا يعد من قبيل الإتلاف للدعامات المادية المحتوية لهذه البرامج والبيانات .

الاتجاه الثاني :

يرى أنصار الاتجاه الثاني أنه لا يوجد ما يمنع وقوع هذه الجريمة على برامج وبيانات الحاسب الآلي واعتمدوا في تبريرهم على الأسباب الآتية :

1- أن نص المادة (361) من قانون العقوبات المصري قد جاء عاماً بالنسبة للأموال محل الجريمة حيث لم يستلزم نص المادة المذكورة أن يكون هذا المحل منقولاً مادياً مما يعني إمكانية تطبيقه على كافة الأموال المنقولة مادية كانت أم معنوية .

([16]) جميل عبدالباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، الكتاب الأول : الجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية ، القاهرة ، 1992م . ص 156 . انظر أيضاً : عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ، مرجع سابق . ص 185 وما بعدها .

([17]) جميل عبدالباقي الصغير ، المرجع السابق . ص 159 . انظر أيضاً : سليمان أحمد فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية ، المرجع السابق . ص 93 وما بعدها.

2- لا يمكن القول بان برامج وبيانات الحاسب الآلي لا تعتبر من قبيل الأموال ، فبرامج وبيانات الحاسب الآلي لها قيمة اقتصادية وقيمة مالية وهي تخضع لجميع التصرفات القانونية التي ترد على حق الملكية وبالتالي فهي قابلة للتملك والاستحواذ عليها ، والقول بغير ذلك يجعل هذه البرامج والبيانات غير محمية بأية حماية قانونية ، الأمر الذي سيشجع المجرمين على الاعتداء عليه وهو ما لا يمكن القبول به.

3- امتنع المشرع عن تحديد وسيلة تتم بها هذه الجريمة ، وينبغي مراعاة النصوص الخاصة التي تجرم استخدام وسيلة معينة لارتكاب هذه الجريمة حيث تفردها بعقوبات مغايرة عن تلك الواردة في المادة (361) من قانون العقوبات المصري. [18]

4- من الممكن أن تكون برامج وبيانات الحاسب الآلي محلاً لهذه الجريمة حتى لو اقتصر الإتلاف عليها دون الدعامات المادية التي تحويها وذلك عند تعريفها لقوى مغناطيسية من شأنها إفساد هذه البرامج والبيانات مما يؤدي إلى التأثير في قيمتها ووظائفها وهو ما يعد إتلافاً لها .

ونرى أن الاتجاه الثاني هو الأولى بالأخذ به ، وهو صلاحية برامج وبيانات الحاسب الآلي لأن تكون محلاً لجريمة الإتلاف على اعتبار أن ذلك يؤدي إلى مسايرة التطور التقني وما يقضي به هذا التطور ن أمور تجعل للأشياء غير المادية قيمة قد تفوق قيمة الأشياء المادية .

ونرى أيضاً أن المشرع بحاجة إلى نصوص جنائية تجرم صراحة إتلاف المال المعلوماتي المعنوي ، وذلك أخذاً بمبدأ أن لا جريمة ولا عقوبة إلا بنص ، وأخذاً بمبدأ التفسير الضيق للنصوص القانونية ، وبما يتناسب مع التطور التقني المعلوماتي [19].

تعد جريمة الإتلاف من الجرائم العمدية التي تتحقق بتوافر القصد الجنائي العام الذي يقوم بتوافر العلم والإرادة . فيتعين أن يعلم الجاني أنه يعتدي على مال معلوماتي مملوك لغيره ، وأن من شأن فعله أن يتلف الشيء أو يعطله أو أن ينتقص من منفعته بشكل يجعله غير صالح للاستعمال بما يؤدي إلى إلحاق الضرر به .

وبناء على ذلك فإذا اعتقد أن المال المعلوماتي المادي محل الإتلاف مملوك له فإن القصد الجنائي لا يتوافر لديه لعدم العلم ، كمن يعتقد أنه مالك لقرص ممغنط أو جهاز حاسب آلي ثم يثبت أنه ملك للغير .

وهذه الجريمة لا تتطلب قصداً خاصاً ، وإنما يكتفى بشأنها القصد العام بعنصريه العلم والإرادة . فيتوافر العلم في حالة إذا كان الجاني عالماً بأنه من شأن سلوكه إتلاف مال الغير بصورة تذهب بقيمته كلها أو

([18]) انظر هدى حامد قشقوش ، المرجع السابق . ص 568 وما بعدها . انظر أيضاً عفيفي كامل عفيفي، المرجع السابق ، ص 188 وما بعدها .

([19]) فهناك حالات تثار فيها مسألة إتلاف بعض أدوات الحاسب الآلي وبما يؤثر على برامجه ومعلوماته ، فقد يحصل الإتلاف بكسر الأسطوانة المسجل عليها البرنامج ، أو قد يحصل مسح للبرنامج أو البيانات بصورة فنية دون أن تصاب الأسطوانات بسوء ، كأن يتم وضع مادة عليها تؤدي إلى تعطيل البرنامج أو محوه. انظر علي عبدالقادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، الطبعة الأولى ، الدار الجامعية للطباعة والنشر ، بيروت ، 1999م ، ص 112 .

انظر أيضاً :

John Conley, and Robert Bryan, A Survey of Computer Crime Legislation in the United States, Information and Communications, Technology Law, Vol 8, 1, 1999.

انظر أيضاً :

Neal Kumar Katyal, Criminal Law in Cyber space, 149 U.Pa. L. Rev 1003, 1013 (2001)

بعضها وبدون سند مشروع مع علمه بملكية هذا المال للغير.[20]

ويشترط أيضاً بالإضافة إلى توافر العلم أن تتجه إرادة الجاني إلى تحقيق نتيجة فعله ، وذلك بإحداث الإتلاف أو التخريب أو التعطيل بشكل يؤدي إلى توافر الضرر الناتج عن فعله . فإذا انتفت هذه الإرادة ينتفي بالتبعية القصد الجنائي ومن ثم الجريمة .

ولذلك إذا كان الإتلاف غير مقصود كما لو حدث شيء عارض وتسبب في إتلاف الحاسب الآلي أو جزء منه أو معداته أو ملحقاته ، فإن الفاعل يسأل عن الخطأ نتيجة إهماله أو رعونته أو تقصيره ، كمن يستخدم قرص ممغنط يحتوي على فيروس في جهاز حاسب آلي مما يؤدي إلى الإضرار به ، أو يقوم بتحميل قرصاً مرناً أو القرص الصلب برامج أو مواقع على شبكة الإنترنت دون التحقق من خلوها من الفيروسات . وكما في حالة قيام أحد الأشخاص بغير قصد بإيقاع إحدى الأسطوانات الممغنطة مما يؤدي إلى كسرها ، ففي هذه الحالة تنتفي الإرادة وبالتالي ينتفي الغرض من الجريمة المذكورة في المادة (361) من قانون العقوبات المصري ، وهذا لا يمنع من قيام جريمة أخرى وهي جريمة إتلاف مال منقول مملوك للغير بإهمال المنصوص عليها في الفقرة (6) من المادة (378) من قانون العقوبات المصري [21].

إلا أن المشرع الإماراتي ذهب إلى اعتبار تحقق جريمة الإتلاف المنصوص عليها في المادة (404) من قانون العقوبات الإماراتي فيما لو وقعت بطريق الخطأ وذلك استناداً إلى المادة (43) من ذات القانون والتي تنص على أن " يسأل الجاني عن الجريمة سواء ارتكبها عمداً أو خطأ ما لم يشترط القانون العمد صراحة"[22].

([20]) فيتوافر العلم في حالة إذا كان الجاني على علم بأن من شان سلوكه إتلاف مال الغير بصورة تذهب بقيمته كلها أو بعضها وبدون سند مشروع مع علمه بملكية هذا المال للغير ، وبالتالي ينتفي العلم ومن ثم القصد الجنائي إذا كان الجاني يعتقد ملكيته لهذا المال وقت القيام بإتلافه مثل الوارث الذي يمحو البيانات والبرامج على أقراص ممغنطة غير مملوكة لمورثه وعثر عليها في التركة عن طريق مورثه مع كونها ليست كذلك . وكذلك في حالة قيام أحد الأشخاص باستخدام اسطوانة مملوكة له ولا يعلم بإصابتها بفيروس في حاسب أحد المشروعات مما يؤدي إلى انتقال هذا الفيروس إليه . انظر : عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ، مرجع سابق . ص 209 وما بعدها .

انظر أيضاً :

Marc Friedman, Infojacking: Crimes on the Information Super Highway, S.J. Proprietary Rts, 2,2,1997

([21]) وقد شدد المشرع المصري العقوبة في هذه الجريمة بمقتضى القانون رقم (29) لعام 1992م حيث ضاعفها إذا ارتكبت لغرض إرهابي ويكفي لتطبيق العقوبة المشددة أن يمثل الغرض الإرهابي (غاية الجاني) من ارتكاب جريمة إتلاف المال الثابت أو المنقول المملوك للغير ، ولو لم يتحقق هذا الغرض فعلاً ، ويمكن بذلك القول أن جريمة الإتلاف المشددة تفترض قصداً خاصاً باعتبار أنها تتطلب انصراف قصد الجاني إلى غاية محددة تتمثل في الغرض الإرهابي . انظر : هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، المرجع السابق . ص 322 . انظر أيضاً عفيفي كامل عفيفي ، جرائم الكمبيوتر ، مرجع سابق . ص 208 وما بعدها .

([22]) وقد قضت محكمة التمييز بإمارة دبي في الإمارات العربية المتحدة بأن للقاضي الجزائي تقرير ركن الخطأ والتقصير للتسبب في إلحاقه الضرر بالمال ، وحسبه أن يقيم قضاءه على أسباب سائغة لها أصلها الثابت في الأوراق وكافية لحمله ، وكل هدم أو إتلاف مال الغير كاف لقيام الجريمة بصرف النظر عن صدور ذلك عمداً أو خطأ . انظر الطعن رقم (28) لعام 1993 (جزاء) جلسة بتاريخ 1993/10/23م محكمة التمييز بدبي . انظر أيضاً محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، دار النهضة العربية ، القاهرة ، بدون تاريخ . ص 215 وما بعدها . انظر أيضاً محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، دار الثقافة ، عمان ، 2004م . ص 221 . انظر أيضاً محمد أمين الرومي ، جرائم الكمبيوتر والإنترنت ، دار المطبوعات الجامعية ، الإسكندرية ، 2003م . ص 55 .

انظر أيضاً :

Jay Lyman , Spam Costs $ 20 Billion Each Year in Lost Productivity , E-Commerce Times, Dec. 29, 2003.

انظر أيضاً :

Larry Lange, Trust a Hacker Under 30, You'd Better, ELEC. Eng' Times, August, 19, 1996.

تتنوع وسائل إتلاف المعلومات والبيانات والبرامج بدءاً من فيروسات الحاسب الآلي (Viruses) ومروراً ببرامج الدودة (Worms) وانتهاء بالقنابل المنطقية والزمنية (Logic and Time Bombs) . ولعل أهم هذه الوسائل، وأكثرها ضرراً هو استخدام الفيروسات ، وسنتناول استخدام الفيروسات ابتداء ، ثم نتعرض لباقي الوسائل المستخدمة في إتلاف المعلومات .

1- الإتلاف باستخدام فيروسات الحاسب الآلي :

الفيروسات هي برامج مشفرة مصممة بشكل يمكنها من التكاثر والانتشار من نظام إلى آخر ، إما بواسطة قرص ممغنط أو عبر شبكة للاتصالات بحيث يمكنها أن تنتقل عبر الحدود من مكان إلى آخر في العالم [23]. ويعرف البعض الآخر الفيروس بأنه عبارة عن معلومة خاطئة أو أمر مضلل يدخله الجاني إلى البرنامج من شأنه كف منفعة البرنامج فيما أعد له ، من خلال تكرار كتابة المعلومات ذاتها إلى آلية إدارة القرص مما يؤدي إلى إيقاف الحاسب الآلي عند حد معين ، ويسبب أعباء إضافية على القرص ويزيد من حرارته نتيجة التشغيل المستمر . أو هو برنامج يتم زرعه على الأقراص والأسطوانات الخاصة بالحاسب ، ويظل خاملاً لفترة محددة ثم ينشط فجأة في توقيت معين ليدمر البرامج والبيانات المسجلة ويمتد أثره التخريبي ليشمل الإتلاف والحذف والتعديل [24]. ويعرفه البعض بأنه برنامج يتكون من عدة أجزاء مكتوب بإحدى لغات البرمجة وبطريقة خاصة تسمح بالتحكم بالبرامج الأخرى ، وقادر على تكرار نفسه بالنسخ ، أي أنه البرنامج الذي يستطيع أن يلحق نسخ تنفيذية من نفسه في برامج أخرى تصبح هي بدورها قادرة على إلحاق نسخ تنفيذية من برامج أخرى [25].

وعرفه المركز الوطني للحاسب الآلي في الولايات المتحدة في تقرير أعده حول الاعتبارات الأمنية في الحاسبات الآلية بأنه " برنامج يهاجم أنظمة الحاسب الآلي بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان وهو في العادة برنامج صغير مكتوب بلغة متدنية المستوى مثل "لغة التجميع " مما يزيد من صعوبة اكتشافه ، ويقوم الفيروس بالتجول في الحاسب الآلي باحثاً عن برنامج غير مصاب ، وعندما يجد واحداً ينتج نسخة من نفسه لتدخل فيه ، وتتم عملية الإدخال هذه في جزء من الثانية ، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ أوامر الفيروس " [26].

([23]) أسامة بن غانم العبيدي ، جرائم الحاسب الآلي والإنترنت ، الصعوبات التي تعترض المكافحة ، المرجع السابق ، ص 88 . انظر أيضاً : نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ، المرجع السابق ، ص 192 وما بعدها.

([24]) هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، المرجع السابق ، ص 116 .

([25]) يقصد بالنسخ التنفيذية أجزاء محددة من البرنامج .انظر عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتعلقة بالحاسب الآلي وأبعادها الدولية ، دار النهضة العربية ، القاهرة ، 1995م . ص 73 ، انظر أيضاً : جريدة الرياض ، الملحق الاقتصادي ، 2 أغسطس 2008م ، العدد 14649 ، السنة الخامسة والأربعون ، ص 7

([26]) ومن أبرز الهجمات الفيروسية التي شهدها عالم الحاسبات الآلية ، ما قام به المواطن الأمريكي ديفيد سميث (David Smith) الذي انشأ فيروس البريد الإلكتروني المعروف باسم مليسا (Melisa) والذي أحدث اضطراباً عالمياً في البريد الإلكتروني وشبكة الإنترنت .

ونرى أن الفيروس هو برنامج حاسب مثل أي برنامج تطبيقي آخر يتم تصميمه بواسطة أحد المخربين لهدف محدد وهو إحداث أكبر ضرر ممكن بنظام الحاسب الآلي ، ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ذاتياً وهو ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة وكذلك بين المواقع المختلفة في الذاكرة حتى يحقق أهدافه التدميرية [27].

وتمتاز الفيروسات بسرعة انتشارها بين ملايين المستخدمين في ثواني معدودة كما أن لديها قدرة فائقة على اختراق أنظمة المعلومات وإتلافها ويقوم بتغيير شكله أو التشبه بالبرامج الأخرى [28].

والفيروسات التي تصيب الحاسب الآلي متعددة ويمكن تقسيمها من حيث تكوينها وأهدافها إلى التالي :

أ- فيروس عام العدوى : وهو ينتقل إلى أي برنامج أو ملف ويهدف إلى تعطيل نظام التشغيل بكامله .

ب- فيروس محدد العدوى : وهو يستهدف نوعاً معيناً من النظم لمهاجمته ويتميز بالبطء في الانتشار ، علاوة على صعوبة اكتشافه .

ج- فيروس عام الهدف ، ويتميز بسهولة إعداده واتساع مدى تدميره وتندرج تحته غالبية الفيروسات .

د – فيروس محدد الهدف : وهذا النوع من الفيروسات يقوم بتغيير الهدف من عمل البرنامج دون أن يعطله ، ويحتاج إلى مهارة عالية بالتطبيق المستهدف[29].

وكذلك الفيروس الذي أطلقه أحد الطلبة الجامعيين الأمريكيين إلى شبكة الإنترنت وانتشر هذا البرنامج خلال مدة لا تتجاوز 24 ساعة عبر الشبكة وغطى أطرافها كلية، وتأثرت به شبكات كثيرة ترتبط بشبكة الإنترنت ، وقام هذا الفيروس بملء ذاكرة (Memory)لآلاف الحاسبات الآلية في الولايات المتحدة الأمريكية بحيث لم يعد بمقدورها القيام بأي عمل أو تنفيذ أي أمر ، مما شكل إتلافاً للمعلومات ، وكذلك فيروس الكريسماس (Christmas Card) ويتمثل هذا الفيروس في شكل رسالة إلكترونية في البريد الإلكتروني ، وفيه يعرض بطاقة تهنئة الكريسماس على شاشة الحاسب الآلي . وفي خلال هذا الوقت يقوم بقراءة الملفات التي تحتوي على عناوين المشتركين في الشبكة ، ويرسل نسخ من نفسه إلى هؤلاء المشتركين مما ينتج عنه توقف النظام كله حتى يتم عزله والقضاء عليه . انظر : أسامة بن غانم العبيدي ، جرائم الحاسب الآلي والإنترنت : الصعوبات التي تعترض المكافحة ، المرجع السابق ، ص 89 .

([27]) هشام فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، المرجع السابق ، ص 26 .

([28]) قامت صحيفة الجارديان البريطانية بنشر تحذير خبراء الحاسب الآلي لمستخدمي الإنترنت باليقظة بعد إصابة نصف مليون حاسب آلي بفيروس خبيث . وذكرت الصحيفة أن محللي الحاسب الآلي في شركة مكافى (McCave)الخاصة بأمن الإنترنت سجلت أكثر من 530.000 ملف من الشراك الخداعية خلال أسبوع واحد فقط ، الأمر الذي جعلهم يؤكدون أن هذا يعتبر أكبر تفشي للفيروس منذ عدة سنوات .

ويعمل البرنامج بطريقة تحميل الميديا العادية كما في تحميل الأفلام ، ولكن بدلاً من تنزيل الفيديو أو الأغنية المتوقعة يتم خداع الضحايا بدخول الفيروس إلى حواسيبهم الآلية ببرنامج سري يغرقهم بعد ذلك بالإعلانات التجارية . وقال أحد الخبراء في شركة مكافى أن هذا الفيروس كان أنجح شفرة خبيثة خلال ثلاث سنوات ، وأن الأمور كان من الممكن أن تكون أكثر سوءاً ولكن لحسن الحظ أن الفيروس كان غير ضار ، ولكن ما يقلق هو أن أشخاصاً آخرين قد يستخدمون نفس النظام في نشر فيروس أكثر خطورة وضرراً من هذا الفيروس. وذكر هذا الخبير بأن التقنية المعروفة بحصان طروادة شائعة ، لكن المتغير الأخير يبدو أنه كان أكثر نجاحاً من نظرائه ، وهذا يمكن أن يكون بسبب زرعه على شبكات تبادل الملفات الضخمة مثل (إي دونكى) و (لايم واير) التي يستخدمها ملايين الأشخاص لتبادل ملفات الموسيقى والأفلام .

وذكر الخبير شبه استحالة كشف مكان دخول الفيروس إلى النظام أو تتبعه مرة أخرى لمعرفة المستفيد منه، فمواقع تبادل الملفات هي فريسة دورية لمؤلفي برامج الفيروسات الخبيثة ، ولكنها كانت تستخدم أيضاً بواسطة بعض شركات الميديا للقبض على منزلي البرامج غير الشرعيين وهم في حالة تلبس .

وقد تم في العام الماضي كشف إحدى الشبكات الأمريكية تدعى ميديا ديفندر (Media Defender) وهي تقوم ببث متعمد لشبكات شعبية بملفات فيديو وموسيقى رديئة الجودة في محاولة لتقليل شعبية أنظمة منافسة . لكن الخبير ذكر أن ليس هناك إشارة إلى أن هذا التفشي الأخير للفيروس كان نتيجة هذا الفعل من جانب الشركة المذكورة . انظر : مجلة الاتصالات والعالم الرقمي ، العدد 259، 2008/6/8م . ص 14 .

([29]) محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، المرجع السابق ، ص 237 وما بعدها . انظر أيضاً عبدالفتاح حجازي ، مكافحة جرائم الكمبيوتر والإنترنت، ص 25 وما بعدها. انظر أيضاً عماد سلامة ، الحماية القانونية لبرامج الحاسب الآلي ، الطبعة الأولى ، دار وائل للنشر ، عمان ، 2005م . ص 32. انظر أيضاً محمد الشوابكة ، جرائم الحاسوب والإنترنت ، المرجع السابق ، ص 220 وما بعدها . انظر أيضاً أحمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الطبعة الثانية ، الإسكندرية 2006م . ص 125 . انظر أيضاً : محمد البشرى ، التحقيق في جرائم الحاسب والإنترنت ، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب ، المجلد 15 ، العدد 30 ، الرياض ، نوفمبر 2000م .

والبرامج الفيروسية لها قدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافها ، كما أنها قد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات ثم تقوم بتدمير نفسها ذاتياً دون أن تترك أثراً يدل عليها ، وعلى الرغم من تدميرها للبرامج والمعلومات ، إلا أنها لا تسبب عادة تدميراً لأي من المكونات المادية للنظام [30].

خطورة الإتلاف باستخدام الفيروسات :

تكمن خطورة الإتلاف باستخدام الفيروسات بالخصائص التي يتمتع بها الفيروس وهي قدرته على التكاثر، أي قدرة البرامج المصابة على إنتاج الفيروس ذاته . مما يؤدي إلى انتشاره بشكل كبير . ومن خطورته أيضاً أنه يرسل عن بُعد ومن خلال شبكات الاتصال، مما يصعب اكتشاف مصدره ، كذلك من الصعوبة على المستخدم أن يكتشفه إلا من خلال برامج خاصة معدة لذلك الغرض ، خاصة أن من خصائص وصفات الفيروس أنه يظل خاملاً وكامناً لمدة محددة ويمكن أن يستهدف برامج معينة دون غيرها [31].

ويتم إفساد أو تعطيل تشغيل برامج الحاسب من خلال إدخال معطيات ومعلومات جديدة أو محو أو تعطيل المعطيات أو البرامج المخزنة بالحاسب لأن هذه الأفعال من شأنها تعطيل تشغيل النظام بصورة كلية أو جزئية ، وهذا يتحقق بإدخال الفيروسات التي يمتد أثرها إلى برامج التشغيل والأنظمة الأخرى الملحقة به ، أي البرامج الخاصة بالمعالجة ، مما يؤدي إلى شغل ذاكرة الجهاز بشكل كامل ، وبالتالي يعجز عن التعامل مع هذه المعلومات أو المعطيات سواء بمعالجتها أو باسترجاعها ، ويعود ذلك إلى أن البرنامج الدخيل يجعل برامج الحاسب الأصلية لا تستجيب للأوامر والتعليمات التي ترسل إليه، وذلك يعود لامتلاء الذاكرة بالمعلومات والبيانات بفعل التأثير الذي يحدثه الفيروس، وبالتالي يعجز الحاسب عن معالجة البيانات أو المعلومات التي ترد إليه مما ينشأ عنه تعطيل البرنامج أو إتلافه ، فالفيروس يعمل على تكرار المعلومات وبالتالي فإن أي عملية حذف لأي جزء من المعلومات والبيانات التي تملأ ذاكرة الحاسب لإحداث سعة في الذاكرة لإدخال معلومات جديدة أو لإصدار أوامر جديدة للتشغيل أو للمعالجة سوف لن تكون ممكنة وبالتالي ينتج عن ذلك توقف العمل بالبرنامج أو عدم إمكانية تشغيله أو استخدامه وبالتالي ينتج عن ذلك إتلاف البرنامج أو تعطيله [32].

([30]) وتستخدم كلمة " الفيروس " في مجال جرائم الحاسب الآلي والإنترنت بشكل عام للدلالة على البرامج الخبيثة التي تسبب تلفاً لأنظمة المعالجة الآلية للمعلومات ، إلا أن الفيروس هو أحد أنواع هذه البرامج ، والتي تشتمل إلى جانبه ، الديدان (Worms) ، حصان طروادة (Trojan Horse) والقنابل المنطقية (Logic Bombs) ، وتتسبب هذه البرامج جميعاً في إتلاف المكونات المنطقية للحاسب الآلي . وتستمد التفرقة بين هذه البرامج أساسها من أسلوب كل منها في أداء مهمتها . فالفيروس هو برنامج قادر على التكاثر وإرسال النسخ الجديدة إلى أنظمة أخرى بحيث يصبح معرفة مصدره أمراً بالغ الصعوبة ، أما البكتريا فهي برنامج مصمم لإتلاف نظام الحاسب الآلي عن طريق إعاقة استخدامه ، وهو قادر أيضاً على التكاثر ولكن إلى الحد الذي يستطيع فيه النظام منعه من أداء أية مهمة أخرى . انظر نائلة عدل قورة ، جرائم الحاسب الآلي الاقتصادية ، المرجع السابق ، ص 191 وما بعدها .

([31]) جميل عبدالقادر الصغير ، الإنترنت والقانون الجنائي ، المرجع السابق . ص62. انظر أيضاً :علي عبدالقادر القهوجي ، الحماية الجنائية لبرامج الحاسب ، المرجع السابق ، ص 37 وما بعدها . انظر أيضاً : محمد حماد الهيتي ، جرائم الحاسوب ، المرجع السابق ، ص 203 وما بعدها. انظر أيضاً : فتحي محمد أنور عزت ، الحماية الجنائية الموضوعية والإجرائية : الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي ، الطبعة الأولى، دار النهضة العربية ، القاهرة ، 2007م . ص 142 وما بعدها . انظر أيضاً عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية) ، المرجع السابق ، ص72 وما بعدها .

([32]) ماجد عمار ، المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها ، دار النهضة العربية ، القاهرة ، 1989م، ص 76 وما بعدها . انظر أيضاً محمد حماد الهيتي، جرائم الحاسوب ، المرجع السابق ، ص 203 وما بعدها . انظر أيضاً :
Carl Benson, Andrew Jabian , Computer Crimes, American C.L. Rev, Vol , 34, No 2, 1997.

2 : برامج الدودة :

تعرف برامج الدودة بأنها تلك البرامج التي تستغل أية فجوات في نظم التشغيل في الحاسبات الآلية ، لتنتقل من حاسب إلى آخر ومن شبكة إلى أخرى عبر الوصلات التي تربط بينها ، وأثناء عملية انتقالها تتكاثر كالبكتريا بإنتاج نسخ منها [33]. وتهدف هذه البرامج إلى العمل على إضعاف كفاءة الشبكة أو إلى التخريب الفعلي للملفات والبرامج ونظم التشغيل ، وذلك بإشغال أي حيز ممكن من سعة الشبكة [34]. وتختلف الديدان في طريقة عملها من نوع إلى آخر ، فبعضها يتناسخ داخل الحاسب الآلي إلى إعداد هائلة بينما بعضها ينتشر عبر البريد الإلكتروني بحيث تقوم بإرسال نفسها في رسائل إلى الأشخاص المسجلة عناوينهم في الجهاز .

وتكمن خطورة الديدان في استقلاليتها وعدم اعتمادها على أي برامج أخرى تلتحق بها مما يعطيها حرية كاملة في الانتشار السريع ، ولعل من أشهر وسائل إنتشار الديدان هو عن طريق الرسائل الإلكترونية المفخخة ، وعادة ما تكون عناوين تلك الرسائل الإلكترونية جذابة كدعوة لمشاهدة صور أحد نجوم كرة القدم المشهورين مثلاً . ومثال ذلك ما قام به أحد الطلاب الجامعيين الألمان في ديسمبر عام 1987م بإرسال تهنئة بمناسبة أعياد الميلاد باستخدام الحاسب الآلي ، وقد قام بتصميم برنامج دودة قادر على قراءة العناوين المخزنة بذاكرة حاسب البريد الإلكتروني وقام بنسخ بطاقة التهنئة التي أرسلها إلى نسخ متعددة وقام بإرسالها إلى كافة العناوين التي قام البرنامج بقراءتها ، الأمر الذي أدى بعد قيامه باختراق شبكة V-net التي تربط الحاسبات الآلية لدول يتجاوز عددها 45 دولة مما أدى إلى تعطيل ما يزيد على نصف مليون حاسب آلي خلال ساعتين وأدى ذلك إلى تعطيل تلك الحاسبات لمدة يومين [35].

كما أطلق طالب أمريكي اسمه روبرت موريس (Robert Morris) وهو طالب في علوم الكمبيوتر بجامعة كورنيل الأمريكية (Cornell University) بولاية نيويورك برنامج دودة الإنترنت (Internet Worm) لكي يثبت عدم ملائمة أساليب وسائل الحماية في شبكات الحاسب الآلي ، ولكنه تسبب في تدمير وإتلاف الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة ، بالإضافة إلى إعاقة طريق ومسلك شبكات الحاسب الآلي ، وفي إعادة البرمجة بتكاليف بلغت عدة ملايين من الدولارات . [36] وتمت محاكمة موريس بموجب القانون الذي يجرم الدخول إلى المواقع الحكومية دون الحصول على تصريح ، وتمت إدانته والحكم عليه بوضعه ثلاث سنوات تحت المراقبة والقيام بخدمة المجتمع لمدة 400 ساعة مع تغريمه مبلغاً وقدره عشرة آلاف

([33]) محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، المرجع السابق ، ص 193. انظر أيضاً محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية المرجع السابق . ص 101 وما بعدها .

([34]) محمد سامي الشوا ، المرجع السابق ، ص 193 .

انظر أيضاً :

David,Whalen, The Unofficial Cookie FAQ Version, at http://www.cookiecentral.com/faq.

انظر أيضا :

Jeffery Rosen, The Unwanted Gaze, The Destruction of Privacy in America 167, Vintage Books, 2001 at 167-169 .

([35]) محمد سامي الشوا ، مرجع سابق ، ص 164 وما بعدها .

([36]) محمد أمين الرومي ، جرائم الكمبيوتر والإنترنت ، المرجع السابق ، ص 57 وما بعدها . انظر أيضاً محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، المرجع السابق ، ص 237 وما بعدها .

وخمسين دولاراً أمريكياً [37].

كما تم اكتشاف حالة من برامج الدودة أطلق عليها مصطلح " البرامج الدودية ضد القتلة مستخدمي الذرة " ورمز إليها برمز "Wank " ، حيث غزت تلك البرامج مرتين خلال عام 1989م شبكة علوم الأرض والفضاء بالولايات المتحدة الأمريكية ، كنوع من أنواع الإحتجاج على إطلاق مكوك فضاء يحمل مجسماً فضائياً مغطى ببودرة نووية [38].

3 : القنابل الزمنية والمنطقية :

القنابل المنطقية (Logic Bombs) هي 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 ، وتعمل هذه البرامج على مبدأ التوقيت وهي تحدث تدميراً وتغييراً في المعلومات والبرامج عند إنجاز أمر محدد في الحاسب الآلي ، أو برنامج محدد[39].

والقنابل المنطقية تظل ساكنة وغير نشطة وبالتالي فهي لا تكتشف لمدة قد تطول وقد تقصر يحددها مؤشر موجود في البرنامج القنبلة .

وهذا المؤشر لا يقتصر على المدة الزمنية ، وإنما قد يمتد إلى ما يعرف بتوافر شروط منطقية معينة داخل برنامج أو ملف معين وذلك وفقاً للرمز الذي يحدده برنامج القنبلة ، فإذا دخل الميعاد أو توافرت هذه الشروط بدأ البرنامج في القيام بمهامه التخريبية [40].

أما القنبلة الزمنية فهي التي تثير حدثاً في لحظة زمنية محددة بالساعة واليوم والسنة، ويتم إدخالها في برنامج وتنفذ في جزء من الثانية أو في بضع ثوان أو دقائق وفقاً للتاريخ المحدد مسبقاً [41].

ومن الأمثلة الواقعية التي استخدمت فيها القنابل الزمنية ما قام به أحد المتخصصين في برمجيات الحاسبات الآلية في بريطانيا من وضع قنبلة زمنية في نظام إحدى الحاسبات الآلية أدت إلى محو أكثر من مائتي برنامج، إضافة إلى محو النسخ الأصلية عند تشغيلها لانتقال آثار القنبلة الزمنية إليها ، وقد تم القبض على المجرم وحكم عليه القضاء البريطاني بالسجن لمدة (3) سنوات[42].

([37]) محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية ، المرجع السابق ، ص 103 .

([38]) أنظر :

John Falvey, J, and Amy M. McCallen, A Survey of Internet Crime Targeting Multiple computers, Albany Law Journal, 2006 PP 22-27

انظر أيضاً :

Jack Brown, E, Jurisdiction to Prosecute Crimes Committed By Use of the Internet, Jurimetrics Journal, Summer, 1998 Symposium, 1998. PP 575-580.

([39]) محمد سامي الشوا ، المرجع السابق ، ص 193 .

([40]) هشام محمد فريد ، قانون العقوبات ومخاطر تقنية المعلومات ، المرجع السابق ، ص 158 . انظر أيضاً سليمان أحمد فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية "الإنترنت" ، المرجع السابق ، ص 101 وما بعدها .

([41]) أسامة بن غانم العبيدي ، جرائم الحاسب الآلي والإنترنت ، الصعوبات التي تعترض المكافحة ، المرجع السابق ، ص 91 .

([42]) محمد سامي الشوا ، المرجع سابق ، ص 195 ، انظر أيضاً محمد أمين الرومي ، جرائم الكمبيوتر والإنترنت ، المرجع السابق ، ص 54 وما بعدها .

وكذلك قيام أحد المحاسبين المتخصصين في نظم معلومات الحاسب الآلي ؛ بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالشركة وذلك بدافع الانتقام من الشركة التي كان يعمل بها وفصل منها ، حيث انفجرت بعد انقضاء ستة أشهر من تركه للشركة ، وترتب على فعلته تلك إتلاف كل البيانات المخزنة في حاسبات الشركة[43].

وفي ألمانيا قام أحد مبرمجي الحاسب الآلي بزرع برنامج قنبلة زمنية في نظام المعلومات الخاص بالشركة التي يعمل بها وقام ببرمجة القنبلة الزمنية بحيث تنفجر بعد عامين من تاريخ فصله من الشركة . وقد ترتب على ذلك إتلاف نظام معلومات الشركة في الوقت الذي قام بتحديده ، وترتب على ذلك إتلاف البيانات والمعلومات المخزنة في شبكة معلومات الشركة[44].

المبحث الثاني – صور جريمة الإتلاف المعلوماتي :

سنتطرق في هذا المبحث لصورتي جريمة الإتلاف وهما صورة إدخال البيانات والمعلومات في نظام المعالجة الآلية للحاسب الآلي وصورة محو أو تعديل البيانات والمعلومات غير المشروع في نظام المعالجة الآلية للحاسب الآلي.

المطلب الأول – إدخال البيانات والمعلومات في نظام المعالجة الآلية للحاسب الآلي:

ويقصد بذلك إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة . ويستوي أن يتم هذا الإدخال بطريق مباشر أو غير مباشر وبدون مراعاة لحقوق الغير.

وقد يكون الإدخال بإدخال معلومات أو بيانات وهمية في النظام المعلوماتي باصطناع المعلومات ، ومثال ذلك ما قام به أحد الموظفين في قسم الحاسب الآلي في إحدى الشركات الفرنسية عندما قام باسترجاع ملفات الموظفين السابقين والذين لهم حقوق مالية على الشركة ، وقام بتحويلها إلى حساب الشخص وحسابات أخرى قام بفتحها خصيصاً لهذا الغرض حيث قام باختلاس أكثر من مليوني يورو[45].

وقد يكون الإدخال بإدخال معلومات أو بيانات مزورة في النظام المعلوماتي عن طريق تزوير المستندات والمعلومات والبيانات المخزنة في الحاسب الآلي ، ويتم التزوير في هذه الحالة أما عن طريق استبدال المعطيات أو بواسطة المحو المنتقى للمعطيات . ويؤدي التلاعب بالمعطيات إلى قيام جريمة التزوير إضافة إلى جريمة الإتلاف .

([43]) محمد سامي الشوا ، المرجع السابق ، ص 196 .

([44]) محمد أمين الشوابكة ، المرجع سابق ، ص 24 . انظر أيضاً أسامة بن غانم العبيدي ، المرجع سابق، ص 80 وما بعدها .

انظر أيضاً :

Nichoel Forrett, Cookie Monster: Balancing Internet Privacy with Commerce, Technology, And Terrorism, Touro Law Review, 2004 at 3-5.

([45]) محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان، 2004م ، ص 232 وما بعدها .

انظر أيضاً :

Leslie Berkowitz, , Computer Security and Privacy: The Third Wave of Property Law, Colorado Lawyer 2004. PP 6-8.

ونرى أن التغيير أو التبديل الذي يقع على المعطيات أو الأوامر المخزنة والمنقولة عبر شبكة الإنترنت (World Wide Web) لا يمكن تطبيق نصوص التزوير عليها ، إذ أن الاعتداء على البيانات بتغيير الحقيقة لا يعد تزويراً إلا إذا تم بصورة محرر مكتوب [46].

ويكون تغيير الحقيقة بالإدخال في نظام المعالجة الآلية عن طريق الإضافة بزيادة عبارات أو بيانات غير صحيحة ، أو الحذف بإزالة إحدى البيانات أو الكلمات أو الرموز ، أو بتغيير محتوى الرسائل المنقولة ، فمثلاً قد يقوم الجاني باصطناع بيانات ليس لها وجود وينسبها إلى غير مصدرها كذباً ، أو قد يقوم الجاني بالتدخل في نظام الحاسب الآلي ويقوم بتسجيل بيانات لم تصدر عن المتعاقدين أو إثبات وقائع كاذبة أو غير صحيحة ، أو يقوم الجاني بإغفال معلومة أو إيرادها على وجه غير صحيح مما يسبب تحريفاً للحقيقة في البيانات المسجلة في ذاكرة الحاسب الآلي [47].

وقد نصت العديد من قوانين العقوبات التي جرمت جريمة الإتلاف المعلوماتي على الإدخال الغير المشروع للبيانات والمعلومات كصورة من صور الركن المادي لهذه الجريمة ، ومنها على سبيل المثال قوانين فرنسا ، والسويد ، وهولندا ، واستراليا . كما أشارت المادة (17) من قانون إساءة استخدام الحاسب الآلي في المملكة المتحدة إلى اعتبار إدخال البيانات والمعلومات إلى محتوى وذاكرة الحاسب الآلي باعتباره صورة من صور التعديل الذي يكون الركن المادي لجريمة الإتلاف .

وقد ذهب القضاء الفرنسي إلى اعتبار إدخال البيانات والمعلومات على نحو غير مشروع مكوناً لهذه الجريمة ، حيث قامت محكمة استئناف باريس عام 1990م بإدانة أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بإدخال بيانات غير صحيحة إلى نظام الحاسب الآلي [48].

([46]) ولهذا السبب ظهر اتجاه في العديد من الدول المختلفة يدعو إلى المساواة بين المحررات الورقية ومستخرجات الحاسب الآلي من اسطوانات وشرائط ممغنطة ومما يتم تسجيله في ذاكرة الحاسب الآلي . انظر: السيد عتيق ، جرائم الإنترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2000م . ص 123.

([47]) هلالى عبدالله أحمد ، تفتيش نظم الحاسب الآلي وضمانات المهتم المعلوماتي ، دار النهضة العربية ، 197م ، ص 214 . انظر أيضاً : محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، مرجع سابق ، ص 232 وما بعدها .

([48]) كما أيدت محكمة النقض الفرنسية عام 1994م حكماً بإدانة أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بتدوين بيانات غير صحيحة تتعلق بالنسب الخاصة بالضرائب ثم قيامه بإدخال هذه البيانات إلى نظام الحاسب الآلي . كما ذهبت محكمة جنح باريس عام 1994م إلى إدانة أحد المتهمين بتهمة إتلاف المكونات المنطقية للحاسب الآلي لقيامه بإدخال برنامج " حصان طروادة " وهو برنامج خبيث إلى نظام الحاسب الآلي مما ترتب عليه إتلاف المعلومات والبيانات المخزنة في الحاسب الآلي فضلاً عن إعاقة النظام عن أداء وظيفته . كما ذهبت محكمة النقض الفرنسية في أحد أحكامها الصادرة عام 1999م إلى أن إدخال بيانات يترتب عليها إتلاف لأي من المكونات المنطقية لنظام الحاسب الآلي هو سلوك يعاقب عليه القانون حتى ولو كان للجاني الحق في دخول هذا النظام . انظر محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، مرجع سابق ، ص 236 . انظر أيضاً : نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ،دراسة نظرية وتطبيقية، المرجع السابق . ص 215 وما بعدها .

المطلب الثاني – محو أو تعديل البيانات والمعلومات غير المشروع في نظام المعالجة الآلية للحاسب الآلي :

ويعني محو البيانات تدميرها، أي إتلافها بصورة جزئية أو كلية والتعديل يعني التلاعب في هذه البيانات بشكل يؤثر في قيمتها بحيث يتحقق معنى الإتلاف [49].

ولقد استخدمت جميع القوانين التي جرمت الإتلاف المعلوماتي تعبير محو البيانات والمعلومات للتعبير عن تدمير المعلومات باعتباره صورة متميزة من صور الإتلاف . ويرى البعض أن إخفاء أحد الملفات ، مثلاً ، لا يترتب عليه محو المعلومات التي يحتوي عليها وإنما يؤدي فقط إلى تعديل قائمة الملفات ، وهذا يعني أن إخفاء المعلومات في هذه الحالة هو مجرد تعديل لها وليس تدميراً .

أما بالنسبة لتعديل البيانات والمعلومات غير المشروع فقد فرقت التوصية الصادرة عن المجلس الأوروبي المتعلقة بجرائم المعلوماتية بين التعديلات التي تؤدي على نتائج سلبية تتعلق بحالة البيانات والمعلومات ، وبين التعديلات غير المصرح بها والتي لا تؤدي إلى إحداث هذه النتائج بل قد تساعد على تحسين أي من المكونات المنطقية للحاسب الآلي ونظامه ، وقد تضمنت التوصية بنداً يطالب بإدراج التعديلات الأولى ضمن القائمة الأساسية للجرائم المعلوماتية ، ولكنه اكتفى في خصوص الثانية بإدراجها ضمن القائمة الاختيارية ، إلا أن الدول التي جرمت إتلاف المعلومات لم تأخذ بهذه التفرقة حيث تم تجريم كافة أشكال التعديل [50].

المبحث الثالث – موقف التشريعات الوطنية من جريمة الإتلاف المعلوماتي :

لم تتفق التشريعات الوطنية في الدول المختلفة على طريقة موحدة للتعامل مع جريمة الإتلاف المعلوماتي ، فبعض هذه التشريعات أوجدت قوانين خاصة تتعامل معها ، وأخرى اكتفت بالنصوص الموجودة في القوانين التقليدية ، وسنتناول في هذا المبحث موقف التشريعات في بعض الدول الصناعية من جريمة الإتلاف المعلوماتي إضافة إلى موقف بعض التشريعات العربية في مواجهة جريمة الإتلاف المعلوماتي .

المطلب الأول – موقف تشريعات بعض الدول الصناعية من جريمة الإتلاف المعلوماتي :

أضافت التشريعات في الدول الصناعية حماية للأموال المعنوية من الاعتداء عليها بالإتلاف وقامت بتجريم فعل الإتلاف الواقع على برامج وبيانات الحاسب الآلي . وسنقوم فيما يلي باستعراض جريمة الإتلاف المعنوي في فرنسا والولايات المتحدة الأمريكية وبريطانيا كأمثلة للدول الصناعية في هذا الشأن .

---

[49] هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، المرجع السابق . ص 569 . انظر أيضاً جميل عبدالباقي الصغير ، الإنترنت والقانون الجنائي ، المرجع السابق ، ص 62 . انظر أيضاً : علي عبدالقادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونياً ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، جامعة الإمارات ، العين ، 1- 3 مايو ، 2000م . ص 37 وما بعدها .

[50] محمد أمين الرومي ، جرائم الكمبيوتر والإنترنت ، المرجع السابق ، ص 56 . انظر أيضاً نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية، المرجع السابق ، ص 215 . انظر أيضاً جميل عبدالباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، الكتاب الأول ، الجرائم الناشئة عن استخدام الحاسب الآلي ، المرجع السابق ، ص43. انظر أيضاً : محمد عبدالله أبوبكر سلامة ، جرائم الكمبيوتر والإنترنت ، المرجع السابق ، ص 152 .

1 - الجمهورية الفرنسية :

جرم المشرع الفرنسي تعطيل أو إفساد نظام المعالجة الآلية وإتلاف المعلومات بالمادتين 462 (3) و 462 (4) من القانون رقم (19) لعام 1988م الخاص بجرائم المعلوماتية ، اللتان حلت محلهما المادتان 323 (2) و 323 (3) من قانون العقوبات الفرنسي الجديد إعاقة أنظمة الحاسبات الآلية وإتلاف المعلومات ، وتناولت المادة 462 (3) تعطيل أو إفساد نظام المعالجة الآلية حيث نصت على أنه " يعاقب بالحبس مدة تتراوح بين ثلاثة أشهر وثلاث سنوات وبالغرامة التي تتراوح ما بين عشرة آلاف ومائة ألف فرنك أو بإحدى هاتين العقوبتين كل من عطل أو أفسد متعمداً ، ودون مراعاة لحقوق الغير ، تشغيل نظام المعالجة الآلية للمعطيات " .

أما المادة 462 (4) فقد تناولت إتلاف المعلومات حيث نصت على انه " يعاقب بالحبس مدة تتراوح بين ثلاثة أشهر وثلاث سنوات وبغرامة تتراوح بين 2000 و 500.000 فرنك أو بإحدى هاتين العقوبتين ، كل من أدخل عمداً إلى نظام للمعالجة الآلية للمعلومات ، بطريقة مباشر أو غير مباشر ، وبدون مراعاة لحقوق الغير ، بيانات أو محى أو عدل في البيانات التي يحويها أو في طرق معالجتها أو نقلها " .

وقد أثارت المادتان السابقتين بعض الانتقادات من الفقهاء لما يشوب عبارة " أو بطريق غير مباشر " الواردة في المادة 462 (4) لصعوبة تفسيرها فيما يتعلق بإدخال البيانات أو تعديل طرق معالجتها أو نقلها[51].

كما انتقد هذا الفقه كذلك عبارة " وبدون مراعاة حقوق الغير " الواردة في المادتين حيث أنها تثير الجدل حول ماهية هذه الحقوق التي ينالها الاعتداء ، وهو ما دعا كثير من الفقهاء الفرنسيين إلى اقتراح استبدال عبارة " بدون مراعاة لحقوق الغير " بعبارة " أضراراً بالغير " .

وقد استبعدت المادتان 323 (2) و 323 (3) من قانون العقوبات الفرنسي الجديد عبارة " بطريق مباشر أو غير مباشر " . كما أتى نص المادة 323 (3) والمتعلقة بجريمة الإتلاف المعلوماتي على النحو التالي : " يعاقب بالحبس ثلاث سنوات وبغرامة قدرها 300.000 فرنك كل من أدخل غشاً إلى نظام للمعالجة الآلية للمعلومات بيانات أو قام بمحو أو تعديل البيانات التي يحتوي عليها" . ويلاحظ أن المشرع الفرنسي لم يحدد شروطاً تتعلق بطبيعة المعلومات محل الإتلاف بل ترك النص عاماً ليشمل كافة أنواع المعلومات ، كما أن الطرق المستخدمة في إتلاف المعلومات الواردة به تتسع لتشمل كافة أشكال الاعتداء على المعلومات بما في ذلك استخدام الجاني للبرامج الخبيثة أياً كانت وسائل إدخالها إلى نظام الحاسب الآلي .

أما المادة 323 (2) فقد نصت على أنه " يعاقب بالحبس مدة ثلاث سنوات وبغرامة قدرها 300.000 فرنك كل من قام بإعاقة أو إفساد نظام للمعالجة الآلية للمعلومات " ويتضح لنا أن النص السالف الذكر يتسع ليشمل كل سلوك من شأنه إعاقة النظام سواء كانت هذه الإعاقة كلية أو جزئية أو اقتصرت على مجرد

([51]) عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ، المرجع السابق ، ص 193 وما بعدها . انظر أيضاً : نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ، دراسة نظرية وتطبيقية ، المرجع السابق ، ص 207 وما بعدها .

الإبطاء من سرعة النظام وتقليل فاعليته [52].

فالمشرع الفرنسي عاقب على الدخول بطريق التدليس إلى نظام المعالجة الآلية للمعلومات ، كما قام بالتشديد في عقوبة الجاني إذا نشأ عن هذا الدخول محو أو تعديل في المعطيات المخزنة في النظام أو إتلاف تشغيل النظام . كما عاقب على تعطيل أو إفساد نظام التشغيل . ومن التطبيقات القضائية للقضاء الفرنسي ، ما ذهبت إليه محكمة الاستئناف بإدانة متهم قام بإدخال فيروس إلى أحد أنظمة المعالجة الآلية للمعلومات عن طريق إدخال الفيروس إلى اسطوانات تحتوي على ملخص لبرنامج ، ثم قام بتوزيع هذه الأسطوانات مع أعداد مجلة متخصصة في مجال المعلوماتية وباستخدام هذه الاسطوانة تم نقل الفيروس إلى نظام التشغيل مما أدى إلى إتلاف المعلومات [53].

كما نصت المادة 323 (1) من قانون العقوبات الفرنسي الجديد على أن " الدخول أو البقاء بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية للمعطيات يعاقب عليه بالحبس لمدة سنة وغرامة مقدارها 100.000 فرنك فإذا نتج عن هذا الدخول محو أو تعديل في المعطيات المخزنة في النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها 200.000 فرنك .

2 - الولايات المتحدة الأمريكية :

قام المشرع الأمريكي بتجريم الاعتداء على النظام المعلوماتي وإتلاف البيانات والبرامج ، خاصة في القانون الفدرالي للإحتيال وإساءة استخدام الحاسب الآلي لعام 1984م .

(The Computer Fraud And Abuse Act) (CFAA)

وقانون خصوصية الاتصالات الإلكترونية .

(Electronic Communications Privacy Act (ECPA)

والتي تقع بعد جريمة الدخول غير المشروع إلى النظام المعلوماتي أو البقاء غير المشروع فيه .

ولعل أبرز ما يميز التشريع الأمريكي اكتفاء المشرع الأمريكي بتوافر الصفة المالية للشيء الواقع عليه الإتلاف لقيام الجريمة ، كما لم يتطلب المشرع الأمريكي اشتراط صفة المنقول أو العقار في المال الواقع عليه الفعل التجريمي . ويحظر قانون الاحتيال وإساءة استخدام الحاسب الآلي الدخول غير المشروع إلى الأنظمة المعلوماتية بهدف الاحتيال (Defraud) أو الإتلاف (Damage) ويعاقب هذا القانون إدخال برنامج ، أو أمر يتسبب في إتلاف حاسب آلي محمي [54].

([52]) محمد حماد الهيتي ، جرائم الحاسوب ، المرجع السابق ، ص 199 وما بعدها . نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ، المرجع السابق ، ص 210 وما بعدها .

([53]) جميل عبدالباقي الصغير ، الإنترنت والقانون الجنائي ، المرجع السابق ، ص 62 وما بعدها . انظر أيضاً : سعود وصل الله الثبيتي ، جرائم الكمبيوتر والإنترنت ، ورقة مقدمة لندوة المجتمع والأمن ، الظاهرة الإجرامية المعاصرة ، الاتجاهات والسمات ، كلية الملك فهد الأمنية ، الرياض ، 25- 28 سبتمبر ، 2005م. ص 467 وما بعدها . انظر أيضاً حسام الدين الأهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي ، بحث منشور في مجلة العلوم القانونية والاقتصادية ، العدد الأول ، السنة الثانية والثلاثون ، مطبعة جامعة عين شمس ، القاهرة ، 1990م . ص 38 وما بعدها .

([54]) 18 U. S.C § 1030 (a) (5) (B) (ii) – (V).

كما يحظر هذا القانون أيضاً الدخول غير المشروع والتسبب في الإتلاف [55].

ويعاقب هذا القانون أيضاً كل شخص قام بدون إذن باستخدام حاسب آلي يستخدم في أغراض تجارية أو اتصالات وسبب إتلافاً في استخدام الحاسب الآلي من قبل آخرين ، وذلك إذا كان الإتلاف عن قصد أو عن طريق الخطأ ، وبالتالي فإن هذا القانون يجرم الفعل إذا تسبب في خسائر أو إتلاف بقيمة 1000 دولار أو أكثر لشخص واحد أو أكثر خلال عام واحد ، أو إذا حور أو أتلف اختبارات طبية ، تحليل طبية ، أبحاث طبية لشخص واحد أو أكثر [56].

ولم يشترط هذا القانون أن يكون الضرر أو الإتلاف الناتج مقصوداً ومتعمداً بل يكفي لتحقيق الجريمة أن يتسبب الإهمال (Recklessness) بذلك .

كما جرم هذا القانون إدخال الفيروسات وإتلاف البيانات والمعلومات [57].

أما قانون خصوصية الاتصالات الإلكترونية (ECPA) فيجرم اعتراض أو إعاقة أو حجز أو تعديل الاتصالات الإلكترونية بدون تصريح بقصد القرصنة أو إفشاء الاتصالات الإلكترونية [58].

كما يجرم قانون ولاية كولورادو (Colorado) لمكافحة جرائم الحاسب الآلي (Colorado Computer Crime Act) الجرائم المرتكبة باستخدام الحاسب الآلي أو التي تستهدف الحاسب الآلي لارتكاب جرائم إتلاف أنظمة الحاسب الآلي أو شبكات الحاسب الآلي أو إتلاف البيانات [59].

ويجرم القانون السالف الذكر أيضاً محو البيانات أو تعديلها والدخول غير المصرح به للحاسبات الآلية [60].

---

(55) 18 U. S.C § 1030 (a) (5) (B) (ii) – (V).

See also Leslie Berkowitz, Computer Security and Privacy: The Third Wave of Property Law, Colorado Lawyer , February, 2004. PP 5-9 □

(56) 18 U. S.C § 1030 (C).

(57) 18 U. S.C § 1030 (a) (5) (B) (ii) – (V).

(58) ECPA , Pub.L.No. 99- 508, 100 stat . 1848 (1096) (codified as amended at 18 U.S. C § 2510-2522 – 2701 – 2711)

See also John Samuelson, Information as Property: Do Rucklshous and Carpenter Signal a Changing Direction in Intellectual Property Law? 38 Cath-U-L.Rev. 365,374 (1989).

(59) See , e.g. People. V. Brown, 726 P,. 2d (638) (1986) .

See also , Eric J Sinrod and William P. Reilly, "Cyber Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Computer and High Tech L.J 177, 181-90 (2000). See also Dana L. Bazelon, Computer , Crimes , American Criminal Law Review, Spring 2006 , at 17 , see alse Neal Kumar, Katyal, Criminal Law in Cyberspace, 149 U.Pa. L. Rev 1003, 1015 (2001).

(60) وفي الولايات المتحدة الأمريكية أدانت محكمة ولاية نيوجيرسي (New Jersey) المدعو ديفيد سميث (David Smith) . حيث أسندت إليه تهمة إنتاج فيروس ميلسا (Melisa) الذي اجتاح الولايات المتحدة الأمريكية عام 1999م وتسبب في تعطيل أكثر من مليون جهاز حاسب آلي ، وخسائر مالية قدرت بثمانين مليون دولار ، وتم الحكم عليه وفقاً لفقرة (A) (S) (a) 1030 من هذا القانون الذي يعاقب على إتلاف البرامج والتسبب في الإضرار بأجهزة الحاسب الآلي المحمية (Protected Computers) والتي عرفها ذلك القانون بأنها أجهزة الحاسب الآلي العاملة لدى الحكومة أو لدى المؤسسات المالية والتجارية . وقامت المحكمة بإدانة المتهم سميث (Smith) لإطلاقه هذا الفيروس وصدر بحقه حكم قضائي بسجنه لمدة 5 سنوات وبتغريمه مبلغاً وقدره 250.000 دولار . وبعد طعنه بهذا الحكم تم تخفيفه إلى السجن لمدة ثلاث سنوات مع الغرامة . انظر : 18 U. S.C § 1030 (a) (5) (A.).

انظر أيضاً :

Jeffrey D, Sullivan, and Michael B. De Leeuw, Spam: How Inconsistent Thinking Has Made a Hash out of Unsolicited Commercial E_mail Policy, 20 Santa Clara Computer and High Tech, L.J 887, 891-92 (2004).

3 - المملكة المتحدة :

صدر في المملكة المتحدة قانون إساءة استخدام الحاسبات الآلية لعام 1990م والذي نص في المادة (3) منه على أن " كل من يقوم بفعل من شأنه إحداث تغييرات غير مصرح بها في محتوى أي حاسب آلي ، متى توافر لديه العلم والإرادة وقت قيامه بهذا الفعل " [61]، ورغم أن المادة (3) من ذلك القانون لم تجرم إعاقة أنظمة الحاسبات الآلية كما جرمت إتلاف المكونات المنطقية للحاسب الآلي ، إلا أن المادة (3) أشارت إلى أن اتجاه المتهم إلى إعاقة نظام الحاسب تتوافر به نية إحداث تغيير في محتوى الحاسب الآلي مما يعد مكوناً لجريمة الإتلاف [62].

المطلب الثاني - موقف بعض التشريعات العربية في مواجهة جريمة الإتلاف المعلوماتي :

ونرى أن المشرعين العرب بحاجة إلى نصوص جنائية تجرم صراحة إتلاف المال المعلوماتي المعنوي ، وذلك إعمالاً لمبدأ المشروعية ومبدأ التفسير الضيق لنصوص القانون الجنائي ، وبما يتناسب مع التطور التقني في مجال المعلوماتية، خصوصاً مع وجود حالات تثار فيها مسألة إتلاف بعض أدوات الحاسب الآلي بشكل يؤثر في برامجه ومعلوماته وبياناته، فقد يتم الإتلاف بكسر أو تخريب الاسطوانة المخزن عليها البرنامج ، أو قد يتم محو البرنامج أو البيانات بشكل فني ودون أن تتأثر الأسطوانة أو تصاب بسوء كأن يتم وضع مادة عليها تؤدي إلى محو البرنامج أو تعطيله أو تعريض الأسطوانة لقوى مغناطيسية من شأنها إفساد هذه البرامج والبيانات مما يؤدي إلى التأثير في قيمتها ووظائفها وهو ما يعد إتلافاً لها .

ولم تتناول غالبية الدول العربية جريمة الإتلاف المعلوماتي ، واكتفت غالبية التشريعات العربية بالنصوص الموجودة في القوانين التقليدية ، ولم تفرز غالبية التشريعات العربية قوانين خاصة للتعامل مع جريمة الإتلاف المعلوماتي فيما عدا المملكة العربية السعودية وسلطنة عمان .

([61]) وقد ذهب القضاء في المملكة المتحدة في تطبيق المادة (3) في الحالة التي قام فيها موظف بإدخال برنامج خبيث إلى نظام الحاسب الآلي للشركة التي يعمل بها ، والمصرح له بالدخول إليه ، مما تسبب في إحداث إتلاف للمعلومات والبرامج التي يحتوي عليها النظام . وقد قامت المحكمة بتطبيق نص المادة (3) من قانون إساءة استخدام الحاسبات الآلية على الرغم من أن المتهم المذكور كان مصرح له بالدخول إلى نظام الحاسب الآلي الذي قام بإتلاف معلوماته وبرامجه .

انظر أيضاً :

Martin Wasik, The Computer Misuse Act 1990, Crime L.J., 1990 P 767.

انظر أيضاً :

Neal Kumar Katyal, Criminal Law in Cyber Space, 149 U.Pa. L. Rev 1003, 1013

انظر أيضاً :

David Bainbridge, Introduction to Computer, Law Fourth Edition, Longman, London, 2000, at 34.

([62]) محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، المرجع السابق ، ص 218 وما بعدها . انظر أيضاً نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ، المرجع السابق ، ص 210 وما بعدها . انظر أيضاً محمد أمين الرومي ، جرائم الكمبيوتر والإنترنت ، المرجع السابق ، ص 42 . انظر أيضاً محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، المرجع السابق ، ص 18 ، انظر أيضاً السيد عتيق ، جرائم الإنترنت ، المرجع السابق ، ص 20 وما بعدها . انظر أيضاً مدحت رمضان ، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية ، القاهرة ،2000م. ص 51 وما بعدها. انظر أيضاً : مدحت رمضان ، جرائم الاعتداء على الأشخاص والإنترنت ، دار النهضة العربية ، القاهرة ، 2000م ، ص 51 وما بعدها . انظر أيضاً : علي عبدالقادر القهوجي ، الحماية الجنائية لبرامج الحاسب ، المرجع السابق ، ص 32 . انظر أيضاً : عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، المرجع السابق ، ص 23 . انظر أيضاً : جميل عبدالباقي الصغير ، القانون الجنائي التكنولوجيا الحديثة ، المرجع السابق ، ص 43 .

وفيما يلي نتعرض بالشرح لبعض التشريعات العربية وموقفها من جريمة الإتلاف المعلوماتي :

1- جمهورية مصر العربية :

نص المشرع المصري على جريمة الإتلاف في المادة 361 من قانون العقوبات المصري بأن " كل من خرب أو أتلف عمداً أموالاً ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تتجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين ، فإذا ترتب على الفعل ضرر مالي قيمته خمسون جنيهاً أو أكثر كانت العقوبة الحبس مدة لا تتجاوز السنتين وغرامة لا تتجاوز خمسمائة جنيه أو بإحدى هاتين العقوبتين .

وتكون العقوبة السجن مدة لا تزيد على خمس سنوات وغرامة لا تقل عن مائة جنيه ولا تتجاوز ألف جنيه إذا نشأ عن الفعل تعطيل أو توقيف أعمال مصلحة ذات منفعة عامة ، أو إذا ترتب عليه جعل حياة الناس أو صحتهم أو أمنهم في خطر ، ويلاحظ أن المشرع المصري لم يقيد النشاط الإجرامي في هذه الجريمة بوسيلة معينة ، ويلاحظ أيضاً على النص السابق أن المشرع لم يجرم نتيجة معينة ، وإنما جرم التخريب والإتلاف وعدم الصلاحية للاستعمال والتعطيل، ويكفي تحقيق إحدى هذه النتائج الأربعة بالفعل للقول بتحقق الجريمة .

وقد تناول المشرع المصري الإتلاف إذا ما وقع على مال ثابت أو منقول مملوك للغير ، فإذا وقع الإتلاف على جهاز الحاسب الآلي أو أدواته أو الأجهزة المتصلة به أو الأشرطة أو الأقراص الممغنطة أو الدعامات أو غيرها مما يختص بالمعلومات وله كيان مادي فهنا لا تثور أي مشكلة قانونية في تطبيق النصوص التقليدية المتعلقة بجريمة الإتلاف على اعتبار أن محل الجريمة مملوك للغير[63].

ولكن المشكلة تثور بخصوص المعلومات والبيانات المخزنة بداخل جهاز الحاسب الآلي والتي يتم إتلافها كنتيجة لإتلاف الحاسب الآلي أو ملحقاته أو إتلاف المعلومات لوحدها دون المساس بالأشياء المادية ، فهل تسري النصوص التقليدية الخاصة بالإتلاف على المعلومات والبيانات المخزنة بجهاز الحاسب الآلي إذا ما تلفت بإتلاف الجهاز الذي يحتويها ؟ ، أو إذا تم إتلافها بصورة مباشرة عن طريق برامج الفيروسات والديدان والقنابل المنطقية والزمنية ؟ ، وقد اختلف الفقه المصري حول تقييد أو إطلاق المشرع للنصوص المتعلقة بجريمة الإتلاف للقول بانطباقها على الأموال المعنوية إلى جانب الأموال المادية . فذهب رأي إلى أن جريمة الإتلاف لا تقع إلا على الأموال المادية دون المعنوية فلا يدخل إتلاف المعلومات ضمن التجريم المنصوص عليه في النصوص التقليدية المتعلقة بالإتلاف [64].

([63]) هدى حامد قشقوش ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق ، ص 558 . انظر أيضاً : محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، دراسة مقارنة ، المرجع السابق ، ص 215 وما بعدها .

([64]) جميل عبدالباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، المرجع السابق ، ص 156.

وذهب الرأي الآخر إلى القول بان المشرع نصَّ على أموال ثابتة أو منقولة وهي لا تقتصر فقط على الأموال المادية ، بل تشمل أيضاً الأموال المعنوية . وكذلك المعلومات المخزنة في الحاسب الآلي فهي جزء لا يتجزأ من هذا الجهاز[65].

ونرى ضرورة تدخل المشرع المصري للنص بتجريم إتلاف البيانات والمعلومات، لينأى عن هذا الخلاف ولينأى عن المساس بمبدأ الشرعية ، ومبدأ التفسير الضيق للنصوص الجنائية[66].

كذلك تنص المادة (74) من القانون رقم (143) لعام 1994م في شأن الأحوال المدنية على أنه " مع عدم الإخلال بأية عقوبة منصوص عليها في قانون العقوبات أو غيره من القوانين يعاقب بالحبس مدة لا تتجاوز ستة أشهر وبغرامة لا تزيد على خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من أطلع أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وثائق التخزين الملحقة بها أو قام بالإضافة أو بالحذف أو بالإلغاء أو المساس بها بأي صورة من الصور " .

كما تنص المادة (75) من ذات القانون " يعاقب الحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن مائتي جنيه ولا تزيد على خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من عطل أو أتلف الشبكة الناقلة لمعلومات الأحوال المدنية أو جزء منها ، وكان ذلك ناشئاً عن إهماله أو رعونته أو عدم احترازه أو عدم مراعاته للقوانين واللوائح والأنظمة " .

2 - المملكة الأردنية الهاشمية :

جرّم المشرع الأردني فعل الإتلاف في المادة (445) من قانون العقوبات الأردني حيث نصت هذه المادة على أن " كل من الحق باختياره ضرراً بمال الغير المنقول ، يعاقب بناء على شكوى المتضرر بالحبس مدة لا تتجاوز سنة أو بغرامة لا تتجاوز خمسين ديناراً أو بكلتا العقوبتين ".

ولم يتطرق المشرع الأردني لجرائم الحاسب الآلي والإنترنت في تشريع مستقل ، ولكن قانون الاتصالات الأردني لعام 1995م في المادة (72) منه ينص على " معاقبة كل من أقدم على تخريب منشآت الاتصالات أو ألحق بها ضرراً إذا تسبب فعله بتعطيل حركة الاتصالات" كما نصت المادة (80) من القانون السالف الذكر على أن " كل من قام متعمداً باعتراض موجات مخصصة للغير أو بالتشويش عليها أو باستخدام موجبات

---

(65) عبدالقادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، المرجع السابق . ص 111 وما بعدها. انظر أيضاً : أسامة بن غانم العبيدي ، جرائم الحاسب الآلي والإنترنت ، الصعوبات التي تواجه المكافحة، المرجع السابق ، ص 90 وما بعدها . انظر أيضاً : عفيفي كامل عفيفي ، جرائم الكمبيوتر ، وحقوق المؤلف والمصنفات الفنية ، المرجع السابق ، ص 188 وما بعدها .

(66) كما أنه من المتصور ظهور جرائم أخرى لا تستطيع النصوص القانونية التقليدية التفاعل معها أو مواجهتها خصوصاً مع التطور التقني السريع في المجال المعلوماتي . انظر : عبدالقادر القهوجي ، الحماية الجنائية لبرامج الحاسب ، المرجع السابق ، ص 61 . انظر أيضاً : أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دراسة مقارنة ، دار النهضة ، القاهرة ، الطبعة الثانية ، 1992م ص 12 وما بعدها . انظر أيضاً : أسامة بن غانم العبيدي ، حماية الحق في الحياة الخاصة في مواجهة جرائم الحاسب الآلي والإنترنت ، المجلة العربية للدراسات الأمنية والتدريب، المجلد 23، العدد 46 ربيع الآخر 1429هـ ، السنة 23 ، ص 82 وما بعدها .

كهرومغناطيسية بدون ترخيص يعاقب بالحبس مدة لا تزيد عن ستة أشهر أو بغرامة لا تقل عن 50 دينار ولا تزيد على 200 دينار أو بكلتا العقوبتين".

ويلاحظ أن نصوص قانون الاتصالات الأردني تنطبق على شبكة الإنترنت وشبكات الاتصالات الداخلية ، وبالتالي فأي تعطيل أو إعاقة لحركة الاتصالات سواء بالدخول إلى نظم المعلوماتية أو بتشويشها أو التأثير عليها دون الدخول إلى النظام المعلوماتي يدخل ضمن نطاق النص[67].

3 - المملكة العربية السعودية :

أقرت المملكة العربية السعودية نظامي التعاملات الإلكترونية ومكافحة الجرائم المعلوماتية ، وقد نص نظام مكافحة الجرائم المعلوماتية في المادة (2) منه على أنه " يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية ، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها ، وبها يؤدي إلى ما يأتي :

1- المساعدة على تحقيق الأمن المعلوماتي .
2- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية .
3- حماية المصلحة العامة ، والأخلاق ، والآداب العامة .
4- حماية الاقتصاد الوطني " [68].

كما نص هذا النظام في الفقرة (3) من المادة (3) منه على أنه " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال ، أو بإحدى هاتين العقوبتين ، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1- الدخول غير المشروع إلى موقع إلكتروني ، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع ، أو إتلافه ، أو تعديله ، أو شغل عنوانه " .

ونص نظام مكافحة الجرائم المعلوماتية في المادة الخامسة منه على إنه : " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، أو بإحدى هاتين العقوبتين ، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

1- الدخول غر المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها ، أو إتلافها ، أو تغييرها، أو إعادة نشرها .
2- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها ،أو تدمير،أو مسح البرامج، أو البيانات الموجودة ، أو المستخدمة فيها ، أو حذفها ،أو تسريبها ، أو إتلافها أو تعديلها .
3- إعاقة الوصول إلى الخدمة ، أو تشويشها ، أو تعطيلها ، بأي وسيلة كانت " .

كما نصت المادة (8) من هذا النظام على أنه " لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية :

([67]) محمود أحمد عبابنه ، جرائم الحاسوب وإبعادها الدولية ، المرجع السابق ، ص 104 وما بعدها . انظر أيضاً : محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، المرجع السابق ، ص 220 وما بعدها .

([68]) نظام مكافحة الجرائم المعلوماتية الصادر بقرار مجلس الوزراء رقم (79) وتاريخ 1428/3/7هـ .

1- ارتكاب الجاني الجريمة من خلال عصابة منظمة .
2- شغل الجاني وظيفة عامة ، واتصال الجريمة بهذه الوظيفة ، أو ارتكابه الجريمة مستقلاً سلطاته أو نفوذه .
3- التغرير بالقُصّر ومن في حكمهم ، واستغلالهم .
4- صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة .

كما عاقب هذا النظام " كل من حرض غيره ، أو ساعده ، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام ، إذا وقت الجريمة بناء على هذا التحريض ، أو المساعدة ، أو الاتفاق ، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية " [69].

ويعاقب هذا النظام أيضاً على حالات الشروع في القيام بأي من الجرائم المنصوص عليها فيه بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة . وهذا أمر يحسب للنظام ومن شأنه الحد من ارتكاب الجرائم التي يعاقب عليها النظام[70].

كما ينص نظام مكافحة جرائم المعلوماتية على جواز الحكم بمصادرة الأجهزة، أو البرامج ، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام أو الأموال المتحصلة منها ، كما يجوز الحكم بإغلاق الموقع الإلكتروني ، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكه ، كما نص النظام في المادة (14) منه على أن " تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة " . ونص أيضاً في المادة (15) منه على أن تتولى هيئة التحقيق والإدعاء العام التحقيق والإدعاء في الجرائم الواردة فيه .

كذلك قامت المملكة بإصدار ضوابط تطبيق التعاملات الإلكترونية الحكومية ، والتي نصت في المادة (21) منها على أنه " تقوم كل جهة حكومية بحماية معلوماتها وبياناتها وأنظمتها المعلوماتية وفق المعايير العالمية ذات العلاقة ، وحسب معايير استرشادية يعدها برنامج التعاملات الإلكترونية الحكومية لهذا الغرض" . كما أكدت هذه الضوابط على جميع الجهات الحكومية بأن تتفادى الازدواجية والتكرار في قواعد المعلومات والبيانات وأن يقوم برنامج التعاملات الإلكترونية الحكومية بالتنسيق مع الجهات الحكومية الأخرى من أجل تكامل المعلومات والبيانات ، بحيث تكون هناك جهة واحدة مسؤولة عن حفظ المعلومات والبيانات ذات النوع الواحد بحسب الاختصاص ، وبما يضمن عدم التكرار والازدواجية ، وتضارب المعلومات والبيانات وتعدد مصادرها ، وبما لا يخل بوجود نسخة احتياطية لكل قاعدة معلومات وبيانات [71].

ونرى أن هذا من شأنه تقليل الضرر في حال حدوث إتلاف لهذه المعلومات والبيانات .

([69]) م (9) ، نظام مكافحة الجرائم المعلوماتية .

([70]) م (10) ، نظام مكافحة الجرائم المعلوماتية .

([71]) ضوابط تطبيق التعاملات الإلكترونية الحكومية ، الصادر بقرار مجلس الوزراء رقم (40) وتاريخ 1427/2/27هـ .

الخاتمة :

تعرضنا في هذا البحث لموضوع جريمة الإتلاف المعلوماتي لما لهذا الموضوع من أهمية كبيرة . وقد تم التوصل في نهاية هذا البحث إلى النتائج والتوصيات التالية :

أولاً : النتائج :

1- أدى انتشار استخدام الحاسب الآلي والإنترنت إلى إنتاج صور مستحدثة للجرائم من حيث أنواعها والوسائل المرتكبة بها ، وهذه الصور لا تنطبق والنصوص القانونية للجرائم في قوانين العقوبات .

2- أن جرائم الحاسب الآلي ومنها جريمة الإتلاف المعلوماتي تستهدف مال معنوي وليس مال مادي ملموس ، وتثير في هذا مشاكل تتعلق بحماية المال المعلوماتي .

3- أن إتلاف المعلومات والبيانات لا بد أن يكون عمدياً . أما الباعث عليه فلا أهمية له حتى ولو كان لتحقيق مصلحة مشروعة .

4- تختلف تشريعات الدول المختلفة في التعامل مع جرائم الحاسب الآلي والإنترنت ومنها جريمة الإتلاف المعلوماتي ، فهناك دول وضعت قوانين خاصة لمكافحة جرائم الحاسب الآلي والإنترنت مثل الولايات المتحدة الأمريكية وبريطانيا وفرنسا ومن الدول العربية المملكة العربية السعودية وسلطنة عمان . كما أن هناك دولاً ليس لديها قوانين لمكافحة جرائم الحاسب الآلي والإنترنت ، ولم تفرد قوانين خاصة تتعامل معها وهو حال غالبية دول العالم الثالث ومنها الدول العربية .

5- يوجد قصور في القوانين الداخلية في العديد من دول العالم تتعلق بإقامة المسئولية الجنائية بحق مرتكبي تلك الجرائم ومعاقبتهم .

ثانياً : التوصيات :

1- ضرورة قيام دول العالم المختلفة بإستحداث تشريعات خاصة لمعالجة استخدام الحاسب الآلي والإنترنت لارتكاب جرائم إتلاف المعلومات والبيانات والتحقيق فيها ، واكتشاف الأدلة واستخدامها أمام المحكمة لإدانة الجاني ، فالنصوص التقليدية الخاصة بإتلاف الأموال لا يمكن تطبيقها في مجال المعلوماتية ، ما لم ينصب الإتلاف على الحاسب الآلي ذاته أو أي من مكوناته المادية .

2- ضرورة تجريم الأفعال العمدية المنطوية على تعديل أو تدمير أو إخفاء أو محو المعلومات والبيانات المبرمجة آلياً ، مما ينتج عنه إتلاف هذه المعلومات والبيانات أو إتلاف الأنظمة التي تحتوي عليها . وسواء كان هذا الإتلاف دائم أو مؤقت أو كان كلياً أو جزئياً ، ويهدف التجريم هنا إلى المحافظة على سلامة معلومات وبرامج وبيانات الحاسب الآلي .

3- ضرورة العمل على تأهيل رجال الشرطة والمحققين والقضاة وتكوين المعرفة لديهم للتعامل مع الجوانب المختلفة بجرائم المعلوماتية .

4- ضرورة التعاون الدولي في مجال مكافحة جرائم الحاسب الآلي والإنترنت حيث أن مكافحة هذا النوع من الجرائم العابرة للحدود لن يكون له التأثير المطلوب إلا إذا كان هناك تعاون دولي في مكافحتها .

5- ضرورة عقد اتفاقيات ومعاهدات دولية لمكافحة هذه الجرائم والمبادرة إلى الانضمام إليها .

المراجـــــع :

المراجع العربية :

أولاً: الكتب والمقالات

1- الأهواني ، حسام الدين ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي ، بحث منشور في مجلة العلوم القانونية والاقتصادية ، العدد الأول، السنة الثانية والثلاثون ، مطبعة جامعة عين شمس ، القاهرة ، 1990م .
2- أحمد ، هلالي عبداللاه ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، دار النهضة العربية ، 1997م .
3- البشرى ، محمد ، التحقيق في جرائم الحاسب الآلي والإنترنت ، المجلة العربية للدراسات الأمنية والتدريب ، المجلد 15 ، العدد 30، أكاديمية نايف العربية للعلوم الأمنية ، نوفمبر 2000م .
4- الثبيتي ، سعود وصل الله ، جرائم الكمبيوتر والإنترنت ، ورقة مقدمة لندوة المجتمع والأمن ، الظاهرة الإجرامية المعاصرة ؛ الاتجاهات والسمات ، كلية الملك فهد الأمنية ، الرياض 25- 28 سبتمبر 2005م.
5- حسني ، محمود نجيب ، شرح قانون العقوبات ، القسم الخاص، دار النهضة العربية ، القاهرة ، 1986م .
6- حجازي ، عبدالفتاح ، مكافحة جرائم الكمبيوتر والإنترنت ، دراسة معمقة في القانون المعلوماتي ، ط 1، دار الفكر الجامعي، الإسكندرية ، 2006م .
7- الحسيني ، عمر الفاروق ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية،دار النهضة العربية، القاهرة،1995م .
8- الحفناوي ، فاروق علي ، قانون البرمجيات ، دراسة معمقة في الأحكام القانونية لبرمجيات الكمبيوتر ، الكتاب الأول ، دار الكتاب الحديث ، القاهرة ، 2001م .
9- رستم ، هشام فريد ، الجرائم المعلوماتية ، مجلة الأمن والقانون ، دبي، العدد (2) ، 1999م .
10- رستم ، هشام فريد ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، أسيوط ، 1994م .
11- الرومي ، محمد أمين ، جرائم الكمبيوتر والإنترنت ، دار المطبوعات الجامعية ، الإسكندرية ، 2003م .
12- رمضان ، مدحت ، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية ، القاهرة ، 2000م .
13- سلامة ، محمد عبدالله ، جرائم الكمبيوتر والإنترنت ، منشأة المعارف، الإسكندرية ، 2002م .
14- سلامة ، عماد ، الحماية القانونية لبرامج الحاسب الآلي ، الطبعة الأولى، دار وائل للنشر ، عمان ، 2005م .
15- الشوابكة ، محمد أمين ، جرائم الحاسوب والإنترنت ، دار الثقافة للنشر والتوزيع ، عمان 2004م.
16- الشوا ، محمد ثورة المعلومات وانعكاساتها على قانون العقوبات ، ط2، دار النهضة العربية ، القاهرة ، 1998م .
17- الصغير ، جميل عبدالباقي ، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول : الجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية ، القاهرة ، 1992م .
18- الصغير ، جميل عبدالباقي ، الإنترنت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، 2002م .
19- العبيدي ، أسامة بن غانم ، جرائم الحاسب الآلي والإنترنت ، الصعوبات التي تعترض المكافحة ، دورية الإدارة العامة ، معهد الإدارة العامة ، المجلد الثامن والأربعون، العدد الأول، يناير 2008م.

20- العبيدي ، أسامة بن غانم ، حماية الحق في الحياة الخاصة في موجهة جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد 23 ، العدد 46 ، ربيع الآخر 1429هـ .
21- عبابنة ، محمود أحمد ، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع ، عمان ، 2005م .
22- عفيفي ، كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ، بدون ناشر ، بدون تاريخ .
23- عبدالله ، عبدالكريم عبدالله ، جرائم المعلوماتية والإنترنت ، الجرائم الإلكترونية ، منشورات الحلبي الحقوقية ، بيروت ، 2007م .
24- عمار ، ماجد ، المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها ، دار النهضة العربية ، القاهرة ، 1989م .
25- عتيق ، السيد ، جرائم الإنترنت ، دار النهضة العربية ، القاهرة ، 2000م .
26- فضل ، سليمان أحمد ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية ، دار النهضة العربية ، القاهرة ، 2007م .
27- فريد ، هشام حمد ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، أسيوط ، 2000م .
28- فتحي ، محمد أنور عزت ، الحماية الجنائية الموضوعية والإجرائية: الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2007م .
29- قورة ، نائلة عادل ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، الطبعة الأولى ، بيروت ، 2005م .
30- قشقوش ، هدى حامد ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد بالقاهرة في الفترة من 25- 28 أكتوبر، 1993م .
31- القهوجي ، علي عبدالقادر ، الحماية الجنائية لبرامج الحاسب الآلي ، الطبعة الأولى ، الدار الجامعية للطباعة والنشر ، بيروت ، 1992م .
32- القهوجي ، علي عبدالقادر ، الحماية الجنائية للبيانات المعالجة إلكترونياً بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، جامعة الإمارات، العين ، 1- 3 مايو 2000م . .

ثانياً : القوانين والضوابط :

1) نظام مكافحة الجرائم المعلوماتية الصادر بقرار مجلس الوزراء رقم (79) وتاريخ 1428/3/7هـ .
2) ضوابط تطبيق التعاملات الإلكترونية الحكومية ، الصادر بقرار مجلس الوزراء رقم (40) وتاريخ 1427/2/27هـ.

ثالثاً : الصحف :

1- جريدة الرياض ، ملحق الرياض الاقتصادي ، 2 أغسطس ، 2008م ، العدد 14649 ، السنة الخامسة والأربعون ، ص 7 .

المراجع الأجنبية :

1. Bainbridge, David, Introduction to Computers, Fourth Edition, Longman, London, 2000, at 34.
2. Berkowitz, Leslie, Computer security and privacy: The third wave of Property Law, Colorado Lawyer 2004. PP 6-8.
3. Brown, Jack E, Jurisdiction to Prosecute Crimes committed By Use of The Internet, Jurimetrics Journal, Summer, 1998 Symposium, 1998. PP 575-580.
4. Conley, John and Robert Bryan, A Survey of Computer Crime Legislation in The United States, Information and Communications, Technology Law, Vol 8, 1, 1999.
5. Falvey, John J, and Amy M. McCallen, A Survey of Internet crime Targeting Multiple Computers, Albany Law Journal, 2006 PP 22-27.
6. Forrett, Nichoel, Cookie Monster: Balancing Internet Privacy With Commerce, Technology, And Terrorism, Touro Law Review, 2004 at 3-5.
7. Friedman, Marc, Infojacking: Crimes on the Information Super Highway, S.J. Proprietary Rts, 2,2,1997.
8. Katyal, Neal Kumar, Criminal Law in Cyber Space, 149 U.Pa. L. Rev 1003, 1013 (2001).
9. Lange, Larry, Trust a Hacker under 30? You'd better, ELEC. Eng' Times, August, 19, 1996.
10. Rosen, Jeffery, the Unwanted Gaze, The Destruction of Privacy in America 167, Vintage Books, 2001 at 167-169.
11. Samuelson,John, Information As Property: Do Rucklshous and Carpenter Signal A Changing Direction in Intellectual Property Law? 38 Cath-U-L.Rev. 365,374.
12. Sharp, Walter, Gary, Redefining National Security in Today's World of Information Technology and Emergent Threats, 9 Duke J Comp and Int'l 383-384 (1999).
13. Sinrod, Eric J and William P Reilly, "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Computer and High Tech L.J 177, 181-90 (2000).
14. Sullivan, Jeffrey D, and Michael B. DeLeeuw, Spam : How Inconsistent Thinking Has Made A Hash Cut of Unsolicited Commercial Email policy, 20 Santa Clara Computer and High Tech, L.J 887, 891-92 (2004).
15. Wasik, Martin, The Computer Misuse Act 1990, Crime L.J., 1990 P 767.
16. Whalen, David, The Unofficial Cookie FAQ Version, at http://www.cookiecentral.com/faq.
17. Wise, Edward, Computer crimes and Others Against Information Technology in The United States, RI S.P. 1993, at 652-654.□