

النظام القانوني للفيروس المعلوماتي

فتيحة حزام: أستاذة محاضرة ب

كلية الحقوق - جامعة أمحمد بوقرة بومرداس

ملخص

تناقش هذه الدراسة أهمية بعض الكيانات الغير مادية التي طالما صنفتم ضمن الأشياء المعنوية كونها تعد عملا ذهنيا خالصا وخصوصا بصاحبه، والتي أصبحت في الوقت الحالي تضم عدة مخاطر لا سيما المرتبطة منها بالتكنولوجيات الحديثة للإعلام والاتصال وتحديدًا منها الفيروس المعلوماتي الذي بات يشكل نظاما قانونيا جديدا نظرا للخصائص التقنية والطبيعة القانونية المتميزة التي يتمتع بها، فضلا عن تأثيره على مختلف المجالات الحيوية ناهيك عن الخسائر المادية والمالية الضخمة المنجرة عن انتشاره فيها، الأمر الذي استدعى ضرورة توخي الحيطة والحذر من النتائج الخطيرة التي يسببها إذا اجتاحت منظومة إعلامية خاصة بالنشاطات التجارية والمالية التابعة للدولة، لذا فقد توصل الفقه الحديث إلى ضرورة إعتبره ضمن الأشياء المادية الخطيرة والتوسع في تحديد المسؤولية الناشئة عن الأشياء. تأسيسا على ذلك، يتطلب الأمر ضرورة تدخل المشرع الجزائي نحو إعادة النظر في تعريفه للأشياء وعدم الإكتفاء بالتوسع في إدراج مفهوم الفيروس المعلوماتي ضمن الأشياء التي حددتها أحكام القواعد العامة والعمل على إيجاد إطار قانوني خاص به.

الكلمات المفتاحية: إلكتروني - فيروس معلوماتي - قانون إلكتروني - نظام قانوني - ملكية فكرية - المعلوماتية.

Abstract

This study is an attempt to discuss the importance of some unmaterial entities, which has for a long time classified among the moral stuff because they are considered as a pure and special mental work, and which include today a lot of risks and specially those associated with modern technologies for information and communication, and specifically the informational virus which has

become a new legal system because of the technical characteristics and the distinct legal nature that enjoyed by, as well as its effect on various intical areas, not to mention the huge material and financial losses caused by its spread it has necessitated the need for caution and beware of the serious consequences caused if swept media system concerning business and financial activities of state. So modern jurisprudence, that has come to the need to be considered within the serious physical stuff and the expansion of the limitation of liability arising ontif the stuff. Based on this, it will be necessary to enter the algerian legislature to reconsider its definition of stuff and not satisfied with the escpansion of the inclusion of the concept of the informational virus within stuff that defined by the provisions of general rules and work to fin dits own legal framework.

مقدمة

إنّ ظاهرة الفيروس المعلوماتي ليست جديدة بل تعود إلى نهاية الأربعينات، وقد يكون أحد أول الاختصاصيين في علم الكمبيوتر (جون فون نيومان) هو أول من فكر بالأمر فقد نشر مقالا حول الموضوع في سنة 1949 تحت عنوان "نظرية التعقيد الأوتوماتيكي"¹.

يهدف الفيروس المعلوماتي للإتلاف الإلكتروني لعناصر المنظومة المعلوماتية عن طريق التلاعب ببياناتها من خلال افتتاح المواقع وتدميرها والعبث بمحتوياتها بإزالتها أو الإستيلاء عليها بهدف تعطيلها عن العمل لأطول فترة ممكنة أو تدميرها نهائيا، ولقد ظهرت بعض عوارض الفيروس في أوائل الخمسينات ألا أنها بقيت محدودة لان أجهزة الحاسب لم تكن مرتبطة ببعضها في تلك الفترة وبالتالي لم يكن لها انتشار واسع، وبقي الأمر على ما هو عليه حتى سنة 1983 عندما تفشى الفيروس في نظام التشغيل UNIX حيث ظهرت بعض الأحداث الفردية للهواة من صغار المبرمجين قاموا بزرع فيروسات في شبكات الحاسب لشركات تتعامل في مجالات علمية وتطبيقية حساسة، فقد قام أحد الطلبة بالسنة النهائية بجامعة ويسكونسن الأمريكية بإعداد برنامج المدمر الذي عطل نظام الحاسوب التابع للجامعة متعمدا ولأكثر من مرة، بغية تدمير المشروعات النهائية لعشرات الطلبة، وقد حكم عليه القاضي بعقوبة الحبس لمدة سنة واحدة مع إيقاف التنفيذ ومغادرة الجامعة.²

لقد كان من الصعوبة بمكان تحديد نشأة الفيروس المعلوماتي³ ، لذا إعتبر عام 1978 أو قبلها بقليل بداية لظهوره ، كما أن مشكلة الفيروس بدأت تتعقد مع استخدام البريد الإلكتروني باستخدام وسائل الاتصالات التي أدت إلى ربط عدد من أجهزة الحاسب بشبكة والاتصال من خلالها من قبل الآلاف المستخدمين الذين يشتركون في نظام الحاسب وعبر مسافات بعيدة جدا⁴ .

أصبح للفيروس المعلوماتي أهمية بالغة في وقتنا الحالي لدى الفقهاء من جهة ولدى مستعملي التكنولوجيات الحديثة من جهة أخرى ، حيث إلى جانب خطورته المتعددة الأشكال ، باعتباره من بين الأسباب المؤدية لإتلاف البرامج المعلوماتية دون التمكن من التنبؤ بتلك الهجمات التي تتم بسرعة فائقة ولا يمكن مقاومتها نظرا لطابعها المفاجئ الذي يعتمد أساسا على الذكاء المعلوماتي ، فقد أدى إلى ظهور قواعد ومبادئ مخالفة لتلك التي كانت سائدة ضمن القواعد الكلاسيكية.

تهدف الدراسة لتبيان خصوصية الأشياء المتعلقة بالإنترنت لا سيما ما يتعلق بالفيروس المعلوماتي ومدى خطورته ، فضلا عن كونه من المواضيع التي يطغى عليها الجانب التقني ، لذا فإن موضوع الدراسة لا يخلو من بعض الصعوبات نظرا للصيغة التقنية التي يتمتع بها والتي نحصرها في صعوبة تحديد طبيعته القانونية باعتباره بالأصل شيئا معنويا ، حيث أنه و مع ظهور التكنولوجيات الجديدة للإتصال فرضت معاملات من نوع خاص فشاع الإتجار بأشياء غير المادية كبيع وشراء البرامج المعلوماتية عبر الفضاء الإلكتروني باستخدام مختلف الوسائط الإلكترونية المتاحة عبره ، فالفيروس قد لا يضرب برنامجا معينا ، بل ينتقل إلى كافة البرامج على ذاكرة الحاسب الآلي ويدمر الجهاز بأكمله ، وينتقل عبر الشبكات والأقراص ، كذلك هناك ما يسمى القنابل الموقوتة ، وهي برامج يتم إدخالها بطرق مشروعة مخفية غالبا عن طريق موظفين شرعيين مع برامج أخرى وتهدف إلى تدمير وتغيير برامج ومعلومات النظام.

تأسيسا على ما سبق بيانه ، وفي ظل غياب أطر قانونية خاصة نظرا لخطورته ، استوجب طرح الإشكالية التالية: هل يمكن إيجاد معايير لتحديد الطبيعة القانونية للفيروس المعلوماتي؟ وهل يمكن لأحكام القواعد العامة المنظمة لمفهوم الأشياء استيعاب خصوصياته؟ من أجل الإجابة عن ذلك ولمعالجة الموضوع إختارنا الإعتماد على المنهج الوصفي مع الإستعانة بالمنهج الإستدلالي الذي تم توظيفه بغرض محاولة إيجاد نظم قانونية مشابهة للفيروس المعلوماتي ومن ثم محاولة إسقاط أحكامها عليه ،

حيث قسمنا الدراسة لمبحثين، خصصنا المبحث الأول للإطار المفاهيمي للفيروس المعلوماتي، أما المبحث الثاني فنتطرق فيه لتحديد طبيعته القانونية.

المبحث الأول: الإطار المفاهيمي للفيروس المعلوماتي

مما لا شك فيه، أنّ الفيروس المعلوماتي لا يأتي من مصدر مجهول ولا ينشأ بسبب خلل بسيط حدث في الحاسوب، بل هو نظام يتم برمجته من قبل المبرمجين أو الشركات ويتم صنعه بشكل متعمد ويتم تصميمه بشكل متقن، يعمل المبرمجون على برمجة الفيروسات وذلك لأهداف عديدة تتنوع من اقتصادية وسياسية وتجارية وعسكرية، فبعض المبرمجين الهواة يعتبرون أن عمل الفيروس نوع من الفن والهواية التي يمارسونها، فمن أهم الأهداف لعمل فيروس الحاسوب هو الهدف التجاري، ذلك عن طريق عمل وصنع الفيروسات من أجل بيع برامج مضادات الفيروسات لأنه بعمل الفيروس يصبح المستخدمون بحاجة إلى برامج مضادة للفيروسات ويضطرون لشراؤها، كما يجب التذكير أنّ المبرمج الذي يعمل الفيروس يعتبر حسب القانون مجرماً وصناعة الفيروس جريمة يحاسب عليها حسب قانون الدولة الموجود بها، كما أنّ معظم شركات مضادات الفيروسات تقوم بصناعة الفيروسات من قبل المبرمجين وتقوم بعمل مضادات لها وذلك لتسويق منتجاتها وبرامجها لدى مستخدمي الكمبيوتر، أمّا الأهداف العسكرية فهي محاولة الدخول لأنظمة الطرف الآخر لكشف أسرار واخذ بيانات عن طريق برامج التجسس، الأهداف الإجرامية فأهمها سرقة بيانات وأرقام حسابات أو أرقام بطاقات الائتمان وكلمات السر لمحاولة الدخول لحسابات المشتركين في البنوك وسرقة أموالهم، أو سرقة بيانات من أجهزتهم، وسرقة الملفات على الحاسوب.

المطلب الأول: ماهية الفيروس المعلوماتي

يعد الفيروس مصطلحا حديثا على مجال صناعة الحاسب الآلي بحيث يمكن عن طريقه غزو الحاسب فهو برنامج للحاسب الآلي مثل أي برنامج آخر، لكنه يهدف إلى إحداث أكبر ضرر بنظام الحاسب وله القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتيا، ويقوم الفيروس بالانتشار بين برامج الحاسب المختلفة وبين مواقع مختلفة في الذاكرة.

الفرع الأول: تعريف الفيروس المعلوماتي

لقد وردت عدة تعاريف للفيروس المعلوماتي، نورد أهمها كالتالي: "مرض يصيب الحاسب الآلي، فهو ليس فيروسا بالمعنى البيولوجي المعروف، ولكنه برنامج

صغير يتم تسجيله أو زرعه على الأقراص أو الأسطوانات الخاصة بالحاسب ويظل هذا الفيروس لفترة محددة ثم ينشط فجأة في وتوقيت معين ليدمر البرامج والبيانات المسجلة والمخزنة في داخل الحاسب ويشمل أثره التخريبي الإتلاف والحذف والتعديل".⁵

⁶ يعتبر فيروس الحاسوب ، برنامجا خارجيا يصممه بعض المخربين لأهداف تدميرية للملفات مع إعطائه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدميره تماما .⁷

كما عرفت كذلك الفيروسات بأنها برنامج حاسوب قائمة بحد ذاتها، وقد تكون جزءا من برنامج آخر يتم إدخاله الحاسوب فيقوم بتعديل المعلومات والبيانات والبرامج أو يشطبها أو يمسخها، وخطورته تكمن في قدرته على التكاثر بشكل سرطاني، مما يسبب الخراب للبرامج والملفات التي يصيبها، وتعتبر هذه الفيروسات من البرامج الشائعة جدا خصوصا مع إزدیاد عملية نقل ملف مصاب إلى حاسوب آخر بواسطة الديسكات، الأمر الذي دفع منتجي البرامج إلى إعداد برنامج خاص لمقاومة الفيروسات ومعالجتها، إلا أن كثرة أعداد وأنواع هذه الفيروسات حالت دون القضاء عليها تماما.⁸

حددت أحد التقارير الصادرة عن المركز القومي للحاسبات الآلية الأمريكي "فيروس الحاسب يعتبر بمثابة "برامج مهاجمة تصيب أنظمة الحاسبات بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان".⁹ ، من ذلك يتضح، تشابه فيروسات الحاسب مع الفيروسات الحيوية أو البيولوجية من عدة أوجه:

- 1- قدرة كل منهما على تحقيق طفرة يكون القصد منها التموه لتجنب الإكتشاف والعلاج بالنسبة للفيروس الحيوي والتصحيح بالنسبة لفيروس الحاسب.
- 2- قدرة كل منهما على إتخاذ محال معينة كهدف له، تتمثل في خلايا جسم الإنسان بالنسبة للفيروس الحيوي وبرامج الحاسب بالنسبة لفيروس الحاسب.
- 3- قدرة كل منهما على التغيير من طبيعة الخلية بالنسبة للفيروس الحيوي ومن طبيعة البرنامج بالنسبة لفيروس الحاسب.
- 4- قدرة كل منهما في السيطرة على الهدف المصاب سيطرة كاملة بل تجنيه لإنتاج نسخ جديدة منه.

- 5- القدرة على الإنتشار السريع وصعوبة إكتشاف المصدر الأصلي له".¹⁰

الفرع الثاني: خصائص الفيروس المعلوماتي

من بين أهم الخصائص التي ينفرد بها الفيروس المعلوماتي عن غيره من البرامج المتلفة والمخرية مايلي:

أولاً- القدرة على الانتشار: يتميز الفيروس أيضاً بقدرة هائلة على الانتشار ويرجع ذلك إلى وسائل الاتصال بين الأجهزة وقابلية الفيروس على نسخ نفسه وضعف برامج الحماية في تلك الأجهزة وأخيراً برمجتها بغرض الفساد أو حماية البرامج.

ثانياً- القدرة على التخفي: للفيروسات قدرة عجيبة على التخفي والخداع عن طريق الارتباط ببرامج أخرى كما تم أيضاً تزويد الفيروسات بخاصية التمويه والتشبه حيث أن الفيروس يرتبط ببرنامج يقوم بأعمال لطيفة أو له قدرة عرض أشياء مثيرة، وعند بداية تشغيله يدخل إلى النظام ويعمل على تخريبه، وللفيروسات عدة وسائل للتخفي منها ارتباطه بالبرامج المحببة إلى المستخدمين ومنها ما يدخل إلى النظام على شكل ملفات مخفية بحيث لا تستطيع ملاحظة وجوده عن طريق عرض ملفات البرنامج، وبعض الفيروسات تقوم بالتخفي في أماكن خاصة مثل ساعة الحاسب وتنتظر وقت التنفيذ، كما أن بعضها تقوم بإخفاء أي أثر لها حتى أن بعض مضادات الفيروسات لا تستطيع ملاحظة وجودها ثم تقوم بنسخ نفسها إلى البرامج بخفة وسرية.

ثالثاً- القدرة التدميرية: عندما يتمكن الفيروس داخل الجهاز يبدأ أعماله التخريبية والتي قد أعدها المبرمج وربما تفقد الكثير من البيانات بل تتعدى أضراره أحيانا أخرى فتصيب hardware بدل من software فقط.

رابعاً- القدرة على الإختراق: مما تتميز به فيروسات الحاسب إمكانية اختراق المواقع

¹¹

التي يقوم المستخدم بتحميل هذه البرامج فيها دون أن يشعر بذلك.

¹²

خامساً- ازدواجية الغرض منه: يستخدم الفيروس بشكل عام لتحقيق أحد الغرضين:

1- الغرض الحمائي: ويكون ذلك لحماية النسخة الأصلية من خطر النسخ غير المرخص به، فينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه، ويعد ذلك بمثابة عقوبة تلحق بالناسخ، وهناك أصابع إتهام تشير إلى أن الشركات الكبرى قد تلجأ أحيانا إلى هذه الحيلة لحماية برامجها من النقل غير المشروع الذي يهدد استثماراتها في هذا المجال، حيث يتم إطلاق هذه الفيروسات عند محاولة النقل غير المشروع.

2- الغرض التخريبي: يتم إعداد هذه الفيروسات من قبل فئة مريضة من خبراء البرامج وذلك بهدف الدعاية أو الابتزاز، فيرمي صانع الفيروس إلى التخريب بحد ذاته أو إلى

التخريب بهدف الحصول على منافع شخصية، "كما يتم زرعه من أجل تحقيق جرائم الإحتيال والغش المعلوماتي"¹³

الفرع الثالث: أنواع الفيروسات

إنّ الفيروسات لا تظهر بالصدفة بل يتم كتابتها من قبل مبرمجين ذوي مهارات عالية، ثم ينشروها في أجهزة المستخدمين عبر شبكات الانترنت أو وسائط التخزين، وكلما أصبحت برامج مكافحة الفيروسات أقوى، زاد المبرمجين من جهودهم لتطوير فيروسات أذكى للتحايل عليها، لقد اشتهرت الفيروسات بقدرتها على الأذى وإحداث الضرر، ولكن في حقيقة الأمر إن الكثير منها غير مؤذ بالمعنى المتعارف عليه ولكن يسبب بعض الأذى، فمثلا قد تستهلك مساحات تخزين على القرص أو في ذاكرة الكمبيوتر، وبالتالي تؤثر على سرعة وكفاءة الجهاز و تأخذ الفيروسات أشكالا عديدة (حين برمجتها) منها :

أولا- تقسيم الفيروسات من حيث النوع: فمن حيث نوعها يمكن تقسيمها لثلاثة أنواع: الفيروس والدودة وحصان طروادة.

1- الفيروس: يمكن القول بأنه برنامج تنفيذي (له امتداد .com , .exe , .bat, .scr). ويعمل بشكل منفصل ويهدف إلى إحداث خلل في نظام الحاسوب. وتتراوح خطورته حسب مهمته فمنه الخطير ومنه الخفيف وكلاهما خبيث. وينتقل بواسطة نسخ الملفات من جهاز به ملفات مصابة إلى جهاز آخر عن طريق الأقراص المدمجة سي دي وذاكرات الفلاش.

2- الدودة/ديدان الحواسيب: هي فيروس ينتشر فقط عبر الشبكات والانترنت ويعمل على الانتشار على الشبكات عن طريق دفتر عناوين البريد الإلكتروني، فمثلا عند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في دفتر العناوين ويرسل نفسه إلى كل شخص وهكذا. مما يؤدي إلى انتشاره بسرعة عبر الشبكة وقد اختلف الخبراء فمنهم من يعتبره فيروس ومنهم من يعتبره برنامج خبيث، وذلك كون الدودة لا تنفذ أي عمل مؤذي، إنما تنتشر فقط مما يؤدي إلى إشغال موارد الشبكة بشكل كبير. ومع التطور الحاصل في ميدان الحوسبة أصبح بإمكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدودة بحيث تؤدي عمل معين بعد انتشارها، (مثلا بعد الانتشار إلى عدد 50000 جهاز يتم تخريب الأنظمة في هذه الأجهزة) أو أي شيء آخر (مثلا في يوم معين أو ساعة أو تاريخ...الخ) وأصبحت الديدان من أشهر الفيروسات على الشبكة العالمية وأشهر

عملياتها التخريبية وأخطرها تلك التي يكون هدفها حجب الخدمة وتسمى (هجمات حجب الخدمة) حيث تنتشر الدودة على عدد كبير من الأجهزة ثم توجه طلبات وهمية لجهاز خادم معين (يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدودة) فيغرق الخادم بكثرة الطلبات الوهمية ولا يستطيع معالجتها جميعا مما يسبب توقفه عن العمل. وهذه الديدان استهدفت مواقع لكثير من الشركات العالمية أشهرها مايكروسوفت وغيرها الكثير.

3- البرامج الماكرا (حصان طروادة) Trojan Horse: سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طرواده والتغلب على جيشها، وهكذا تكون آلية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج، أي يكون جزءا من برنامج دون أن يعلم المستخدم. وعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما حيث ينشط ويقوم بعمله التخريبي. ومثال ذلك ما حدث عندما تم توزيع قرص مجاني على المشايخ به برنامج حول مرض الإيدز (أسبابه - طرق انتشاره - طرق العلاج.. إلخ) وبعد مدة شهر من تشغيل البرنامج تم تشفير المعلومات على الحواسيب الحاضنة للفيروس وظهرت رسالة مفادها أن الحاسب مصاب بالإيدز (المقصود هنا أنه تم تشفير ملفات الحاسب وإيقافها عن العمل بطريقة نظامية) وطلب المخرب إرسال مبلغ كذا إلى الحساب كذا ليتم إرسال رقم فك الشيفرة، مما أجبر المختصين بالرضوخ للطلب كونهم لم يستطيعوا فك التشفير.

ثانيا- تقسيم الفيروسات من حيث السرعة: توجد عدة تقسيمات للفيروسات، فمثلاً من حيث سرعة الانتشار هناك فيروسات سريعة الانتشار وفيروسات بطيئة الانتشار ومن حيث توقيت النشاط فهناك فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط ومن حيث مكان الإصابة فيروسات مقطع التشغيل boot sector على الأقراص وهي الأكثر شيوعاً، وفيروسات الماكرو macro التي تختص بإصابة الوثائق والبيانات الناتجة عن حزمة مايكروسوفت أوفيس، أما من حيث حجم الضرر فهناك الفيروسات المدمرة للأجهزة طبعاً لا يوجد فيروسات خارقة بحيث أنها تدمر الأجهزة كما نسمع أحيانا (احترق المعالج بسبب الفيروس تعطلت وحدة التغذية بسبب الفيروس أو تلفت الشاشة بسبب الفايروس) ولكن يمكن للفيروس أن يؤدي الذاكرة روم في الحاسب كما في فيروس تشرنوبل أو أن يمحي معلومات الـ (Main) MBS Boot Sector على القرص الصلب فتعود الأقراص الصلبة كما أتت من المصنع وفي الحالتين السابقتين لا يتم إقلاع الجهاز مما يوحى للبعض أن الفيروس (حرق) الحاسب.

بالطبع هذه الفيروسات تعتبر خطيرة جدا لأنها تتسبب في إتلاف البيانات المخزنة والتي قد تكون (البيانات) نتاج عشرات السنين مما يؤدي إلى خسائر جسيمة أو إلى توقف الحاسبات عن العمل كما في تشرنوبل مما يؤدي إلى توقف الخدمات المقدمة، وهنالك أيضا الفيروسات المدمرة للبرامج وتأثيرها محدود طالما أن البيانات لم تتأثر حيث يمكن تخزين البيانات وإعادة تهيئة الحاسب وإعادة البرامج المتضررة من أقراسها الأصلية. وهناك فيروسات عديمة الضرر وهي التي لا تقوم بأي عمل مؤذي وإنما تم برمجتها لإثبات الذات والقدرة على البرمجة من بعض المراهقين، فمنها ما يرسم كرة أو أي شكل على الشاشة طوال فترة عمل الكمبيوتر ومنها ما يغير بعض الأحرف (كتغيير حرف بحرف أينما وجد) أو تغيير مؤشر الماوس.¹⁴

ثالثا - تقسيم الفيروسات من حيث طريقة عملها

1- الفيروسات متعددة القدرة التحويلية (مخادع) : هذه الفيروسات لديها القدرة الديناميكية على تحويل وتغيير شفرتها عند الانتقال من ملف إلى آخر لكي يصعب اكتشافها.

2- فيروسات قطاع التشغيل : تستقر هذه الفيروسات في الأماكن التي يقرأها الكمبيوتر بالقرص الصلب عند إقلاعه (تشغيله) ليستقر في الذاكرة وينفذ شفرته.

3- فيروسات الماكرو: وهو أحدث أنواع الفيروسات وهو فيروس يكتب بلغة الورد WORD ويصيب هذا الفيروس ملفات البيانات. ويصيب ملفات الأوفيس

4- الفيروسات متعددة الملفات: يبدأ هذا الفيروس في الجهاز بصيغة أوليه ثم يتحول لصيغ أخرى ليصيب ملفات أخرى.

5- الفيروسات الخفية : تختبئ هذه الفيروسات في الذاكرة ثم تتصدى لأي طلب تشخيص وفحص قطاع التشغيل ليرسل تقريرا بأن قطاع التشغيل سليم وغير مصاب.

6- فيروسات الملفات التنفيذية: تلصق هذه الفيروسات نفسها مع ملفات البرامج التنفيذية مثل command.com و win.com

7- الفيروسات متعددة الأجزاء (أو متعددة المهام) : يصاب هذه الفيروس قطاع الإقلاع (بدأ التشغيل) والملفات في وقت واحد.

8- فيروسات قطاع التشغيل Boot Sector : وهي أخطر أنواع الفيروسات حيث تصيب المقطع التشغيلي في القرص الصلب.

9 - **الفيروسات الطفيلية**: تلتصق هذه الفيروسات مع الملفات التنفيذية لتستقر في الذاكرة عند عمل أحد البرامج المصابة ثم تنتظر في الذاكرة إلى أن يشغل المستخدم برنامجا آخر فتقوم بإصابته ونقل العدوى له.

10- **الفيروسات المتطورة** : وسميت بذلك لأنها تغير شفرتها أيضا ولكن عند الانتقال من جهاز لآخر.

رابعاً- تقسيم الفيروسات من حيث خطورتها: توجد أنواع كثيرة من الفيروسات يصعب حصرها، بعضها يعيب الملفات والبعض الآخر يعيب قطاع التحميل، ولذلك سوف نتعرض للفيروسات الأشد خطورة فيما يلي:

ج-1- الكرة المرتدة ويظهر هذا Bouncing Ball

الفيروس في شكل كرة صغيرة تتحرك على الشاشة، وترتد بعيدا كلما اصطدمت بأحد جوانب الإطار الذي تتحرك فيه، ويؤثر هذا الفيروس على قطاع بدء التشغيل، وعلى القرص الصلب حيث يدمرها، وبالتالي لا يمكن إستعمال هذا القرص سوى بعد معالجته.

ج-2- مايكل أنجلو

وهذا الفيروس يتلف قطاع بدء التشغيل على القرص الصلب، كما يتلف جدول تجزئة القرص الصلب.

ج-3- المخ Brain

يسبب هذا الفيروس أضرارا بالغة بالقرص الصلب، لأنه يكتب على قطاع بدء التشغيل بمجرد تشغيل الجهاز، وقبل التمكن من تحميل أي برامج مضادة له، وبالطبع فهو يقوم بإخفاء نفسه في القطاعات التالفة للقرص الصلب، ويقوم كذلك بحماية نفسه من أي برامج مضادة تحاول إكتشافه، والخطورة هنا تتمثل في أن الفيروس يقوم بتعديل بعض البرامج المخزنة على القرص.

ج-4- بطاقة عيد الميلاد

إنتشر هذا الفيروس عن طريق البريد الإلكتروني، ويقوم بعرض بطاقة عيد الميلاد على الشاشة، وينتقل بسرعة على الشبكة مما يؤدي إلى توقف النظام فترة من الزمن، وقد استطاع المتخصصون عزله والقضاء عليه.

ج-5- " الجمعة 13 "

وهذا الفيروس له عدة أنواع، وقد ظهر في إسرائيل، وتم إكتشافه في جامعة القدس، ويؤدي إلى التقليل من سرعة النظام، وفي يوم الجمعة 13 من أي شهر ينشط الفيروس ويمسح الملفات التي أصابها .

ج-7- السبت 14

يظل هذا الفيروس ساكنا في الذاكرة، لكنه في أي يوم سبت يوافق 14 من الشهر ينشط ويتلف القرص، ومن ثم قطاع التحميل وجدول توزيع الملفات والفهرس الرئيسي.

ج-9- القنبلة المعلوماتية: les bombes informatique

هي فيروسات هدفها تدمير البرامج ومن ثم إتلافها، وينشط الفيروس ويبدأ آثاره المدمرة عند حصول واقعة معينة محددة، في تاريخ محدد، ولذلك فالقنابل المعلوماتية منطقية وزمنية، فالقنبلة المنطقية هي تلك التي تنشط بمجرد حصول واقعة معينة مثل بدء تشغيل الجهاز، ومثالها الفيروس الباكستاني وأما القنبلة الزمنية، فإن الفيروس فيها ينشط في تاريخ معين، ومثاله فيروس الجمعة 13، حيث ينشط الفيروس في أي يوم جمعة يصادف يوم 13 ويبدأ نشاطه التدميري، وتوجد أنواع كثيرة منها في إسرائيل والولايات المتحدة تحديدا .

ج-10- الدورة المعلوماتية

وهي عبارة عن برنامج له القدرة على تعطيل وإيقاف نظام الحاسب الآلي بصورة كاملة، وهو ينسخ نفسه عدة مرات، وينتشر من خلال الوصلات الإلكترونية ويدفع بمعلومات غير صحيحة، تؤدي في النهاية إلى إغلاق النظام ومن ثم تلفه، وهو يعمل على الجزء المتعلق بنظام التشغيل، وهو الجزء الذي يحتوي على مجموعة برامج تتحكم في إمكانيات الحاسب الآلي والعمليات التي تعتمد عليها هذه الإمكانيات ¹⁵ .

المطلب الثاني: آلية عمل الفيروس المعلوماتي

يقوم من أنشأ الفيروس ببرمجة الفيروس بعد تكوّنه ¹⁶، وتوجيه الأوامر له حيث يقوم بتحديد الزمان و متى وكيف يبدأ الفيروس بالنشاط وعادة ما تعطى فرصة كافية من الوقت للفيروس حتى يضمن حرية الانتشار دون أن يلفت الإنتباه ليتمكن من إصابة أكبر عدد ممكن من المستخدمين، وتختلف الفيروسات من حيث بدأ النشاط فهناك من يبدأ بتاريخ أو وقت محدد و هنالك من يبدأ بالعمل بعد تنفيذ أمر

معين في البرنامج المصاب وهناك من الفيروسات من يبدأ بالنشاط بعد التكاثر والوصول الى رقم معين من النسخ، فبعد أن ينشط الفيروس يقوم بعدة أنشطة تخريرية حسب الغرض من انشاء ذلك الفيروس فهناك من يقوم بعرض رسالة تستخف بالمستخدم أو تقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة وهناك أنواع أخرى تقوم بحذف أو تعديل بعض الملفات وهناك من يقوم بتكرار ونسخ نفسه حتى يشل جهازك تماما وهناك أنواع اشد فتكا فتقوم بمسح كل المعلومات من القرص الصلب.

الفرع الأول: عناصر النظام المعلوماتي المستهدفة

تنقسم عناصر النظام المعلوماتي من قسمين فيتعلق القسم الأول بالمكونات المادية للحاسوب التي تشمل وحدات الإدخال (كلوحة المفاتيح والفأرة القلم الضوئي، الماسح ..) ووحد الذاكرة الرئيسية ووحد المعالجة المركزية ووحد المساعدة ووحدات الإخراج، أما القسم الثاني فيخص المكونات البرمجية للحاسوب وتشمل البرامج اللازمة لتشغيل الحاسوب وبرامج التطبيقات وهي عبارة عن الأوامر المرتبة منطقيا والموجهة إلى الحاسب بعد ترجمتها إلى اللغة الوحيدة التي يفهمها وهي لغة الأرقام الثنائية¹⁷.

بشكل عام الفيروس تصيب الملفات التنفيذية أو الملفات المشفرة غير النصية مثل

التالية:

1. الملفات ذاتية التنفيذ مثل ملفات ذات امتداد (.EXE, .DLL, .COM). ضمن أنظمة التشغيل دوس وميكروسوفت ويندوز، أو (ELF) في أنظمة لينكس.
2. سجلات الملفات والبيانات (VOLUME BOOT RECORD) في الأقراص المرنة والصلبة والسجل رقم (0) في القرص الصلب MASTER BOOT.
3. ملفات الأغراض العامة مثل ملفات الباتش والسكريبت في ويندوز وملفات الشل في يونيكس.
4. ملفات الاستخدام المكتبي في نظام تشغيل مايكروسوفت ويندوز التي تحتوي ماكرو مثل مايكروسوفت وورد ومايكروسوفت إكسل ومايكروسوفت أكسس.
5. قواعد البيانات وملفات الأوتولوك لها دور كبير في الإصابة ونشر الإصابة لغيرها لما تحويه من عناوين البريد الالكتروني.
6. الملفات من النوع (نسق المستندات المنقولة) وبعض نصوص لغة ترميز النص الفائق احتمال احتوائها على كود خبيث.

7. الملفات المضغوطة مثل ZIP وRAR وملفات إم بي 3.

فعند تشغيل البرنامج المصاب فإنه قد يصيب باقي الملفات الموجودة معه في القرص الصلب أو المرن، لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر، بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من البريد الإلكتروني أو الإنترنت أو تبادل الأقراص المرنة، فتعمل الفيروسات بطبيعتها على تعطيل عمل الحاسوب أو تدمير ملفاته وبرامجه. هناك فيروسات تعمل على خلق رسائل مزعجة وأنواع تعمل على تشغيل برامج غير مطلوبة وأنواع تعمل على إشغال المعالج بحيث تبطل سرعة الحاسوب أو سرقة بيانات من حاسوب المستخدم مثل أرقام الحسابات وكلمات السر أو أرقام بطاقات الائتمان وبيانات مهمة أخرى، وهذه أهم أهداف الفيروسات الحديثة وبرامج التجسس التي يتم تطويرها يوما بعد يوم.

الفرع الثاني: الأضرار اللاحقة بالعناصر المستهدفة

نظرا للانتشار السريع للفيروس فإنه يحتل أماكن في الذاكرة مما يجعلها غير صالحة للاستعمال مما يتسبب في إجهاد الأجزاء الميكانيكية يصيب المستخدم بخسارة مادية فادحة، فقد يصيب مكونات الحاسوب المادية. (HARDWARE) أو إحداث عطل في جهاز التحكم في وحدة الأقراص، تغيير اتجاه الطابعة بتجميع الورق داخلها وتعطيلها فتؤدي إلى إبطاء تشغيل الكمبيوتر، تدمير قطاع التشغيل، تدمير جدول توزيع (SOFTWARE) كما قد تمس الفيروسات برامج الملفات، تحطيم الفهرس الرئيسي، التجسس وذلك بالحصول على بيانات سرية لغرض تحقيق مكاسب شخصية.¹⁸

يقوم الفيروس بمسح أجزاء من الملفات المخزنة مما يجعل الملف غير قابل للاسترجاع ومن ثم لا يستطيع المستخدم أن يصل إلى الملف المفقود، وفي إحدى القضايا بالولايات المتحدة فقد أصدرت المحكمة حكمها على البائع بغرامة قدرها ألفا وخمسين دولارا نظير التلف الفعلي، وعشرة آلاف دولار تعويضا، وقد سببت المحكمة قرارها بأن المورد خدع المستخدم، ووجه إليه فيروسا منعه من استخدام النظام، والدخول على ملفات عملائه، علاوة على التلف الكبير الذي أصاب البيانات والأضرار البالغة التي أصابت المستخدم نتيجة لعدم تمكنه من استخدام النظام.

المبحث الثاني: الطبيعة القانونية للفيروس المعلوماتي

لقد أثار الفيروس المعلوماتي صعوبة تتعلق بتحديد طبيعته القانونية باعتباره عملا ذهنيا غير محسوس لذا فهناك من اعتبره ضمن الكيانات المنطقية، وهناك من اعتبره من قبيل الأشياء المعنوية وهناك اتجاه حديث اعتبره من قبيل الأشياء المادية،

لذا سنعمل على تبيان تلك الآراء مع الوقوف عند مبررات كل إتجاه وذلك من خلال المطلبين التاليين:

المطلب الأول: الفيروس المعلوماتي من قبيل الكيانات المنطقية

لما كان الفيروس عبارة عن برنامج صغير يتم تسجيله أو زرعه على الأقراص أو الأسطوانات الخاصة بالحاسب فليس له بذلك كيان مادي فنرى أنه يندرج ضمن الكيانات المنطقية، حيث يقصد بالكيان المنطقي وفقا للمنشور الفرنسي الصادر في 22 نوفمبر 1981 بأنه: "مجموع البرامج والأساليب والقواعد وعند الإقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"¹⁹.

الفرع الأول: تحديد الكيانات المنطقية

يشتمل الكيان المنطقي على جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي وهو الجهاز بمكوناته المادية المحسوسة وقد يطلق عليه الآلة أو الحاسب الآلي فهو المظهر أو الجانب الصلب الملموس لنظام المعلومات،²⁰ فلقد أثارت الكيانات المنطقية جدلا فقهيًا حول طبيعتها القانونية فإذا كان الكيان المنطقي مجرد عمل ذهني إلا أنه يختلف عن سائر الأعمال الذهنية من حيث تكوينه وطبيعته وما يحدثه من آثار، كما أن أهم ما يميز الكيانات المنطقية لا سيما البرامج المعلوماتية تكاليفها الباهضة من جهة وسهولة استنساخها من جهة أخرى وهو الأمر الذي فرضه عصر الثورة المعلوماتية إذ طرح لأول مرة في التاريخ مشكلة التعامل مع شكل جديد من أشكال الملكيات يمكن تسميتها "الملكية الرقمية" كالبرمجيات، الفيروسات، البيانات، الكتب والمقالات الرقمية، البريد الإلكتروني، المعطيات المعلوماتية وما شابه ذلك.²¹

الفرع الثاني: البرامج التي تعد كيانات منطقية

لم يضع المشرع الجزائري كسائر التشريعات العربية تعريفا لبرامج الحاسوب باعتبارها كيانات منطقية تدرج ضمن المصنفات الفكرية المشمولة بالحماية القانونية،²² لذا فبرجوعنا لقانون حقوق المؤلف والحقوق المجاورة الجزائري نجدده يحمي جملة من البرامج تتمثل في البرامج الأصلية والمشتقة والتي حددتها المادة 5 من الأمر 05/03 وبرامج التطبيق وبرامج التشغيل.

ونظرا لكون الفيروس المعلوماتي برنامجا للتطبيق مهمته الإتلاف باعتباره مجموعة التعليمات الموجهة من الإنسان إلى آلة والتي تسمح لها بتنفيذ مهمة معينة تمثلت في الإتلاف الإلكتروني لعناصر المنظومة المعلوماتية وبالتالي فهو يندرج ضمن تلك الكيانات المنطقية.

المطلب الثاني: اعتبار الفيروس المعلوماتي من قبيل الأشياء المادية

من المعلوم أن الشيء هو كل موجود، والأصل في الأشياء أن تكون مادية أي لها حيز مادي ملموس أو محسوس، والأشياء غير المادية هي تلك التي تدرك بالحس وإنما يكون إدراكها بالفكر، وتطلق على الحقوق الواردة عليها الحقوق الذهنية²⁴، أما فيما يخص فيروس الحاسب ما هو إلا برنامج من برامج الحاسب الخاصة بالتطبيقات ولكنه صمم لأهداف تخريبية، والبرنامج هو كيان ليس ماديا وإنما هو كيان معنوي أو ذهني لأنه خلاصة فكر خبير البرمجة الذي صاغه في شكل أوامر مرتبة ترتيبا منطقيا وجهها للحاسب بعد ترجمتها إلى اللغة الوحيدة التي يفهمها، لذا فيرى الفقيه "Ulrich Siéber" بوجود مغايرة الرؤى حول آليات حماية المعطيات والبرامج المعلوماتية من آليات حماية الأموال المادية المنطلقة أساسا من الإعراف بطبيعتها الخاصة ومراعاة ماهيتها وخصائص الجرائم الواقعة عليها، حيث اتجه فريق من الفقهاء إلى بسط وصف "المال" على "المعلومات" في ذاتها مجردة عن دعامتها²⁵ المادية نظرا لقابليتها للحياة والتملك .

لقد توصل الفقه الحديث لإعتبار الفيروس المعلوماتي يدخل في عداد الأشياء المادية، فهو برنامج من البرامج الخاصة بالتطبيقات، يتم تصميمه لأهداف تخريبية وهو كيان منطقي يتمثل في نبضات أو إشارات إلكترونية ممغنطة داخل الشرائح الموجودة في ذاكرة الحاسب، فقد اعتبر أنه كيان مادي ملموس ومحسوس للإعتبارات الآتية :

أولا- أن البرنامج يشغل حيزا من ذاكرة الحاسب، وهذه الذاكرة عبارة عن شرائح إلكترونية ترى بالعين المجردة ولها مكان معلوم بجهاز الحاسب وتشغل حيزا ماديا معين يختلف حجمه حسب نوع جهاز الحاسب وإمكاناته.

ثانيا- أن البرنامج ينم داخل هذه الشرائح الإلكترونية على شكل نبضات إلكترونية وهي اللغة الوحيدة التي يفهمها الحاسب وهذه النبضات تشبه الكهرباء التي استقر الفقه على اعتبارها شيئا ماديا خطرا يثير مسؤولية حارس الأشياء إذا توافرت شروطها .

ثالثا- أن للفيروس قدرة كبيرة في نسخ نفسه في الذاكرة، وعلى جميع وسائط التخزين، فهو بذلك يشغل حيزا ماديا يمكن قياسه بمقياس معين هو "البايت".

رابعا- أن الفيروس يعد شيئا خطرا بطبيعته نظرا لآثاره الخطيرة وقوته المدمرة على الثروة المعلوماتية وأجهزة الحاسب التي أصبحت تدير أكبر الآلات في المصانع

26

وتتحكم في الكثير من الأجهزة الهامة . فحاليا يتجه فقه قانون الأنترنت والمعاملات الرقمية أو ما يسمى بالقانون المدني عبر الأنترنت نحو التوسع في مجال المسؤولية عن الأشياء المادية لتطال الأشياء المعنوية نظرا لأهمية بعضها وخطورة بعضها الآخر، الأمر الذي أدى لإستحداث نظام جديد عن الأشياء غير المادية بعد أن توصل الإجتهد القضائي لمعيار خطورة الشيء بغض النظر ما إذا كان هذا الشيء ماديا أو غير مادي وهو ما ندرجه ضمن المفهوم الموسع للأشياء الذي حددته المادتين 138 و140 من التقنين المدني .²⁷

الفرع الأول- إمكانية إسقاط أحكام الطاقة الكهربائية على الفيروس المعلوماتي (معييار درجة الخطورة)

إنّ الأشياء المعنوية يمكن أن تأخذ حكم الأشياء المادية ما دامت موجودة لخدمتها وما دامت الأشياء المعنوية أكثر أهمية من الناحية الإقتصادية، وهي سبب إقتناء الأشخاص لبرامج الحاسوب، أخذا بعين الاعتبار أنّ الأشياء المعنوية في هذه الحالة لا يمكن الإستفادة منها البتة إلاّ بواسطة الأشياء المادية وهذا أمر ليس غريبا ، فكم من منقولات عدة عقارات وفق نظرية العقارات بالتخصيص²⁸ . صحيح أنّ برامج الحاسوب ما هي إلاّ نتاج أفكار المبرمج الذي قام بإعدادها على شكل أوامر وتعليمات مرتبة ترتيبا منطقيا ، إلاّ أنّ هذه الأفكار لا يمكن أن تأتي ثمارها ما لم تنتقل من مجرد أفكار وتتحول إلى نبضات إلكترونية تمثل الرقمين (0، 1) وهي لغة الحاسوب، كما أنّ هذه البرامج وعندما تحوّل إلى نبضات إلكترونية فإنها تتحد مع الكهرباء من حيث التكوين، وهذه الأخيرة، استقر الفقه على إعتبارها شيئا ماديا خطرا يثير مسؤولية حارس الأشياء إذا توافرت أركانها²⁹ ، فيمكن وقياسا على درجة خطورة الفيروس المعلوماتي إسقاط أحكام الكهرباء عليه فيعتبر بذلك شيئا ماديا هذا من جهة، من جهة أخرى فبرجوعنا لنص المادة 687 م التي تنص: "تنظم قوانين خاصة الحقوق التي ترد على الأشياء غير المادية." من خلال هذا النص يمكننا إعتباره أساسا لإقرار الطبيعة الخاصة للفيروس المعلوماتي.

فضلا عن ذلك، هناك اتجاه يرى بتصنيف الأشياء غير المادية ضمن المفهوم الواسع لكلمة شيء، كما توصل الإجتهد القضائي الحديث لمعيار جديد لتحديد الأشياء هو درجة خطورتها بغض النظر ما إذا كان هذا الشيء ماديا أو معنويا³⁰ ، وما دام أنّ المفهوم الواسع للشيء يشمل الشيء المادي والشيء المعنوي فإن الفيروس المعلوماتي يعد شيئا سواء كان ماديا أو معنويا.

الفرع الثاني- إعتبار الفيروس المعلوماتي من قبيل الأموال المنقولة المادية

انطلاقاً مما سبق يجب ألا ننكر أن الفيروس المعلوماتي باعتباره برنامجاً معلوماتياً فهو يشكل عملاً ذهنياً من حيث نشأته، ويمكن إعتباره شيئاً مادياً بالعودة لمكوناته المادية، فهو يتمتع بطبيعة قانونية مركبة فبتتبعنا لقوانين العقوبات نجدها تستلزم لتحقيق جريمة الإتلاف أن يقع الإعتداء على مال منقول أو عقار.

ولقد اعتبر المشرع الفرنسي والجزائري النظام المعلوماتي "مال" من خلال تجريم المساس به في قسم الجرائم ضد الأموال، لذا فإنّ اعتبار المعطيات المعلوماتية بدورها مالا يعد منطقياً باعتبارها جزءاً لا يتجزأ من النظام المعلوماتي وهي عنصر أساسي فيه³¹، بناءً على ذلك يمكن اعتبار الفيروس المعلوماتي نظراً لكونه مجموعة معطيات مكونة لنظام معلوماتي مالا لكن دون تحديد ما إذا كان مالا مادياً أو معنوياً، وعلى نفس النهج سار قانون العقوبات الأردني في المادة 443 والذي تم تعديله سنة 2001 ليجرم اختراق شبكات الحاسوب وتخريبها وذلك بموجب القانون رقم 54 لسنة 2001 المعدل لقانون العقوبات³²، وقانون ليبيا المادة 457 من تقنين العقوبات، والقانون المصري في المادة 361 من قانون العقوبات.

تأسيساً على ذلك فإنّ إشتراط كون المال المتلف من العقارات أو المنقولات يخرج المعلومات والبرامج المعلوماتية من إطار الحماية الجنائية التي يوفرها قانون العقوبات للأموال، لأنّ المعلومات والبرامج بالرغم من قيمتها الإقتصادية "قابلة للإستغلال" إلّا أنّها ورغم ذلك نستطيع إعتبارها من قبيل الأموال المنقولة المادية.

أما بالنسبة للولايات المتحدة الأمريكية فهي تقر عقوبة جنائية خاصة بإتلاف البرامج المعلوماتية ضمن القانون رقم (18) المتعلق بجرائم الحاسب الآلي فقرة 1030 (4) البند الخامس من المرسوم رقم 18 يعاقب إتلاف البرامج، أما بالنسبة للتشريع الفرنسي فضمن القانون العقوبات لسنة 1993 ضمن المادة 3/323 أقرت عقوبة خاصة لـ: "كل من يدخل بطريقة مخادعة لمعطيات المعالجة الآلية أو يحذف أو يعدل...يعاقب

بالسجن لمدة 3 سنوات وغرامة مالية...³³، حيث فرق المشرع الفرنسي ما بين الإعتداء على سير عمل النظام المعلوماتي بإعاقته أو إفساده أو تعطيله وبين الإعتداء عليه بإتلاف البيانات والمعلومات.³⁴ (وعلى نفس النهج سار المشرع الجزائري، حيث بموجب

المادة 394 مكرر من تقنين العقوبات المعدل والمتمم بالقانون رقم 04-15 للفصل الثالث المؤرخ في 10 نوفمبر 2004³⁵ نجدها تنص: "يعاقب بالحبس....كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول

ذلك، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى 2 سنة والغرامة من 50000 د ج إلى 150.000 د ج"، من ذلك يتضح أنّ المشرع الجزائري يولي أهمية بالغة للبرامج المعلوماتية حيث أقر لها عقوبة خاصة لمتلفها دون الفصل في طبيعتها أي من قبيل الأشياء المادية أو غير المادية.

الختامة

إن حماية المتعاملين في عقود التجارة الإلكترونية تقتضي وجوب تفعيل الضمانات في ظل إنعدام النصوص القانونية أو تواضعها لدى المشرع العربي لا سيما المشرع الجزائري، وفي ظل الحاجة الملحة لحماية المستهلك باعتباره الطرف الضعيف تتجه النظم القانونية المعاصرة إلى حماية مشتري البرامج المعلوماتية - المستهلك - في مواجهة المهني أيا كانت صفته منتج، بائع، موزع من خلال تشديد المسؤولية من جهة وزيادة إلتزاماته من جهة أخرى، وذلك بضرورة توافر عامل الأمان من الفيروس المعلوماتي الخطير الذي يعمل على تهديم البرامج المعلوماتية خصوصا إذا كان صادرا عن المنتج باعتباره الطرف المتحكم في تلك البرامج، الأمر الذي يحول دون السير الحسن لها ذلك أن الإحتراف أو الخبرة يستوجب العلم بالشيء أو السلعة، حيث أن أجهزة وبرامج الحاسب المعيبة أو المصابة بالفيروس يمكن أن ترتب مخاطر مادية جسيمة. لذا نقترح من أجل ضمان فاعلية أحكام حماية مستغلي البرامج والشبكات المعلوماتية أن يحذو المشرع الجزائري حذو المشرع الفرنسي ويخصص أحكام خاصة تتعلق بحماية البرامج المعلوماتية ضد مخاطر الفيروسات لتتفق مع الطبيعة الخاصة لتلك الكيانات المنطقية بصفة عامة والفيروسات المعلوماتية مع تحديد اعتبارها من قبيل الأشياء المادية الخطرة بصفة خاصة.

إنّ تكييف الفيروس المعلوماتي والتوصل لاعتباره من قبيل الأشياء المادية سيجبر المشرع الجزائري لإعادة النظر في مفاهيم كانت مستقرة حول الأشياء المادية وغير المادية، وعدم الإكتفاء بتطويع أحكام القواعد العامة حتى يتماشى مع ما استحدثت في إطار تحديد مفهوم الأشياء .

الهوامش

- 1- أنظر: نهلا عبد القادر المومني: الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، الطبعة الأولى، 2008، دار الثقافة للنشر والتوزيع، عمان الأردن، 126.
- 2- راجع: عايد رجا الخلايلة: المسؤولية التقصيرية الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، ط1، 2009، ص109.
- 3- إن بداية اكتشاف الفيروس كانت عن طريق مبرمج هندي الأصل قام ببرمجة برامج الطباعة واستخدم وقتها للصحفيين وحينما لاحظ قلة المشترين بعد فترة وجد أنها تنسخ وتوزع بأقل الأسعار، فخطرت بباله فكرة حماية برنامجه من النسخ فقام بعمل هذا البرنامج الخفي الذي يدخل على الملفات التشغيلية في حالة النسخ ومن ثم يقوم بعملية تخريب للملفات التنفيذية، وكان هذا حافزا للمبرمجين لبرمجة هذا النوع من البرامج وهو للمحافظة على برامجهم وقد يكون هذا السبب هو الأقوى لكونه مرتبطا بجهاز واحد ويتم نقله عن طريق شراء المنتج وليس شبكة بين الأجهزة وأظنه لم تكن في تلك الفترة من شبكات، أنظر: د.دلال صادق، حميد ناصر الفتال: أمن المعلومات، دار اليازوري العلمية للنشر، الأردن، 2008، ص71 وما يليها.
- 4- أنظر: د.دلال صادق، حميد ناصر الفتال: أمن المعلومات، دار اليازوري العلمية للنشر، الأردن، 2008، ص71 وما يليها.
- 5- عبد الفتاح بيومي حجازي: النظام القانوني لحماية التجارة الإلكترونية، دون طبعة، دار الفكر الجامعي، الإسكندرية، 2002، ص8.
- 6- سبب تسميته: الفيروس (Virus) بهذا الاسم لأنها تشبه تلك الكائنات الحية المتطفلة في صفتين رئيسيتين:- الفيروسات دائماً تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أيضا. -تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكرة مثلا وتصيب أي ملف يشغل في أثناء وجودها بالذاكرة مما يزيد عدد الملفات المصابة كلما طال وقت اكتشاف الفيروس، لمزيد من التفصيل راجع/عزة أحمد خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب، رسالة دكتوراه، جامعة مصر، 1994، ص37 وما بعدها.
- 7- راجع: عايد رجا الخلايلة: المسؤولية التقصيرية الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، ط1، 2009، ص110.
- 8- أنظر عامر محمود الكسواني: التجارة عبر الحاسوب، دراسة مقارنة، دار الثقافة للنشر والتوزيع، الأردن، الطبعة الأولى، 2008، ص191.

- 9- نظر: نهلا عبد القادر المومني: الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، الطبعة الأولى، 2008، دار الثقافة للنشر والتوزيع، عمان الأردن، 125.
- 10- أنظر: نهلا عبد القادر المومني: الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، الطبعة الأولى، 2008، دار الثقافة للنشر والتوزيع، عمان الأردن، 125 ومشار له كذلك لدى أنظر: د.دلال صادق، حميد ناصر الفتال: أمن المعلومات، دار اليازوري العلمية للنشر، الأردن، 2008، ص72 وما يليها.
- 11- مشار له لدى: دلال صادق، حميد ناصر الفتال: أمن المعلومات، دار اليازوري العلمية للنشر، الأردن، 2008، ص71 وما 12: أنظر: نهلا عبد القادر المومني: الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، الطبعة الأولى، 2008، دار الثقافة للنشر والتوزيع، عمان الأردن، 127.
- 12- أنظر: نهلا عبد القادر المومني: الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، الطبعة الأولى، 2008، دار الثقافة للنشر والتوزيع، عمان الأردن، 127.
- 13- أنظر: علي جبار الحسيناوي، جرائم الحاسوب والأترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009، ص73..
- 14- أنظر/عايد رجا الخلايلة: المسؤولية التقصيرية الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، ط1، 2009، ص111 وما بعدها
- 15- عبد الفتاح بيومي حجازي: النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص93.
- 16- يتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسية وهي:
- أ-آلية التناسخ The Replication Mechanism وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه.-آلية التخفي The Protection Mechanism وهو الجزء الذي يخفي الفيروس عن الاكتشاف.
- ب-آلية التنشيط The trigger Mechanism وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة في الحاسوب كما في فيروس (Michelangelo) الذي ينشط في السادس من آذار من كل عام.
- ج-آلية التنفيذ The Payload Mechanism وهو الجزء الذي ينفذه الفيروس عندما يتم تنشيطه، أما اللغات التي يكتب بها الفيروس هي لغة التجميع اسمبلي لسهولة الوصول لعتاد الحاسوب وهناك أيضاً اللغات الراقية مثل لغة سي وسي++ وفيجوال سي وفيجوال بيسك،

راجع المزيّد عن طرق عملها: محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر 2003، ص295 وما بعدها.

17- راجع المزيّد: عايد رجا الخلايلة: المسؤولية التقصيرية الإلكترونية، المرجع السابق، ص32 وما بعدها.

18- أنظر: دلال صادق، حميد ناصر الفتال: أمن المعلومات، دار اليازوري العلمية للنشر، الأردن، 2008، ص77 وما يليها.

19- راجع: رشا مصطفى محمد أبو الغيط: الحماية القانونية للكيانات المنطقية، دون طبعة، ملتقى الفكر الازاريطة، الإسكندرية، 2000، ص5. 20: نظام المعلومات: هو مجموع عناصر مادية وغير مادية يمكن باجتماعها التعامل الفوري مع المعلومة".

21- أنظر مشري راضية: الحماية الجنائية لبرامج الحاسوب في ظل قانون حق المؤلف، المجلة النقدية للقانون والعلوم السياسية لجامعة مولود معمري، تيزي وزو، سنة 2010، العدد 2، ص262.

22- راجع: مشري راضية: الحماية الجنائية لبرامج الحاسوب في ظل قانون حق المؤلف، المرجع السابق، ص265 وما بعدها.

23- أنظر الأمر 03-05 المؤرخ في 19 يوليو 2003 يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر عدد 44 المؤرخة في 23 يوليو 2003.

24- راجع سمير عبد السميع الأودن: العقد الإلكتروني، المرجع السابق، ص110.

25- راجع: أحمد عوض الفقي: المعاملات الإلكترونية والاتفاقيات والعقود الرقمية، الدولية للبرمجيات للنشر، القاهرة، 2000، ص500 وما بعدها.

26- عزة خليل: مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب، المرجع السابق، ص37 وما بعدها.

27- أنظر علي فيلاي: الالتزامات: الفعل المستحق للتعويض، المؤسسة الوطنية للفنون المطبعية، الرغاية، الجزائر، 2015، ص169 وما يليها.

28- أنظر: د.عايد رجا الخلايلة: المسؤولية التقصيرية الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، الطبعة الأولى، 2009، ص226.

29- نفس المرجع أعلاه.

30- نفس المرجع أعلاه.

- 31- أنظر: دردور نسيم: جرائم المعلوماتية على ضوء القانون الجزائري والمقارن ، مذكرو ماجستير، فرع جنائي، جامعة منتوري قسنطينة 2013، ص 40 .
- 32- المنشور على الصفحة 4467 من ج ر رقم 4510 الصادرة بتاريخ 2001/10/8، راجع عايد رجا الخلايلة، المرجع السابق، ص 95.
- 33- راجع تفصيلا في ذلك: علي فيلالي: الإلتزامات: الفعل المستحق للتعويض، المرجع السابق، ص 169 وما يليها.
- 34- أنظر محمد أمين أحمد الشوابكة: جرائم الحاسوب والأنترنيت، مجلة الإتجاهات الحديثة في المكتبات والمعلومات، الكويت العدد 1 لسنة 2014، ص 268-269.
- 35- راجع الجريدة الرسمية العدد 71 لسنة 2004، ص 11 و 12 .