المسؤولية المدنية عن فيرسة النظم المعلوماتية عبر الإنترنت

الدكتور/ سامح عبدالواحد التهامي
أستاذ القانون المدني المساعد بجامعة الزقازيق
ومعار لجامعة الشارقة

ملخص:

تعتبر شبكة الإنترنت شبكة مفتوحة لا قيود على الدخول فيها، مما يؤدي إلى سرعة انتشار الفيروسات في مواقع الشبكة، كما أن هذه الفيروسات تتطور بشكل كبير، مما يجعل من الصعوبة على برامج الحماية منها أن تتطور مثلها لتلاحقها.

ستحاول هذه الدراسة أن تضع حلولاً لمشكلات المسؤولية المدنية عن مضار الفيروسات، وذلك في ضوء الطبيعة الخاصة لشبكة الإنترنت باعتبارها شبكة مفتوحة، وبالتالي سنحاول وضع حلول متسقة مع طبيعة هذه الشبكة، ولا تخالف القواعد التقليدية للمسؤولية المدنية حتى تكون هذه الحلول قابلة للتطبيق على واقع شبكة الإنترنت.

ولذلك ستتناول هذه الدراسة أمرين أساسيين:

الأمر الأول هو المسؤولية التقصيرية لمن قام بإصابة النظام المعلوماتي بالفيروسات، وأحدث الضرر المطلوب جبره.

الأمر الثاني هو المسؤولية التعاقدية للمسؤول عن تأمين هذا النظام المعلوماتي من الإصابات الفيروسية.

مقدمة:

مصطلح فيرسة النظم المعلوماتية يقصد به إصابة النظام المعلوماتي بفيروسات الكومبيوتر، وفيروس الكومبيوتر هو برنامج صنع عمداً بغرض القيام بإزالة أو تعديل أو تخريب الملفات والبيانات بالأنظمة المعلوماتية التي يصيبها، أو السيطرة عليها، أو سرقة بيانات مهمة، أو اضطراب في عمل[١].

(١) Margaret ROUSE, virus, Art on the internet at:, the date of publishing is: July 2006.
http://www.searchsecurity.techtarget.com/definition/virus.
النظام المعلوماتي هو مجموعة من البرامج المعلوماتية المعدة لمعالجة وإدارة وتخزين المعلومات.

وتتستر الفيروسات دائماً خلف برنامج آخر، حيث تسيطر على هذا البرنامج، فحين يتم تشغيل البرنامج المصاب يتم تشغيل الفيروس حتى يبدأ في العمل لإصابة باقي أجزاء النظام المعلوماتي(٢).

والفيروسات متعددة ولا حصر لها، فضلاً عن أن كل يوم تظهر فيروسات جديدة، ومن أشهر تلك الفيروسات: فيروس الدودة وفيروس حصان طروادة(٣).

وأهم طرق انتقال الفيروسات الآن هي شبكة الإنترنت، حيث إنها وسيلة سهلة لانتقال الفيروسات من نظام معلوماتي لآخر عبر المواقع الإلكترونية، أو من خلال البريد الإلكتروني، ويأتي في المرتبة الثانية وسائط التخزين مثل ذاكرة الفلاش، والأقراص الضوئية(٤).

ويعمل المبرمجون على برمجة الفيروسات لأهداف عديدة: فبعض المبرمجين يعتبرون أن عمل الفيروس نوع من الهواية التي يمارسونها، والبعض الآخر يبرمج الفيروسات من أجل سرقة بيانات وأرقام حسابات أو أرقام بطاقات الائتمان وكلمات السر؛ لمحاولة الدخول لحسابات المشتركين في البنوك وسرقة أموالهم(٥).

وتتم حماية الأنظمة المعلوماتية من الفيروسات باستخدام أنظمة الحماية، مثل الجدران النارية، وبرامج الحماية من الفيروسات(٦).

أولاً – أهمية البحث:

إذا تحدثت الأرقام عن أضرار الفيروسات وَضُحَ بجلاء حجم المشكلة التي نتناولها، وحجم الأضرار التي تترتب عليها، ففي عام ٢٠٠٩ قدرت الخسارة السنوية للاقتصاد العالمي من جراء الفيروسات الإلكترونية ب ٨٦ بليون دولار، وفي عام ٢٠١٠ أصدرت شركة (مكافى) – المتخصصة في تأمين الأنظمة المعلوماتية –

(٢) Marshall BRAIN and Wesley FENLON, How Computer Viruses Work, Art on the internet at:, the date of reading: 17 April 2013.

(٣) Jonathan STRICKLAND, 10 Worst Computer Viruses of All Time, Art on the internet at: http:// www.howstuffworks.com, the date of reading: 17 April 2013.

(٤) Jeff TYSON, How Firewalls Work, Art on the internet at: http://www.how-stuffworks.com, the date of reading: 17 April 2013.

(٥) Margaret ROUSE, virus, Op.cit.

(٦) TRICKLAND, How to Remove a Computer Virus, Art on the internet at: http:// www.howstuffworks.com, the date of reading: 17 April 2013.

تقريراً قدرت فيه الخسارة اليومية للاقتصاد العالمي من جراء الهجمات الفيروسية بـ ٦,٣ مليون دولار(٧).

والجدير بالذكر هنا أن هذه الأرقام تتناول الأضرار المباشرة وغير المباشرة التي تحدثها الفيروسات للمضرور من جراء إصابة النظام المعلوماتي الخاص به(٨).

ويرى البعض بأن هذه الأرقام السابقة تقل عن الأرقام الحقيقية؛ وذلك لأن هناك كثيراً من الشركات لا تعلن عن إصابة نظامها المعلوماتي بالفيروسات؛ خوفاً من فقدان الثقة في نظامها التأميني وعزوف العملاء عن التعامل معها، خاصة الشركات التي تمارس أعمال التجارة الإلكترونية(٩).

ويزداد حجم هذه المشكلة من آن لآخر؛ نظراً لازدياد اعتماد أغلب المؤسسات الحكومية والخاصة على النظم المعلوماتية في إدارة أعمالها، بحيث يعتبر النظام المعلوماتي هو المحرك الذي تعتمد عليه المؤسسة في إدارة عملها(١٠).

ويختلف حجم الضرر المترتب على الإصابات الفيروسية باختلاف النظام المعلوماتي المصاب، فالضرر يكون كبيراً إذا كان النظام المعلوماتي المصاب مملوكاً لشركة كبيرة تعتمد في كل أعمالها عليه، وقد يقل الضرر إذا كان النظام المعلوماتي خاصاً بكمبيوتر شخصي أو هاتف محمول خاص بمستخدم عادي، وإن كان الضرر في هذه الحالة لا يمكن تجاهله، ففقد البيانات والملفات هو ضرر كبير في نظر المضرور نفسه، فكل ضرر مترتب على الفيروسات يحق للمضرور المطالبة بالتعويض عنه.

ثانياً – مشكلة البحث:

تتمثل المشكلة الرئيسة للبحث في طبيعة شبكة الإنترنت باعتبارها شبكة مفتوحة لا قيود على الدخول فيها واستعمالها، مما يؤدي إلى سرعة انتشار

---

(٧) Eleanor MCKENZIE, Computer Viruses and How They Affect Our Economy, Art on the internet at: http:// www.ehow.com, date of publishing: 2011.

لم نجد تقارير موثوقاً بها عن حجم الخسائر الناجمة عن الهجمات الفيروسية في عام ٢٠١٢ أو ٢٠١٣.

(٨) Ibid.

(٩) Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, canadian journal of law and technology, Vol 3 Number 1,March 2004.

(١٠) Meiring VILLIERS, Information security standards, Journal of internet law, January 2010.

الفيروسات في مواقع الشبكة، كما أن هذه الفيروسات تتطور بشكل كبير، مما يجعل من الصعوبة على برامج الحماية منها أن تتطور مثلها لتلاحقها هذا من ناحية.

ومن ناحية أخرى لم تعد برمجة الفيروسات أمراً صعباً، بل أصبح هناك برامج جاهزة لتصنيع الفيروسات بسهولة وسرعة كبيرة، ومواقع على شبكة الإنترنت لتعليم برمجة الفيروسات لمن يريد ذلك من مستخدمي شبكة الإنترنت، حتى ولو لم يكن مبرمجاً محترفاً(١١).

وهذا يؤدي إلى صعوبة – في بعض الأحيان – في تكييف الفعل على أنه خطأ عقدي، باعتبار أن ذلك يتطلب إخلال بالتزام عقدي، وهو ما يكون تكييفه أمراً دقيقاً في ضوء عدم القدرة على تحديد الإخلال بالالتزام نتيجة للتطور السريع واليومي للفيروسات، وعدم قدرة أنظمة الحماية على ملاحقة هذا التطور هذا من جهة.

ومن جهة أخرى قد يصعب تحديد الشخص الذي قام ببرمجة الفيروس الذي انتشر على شبكة الإنترنت، بحيث إن النظام المعلوماتي قد لا يُصاب مباشرة من فعل المخطئ الذي قام بتصنيع الفيروس، ولكن يُصاب عن طريق شخص آخر قام بنقل الفيروس دون قصد، وهو ما يؤدي إلى تعدد من قام بالفعل الخاطئ.

ولكن من ناحية أخرى هناك ضرر جسيم – كما ذكرنا سابقاً – يلحق الأنظمة المعلوماتية لمستخدمي شبكة الإنترنت من جراء الفيروسات التي تصيب هذه الأنظمة أثناء الولوج إلى المواقع الإلكترونية للشبكة، هذا الضرر يجب جبره وفقاً للقواعد التقليدية للمسؤولية المدنية.

ثالثاً – منهج البحث:

سنقوم في هذه الدراسة بتطبيق القواعد العامة للمسؤولية المدنية بشقيها التقصيري والتعاقدي لتعويض الضرر الناتج عن الإصابة الفيروسية للأنظمة المعلوماتية.

وسنحاول أن نضع حلولاً لمشكلات المسؤولية المدنية عن مضار الفيروسات، وذلك في ضوء الطبيعة الخاصة لشبكة الإنترنت باعتبارها شبكة مفتوحة، وبالتالي سنحاول وضع حلول متسقة مع طبيعة هذه الشبكة، ولا تخالف القواعد التقليدية للمسؤولية المدنية حتى تكون هذه الحلول قابلة للتطبيق على واقع شبكة الإنترنت.

(١١) Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, Op.cit.

رابعاً – خطة البحث:

حتى نتناول المسؤولية المدنية، فإنه يجب أن نتناول أمرين أساسيين:

- **الأمر الأول** هو المسؤولية التقصيرية لمن قام بإصابة النظام المعلوماتي بالفيروسات، وأحدث الضرر المطلوب جبره.
- **الأمر الثاني** هو المسؤولية التعاقدية للمسؤول عن تأمين هذا النظام المعلوماتي من الإصابات الفيروسية.

وبناءً على ذلك فسوف نقوم بتقسيم هذه الدراسة إلى:

الفصل الأول: المسؤولية التقصيرية.

الفصل الثاني: المسؤولية العقدية.

الفصل الأول
المسؤولية التقصيرية

تمهيد وتقسيم:

تنص المادة ١٦٣ من القانون المدني المصري على **(كل خطأ سبب ضرراً للغير يلزم من ارتكبه بالتعويض)**.

فالمسؤولية التقصيرية لها أركان ثلاثة هى الخطأ، الضرر، وعلاقة السببية، فعلى المضرور من الإصابة لنظامه المعلوماتي أن يثبت هذه الأركان الثلاثة حتى تتقرر مسؤولية المخطئ التقصيرية، ويلتزم بناءً على ذلك بتعويض المضرور عن الأضرار التي سببها الفيروس لنظامه المعلوماتي.

والمشكلة الحقيقية تكمن في تحديد المخطئ، فهناك شخص يقوم ببرمجة الفيروس ووضعه على مواقع شبكة الإنترنت، فيصاب المضرور إما من جراء رسالة إلكترونية مصابة بالفيروس أرسلها له أحد الأشخاص، أو من جراء تحميل أحد الملفات من أحد مواقع شبكة الإنترنت، فهل المخطئ هو فقط من قام ببرمجة الفيروس؟ أم مالك الموقع الإلكتروني؟ وهل من الممكن إقامة مسؤولية مرسل الرسالة الإلكترونية التي بها فيروس بالرغم من عدم علمه بوجود فيروس بها؟(١٢)

من ناحية أخرى قد يساهم فعل المضرور في حدوث الضرر؛ فقد يكون النظام المعلوماتي للمضرور غير مؤمن جيداً ببرامج مكافحة الفيروسات؛ مما يؤدي إلى إصابته بالضرر نتيجة لذلك، فهل يعفي ذلك من مسؤولية المخطئ؟

سنقوم بالإجابة على هذه التساؤلات من خلال تطبيق القواعد العامة في المسؤولية التقصيرية، وذلك بتقسيم هذا الفصل إلى:

المبحث الأول: الخطأ

المبحث الثاني: الضرر

المبحث الثالث: علاقة السببية

(١٢) Meiring VILLIERS, Computer viruses and civil liability: a conceptual framework, Tort trial and insurance practice law journal, fall 2004(40) (1), p123- 179.

المبحث الأول
الخطأ

إذا أصيب النظام المعلوماتي بالفيروسات عبر شبكة الإنترنت، فإن ذلك يحدث نتيجة قيام المضرور بتحميل أحد الملفات المصابة بالفيروس من أحد مواقع الشبكة أو بفتح رسالة إلكترونية مصابة بالفيروس، فينتقل الفيروس فوراً إلى النظام المعلوماتي للمضرور.

ولكن هذا الفيروس يتم برمجته من قبل أحد الأشخاص، ويقوم بنشره عبر شبكة الإنترنت، ليصيب الملفات الموجودة على مواقع الشبكة، ويصيب الأنظمة المعلوماتية لمستخدمي الشبكة.

وبالتالي فقد يرجع المضرور على من قام ببرمجة الفيروس، أو يرجع على مالك الموقع أو يرجع على مرسل رسالة البريد الإلكتروني له، فهل من الممكن نسبة الخطأ لكل هؤلاء؟

سنبحث ذلك من خلال تقسيم هذا المبحث إلى:

المطلب الأول: خطأ مبرمج الفيروس.

المطلب الثاني: خطأ مالك الموقع الإلكتروني.

المطلب الثالث: خطأ مرسل الرسالة الإلكترونية.

المطلب الأول
خطأ مبرمج الفيروس

الخطأ في المسؤولية التقصيرية عبارة عن إخلال بالتزام قانوني مقتضاه الالتزام باليقظة والتبصر حتى لا يضر بالغير، فإذا انحرف الشخص عن هذا السلوك الواجب، وكان من القدرة على التمييز بحيث يُدرك أنه قد انحرف، فإن ذلك يعد خطأ يستوجب مسؤوليته التقصيرية(١٣).

ومن ثم يقوم الخطأ في المسؤولية التقصيرية على ركنين: الركن الأول مادي وهو التعدي، والركن الآخر معنوي وهو الإدراك.

---

(١٣) عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني، نظرية الالتزام بوجه عام، مصادر الالتزام، منشورات الحلبي الحقوقية، بيروت، الطبعة الثالثة، ٢٠٠٩، ص ٨٨١-٨٨٢، الفقرة ٥٢٧.

- التعدي:

إذا كان هناك نص تشريعى يجرم برمجة الفيروسات، فإن قيام المبرمج بذلك يعد خطأً؛ لأنه يكون قد خالف التزام قانوني بارتكابه لجريمة منصوص عليها قانوناً، إلا أن المشرع المصري لم يصدر - إلى الآن- تشريعاً للجرائم الإلكترونية(١٤).

وبالتالي فإنه بالنسبة للقانون المصري يتم الرجوع لتعريف ركن التعدي وفقاً للقواعد العامة باعتبار أنه انحراف في السلوك، فهو مجاوزة للحدود التي يجب على الشخص التزامها في سلوكه، فيقع الانحراف إذا تعمد الشخص الإضرار بالغير أو أهمل وقصر فأصاب الغير بضرر(١٥).

ويمكن بسهولة نسبة التعدي لمبرمج الفيروس باعتبار أنه قد تعمد الإضرار بالغير، فيعتبر قد انحرف عن سلوك الشخص المعتاد، فمبرمج الفيروس عندما يقوم بذلك يقصد الإضرار بالغير، وهم مستخدمو شبكة الإنترنت، حيث يقصد تدمير الأنظمة المعلوماتية الخاصة بهم، أو على الأقل تدمير بعض بيانات تلك الأنظمة(١٦).

---

(١٤) فمثلاً نجد المادة ١/٣/٣٢٣ من قانون العقوبات الفرنسي تنص صراحة على تجريم إرسال الفيروسات إلى الأنظمة المعلوماتية، وقد تم إضافة هذا النص بمقتضى قانون ٢١ يونيو لسنة ٢٠٠٤ الخاص بتكنولوجيا المعلومات.

Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF nº0143 du 22 juin 2004 page 11168.

V: Marie BAREL, Le point de vue d'une jurist, Revue de sécurité informatique, Sept 2005, N° 54.

وكذلك نص القانون الإماراتى الخاص بمكافحة جرائم تقنية المعلومات صراحة في المادة العاشرة على تجريم إدخال الفيروسات إلى الشبكات المعلوماتية أو الأنظمة المعلوماتية، وعاقب الفاعل على ذلك بالسجن مدة لا تقل عن خمس سنوات، والغرامة التي لا تقل عن خمسمائة ألف درهم، ولا تجاوز ثلاثة ملايين درهم.

بل إن نص المادة السابقة قد عاقب على مجرد الشروع في الجريمة، أي إذا لم يؤدِّ الفيروس إلى إحداث أي ضرر للشبكة المعلوماتية أو النظام المعلوماتي، أي أن مجرد إدخال الفيروس للشبكة أو النظام معاقب عليه حتى ولو لم يحدث الفيروس أي ضرر لسبب خارج عن إرادة الجاني، كأن يبطل مفعول الفيروس برامج الحماية من الفيروسات.

القانون الاتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات.

(١٥) عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٨٨٢، فقرة ٥٢٨.

(١٦) Murielle CAHEN, La sécurité et les systèmes informatiques, Art disponible sur: http:// www.murielle-cahen.fr, La date de mise en ligne est: 17 mai 2012.

اعتبرت محكمة النقض الفرنسية أن تعمد إصابة النظام المعلوماتي بفيروس عن طريق قرص =

ولا يمنع من نسبة التعدي لمبرمج الفيروس عدم قصده الإضرار بشخص معين؛ لأنه عندما يبرمج هذا الفيروس يقصد الإضرار بأي شخص يصيبه هذا الفيروس، فهو يقصد الإضرار بأكبر عدد ممكن من مستخدمي شبكة الإنترنت، وهذا يكفي لنسبة ركن التعدي له.

- الإدراك:

لا يكون الشخص مسؤولاً إلا إذا توافر له العقل الذي يمكنه من توقع ما ينجم عن فعله من ضرر للغير، ولذلك فالصغير غير المميز والمجنون والمعتوه لا يُسأل أيٌّ منهم عما يترتب عن أفعاله من أضرار(١٧).

والواقع أن مبرمج الفيروس يتمتع بقدر عال من الذكاء الذي يساعده على برمجة هذا الفيروس لإحداث كل هذا الضرر، إلا أن أغلب هؤلاء المبرمجين يكونون في سن صغيرة، لكن لا يتصور أن يستطيع صبي غير مميز أن يقوم ببرمجة فيروس.

فقد اشترط المشرع أن يكون الشخص مميزاً حتى يسأل عن فعله؛ أي يكون قد بلغ سن السابعة، فلا يتصور عملاً أن يستطيع صبي غير مميز يقل سنه عن السابعة أن يقوم ببرمجة فيروس.

وبالتالي ننتهي من ذلك إلى أن مبرمج الفيروس يُنسب إليه الخطأ وفقاً لمفهومه في القانون المدني المصري باعتبار أنه الركن الأول في المسؤولية التقصيرية.

- مشكلة عملية:

إلا أن ما انتهينا إليه هو أمر صحيح من الناحية النظرية ولكنه سيصطدم بمشكلة عملية تتمثل في التعرف على مبرمج الفيروس، فالمضرور من الفيروس لا يستطيع أن يعرف من هو مبرمج هذا الفيروس حتى يدعي ضده بالمسؤولية

= مرن هو خطأ تقصيري يقتضي مسؤولية مرتكبه عن تعويض الضرر الذي أصاب النظام المعلوماتي.

Cass.Crim, 12 Décembre 1996, N° 95-82.198, Bull.crim 1996 N° 465 p. 1353.

(١٧) مصطفى الجمال، مصادر الالتزام، دار المطبوعات الجامعية، الإسكندرية، مصر، ١٩٩٩، ص ٤٠٦، الفقرة ٣٣٤.

ولكن تتقرر في هذه الحالة مسؤولية متولي الرقابة عمن هم تحت رقابته، ولذلك نصت الفقرة الأولى من المادة ١٦٤ من القانون المدني المصري على (يكون الشخص مسؤولاً عن أعماله غير المشروعة متى صدرت منه وهو مميز).

التقصيرية، فالمبرمج يضع الفيروس على مواقع شبكة الإنترنت ويتركه لينتشر ويصيب الأنظمة المعلوماتية دون أن يعرف أحد من قام بذلك(١٨).

وهذه المشكلة العملية يستطيع رجال الشرطة المختصة بمكافحة الجريمة المعلوماتية حلها بشكل كبير، حيث يستطيعون في كثير من الأحيان تتبع الفيروس والتعرف على مصدره، ومن قام بوضعه على الشبكة، ثم القبض عليه ومحاكمته جنائياً، فيستطيع المجني عليهم الادعاء بالمسؤولية التقصيرية للفاعل وطلب الحكم عليه بتعويض الضرر.

وهذا الأمر غير متصور في القانون المصري؛ لأن برمجة فيروس لا تعد جريمة جنائية، لعدم وجود أي تشريع خاص بمكافحة الجرائم المعلوماتية.

وبالتالي سيكون من الأوفق للمضرور أن يدعي بمسؤولية مالك الموقع الإلكتروني الذي انتقل الفيروس منه للنظام المعلوماتي الخاص به، أو مسؤولية مرسل الرسالة الإلكترونية التي تحمل الفيروس.

المطلب الثاني
خطأ مالك الموقع الإلكتروني

إذا أصيب النظام المعلوماتي للمضرور بفيروس من جراء أحد الملفات التي قام بتحميلها من أحد المواقع الإلكترونية، فهل من الممكن نسبة الخطأ لمالك الموقع الإلكتروني؟

الفرض هنا أن مالك الموقع لا يتعمد الإصابة الفيروسية للأنظمة المعلوماتية لمستخدمي الموقع، وإنما حدث ذلك دون علمه، حيث يضع أحد المستخدمين أحد الملفات المصابة بفيروس على الموقع، ويقوم المضرور بتحميل هذا الملف المصاب على نظامه المعلوماتي فينتشر الفيروس في النظام المعلوماتي ويبدأ في إصابته.

فدور مالك الموقع هنا هو أنه يتيح مكاناً لمستخدمي الإنترنت على الخادم الخاص به(١٩) لتبادل الملفات فيما بينهم، حيث يقوم أحدهم بوضع الملف، ويقوم الآخرين بتحميل هذا الملف مثل موقع (YOU TUBE).

---

(١٨) Mark COLOMBELL, The legislative response to the evolution of computer viruses, the Richmond journal of law and technology, vol VIII, Issue 3, spring 2002.

(١٩) الخادم هو حاسب آلي يعمل كنقطة تحكم مركزية لأية شبكة أو موقع إلكتروني من أجل إدارة التطبيقات. =

وحتى ننسب خطأ لمالك الموقع، فإنه يجب أن نتساءل أولاً: هل هناك التزام قانوني على عاتق مالك الموقع في تأمين الموقع الإلكتروني من الفيروسات؟

وبالنسبة للقانون المصري يمكن القول بسهولة بعدم وجود أي التزام قانوني على عاتق مالك الموقع باتخاذ إجراءات الحماية لهذا الموقع، حيث إنه لا يوجد في القانون المصري تشريع متكامل خاص بالإطار القانوني لتكنولوجيا المعلومات(٢٠).

وبالتالي يجب أن نبحث في مفهوم الخطأ بصفة عامة باعتبار أنه انحراف في السلوك قد يقع عمداً أو إهمالاً دون تعمد الإضرار بالغير.

مما لا شك فيه أن مالك الموقع لا يتعمد إصابة الأنظمة المعلوماتية لمستخدمي موقعه بالفيروسات، بل على العكس هو يطمح في زيادة عدد المستخدمين لموقعه، حتى يجذب شركات الدعاية لوضع الإعلانات على الموقع، ويكون ذلك مصدر ربح كبير له، وهذا هو الغرض الأساسي لإنشاء هذه المواقع(٢١).

ويترتب على ذلك أننا يجب أن نبحث في الصورة الأخرى للخطأ وهي (الإهمال)، أي هل من الممكن أن ننسب إهمالاً لمالك الموقع نتيجة الإصابة الفيروسية للنظام المعلوماتي لمستخدم واحد أو لعدة مستخدمين نتيجة تحميل ملف من هذا الموقع ثبت إصابته بالفيروس؟

والإهمال هو الإخلال بواجب قانوني، هذا الواجب قد يتعين بنص القانون، فإذا لم يكن متعيناً بنص القانون، فإن تقدير وجود الإهمال من عدمه يكون بالرجوع إلى المعيار الموضوعي الخاص بمسلك الرجل العادي في مثل الظروف الظاهرة التي وقع فيها الخطأ(٢٢).

فحتى نحدد ما إذا كان المدعى عليه قد أهمل أم لا، فيجب أن نرى ماذا كان الرجل العادي سيفعل إذا كان في نفس ظروف المدعى عليه، هل كان سيقوم بنفس

= انظر: روب سميس ومارك سبيكر ومارك تومسون، التجارة الإلكترونية: ترجمة د. خالد العامري، دار الفاروق للنشر والتوزيع، القاهرة، ٢٠٠٠، ص ٤٩٧.

(٢٠) الخطوة الوحيدة التي اتخذها المشرع المصري لمواجهة التطورات التكنولوجية الحديثة هو فقط القانون رقم ١٥ لسنة ٢٠٠٤ الخاص بالتوقيع الإلكتروني.

(٢١) Meiring VILLIERS, Computer viruses and civil liability: a conceptual framework, Op.cit.

(٢٢) سليمان مرقس، الوافي في شرح القانون المدني: الالتزامات: الفعل الضار والمسؤولية المدنية، الطبعة الخامسة، ١٩٩٢، بدون ناشر، ص ٢٦٣.

سلوكه، فإذا كان سيتخذ نفس السلوك فلا يمكن القول بوجود إهمال في حق المدعى عليه، أما إذا كان سيتخذ سلوكاً آخر أكثر حذراً فهنا يمكن القول بوجود إهمال على عاتق المدعى عليه.

وإذا طبقنا هذا المعيار على الحالة التي نتناولها، فإننا يجب أن نتساءل عن السلوك المعتاد لمالكي مواقع تحميل الملفات، هل يعتبر سلوكاً معتاداً أن يقوموا بتأمين هذه المواقع ببرامج تمنع من وضع ملفات مصابة بالفيروسات، أم أنه لا يقع على عاتقهم هذا الأمر؟

يكاد يجمع الفقه(٢٣) على أن مالك الموقع الخاص بتبادل الملفات يعلم بوجود مشكله عامة وهى مشكلة الفيروسات التي يمكن أن تصيب الأنظمة المعلوماتية عن طريق انتقال الملفات إلى هذه الأنظمة، وبما أنه قام بإنشاء موقع لهذا الغرض، فإنه يجب ألا يسمح بوضع ملف مصاب بالفيروس على موقعه، وذلك بأن يضع برنامج حماية من الفيروسات في هذا الموقع، بحيث يقوم هذا البرنامج بمسح الملف قبل وضعه على الموقع؛ ليتأكد من خلوه من الفيروسات بحيث لا يسمح له بالتحميل على الموقع إلا إذا كان خالياً من الفيروسات.

---

(٢٣) Blandine POIDEVIN, Quelle responsabilité en matière de sécurité informatique?, Art disponible sur: http://www.jurisexpert.net, La date de mise en ligne est: 8 Avril 2002.
- Robin BROOKS, Deterring the spread of viruses online: Can tort law tighten the 'net'? Rev. Litig 17 (1998)343.
- Philippe HELIS & Philippe MOZAS, Chronique multimedia, Petites affiches, 18 (1998) 89.
- Vicky ROBBINS, Vendor liability for computer viruses and undisclosed disabling devices in software, Computer Law, 20 (1993) 10.
- Philip FITES and others, The Computer Virus Crisis, 2e éd. New York, Van Nostrand Reinhold, 1992, p. 141-142, note 24.
- Clive GRINGRAS, The Laws of the Internet, Londres, Butterworths, 1997, p62, note 15.
- Stefan MARTIN, L'exploitation d'un serveur Internet: droits et obligations des institutions à l'égard des créateurs: du public et des étudiants, dans Développements récents en droit de l'éducation, Cowansville, éditions Yvons Blais, 1996 p167.
- Alain BENSOUSSAN, Virus: combiner l'approche légale avec l'approche technique, Les Echos nº 17083 du 09 fevrier 1996, p 45.
- Katie MATISON, Liability forbreach of e-commerce security standards, Art on line at: http://www.lanepowell.com/, the date of publishing is: 2001.
- Meiring VILLIERS, Information security standards, Op.cit.

ويؤسس الفقه ذلك على أساس أن مالك الموقع يتربح من تبادل الملفات على موقعه، حيث يصبح الموقع جاذباً للدعاية، فيكون في المقابل واجب عليه ألا يقصر في حماية هؤلاء العملاء، وألا يعرضهم للخطر، كما أنه أصبح من المعتاد استخدام وسائل التأمين للمواقع الإلكترونية على شبكة الإنترنت للحفاظ على هذه المواقع(٢٤).

بل إن البعض يرى بأن مالك الموقع يجب أن يتخذ أحدث إجراءات التأمين الممكنة، فلا يكفي أن يتخذ أي إجراء تأميني فقط، وإنما يجب أن يضع نظاماً تأمينياً مكتملاً ليس به أية عيوب، ويستخدم أحدث وأدق برامج الحماية من الفيروسات، فلا يجوز له أن يستخدم البرامج المجانية الضعيفة المتاحة على شبكة الإنترنت، وإنما يستخدم البرامج القوية غالية الثمن(٢٥).

ويذهب هذا الرأي إلى أنه إذا تم استخدام برنامج حديث للحماية من قبل ٩٠٪ من مالكي المواقع الإلكترونية، فإن استخدام هذا البرنامج يكون سلوكاً معتاداً من قبل هؤلاء، ويصبح عدم استخدام هذا البرنامج إهمالاً يُسأل صاحبه عن الضرر الناجم عنه، حتى ولو كان هذا البرنامج غالي الثمن(٢٦).

ويمكن من جانبنا أن نعضد وجهة النظر السالفة للفقه بحكم **لمحكمة النقض الفرنسية** أقر بمسؤولية دار نشر عن الأضرار التي أصابت قراء المجلة التي تصدرها نتيجة فيروس موجود على قرص مرن تم توزيعه مجاناً مع المجلة، فدور دار النشر في هذه الواقعة مماثل لدور مالك الموقع الإلكتروني الآن.

فقد قضت محكمة النقض الفرنسية بشأن أحد الطعون الذي طُرح أمامها أن **(دار النشر قامت بتوزيع هذا القرص المرن مجاناً مع المجلة مبتغية الترويج لهذه المجلة، فكان يجب أن تأخذ الاحتياطات اللازمة حتى لا تصيب القراء بالضرر، وذلك بالتأكد من خلو هذا القرص من أي فيروسات، خاصة أن الفيروسات المعلوماتية أصبحت خطراً معتاداً ومعروفاً في مجال تكنولوجيا المعلومات، وأنه أصبح من المعتاد استخدام برامج مكافحة الفيروسات لتوقي هذا الضرر، فكان من الواجب على دار النشر استخدام هذا**

---

(٢٤) Daphyne THOMAS and other, Legal and social aspects of e-commerce, Art on line at: www.iacis.org, the date of publishing is: 2003.

(٢٥) Nicholas VERMEYS, Virus informatiques: Responsables et responsabilité, Les Éditions Thémis, Canada, 2007, P 130.

(٢٦) Nicholas VERMEYS, Computer "Insecurity" and Viral attacks: Liability issues Regarding Unsafe Computer Systems under Quebec Law, Lex Electronica, Vol.9, n°1, Hiver 2004.

البرنامج للتأكد من عدم وجود فيروسات في الملفات الموجودة على القرص، وعدم استخدام هذا البرنامج يُعد إهمالاً من جانب دار النشر)[٢٧].

فهذا الحكم الأخير يعضد وجهة النظر بوجود التزام على عاتق مالك الموقع الإلكتروني بفحص الملفات الموجودة على موقعه، لأن دار النشر في الحكم السابق كانت مسؤولة عن إهمالها في عدم فحص الملف الموجود على القرص الذي قامت بتوزيعه.

ونستنتج من ذلك أن مالك هذا النوع من المواقع عليه واجب بفحص الملفات التي يتم وضعها على موقعه باستخدام برنامج مكافحة الفيروسات، فإذا لم يقم بفحص الملفات التي يتم وضعها على موقعه يكون قد أهمل، ويُسند إليه الخطأ، وتقوم مسؤوليته عن تعويض المضرور من الإصابة الفيروسية لنظامه المعلوماتي من جراء تحميل ملف مصاب بالفيروس من هذا الموقع.

إلا أنه يجب أن نقرر هنا أن التزام مالك الموقع بمنع الملفات المصابة بالفيروسات من الدخول إلى موقعه هو التزام ببذل عناية، وليس التزام بتحقيق نتيجة، بمعنى أنه يجب على مالك الموقع أن يستخدم برنامج مكافحة الفيروسات ويقوم بتحديثه بصفة دائمة، فإذا لم يستطع البرنامج – رغم ذلك – اكتشاف الفيروس الموجود بأحد الملفات، فلا يمكن أن ننسب أي إهمال لمالك الموقع؛ لأنه لم يقصر بل قام بالتزامه على أكمل وجه.

أما مسألة عدم تحقق النتيجة لعدم اكتشاف الفيروس، فذلك يرجع لطبيعة الفيروسات المتجددة؛ حيث تتطور الفيروسات أسرع من تطور البرامج المكافحة لها، مما يؤدي إلى إمكانية عدم اكتشاف أحد برامج مكافحة الفيروسات لفيروس جديد.

المطلب الثالث
خطأ مرسل الرسالة الإلكترونية

لقد أصبحت الرسائل الإلكترونية أكثر الوسائل التي يتم عن طريقها انتشار الفيروسات، حيث تشير الإحصاءات إلى أن ١٠٪ على الأقل من الرسائل الإلكترونية تكون محملة بملفات مصابة بالفيروسات[٢٨].

---

(٢٧) Cass.Com, 25 Nov 1997, N° 95-14603, Bull 1997 IV N° 308 p. 264.

(٢٨) Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, Op.cit.

فإذا أرسل مستخدم إلى آخر رسالة إلكترونية بها ملف مصاب بفيروس، فإن هذا الفعل يعتبر خطأً إذا كان المرسل يقصد إصابة المُرسل إليه بضرر عن طريق إصابة النظام المعلوماتي له بالفيروس الموجود في الرسالة.

أما إذا كان المستخدم لا يعلم بوجود فيروس في الملف الملحق بالرسالة، فهل من الممكن أن يُنسب إليه الإهمال؟

عدم علم المستخدم الذي أرسل الرسالة بوجود فيروس بالملف الملحق بها، يرجع لعدم وجود برنامج للحماية من الفيروسات على النظام المعلوماتي الخاص به، فهذا يدفعنا إلى التساؤل عن مدى وجود التزام على عاتق المستخدم العادي باستخدام برنامج للحماية من الفيروسات على نظامه المعلوماتي؟

فإذا كان المستخدم العادي ملتزماً بوضع برنامج للحماية وفقاً لمعيار سلوك الشخص المعتاد، فإن هذا المستخدم الذي أرسل الرسالة المحملة بملف مصاب بالفيروس، يكون قد أهمل ويُنسب إليه الخطأ، أما إذا كان المستخدم العادي غير ملتزم باستخدام هذا البرنامج، فلا يعتبر قد أهمل ولا ينسب إليه أي خطأ.

إذاً هل أصبح استخدام برامج الحماية من الفيروسات سلوكاً معتاداً بالنسبة للأفراد العاديين؟

انقسم الفقه إلى اتجاهين إزاء هذه المسألة؛ حيث يرى الرأي الأول(٢٩) أن مستخدم الإنترنت يجب أن يكون حذراً في جميع الأحوال عند اتصاله بشبكة الإنترنت وخاصة عند إرسال أية رسالة إلكترونية، وذلك باتخاذ الاحتياطيات اللازمة لمنع الإضرار بالغير عن طريق إرسال فيروس إليه، وتكون هذه الاحتياطيات باستخدام برنامج لمكافحة الفيروسات على نظامه المعلوماتي، أو على الأقل فحص الملف الذي سيرسله من خلال خدمة فحص الملفات الموجودة على بعض المواقع على شبكة الإنترنت.

(٢٩) - Philippe HELIS & Philippe MOZAS, Chronique multimedia, Op.cit.
- Mark GROSSMAN, Liability for you if you have been hacked, on the internet at: http://www.pdesign.net, the date of publishing: 1 August 2000.
- Roland STANDLER, Possible vcarious liability for computer users in the USA?, on the internet at: http://www.rbs2.com, date of publishing: 17 April 2004.
- Cheryl MASSINGALE & Faye BORTHICK, Risk allocation for computer system security breaches: Potential liability for providers of computer services, Western New England Law Rev, Vol 12, Issue 2, 1990.

ويستند هذا الرأي إلى أن مسألة انتشار الفيروسات أصبحت أمراً معتاداً على شبكة الإنترنت، ويكون من السلوك المعتاد لمستخدم الشبكة أن يفحص أي ملف يقوم بإرساله لمستخدم آخر؛ لأن خطر الإصابة بالفيروس عن طريق هذا الملف المُرسَل هو أمر متوقع من مُرسل الرسالة يجب عليه أن يتخذ الاحتياطيات اللازمة لمنع وقوع هذا الضرر، وإلا كان مهملاً ويُسند إليه الخطأ.

فمستخدم شبكة الإنترنت عليه التزام بعدم الإضرار بمستخدم آخر، ويكون ذلك باتخاذ كافة الاحتياطات بعدم إرسال ملف مصاب بفيروس للغير، فيجب على كل مستخدم استعمال برامج مكافحة الفيروسات المتاحة، وإلا كان مهملاً.

ويرى الجانب الآخر من الفقه(٣٠) أن الحكم يجب ألا يكون عاماً، بمعنى أنه يجب أن نفرق بين صفة المستخدم الذي أرسل الرسالة، هل هو شخص محترف لاستخدام الإنترنت، أم هو شخص عادى، فإذا كان شخص محترف فعليه التزام باستخدام أحدث برامج مكافحة الفيروسات، فمثلاً إذا كان مرسل الرسالة الإلكترونية هو مالك لموقع إلكتروني أو هو شركة دعائية أو هو مؤسسة أو جامعة مثلا.... إلخ، كل هذه المؤسسات والهيئات تمتلك أنظمة معلوماتية في المعتاد يكون لها مسؤول لتأمين هذا النظام وبرامج حديثة للتأمين، كما أن المُرسَل إليه يتعامل مع الرسالة المرسلة منها بثقة لاعتقاده الجازم بالتأمين التام للنظام المعلوماتي المرسل منه الرسالة، فعدم استخدام برنامج للتأمين متقدم يعتبر خطأ في جانب هذه الجهة.

أما إذا كان المستخدم شخصاً عادياً فيرى هذا الجانب من الفقه أنه ملتزم أيضاً باتخاذ الاحتياطات المعقولة لتأمين نظامه المعلوماتي، وفحص الملفات قبل إرسالها،

(٣٠) - Lilian EDWARDS, Dawn of the death of distributed denial of service: How to kill zombies, on the internet at: http:// www.cardozoaelj.com, the date of publishing: 2006.
- Sarah FAULKNER, Invasion of the information snatchers: Creating liability for corporations with vulnerable computer networks, The John Marshall Journal of Computer & Information Law, (2000) 18.
- Nicolas VERMEYS, Réflexion juridique autours de la notion de désinformation eu égard à la transmission de métavirus, Lex Electronica, vol.10 nº3, Hiver/Winter 2006.
- Blandine POIDEVIN, Quelle responsabilité lors de la diffusion de virus?,Art disponible sur: www.jurisexpert.net, La date de mise en ligne est: 20 décembre 2001.
- Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, Op.cit.

وذلك باستخدام برامج مكافحة الفيروسات المجانية الموجودة على الإنترنت، أو على الأقل خدمة فحص الملفات المجانية الموجودة على الشبكة دون التزام عليه باستخدام برامج متقدمة عالية التكلفة، فتقدير وجود الخطأ يختلف بحسب طبيعة مرسل الرسالة.

مما لا شك فيه أن ما قال به الرأي الثاني هو الأقرب للمنطق، فلا يجوز معاملة المستخدم العادي مثل المستخدم المحترف؛ لأن معيار السلوك المألوف للشخص المعتاد يأخذ في الاعتبار الظروف الخارجية الظاهرة للملأ، وتكون منظورة للغير المضرور مثل ظرف السن والتعليم والتخصص والخبرة والبيئة الاجتماعية(٣١).

وبناءً على ذلك فيجب – في رأينا – أن يأخذ القاضي في اعتباره – عند تقدير وجود الإهمال بالنسبة للمستخدم العادي غير المحترف – الخبرة الشخصية لهذا المستخدم في التعامل مع تقنية المعلومات، أي منذ متى وهو يتعامل مع هذه التقنيات؟ ففي مجتمعاتنا العربية يُعد استخدام تكنولوجيا المعلومات أمراً حديثاً نسبياً، وبالتالي لا يمكن القول بوجود الوعي الكامل لدى المستخدمين بأهمية تأمين النظام المعلوماتي الخاص بهم، فهذا الوعي يبدأ في التكون مع مرور الوقت في التعامل مع هذه التقنيات.

ومن ثم فالقاضي عند تقديره للأمر لن يعامل المستخدمين على حد سواء، بل يجب التفرقة بين مستخدم تعامل مع تكنولوجيا المعلومات منذ وقت بعيد، وآخر حديث في التعامل مع هذه التكنولوجيا.

المبحث الثاني
الضرر

الضرر هو الركن الثاني للمسؤولية التقصيرية، فلا يكفي الخطأ وحده لانعقاد المسؤولية مهما كانت جسامته، وإنما يجب أن يترتب عليه ضرر.

والضرر على نوعين: مادي وأدبي؛ الضرر المادي هو ما يصيب الشخص في جسمه وماله، فهو إخلال بمصلحة ذات قيمة مالية. والضرر الأدبي هو ما يصيب الشخص في شعوره أو عاطفته أو كرامته أو شرفه أو أي معنى آخر من المعاني التي يحرص الناس عليها(٣٢).

(٣١) انظر: محمد حسين منصور، النظرية العامة للالتزام: مصادر الالتزام، دار الجامعة الجديدة للنشر بالإسكندرية، مصر، ٢٠٠٦، ص ٥٣٢.

(٣٢) السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٩٧٠، فقرة ٥٦٩.

وإصابة النظام المعلوماتي بالفيروس (الفيرسة) لا يُعد ضرراً في حد ذاته، فهذه الإصابة لا تثير مسؤولية من قام بها إلا إذا ترتب عليها أثر يُعد ضرراً مالياً أو أدبياً.

فهناك فيروسات قد تدخل للنظام المعلوماتي ولا تنشط إلا إذا قام المستخدم بفتح الملف الذي التصق فيه هذا الفيروس، فطالما لم يفتح المستخدم الملف يظل الفيروس ساكناً غير محدث لأي ضرر، أما عندما يفتحه المستخدم يبدأ الفيروس في إحداث الضرر، وبالتالي لا يُسأل المخطئ إلا عند تحقق الضرر بالفعل، ولا يمكن هنا أن نقول إن هذا الضرر محقق الوقوع في المستقبل؛ لأن المستخدم قد لا يفتح هذا الملف أو قد يزيله أو قد يقوم بتحديث برنامج مكافحة الفيروسات فينبهه لوجود الفيروس فيزيله من نظامه المعلوماتي(٣٣).

كذلك الحال بالنسبة لفيروسات (القنبلة الموقوتة) التي تدخل النظام المعلوماتي ولا تقوم بإحداث الضرر إلا في الوقت المحدد من قبل مبرمجه، فالضرر لم يحدث بعد، كما أنه غير محقق الوقوع في المستقبل؛ لأن المستخدم قد لا يقوم بتشغيل النظام المعلوماتي في الوقت المحدد لتنشيط الفيروس، أو قد يكتشفه برنامج مكافحة الفيروسات ويقوم بمسحه قبل الوقت المحدد(٣٤).

ويرى البعض بأنه قد يكون هناك ضرر يصيب المستخدم حتى لو لم ينشط الفيروس بعد، هذا الضرر متمثل في الوقت الذي يقضيه المستخدم في إزالة الفيروس من النظام المعلوماتي(٣٥).

فى رأينا أن ذلك لا يعد ضرراً يُذكر؛ نظراً لأن برامج مكافحة الفيروسات تعمل بطريقة تلقائية في إزالة الفيروسات دون حاجة لتدخل من جانب المستخدم.

- الضرر المادي:

ويمكن التصور بأن يترتب على الإصابة الفيروسية للنظام المعلوماتي أضرار

---

(٣٣) لا يمنع عدم تحقق الضرر من عقاب من قام ببرمجة الفيروس جنائياً إذا كان القانون يجرم هذا الفعل، مثلما هو الحال في المادة العاشرة لقانون مكافحة جرائم تكنولوجيا المعلومات الإماراتي الذي يعاقب على مجرد إصابة النظام المعلوماتي بالفيروس.

(٣٤) عزة خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب: دراسة في القانون المدنى والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق بجامعة القاهرة، ١٩٩٤، ص ٢٩٦ – ٢٩٧.

(٣٥) Meiring VILLIERS, Computer viruses and civil liability: a conceptual framework, Op.cit.

مادية، هذه الأضرار المادية قد تكون حدوث بطء في النظام المعلوماتي، وهذا البطء يعتبر خسارة مادية كبيرة لعدم إنجاز الأعمال بالسرعة المطلوبة(٣٦).

ويترتب هذا البطء على بعض أنواع الفيروسات التي تقوم بعمل أوامر كثيرة غير مطلوبة في البنية التحتية للنظام المعلوماتي، مما يؤدي لعدم قدرة النظام المعلوماتي على الاستجابة لهذه الأوامر الكثيرة في ذات الوقت، فيؤدي إلى بطء في تنفيذها(٣٧).

وقد يكون الضرر هو توقف النظام المعلوماتي تماماً عن العمل لفترة من الوقت، طويلة أو قصيرة، بحيث يكون هناك شلل تام في العمل في النظام(٣٨).

بطء النظام المعلوماتي أو توقفه يمكن دائماً ترجمته إلى قيمة مادية هي قيمة الوقت الضائع على مستخدم النظام المعلوماتي نتيجة البطء أو التوقف(٣٩).

وقد يترتب على الإصابة الفيروسية التلاعب بالبرامج التطبيقية الموجودة بالنظام المعلوماتي وتغيير وظائفها، بحيث لا تؤدي هذه البرامج الوظائف المنوطة بها، وإنما تقوم بوظائف أخرى غير مطلوبة للمستخدم(٤٠).

وقد يترتب على الإصابة عدم قيام البرامج التطبيقية بكل الوظائف المطلوبة منها بل القيام ببعضها وتعطيل البعض الآخر(٤١).

وقد يترتب على الإصابة الفيروسية تعديل بعض أو كل البيانات الموجودة في النظام المعلوماتي، أو تدمير بعض الملفات الموجودة في النظام، وهنا تكون الخسارة أكبر من الحالات السابقة لاعتماد المضرور على هذه البيانات والملفات في تسيير

---

(٣٦) Mark COLOMBELL, The legislative response to the evolution of computer viruses, Op.cit.

(٣٧) Nicolas VERMEYS, Réflexion juridique autours de la notion de désinformation eu égard à la transmission de métavirus, Lex Electronica Rev, vol.10 nº3, Hiver/Winter 2006.

(٣٨) David HARLEY and others, Viruses Revealed, Berkeley, McGraw-Hill, 2001, note 3, p7.

(٣٩) عزة خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب: دراسة في القانون المدني والشريعة الإسلامية، مرجع سابق، ص ٢٩٢.

(٤٠) عابد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية: المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والإنترنت، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، الأردن، ٢٠٠٩، ص ١٣٨.

(٤١) Meiring VILLIERS, Computer viruses and civil liability: a conceptual framework, Op.cit.

أعماله، وفي الغالب يكون قد أخذ وقتاً كبيراً لتكوين قواعد البيانات أو الملفات بداخل النظام(٤٢).

وقد يترتب على الإصابة الفيروسية تدمير النظام المعلوماتي بالكامل، وهذه هي أكبر خسارة ممكنة تترتب على الفيروس؛ لأن المضرور يكون في حاجة إلى وضع نظام معلوماتي جديد، ومحاولة تكوين قواعد البيانات والملفات التي فقدها، وهذا يكون أمراً صعباً للغاية(٤٣).

مما لا شك فيه أن كل الصور التي ذكرناها سابقاً للضرر المادي المترتب على الإصابة الفيروسية للنظام المعلوماتي هى إخلال بمصلحة مالية للمضرور؛ لأن توقف النظام المعلوماتي أو تدميره أو تعديل البيانات والملفات أو إلغاءها هي كلها صور لخسارة مالية قد تلحق بالمضرور(٤٤).

ولذلك يقع على عاتق المضرور إثبات أن البيانات التي أصيبت كانت ذات قيمة مالية له، كأن تكون بيانات عملاء الشركة، ويكون للقاضي سلطة مطلقه في تقدير وجود الضرر من عدمه، ومدى مقداره بحسب كل حالة على حدة(٤٥).

مما لا شك فيه أن تقدير حجم الضرر يختلف باختلاف طبيعة المضرور ومدى أهمية النظام المعلوماتي له، فإذا كان المضرور مستخدماً عادياً لا يحتوي نظامه المعلوماتي إلا على ملفات بسيطة شخصية أو مجرد ألعاب أو أفلام، فإن الضرر هنا يكون بسيطاً جداً، وقد يقدر القاضي بأنه لا يوجد ضرر يُذكر.

أما إذا كان النظام المعلوماتي المصاب خاصاً بشركة أو هيئة أو جامعة – مثلاً – تعتمد كلياً في تسيير عملها على هذا النظام المعلوماتي، فالضرر هنا يكون كبيراً يقدره القاضي بحسب حجم الإصابة التي لحقت بالنظام.

---

(٤٢) David COHEN & Roberta ANDERSON, Insurance coverage for cyber-losses, Tort & Insurance Law Journal, Vol. 35, N°. 4, Summer 2000.

(٤٣) Nicholas VERMEYS, Computer "Insecurity" and viral attacks, Op.cit.

(٤٤) Meiring VILLIERS, Computer viruses and civil liability, Op.cit.

(٤٥) Meiring VILLIERS, Information security standards, Op.cit.

الجدير بالذكر هنا أن القضاء الإنجليزي قد اعترف منذ وقت كبير بالقيمة المالية للمعلومات الموجودة بالأنظمة المعلوماتية، انظر:

- CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).
- Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559 (1996).
- American Guarantee & Liability Insurance Co. V Ingram Micro Inc., No. Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299 (D. Ariz. April 19, 2000).

ولا يتصور وجود ضرر قد لحق بمالك النظام المعلوماتي، إذا كانت الإصابة الفيروسية قد أدت لتدمير بعض قواعد البيانات أو الملفات التي يكون هذا الشخص قام بعمل نسخ احتياطية لها؛ لأنه لم يفقد هذه البيانات بل يقوم باستخدام النسخ الاحتياطية(٤٦).

ويجب في جميع الأحوال أن يثبت المضرور القيمة الهامة للبيانات والمعلومات التي أصيبت من جراء الإصابة الفيروسية للنظام المعلوماتي، حتى يتسنى له إثبات وجود ضرر قد حاق به من جراء هذا الخطأ.

- الضرر الأدبي:

الضرر الأدبي هو الضرر الذي يصيب الشخص في قيمة غير مالية، فهو كل ما يؤذي شعور الشخص أو عاطفته فيسبب له ألماً أو حزناً(٤٧).

وقد نص القانون المدني المصري صراحة في الفقرة الأولى من المادة ٢٢٢ على أن التعويض يشمل الضرر الأدبي أيضاً.

ومن المتصور أن يترتب على الإصابة الفيروسية للنظام المعلوماتي ضرر أدبي متمثل في الأذى الذي يصيب شعور المضرور؛ نتيجة إحساسه بالعجز لعدم قدرته على استخدام النظام المعلوماتي الخاص به بعد توقفه؛ نتيجة الإصابة الفيروسية(٤٨).

كذلك قد يُعتبر مجرد شعور المستخدم بالذعر ضرراً أدبياً؛ نتيجة وجود الفيروس على نظامه المعلوماتي، حتى ولو لم ينشط هذا الفيروس بعد(٤٩).

وتقدير مدى اعتبار الأمثلة السابقة ضرراً أدبياً من عدمه، أمر خاضع للسلطة التقديرية المطلقة لقاضي الموضوع في كل حالة على حدة.

---

(٤٦) Nicholas VERMEYS, Virus informatiques: Responsables et responsabilité, Op.cit, P 56.

(٤٧) أنور سلطان، الموجز في النظرية العامة للالتزام، مرجع سابق، ص ٣٤٧، فقرة ٤٠٠.
سمير تناغو، مصادر الالتزام، ٢٠٠٠، بدون ناشر، ص ٢٤٨، فقرة ١٧٨.

(٤٨) عابد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية: المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والإنترنت، مرجع سابق، ص ١٤٢.

(٤٩) Meiring VILLIERS, Computer viruses and civil liability, Op.cit.

المبحث الثالث
علاقة السببية

علاقة السببية هى تلك العلاقة المباشرة التي تقوم بين الخطأ الذي ارتكبه المسؤول، وبين الضرر الذي أصاب المضرور، وهو ركن ثالث من أركان المسؤولية، فلا يكفي الخطأ والضرر لقيام المسؤولية، بل لابد أن يكون الخطأ هو السبب في وقوع الضرر، فقد يقع الخطأ والضرر ولا توجد بينهما رابطة سببية فلا تقوم المسؤولية(٥٠).

تثير علاقة السببية كثير من المشكلات فيما يتعلق بالمسؤولية عن الإصابة الفيروسية للأنظمة المعلوماتية، هذه المشكلات تنبع من طبيعة الفيروسات باعتبار أنها سريعة الانتشار عبر شبكة الإنترنت، وأن هناك كثيراً من الأشخاص يساهمون في انتشارها بخطئهم نتيجة لإهمالهم في اتخاذ احتياطيات تأمين الأنظمة المعلوماتية، مما يؤدي إلى تعدد مرتكبي الخطأ المحدث للضرر هذا من ناحية(٥١).

ومن ناحية ثانية، فقد يدفع المُدَعى عليه الادعاء بمسؤوليته بوجود حادث مفاجئ، أو خطأ من جانب المضرور نفسه لعدم قيام المضرور بتأمين النظام المعلوماتي المصاب ببرامج مكافحة الفيروسات.

كما أن إثبات علاقة السببية يكون دقيقاً في بعض الأحيان؛ وذلك عندما يحدث الضرر، ويتبين أن هناك عدة فيروسات موجودة على النظام المعلوماتي للمضرور، ولا يُعرف من منهم قد أحدث الضرر فعلاً، أو تكون كلها قد اشتركت في إحداث الضرر.

كما أن الأضرار المترتبة على الإصابة الفيروسية يكون مداها واسعاً، بحيث من الممكن أن تتعاقب الأضرار المترتبة على الإصابة الفيروسية.

سنحاول أن نضع حلولاً لكل هذه المشكلات من خلال تقسيم هذا المبحث إلى:

المطلب الأول: الحادث المفاجئ.

المطلب الثاني: خطأ المضرور.

المطلب الثالث: خطأ الغير.

المطلب الرابع: تعدد الأسباب.

المطلب الخامس: تعاقب الأضرار.

---

(٥٠) رمضان أبو السعود، مصادر الالتزام، دار الجامعة الجديدة بالإسكندرية، مصر، ٢٠٠٧، ص ٣٦٦.

(٥١) Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, Op.cit.

المطلب الأول
الحادث المفاجئ

الحادث المفاجئ هو حادث غير ممكن التوقع ومستحيل الدفع، فيجب أن يكون الحادث المفاجئ غير مُستطيع التوقع لا من جانب المدعى عليه فقط، بل من جانب أشد الناس يقظة، فالمعيار هنا موضوعي لا ذاتي، وعدم إمكان التوقع في المسؤولية التقصيرية يكون وقت وقوع الحادث ذاته(٥٢).

ويجب أيضاً أن يكون الحادث المفاجئ مستحيل الدفع، فإذا أمكن دفع الحادث، حتى لو استحال توقعه لم يكن قوة قاهرة أو حادثاً فجائياً.

هل يستطيع مالك الموقع أو مرسل الرسالة الإلكترونية أن يدفع المسؤولية عن نفسه بالادعاء بوجود حادث فجائي متمثل في هجمة فيروسية على شبكة الإنترنت، وذلك لقطع علاقة السببية بين خطأه – المتمثل في الإهمال في استخدام وسائل التأمين الكافية – والضرر الذي أصاب النظام المعلوماتي للمضرور؟

نرى أن هذا الدفع غير مقبول؛ لأن شرط عدم التوقع غير متوافر في الهجمات الفيروسية، باعتبار أن هذا أصبح أمراً متوقعاً لأي مستخدم لتكنولوجيا المعلومات، وكما عبرت محكمة النقض الفرنسية (**أن الفيروسات المعلوماتية أصبحت خطراً معتاداً ومعروفاً في مجال تكنولوجيا المعلومات**)(٥٣).

وبالتالي لا يمكن الادعاء بعدم توقع أي هجمات فيروسية مهما كانت شدتها، فذلك لا ينفي الخطأ المتمثل في الإهمال في اتخاذ إجراءات التأمين المناسبة.

المطلب الثاني
خطأ المضرور

قد يدعي المخطئ بأن المضرور لم يقم باتخاذ الاحتياطيات اللازمة لتأمين النظام المعلوماتي الخاص به، وبالتالي يكون مرتكباً لخطأ، مما ينفي عن المخطئ المسؤولية.

إذا صح ادعاء المخطئ بعدم قيام المضرور باتخاذ أي احتياطيات لتأمين النظام المعلوماتي الخاص به، فهل يعد ذلك خطأً ينفي مسؤولية المدعى عليه؟

---

(٥٢) السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٩٩٦-٩٩٧.

(٥٣) Cass.Com, 25 Nov 1997, N° 95-14603, Bull 1997 IV N° 308 p. 264.

ذكرنا سابقاً أن الفقه قد انتهى إلى أنه أصبح من المألوف على مستخدم شبكة الإنترنت، حتى لو كان مستخدماً عادياً أن يقوم بتأمين النظام المعلوماتي الخاص به ببرامج مكافحة الفيروسات، وأن عدم قيامه بذلك يُعد إهمالاً، ويُسند إليه الخطأ، إلا أن درجة خطئه تكون أقل من درجة خطأ المستخدم المحترف للشبكة، ويُقدر القاضي درجة الخطأ في ضوء ظروف المستخدم.

يمكن القول أنه أصبح من الثابت فعلاً أن مستخدم الإنترنت ملتزم بتأمين النظام المعلوماتي الخاص به ببرامج مكافحة الفيروسات.

وبالتالي فهناك خطأ في جانب المضرور لعدم قيامه باستخدام برنامج لمكافحة الفيروسات، إلا أن هذا الخطأ قد يستغرقه خطأ المدعى عليه، وقد لا يستغرقه، ولكن يستقل عنه بحيث يشترك معه في إحداث الضرر، ويتوقف ذلك على حسب جسامة خطأ المدعى عليه(٥٤).

أ – استغراق خطأ المدعى عليه لخطأ المضرور:

ويتصور ذلك عندما يكون المدعى عليه هو مبرمج الفيروس الذي قام بوضعه على شبكة الإنترنت، فهذا المبرمج متعمد إحداث الضرر بالغير، ومن ثم فخطأه يستغرق خطأ المضرور المتمثل في الإهمال في اتخاذ وسائل الحماية من الفيروسات.

فى هذه الحالة تكون مسؤولية مبرمج الفيروس كاملة غير منقوصة، ولا يؤثر فيها خطأ المضرور، ويقع على المبرمج تعويض المضرور عن الضرر.

ب – الخطأ المشترك:

إذا كان المدعى عليه هو مالك الموقع الإلكتروني الذي انتقل الفيروس منه إلى النظام المعلوماتي للمضرور، فإن خطأه المتمثل – كما ذكرنا سابقا – في عدم تأمين موقعه بحيث يتم وضع ملفات مصابة بالفيروسات عليه هو إهمال من جانبه، وبالتالي فهو خطأ لا يستغرق خطأ المضرور المتمثل في الإهمال أيضا، ويترتب على ذلك أن خطأ المدعى عليه يشترك مع خطأ المضرور في إحداث الضرر.

وكذلك الحال إذا كان المدعى عليه هو مرسل الرسالة الإلكترونية الذي تسبب بإهماله في إرسال ملف مصاب بفيروس للمضرور، في هذه الحالة لا يستغرق خطأ المدعى عليه خطأ المضرور، بل يشتركان في إحداث الضرر؛ لأن كلاً منهم يمثل إهمالاً.

(٥٤) Clive GRINGRAS, The Laws of the Internet, Op.cit, P 77.

فى الحالتين السابقتين يكون كل من المُدَعى عليه والمضرور مسؤولاً؛ لأن خطأ كل منهم كان سبباً في وقوع الضرر كله، فتوزع المسؤولية بينهما.

فطالما أن أحد الخطأين لم يستغرق الخطأ الآخر، فإن كل خطأ يكون مستقلاً عن الخطأ الآخر، وقيل أن هناك خطأ مشتركاً، والأصل أن كلا من الخطأين يعتبر سبباً متكافئاً أو منتجاً في إحداث الضرر، ولذا لا يتحمل المدعى عليه كامل المسؤولية بل توزع بينه وبين المضرور(٥٥).

وقد نص القانون المدني المصري في المادة ١٦٩ على أنه إذا تعدد المسؤولون عن الضرر تكون المسؤولية بينهم بالتساوي إلا إذا عين القاضي نصيب كل منهم في التعويض.

وبالتالي يقع على عاتق القاضي تقدير مدى جسامة خطأ كل منهما عند توزيع المسؤولية، فقد يقدر تساوي خطأ المدعى عليه والمضرور في الجسامة، فيوزع المسؤولية عليهما بالتساوي، ويتصور ذلك عندما يكون المدعى عليه هو مستخدم عادي مرسل الرسالة الإلكترونية، والمضرور مستخدم عادي، وكل منهما أهمل في عدم استخدام برنامج لمكافحة الفيروسات.

وقد يقدر القاضي أن أحد الخطأين أكثر جسامة من الآخر، ويتصور ذلك عندما يكون المدعى عليه هو مالك الموقع الإلكتروني المفترض فيه اتخاذ أحدث وسائل التأمين لموقعه، فيقدر القاضي أن خطأه أكثر جسامة من خطأ المضرور فيجعل مسؤوليته أكبر من مسؤولية المضرور.

وبالتالي يقدر القاضي الأمر في كل حالة على حدة حسب صفة المدعى عليه والمضرور، ما إذا كان مستخدماً عادياً أم مستخدماً محترفاً، وما يفترض فيه أن يتخذه من إجراءات تأمين لنظامه المعلوماتي.

المطلب الثالث
خطأ الغير

من المشكلات المتعلقة بالمسؤولية عن الإصابة الفيروسية للنظم المعلوماتية تعدد الأشخاص الذين يساهمون في الإصابة الفيروسية، بحيث يمكن أن يُسند الخطأ لهم جميعاً في إحداث هذه الإصابة، بحيث أن المدعى عليه يمكن أن يدفع بوجود خطأ لشخص آخر أدى لإحداث الضرر.

(٥٥) أنور سلطان، الموجز في النظرية العامة للالتزام، مرجع سابق، ص ٣٦٣، فقرة ٤٢٤.

فمثلاً إذا قام أحد الأشخاص بتحميل ملف مصاب بالفيروس من أحد المواقع وكان هذا الشخص لا يستخدم برنامج مكافحة الفيروسات، وكذلك الحال الموقع الذي تم تحميل الملف منه، ثم قام هذا المستخدم بإرسال الملف المصاب عبر البريد الإلكتروني إلى أحد أصدقائه فأصاب النظام المعلوماتي له، على الرغم من استخدامه لبرنامج مكافحة الفيروسات، فإن المضرور سيرجع على مرسل الرسالة الإلكترونية باعتبار أنه المسؤول عن إرسال هذه الرسالة، وأنه مخطئ لعدم استخدام برنامج مكافحة الفيروسات.

ولكن سيدفع المدعى عليه هذا الادعاء بأن هناك خطأ من جانب مالك الموقع الذي تم تحميل الملف منه؛ لأنه لم يستخدم برنامجاً لمكافحة الفيروسات، وكذلك فإن مالك الموقع سيدفع الادعاء بوجود خطأ في جانب مبرمج الفيروس نفسه.

ويمكن القول إنه في الفرض السابق توجد ثلاثة أخطاء أدت لإحداث الضرر، خطأ مبرمج الفيروس، خطأ مالك الموقع الإلكتروني، وخطأ مرسل الرسالة الإلكترونية.

والمعيار هنا هو مدى استغراق خطأ الغير لخطأ المدعى عليه من عدمه، فإذا استغرق خطأ الغير خطأ المدعى عليه، ففي هذه الحالة لا يُعتد بخطأ المدعى عليه، وتقوم مسؤولية الغير كاملة، أما إذا كان خطأ المدعى عليه مستغرقاً لخطأ الغير فلا يُعتد بخطأ الغير، وتقوم مسؤولية المدعى عليه كاملة، وإذا استقل كل من الخطأين عن الآخر اعتبر أن كلا منهما سبب في إحداث الضرر، حيث يحدد القاضي مدى جسامة خطأ كل منهم حتى يحدد مقدار التزامه بالتعويض(٥٦).

وإذا طبقنا هذا المعيار على الفرض السابق، فيمكن القول إن خطأ مبرمج الفيروس يستغرق خطأ مالك الموقع، ويستغرق خطأ مرسل الرسالة الإلكترونية، باعتبار أن خطأ مبرمج الفيروس خطأً عمدياً، في حين أن خطأ مالك الموقع ومرسل الرسالة يتمثل في الإهمال، وبالتالي ينفي خطأ مبرمج الفيروس خطأ مالك الموقع ومرسل الرسالة فتنتفي مسؤوليتهما وتلقى المسؤولية كاملة على مبرمج الفيروس.

أما إذا كان المدعى عليه هو مرسل الرسالة والغير هو مالك الموقع، فإن خطأ كل منهما مستقل عن الآخر، فخطأ كل منهما هو سبب في الضرر؛ لأن خطأ كل منهما هو الإهمال فقط في عدم تأمين النظام المعلوماتي، وبالتالي يكون كل منهما مسؤولاً عن إحداث الضرر، وإن كان بإمكان القاضي أن يقدر أن خطأ مالك الموقع

(٥٦) أنور سلطان، الموجز في النظرية العامة للالتزام: مصادر الالتزام، دار الجامعة الجديدة للنشر بالإسكندرية، مصر، ٢٠٠٥، ص ٣٦٢-٣٦٣.

أكثر جسامة من خطأ مرسل الرسالة، باعتبار أن مالك الموقع مفترض فيه اتخاذ أقصى احتياطيات التأمين لنظامه المعلوماتي، بعكس المستخدم العادي الذي يكفيه اتخاذ احتياطات بسيطة، وبالتالي قد يرى القاضي التزام مالك الموقع بدفع الجزء الأكبر من التعويض، وإلزام مرسل الرسالة بدفع الجزء الأصغر.

ويتصور أخيراً أن يشترك خطأ المدعى عليه، وخطأ الغير، وخطأ المضرور في إحداث الضرر، في هذه الحالة يقوم القاضي بتوزيع المسؤولية عليهم بحسب جسامة خطأ كل منهم(٥٧).

فإذا كان المضرور ومرسل الرسالة الإلكترونية ومالك الموقع قد أهملوا جميعا في تأمين الأنظمة المعلوماتية، فإن كلاً منهم يكون مسؤولاً عن إحداث الضرر، ويقوم القاضي بتوزيع المسؤولية عليهم بحسب جسامة خطأ كل منهم.

المطلب الرابع
تعدد الأسباب

مشكلة الإصابات الفيروسية للأنظمة المعلوماتية أنه في بعض الأحيان لا يُعرف السبب الحقيقي لإحداث الضرر، ويُتصور ذلك عندما يكون النظام المعلوماتي للمضرور غير مُؤَمن بحيث توجد عليه فيروسات متعددة لا يُعرف أي منهم قد أحدث الضرر بالنظام المعلوماتي، ومن الممكن أن تكون كل هذه الفيروسات أو بعضها قد اشترك في إحداث الضرر(٥٨).

من الناحية الفنية قد يصعب في بعض الأحيان التعرف على الفيروس محدث الضرر، وفي بعض الأحيان قد تستطيع بعض البرامج تحديد الفيروس مصدر الضرر الذي أصاب النظام المعلوماتي(٥٩).

وبالتالي نحن أمام فرضين: فإما أن نستطيع تحديد الفيروس الذي أحدث الضرر، وإما لا نستطيع تحديد الفيروس محدث الضرر بالنظام المعلوماتي.

وبالنسبة للفرض الأول: فالمسؤولية تقع على عاتق المخطئ الذي وضع هذا

(٥٧) رمضان أبو السعود، مصادر الالتزام، مرجع سابق، ص ٣٨٢.

(٥٨) Daniel HANSON, Easing Plaintiffs' Burden of Proving Negligence for Computer Malfunction, Iowa Law Rev, 69 (1983)241.

(٥٩) Nicholas VERMEYS, Virus informatiques: Responsables et responsabilité, Op.cit, P 62.

الفيروس على هذا النظام المعلوماتي سواء أكان مبرمج الفيروس، أم مالك الموقع الإلكتروني، أو مرسل الرسالة الإلكترونية المحملة بالملف المصاب بالفيروس، وذلك على النحو الذي ذكرناه سالفاً.

أما بالنسبة للفرض الثانى فهنا تكون المشكلة في عدم القدرة على تحديد أي فيروس قد تسبب في إحداث الضرر، فهناك صعوبة في تحديد أي الأخطاء هو الذي أدى إلى إحداث الضرر، على الرغم من إثبات المضرور للخطأ في جانب مبرمج الفيروس، ومالك الموقع الإلكتروني، ومرسل الرسالة الإلكترونية.

والحل – في رأينا – يكون بالرجوع إلى نظرية هجرها الفقه والقضاء وهي نظرية (**تكافؤ الأسباب**)، فهذه النظرية قابلة للتطبيق على الحالة محل البحث، وتؤدي إلى نتائج أقرب إلى المنطق والعدل فيما يتعلق بهذا الأمر؛ لأن عدم الأخذ بها معناه عدم تعويض المضرور عن الضرر الذي أصاب نظامه المعلوماتي إطلاقاً لعدم قدرته على تحديد الخطأ محدث الضرر على الرغم من إثباته وجود ضرر ووجود أخطاء متعددة.

ومضمون هذه النظرية أنه إذا كان الضرر واحداً واشتركت عدة عوامل في إحداثه، بحيث كان من الصعب تعيين ما يعتبر سبباً حقيقياً لهذا الضرر وما لا يعتبر كذلك، فإن جميع هذه العوامل التي أدى اشتراكها إلى حدوث الضرر تعتبر أسباباً لإحداث الضرر، وتعد كلها متعادلة من حيث التسبب في وقوعه(٦٠).

وبالتالي فتطبيق هذه النظرية يؤدي إلى افتراض أن جميع الفيروسات كانت سبباً في إحداث الضرر، حيث تتوزع المسؤولية على جميع المدعى عليهم المنسوب إليهم الخطأ، ولكن هذه القرينة قابلة لإثبات العكس، فيستطيع أي من المدعى عليهم أن ينفي المسؤولية عن نفسه بنفي علاقة السببية، وذلك بإثبات أن الضرر قد حدث بسبب فيروس آخر غير الفيروس الذي تسبب هو فيه، ويخضع الأمر للسلطة التقديرية الكاملة لقاضي الموضوع الذي قد يأخذ بدفع المدعى عليه أو يطرحه جانباً(٦١).

(٦٠) سليمان مرقس، الوافي في شرح القانون المدني: الالتزامات: الفعل الضار والمسؤولية المدنية، مرجع سابق، ص ٤٥٩-٤٦٧.

(٦١) Nicholas VERMEYS, Computer "Insecurity" and viral attacks,Op.cit.

المطلب الخامس
تعاقب الأضرار

من المألوف في مجال الإصابات الفيروسية أن تتعاقب الأضرار المترتبة على إصابة النظام المعلوماتي، فتكون هناك أضرار مباشرة وأضرار غير مباشرة.

وفقاً لنص المادة ٢٢١ من القانون المدني، فإنه إذا ترتب على الخطأ الواحد أضرار مباشرة وأخرى غير مباشرة، فإن المخطئ يُسأل فقط عن تعويض الأضرار المباشرة، ولا يُسأل عن تعويض الأضرار غير المباشرة.

الإشكالية في الأضرار المترتبة على الإصابات الفيروسية هى تحديد الضرر المباشر الذي يُسأل عنه المخطئ، والضرر غير المباشر الذي لا يُسأل عنه، وذلك نظراً لسرعة تعاقب الأضرار المترتبة على الإصابات الفيروسية واتساع انتشارها.

وقد وضعت المادة ٢٢١ المعيار الذي يمكن اتباعه للتمييز بين الضرر المباشر وغير المباشر، فالضرر المباشر هو ما كان نتيجة طبيعية للخطأ، ويعتبر الضرر نتيجة طبيعية إذا لم يكن في استطاعة المضرور توقيه ببذل جهد معقول.

فمثلاً إذا أصاب الفيروس النظام المعلوماتي لمصرف، وأدى لتدميره وتدمير ملفات العملاء، وأدى ذلك إلى شلل تام بالعمل في هذا المصرف، وقيام كثير من العملاء بسحب أرصدتهم بسبب اهتزاز سمعة المصرف، فأدى ذلك لخسارة مالية كبيرة، وفقد كثير من العملاء.

ويمكن القول إن الخطأ المتمثل في إصابة النظام المعلوماتي بالفيروس قد ترتب عليه عدة أضرار وهي تدمير النظام المعلوماتي، وتدمير جميع الملفات الموجودة عليه، وتوقف العمل تماماً بالمصرف للاعتماد التام على النظام المعلوماتي، وأخيراً سحب كثير من العملاء لأرصدتهم.

وبالنسبة للضرر الأول المتمثل في تدمير النظام المعلوماتي، فإنه يُعتبر ضرراً مباشراً؛ وذلك لأن المصرف لا يستطيع توقيه ببذل جهد معقول، فمجرد وجود برنامج لمكافحة الفيروسات محدث طبقاً لأحدث الإصدارات يعتبر جهداً معقولاً من جانب البنك، وهو في ذات الوقت التزام عليه – كما ذكرنا – سابقاً.

وبالنسبة لضرر تدمير جميع الملفات، فهذا الضرر قد يكون غير مباشر؛ وذلك لأن المصرف يستطيع بجهد معقول عمل نسخ احتياطية لملفات العملاء إلكترونية أو ورقية.

وبالنسبة للضرر الخاص بتوقف سير العمل، فهذا قد يكون ضرراً مباشراً إذا لم

يكن في استطاعة المصرف بجهد معقول عمل نظام ورقي لسير العمل لحين إصلاح النظام المعلوماتي، وقد يكون ضرراً غير مباشر إذا كان المصرف بجهد معقول يستطيع عمل نظام ورقي لسير العمل.

وهنا تظهر سلطة القاضي التقديرية في تحديد إمكانية تفادي الضرر بجهد معقول، فقد يرى القاضي أنه من الصعب عمل نظام ورقي لإدارة مصرف كبير، يعتمد على تكنولوجيا المعلومات في تسيير العمل به، ويعتبر أن ضرر توقف العمل هو ضرر مباشر يُسأل عنه المخطئ.

وقد يرى القاضي أن عمل نظام ورقي احتياطي هو أمر معتاد لدى المصارف لمواجهة توقف النظام المعلوماتي لأي سبب كان، فيعتبر أن ضرر توقف العمل هو ضرر غير مباشر لا يُسأل عنه المخطئ.

وكذلك الحال فيما يتعلق بسحب العملاء لأرصدتهم من البنك، فهذا الضرر قد يكيف على أنه ضرر مباشر، إذا لم يستطع المصرف إعادة سير العمل ببذل جهد معقول، كأن يحاول إصلاح النظام المعلوماتي ولكن يتأخر ذلك لشدة تدمير النظام.

وقد يكون الضرر غير مباشر إذا كان إصلاح النظام المعلوماتي لا يحتاج وقتاً كبيراً، ولكن المصرف لم يبذل جهداً معقولاً لذلك.

المهم أن القاضي في كل حالة على حدة منوط به تحديد مدى إمكانية بذل جهد معقول لتفادي الضرر من عدمه؛ حتى يحدد طبيعة الضرر إذا كانت مباشرة أم غير مباشرة.

الفصل الثاني
المسؤولية العقدية

تناولنا في الفصل السابق المسؤولية التقصيرية المترتبة على إصابة النظام المعلوماتي بالفيروس، وقد تبين لنا أن القواعد العامة في المسؤولية التقصيرية تقضي بإقامة المسؤولية على عاتق المخطئ سواء أكان مبرمج الفيروس أم مالك الموقع الإلكتروني، أم مرسل الرسالة الإلكترونية.

ولكن المشكلة قد تدق من الناحية العملية في إثبات الخطأ، فالمضرور يقع عليه عبء إثبات الخطأ في حق المُدعى عليه، وهذا الأمر قد يواجه بعض الصعوبات من الناحية الفنية، فمن الصعوبة معرفة مبرمج الفيروس إلا باتباع أساليب فنية للتتبع لا تكون متوافرة إلا لأجهزة مكافحة الجريمة المعلوماتية.

وكذلك فقد يحدث الضرر بعد وقت طويل من إصابة النظام المعلوماتي، حيث يدخل الفيروس للنظام ويبقى فيه، ولا ينشط إلا بعد مدة طويلة عندما يتم تشغيل الملف الذي التصق به الفيروس، فيبدأ في إحداث التلف بالنظام، في هذه الحالة يكون قد فات وقت طويل على دخول الفيروس للنظام، فيكون من الصعوبة بمكان تحديد مصدر الإصابة.

كل ذلك يدفع المضرور للرجوع على مسؤول تأمين النظام المعلوماتي بالتعويض لوجود خطأ من جانبه في الإخلال بالتزامه التعاقدي بتأمين النظام؛ مما أدى لإحداث الضرر الذي نتج عن الإصابة الفيروسية.

ويتصور ذلك عندما يرتبط بعقد مع شخص طبيعي أو معنوي، يكون مضمونه التزام الأخير بتأمين النظام المعلوماتي، ويخل هذا الأخير بالتزامه الوارد في العقد.

حتى نتناول المسؤولية العقدية المترتبة على الإصابة الفيروسية للنظام المعلوماتي، فسوف نقوم بتقسيم هذا الفصل إلى:

المبحث الأول: عقد التأمين المعلوماتي.

المبحث الثاني: أركان المسؤولية العقدية.

المبحث الثالث: الإعفاء من المسؤولية أو التخفيف منها.

المبحث الأول
عقد التأمين المعلوماتي

عقد التأمين المعلوماتي هو العقد الذي يُبرم بين مالك النظام المعلوماتي والمسؤول عن تأمين هذا النظام، ويكون محله التزام مسؤول التأمين بتوفير التأمين اللازم للنظام المعلوماتي من أي هجمات للقراصنة (HACKERS) أو من الإصابة بأي فيروسات من خلال شبكة الإنترنت أو حتى الوسائط التقليدية.

ويأخذ هذا العقد صورتين هما: الصورة الأولى تكون بين مالك النظام المعلوماتي وشركة متخصصة في تأمين الأنظمة المعلوماتية، وتنتشر هذه الصورة بالنسبة للهيئات والمؤسسات والشركات الكبيرة التي تمتلك أنظمة معلوماتية تعتمد عليها في إتمام عملها، ويسمى هذا العقد عقد تأمين النظام المعلوماتي.

أما الصورة الثانية فهي عقد ترخيص برنامج مكافحة الفيروسات، وهو عقد مبرم بين مبرمج البرنامج ومستخدم البرنامج، حيث ينص على حق المستخدم في استخدام البرنامج لمكافحة الفيروسات في مقابل مبلغ نقدي يلتزم بدفعه للمبرمج.

سنتناول صور هذا العقد من خلال تقسيم هذا المبحث إلى:

المطلب الأول: عقد تأمين النظام المعلوماتي.

المطلب الثاني: عقد ترخيص برنامج مكافحة الفيروسات.

المطلب الأول
عقد تأمين النظام المعلوماتي

هو العقد الذي يُبرم بين شركة متخصصة في تأمين الأنظمة المعلوماتية ومالك النظام المعلوماتي، ويكون الهدف منه تأمين النظام المعلوماتي من أي اختراق أو فيرسة، وذلك طيلة المدة المحددة في العقد(٦٢).

وقد يكون الالتزام بتأمين النظام المعلوماتي هو شرط داخل عقد أكبر يُبرم بين شركة متخصصة في تكنولوجيا المعلومات ومالك هذا النظام، بحيث تكون الشركة مسؤولة عن بناء النظام المعلوماتي وتأمينه طوال الفترة المحددة في العقد(٦٣).

---

(٦٢) Raphael PEUCHOT, Rudiments juridiques à l'usage des clients de prestations d'intrusion informatique, Lamy Lexel, 26 mars 2002.

(٦٣) Dana ROSENFELD and Alysa HUTNIK, Data Security Contract Clauses for Service Provider Arrangements, Practical Law Publishing Limited, USA, 2011, p1.

عقد تأمين النظام المعلوماتي هو دائماً عقد محدد المدة تلتزم الشركة المتخصصة في تأمين الأنظمة المعلوماتية بمقتضاه باتخاذ كافة الاجراءات التقنية اللازمة لمنع أي اختراق أو فيرسة للنظام المعلوماتي هذا من ناحية(٦٤).

ومن ناحية أخرى، يلتزم مالك النظام المعلوماتي بأن يدلي لمسؤول التأمين (شركة تأمين الأنظمة المعلوماتية) بكل البيانات والمعلومات التي تطلبها الشركة، والمتعلقة بالنظام المعلوماتي، والتى من شأنها مساعدة الشركة في اتخاذ الإجراءات الملائمة لحماية النظام(٦٥).

قد يتم النص في العقد على التزام شركة تأمين الأنظمة المعلوماتية باتخاذ كافة وسائل التأمين المتاحة لتأمين النظام المعلوماتي، في هذه الحالة تلتزم الشركة باتخاذ أحدث وسائل التأمين المتاحة في سوق تكنولوجيا المعلومات.

ولكن من ناحية أخرى من الممكن النص في العقد على أن التزام الشركة منحصر في إجراء تأميني معين كأن تلتزم باستخدام برامج مكافحة فيروسات من إصدار ٢٠١٣ مثلاً، في هذه الحالة لا تلتزم الشركة باستخدام الإصدارات الأحدث من البرامج التي ستظهر في مدة تنفيذ العقد(٦٦).

وغالباً ما يتضمن العقد التزاماً على عاتق شركة تأمين الأنظمة المعلوماتية في اتخاذ الإجراءات التقنية لإزالة أي فيروسات تصيب النظام المعلوماتي في الحال قبل أن تنشط هذه الفيروسات وتُلحق ضرراً بالنظام، ويمتد الالتزام إلى القيام بالإزالة حتى بعد إحداث الضرر تفادياً لأضرار أخرى أكبر(٦٧).

---

(٦٤) Raphael PEUCHOT, Rudiments juridiques à l'usage des clients de prestations d'intrusion informatique, Op.cit.

(٦٥) Ibid.

(٦٦) Dana ROSENFELD and Alysa HUTNIK, Data Security Contract Clauses for Service Provider Arrangements, Op.cit, p8.

(٦٧) Ibid, p11.

لمزيد من التفاصيل عن إبرام العقود عبر الإنترنت انظر:

- Michelle BAPTISTE et Xavier STRUBEL, Cre?er et exploiter un commerce e?lectronique, litec, 1998, p 103.
- Christiane SCHUHL, cyber droit: le droit à l'épreuve de l'internet, Dalloz, 2 éme éd, 2001, p 159.
- Sylvette GUILLEMARD, Le droit international prive? face au contrat de vente cyberspatial, thèse de doctorat, fac de droit, univ Paris II, 2003, p 310.
- Michel ZOIA, La notion de consentement a? l'e?preuve de l'e?lectronique, Gaz pal, 15-17 juillet 2001, p 16. =

ويلتزم مالك النظام المعلوماتي بدفع مقابل نقدي لشركة تأمين الأنظمة المعلوماتية، يتحدد مقداره بحسب مدى التزام الشركة باتخاذ أحدث وسائل التأمين المتاحة، أم تنحصر فقط في اتخاذ إجراء تأميني معين، فيزيد المقابل أو ينقص تبعاً لزيادة أو نقصان التزام شركة التأمين.

المطلب الثاني
عقد ترخيص برنامج مكافحة الفيروسات

هو العقد الذي يُبرم بين مبرمج برنامج مكافحة الفيروسات ومستخدم هذا البرنامج، بحيث يرخص للمستخدم أن يستعمل هدا البرنامج لمكافحة الفيروسات الموجودة في نظامه المعلوماتي.

في الغالب يتم إبرام هذا العقد عبر شبكة الإنترنت، بحيث تكون شروط العقد موجودة على موقع الشركة، ويوافق عليها المرخص له بالضغط على أيقونة القبول، ويقوم بدفع المقابل عبر الإنترنت باستخدام بطاقة الدفع الإلكتروني، فيسمح له المبرمج بتحميل البرنامج وتشغيله على النظام المعلوماتي الخاص به.

ويعتبر وجود شروط العقد ومقابل الترخيص على الموقع الإلكتروني إيجاباً من جانب المبرمج، والضغط على أيقونة القبول هو قبول من جانب المُرخص له ينعقد به العقد تاماً(٦٨).

وقد يقوم المرخص له بشراء أسطوانة محمل عليها البرنامج، بحيث تظهر شروط الترخيص فور تشغيل هذه الأسطوانة، ولا يعمل البرنامج إلا بقيام المرخص

= - Murielle CAHEN, Le consentement sur internet, Art disponible sur, la date de mise en ligne est 15/3/2004.

(٦٨) لمزيد من التفاصيل عن إبرام العقود عبر الإنترنت انظر:
- Michelle BAPTISTE et Xavier STRUBEL, Créer et exploiter un commerce électronique, litec, 1998, p 103.
- Christiane SCHUHL, cyber droit: le droit à l'épreuve de l'internet, Dalloz, 2 éme éd, 2001, p 159.
- Sylvette GUILLEMARD, Le droit international priveé face au contrat de vente cyberspatial, thèse de doctorat, fac de droit, univ Paris II, 2003, p 310.
- Michel ZOIA, La notion de consentement à l'épreuve de l'électronique , Gaz pal, 15-17 juillet 2001, p 16 .
- Murielle CAHEN, Le consentement sur internet, Art disponible sur www.droit-tic.com , la date de mise en ligne est 15/3/2004.

له بقبول هذه الشروط بحيث ينعقد عقد الترخيص فور قبول هذه الشروط، فيبدأ البرنامج في التحميل والعمل بعدها.

ويتضمن عقد ترخيص برنامج المكافحة من الفيروسات عدة شروط أهمها: صلاحية البرنامج وكفاءته لمكافحة الفيروسات، والتزام المرخص (المبرمج) بتوفير التحديث للبرنامج عبر شبكة الإنترنت، كلما ظهرت فيروسات جديدة، بحيث يكون البرنامج صالحاً للتصدي لها(٦٩).

ونعتقد أنه من الصعب أن نكيف اتفاق ترخيص برنامج مكافحة الفيروسات، وفقاً لأي عقد من العقود المسماة في القانون المدني، ولكن يمكن أن نعتبر اتفاق الترخيص هو عقد من العقود غير المسماة التي يرخص بمقتضاها المبرمج للمستخدم في استخدام البرنامج لمكافحة الفيروسات التي قد تصيب نظامه المعلوماتي، ويلتزم المرخص له بالوفاء بالمقابل النقدي المتفق عليه، وباحترام قواعد حماية حق المؤلف الواردة في قانون حماية الملكية الفكرية.

ويُلاحظ أن هذا الاتفاق هو دائماً عقد إذعان؛ وذلك لأن المبرمج يضع مجموعة من الشروط في العقد، ولا يقبل إطلاقاً بأي مناقشة أو تفاوض لتعديل هذه الشروط من قبل المستخدم، كما أن هذا العقد تكون شروطه واحدة بالنسبة لجميع المستخدمين فلا تتغير من مستخدم إلى آخر(٧٠).

---

(٦٩) Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, Op.cit.

(٧٠) Eric A CAPRIOLI et Noelle LEBOEUF, Innovation informatique: Les risques des logiciels open source, Art disponible sur: www.caprioli-avocats.com, La date de mise en ligne est: octobre 2007.

الجدير بالذكر أن هناك خلافاً بين الفقه الفرنسي والفقه المصري حول مفهوم عقد الإذعان، فالفقه الفرنسي يرى أن عقد الإذعان هو عقد يكون بين طرفين غير متساويين اقتصادياً، ويقوم الطرف القوي بإعداد شروط العقد سلفاً، ولا يقبل أي تفاوض من الطرف الآخر، فلا يكون أمام الطرف الضعيف سوى قبول كل هذه الشروط أو رفضها. انظر:

- Jean CARBONNIER, Droit civil: les obligations, presses universitaires de France, 9 ème éd, 1976, P 57.
- Eric FLOUR et Jean AUBERT, Droit civil, les obligations, V.I: l'acte juridique, deuxième éd, 1977, pcollection u, Armand colin, P 125, nº183.
- Christian LARROUMET, Droit civil: les obligations: le contrat, t.3, 4 ème éd, paris, Economica, 1998, P 234et S.
- Alex WEILL et François TERRE, Droit civil: les obligations, DALLOZ, 4 ème éd, 1986, PP 91- 92, nº95.

=

المبحث الثاني
أركان المسؤولية العقدية

حتى تقوم المسؤولية العقدية في حق المدين يجب أن يخل المدين بالتزامه العقدي، وأن يترتب على ذلك الإخلال ضرر يصيب الطرف الآخر في العقد، وبالتالي فأركان المسؤولية العقدية هي الخطأ العقدي والضرر وعلاقة السببية بينهما.

ومن ثم فحتى تقوم المسؤولية العقدية عن الإصابة الفيروسية للنظام المعلوماتي، فيجب أن يكون مسؤول التأمين المعلوماتي قد أخل بالتزامه المُلقى على

= بينما استقر الفقه المصري التقليدي على أن هناك ثلاثة شروط يجب توافرها في العقد حتى يمكن وصفه بأنه عقد إذعان، هذه الشروط هي:
أولاً: أن يتعلق العقد بسلع أو مرافق تعتبر من الضروريات بالنسبة للمستهلكين أو المنتفعين؛
ثانياً: احتكار الموجب لهذه السلع أو المرافق احتكاراً قانونياً أو فعلياً، أو على الأقل سيطرته عليها سيطرة تجعل المنافسة فيها محدودة النطاق؛
ثالثاً: توجيه الإيجاب إلى الناس كافة وبشروط واحدة.
انظر: – السنهوري، الوسيط، نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ١٩١-٢١٩، رقم ١١٦.
– محمود جمال الدين زكي، نظرية الالتزام في القانون المصري، الجزء الأول: مصادر الالتزام، مطبعة جامعة القاهرة والكتاب الجامعي، الطبعة الثانية، ١٩٧٦، ص ٨٢،٨٣، رقم ٤٧.
– سمير تناغو، نظرية الالتزام، منشأة المعارف بالإسكندرية، مصر، بدون سنة نشر، ص ٤٦-٤٧، رقم ٣٤.
– أنور سلطان، الموجز في النظرية العامة للالتزام، مرجع سابق، ص ٦٨.
– عبد الودود يحيى، الموجز في النظرية العامة للالتزامات، دار النهضة العربية، مصر، ١٩٩٤، ص ٤٦، رقم ٣٢.
– عبد الناصر توفيق العطار، مصادر الالتزام، ١٩٩٠، بدون ناشر، ص ١١٧.
– جلال علي العدوي، أصول الالتزامات: مصادر الالتزام، منشأة المعارف بالإسكندرية، مصر، ١٩٩٧، ص ٥٦،٥٥، رقم ١١٠.
وهناك رأى في الفقه المصري – نميل إليه – يأخذ بمفهوم حديث لعقد الإذعان، وهو أنه العقد الذي يسلم فيه أحد الأطراف بالشروط التي يضعها الطرف الآخر دون أن يكون له القدرة على التفاوض، وقد استند هذا الرأي إلى الصياغة العامة لنص المادة ١٠٠ من القانون المدني، والتي وضعت تحديداً عاماً لعقد الإذعان بأن القبول فيه يقتصر على مجرد التسليم بشروط مقررة يضعها الموجب، ولا يقبل أي مناقشة فيها. انظر:
– حمدي عبد الرحمن، الوسيط في النظرية العامة للالتزامات: المصادر الإرادية للالتزام، دار النهضة العربية، الطبعة الأولى، ١٩٩٩، ص٥٧-٥٩.

عاتقه في عقد التأمين المعلوماتي، وأن يترتب على ذلك الإخلال أن يصيب الفيروس النظام المعلوماتي بضرر.

سنتناول أركان المسؤولية العقدية من خلال تقسيم هذا المبحث إلى:

المطلب الأول: الخطأ العقدي.

المطلب الثاني: الضرر.

المطلب الثالث: علاقة السببية.

المطلب الأول
الخطأ العقدي

الخطأ العقدي هو عدم قيام المدين بتنفيذ التزامه الناشئ عن العقد أياً كان سبب عدم التنفيذ، ويستوي في ذلك أن يكون عدم قيام المدين بالالتزام ناشئاً عن عمده أو عن إهماله، بل إن الخطأ العقدي يتحقق حتى لو كان عدم قيام المدين بالالتزام ناشئاً عن سبب أجنبي لا يد له فيه كالقوة القاهرة، ولكن يُلاحظ في هذه الحالة الأخيرة أنه إذا تحقق الخطأ العقدي، فإن علاقة السببية – وهي ركن في المسؤولية العقدية – تنعدم، ولا تتحقق المسؤولية تبعاً لذلك(٧١).

عدم تنفيذ الالتزام تختلف صورته بحسب نوع الالتزام، فهناك نوعان من الالتزامات؛ الالتزام بتحقيق نتيجة والالتزام ببذل عناية، فالالتزام بتحقيق نتيجة هو الالتزام الذي يوجب على المدين تحقيق نتيجة معينة هى محل الالتزام، ويتمثل عدم تنفيذ الالتزام في مجرد عدم تحقيق النتيجة، ولو بذل المتعاقد كل جهده في العمل على تحقيقها(٧٢).

أما الالتزام ببذل عناية فهو التزام لا يوجب على المدين تحقيق نتيجة معينة، بل

---

(٧١) عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٦٥٦، فقرة ٤٢٧.
– سمير تناغو، مصادر الالتزام، مرجع سابق، ص ١٦٩، فقرة ١٣٢.
– أنور سلطان، الموجز في النظرية العامة للالتزام، مرجع سابق، ص ٢٤٩-٢٥٠، فقرة ٢٨٣.
– محمد حسين منصور، النظرية العامة للالتزام، مرجع سابق، ص ٣٩٣-٣٩٤.
– حمدي عبد الرحمن، الوسيط في النظرية العامة للالتزامات، مرجع سابق، ص ٥٠٥-٥٠٦.
– رمضان أبو السعود، مصادر الالتزام، مرجع سابق، ص ٢٣٥.

(٧٢) محمد حسين منصور، النظرية العامة للالتزام، مرجع سابق، ص ٣٩٤.

يلزمه فحسب بأن يبذل قدراً معيناً من العناية للوصول إلى غرض معين، فالمدين لا يأخذ على عاتقه تحقيق نتيجة معينة يبتغيها الدائن، وإنما يتعهد بمجرد بذل جهد معين للوصول إلى هذه النتيجة، سواء تحققت بالفعل أو لم تتحقق. فإذا بذل المدين هذا القدر من العناية فحسبه ذلك، ولا عليه بعد ذلك إذا لم يتحقق الغرض المقصود(٧٣).

فيما يتعلق بالالتزام بتحقيق نتيجة يكفي أن يثبت الدائن عدم قيام المدين بتحقيق النتيجة حتى يثبت إخلال المدين بالتزامه وإسناد الخطأ العقدي إليه، أما في الالتزام ببذل عناية، فلا يكفي إثبات الدائن عدم قيام المدين بتحقيق النتيجة، وإنما يجب أن يثبت عدم قيام المدين ببذل عناية الشخص المعتاد في تنفيذ التزامه(٧٤).

- خطأ شركة تأمين النظام المعلوماتي

لا يوجد خلاف على أن التزام شركة تأمين النظام المعلوماتي هو التزام ببذل عناية، وليس التزام بتحقيق نتيجة، فتعتبر الشركة قد أوفت بالتزامها إذا استخدمت كل وسائل التأمين من الفيروسات المطروحة، حيث يجب عليها أن تستخدم برامج المكافحة من الفيروسات المتاحة(٧٥).

ويرجع ذلك للتطور المستمر للفيروسات، وعدم قدرة وسائل التأمين على ملاحقة هذا التطور، فغالباً ما يسبق التطور في الفيروسات التطور الحادث في برامج المكافحة منها(٧٦).

فحتى نقول إن شركة تأمين النظام المعلوماتي قد أوفت بالتزامها، فإنه يجب أن تكون قد اتخذت وسائل التأمين المعتادة لتأمين النظام المعلوماتي، ووسائل التأمين المعتادة هى الوسائل التقنية التي يستخدمها مسؤولو التأمين عادة لتأمين النظام المعلوماتي.

إلا أننا يجب ألا نغفل أمراً هاماً وهو التطور المستمر لتكنولوجيا المعلومات

---

(٧٣) المرجع السابق، ص ٤٩٥-٤٩٦.

(٧٤) أنور سلطان، الموجز في النظرية العامة للالتزام، مرجع سابق، ص ٢٥٤-٢٥٥.

(٧٥) Jean-Vasken ALYANAKIAN, Quels recours en cas de manquement contractuel ou de fraude?, Art disponible sur: www.01net.com, La date de mise en ligne est: 06/05/2011.
- Raphael PEUCHOT, Rudiments juridiques à l'usage des clients de prestations d'intrusion informatique, Op.cit.

(٧٦) Meiring VILLIERS, Computer viruses and civil liability, Op.cit.

والفيروسات الذي لا يكفي معه – في رأينا – القول باستخدام وسائل التأمين المعتادة، وإنما استخدام أحدث وسائل التأمين المتاحة في سوق تكنولوجيا المعلومات.

وبالتالي فالمعيار – في رأينا – لتحديد وجود خطأ عقدي في جانب شركة تأمين النظام المعلوماتي هو مدى استخدامها لأحدث وسائل التأمين المعلوماتي المتاحة في سوق تكنولوجيا المعلومات من عدمه.

فإذا أثبت المضرور عدم قيام شركة تأمين النظام المعلوماتي باستخدام أحدث وسائل التأمين المتاحة في سوق تكنولوجيا المعلومات، فإنه يكون قد أثبت الخطأ العقدي في جانب الشركة.

ولكن يكون من حق شركة تأمين النظام المعلوماتي أن تنفي الخطأ بإثبات قيامها باتخاذ أحدث وسائل التأمين المتاحة، ولكن هذه الوسائل لم تفلح في صد الهجمة الفيروسية(٧٧).

ولكن ما ذكرناه سالفاً لا ينطبق في حالة ما إذا كان منصوصاً في عقد تأمين النظام المعلوماتي على التزام مسؤول التأمين باتخاذ إجراء تأميني معين، هنا ينحصر التزامه بهذا الإجراء دون غيره(٧٨).

ويعتبر خطأ من جانب شركة تأمين النظام المعلوماتي عدم اتخاذ الإجراءات التقنية لإزالة الفيروسات التي تكون قد أصابت النظام المعلوماتي بالفعل قبل أن تنشط وتحدث ضرراً، أو قبل أن تحدث ضرراً أكبر من الذي أحدثته.

ويجب أن نقرر أخيراً أن تقدير ما إذا كانت شركة تأمين النظام المعلوماتي قد اتخذت وسائل التأمين الملائمة من عدمه هو أمر يخضع للسلطة التقديرية لقاضي الموضوع في كل حالة على حدة.

فقد يقدر القاضي أن شركة تأمين النظام المعلوماتي لم تتخذ الإجراءات التأمينية الملائمة، إذا كانت الإصابة قد حدثت من فيروس قديم تم تحديث برامج المكافحة للقضاء عليه، وقد يقدر القاضي أن شركة تأمين النظام المعلوماتي قد اتخذت كل وسائل التأمين الممكنة إذا كانت الإصابة قد حدثت من فيروس جديد لم يتم تحديث برامج مكافحة الفيروسات للقضاء عليه بعد(٧٩).

---

(٧٧) Jean-Vasken ALYANAKIAN, Quels recours en cas de manquement contractuel ou de fraude?,Op.cit.

(٧٨) Raphael PEUCHOT, Rudiments juridiques à l'usage des clients de prestations d'intrusion informatique, Op.cit.

(٧٩) Blandine POIDEVIN, Quelle responsabilité en matière de sécurité informatique?,Op.cit.

وتطبيقاً لذلك قضت محكمة النقض الفرنسية – بشأن أحد الطعون الذي طرح أمامها – بوجود خطأ عقدي في جانب مسؤول التأمين لعدم قيامه باستخدام أحدث وسائل التأمين المتطورة والمتاحة، مما أدى لإصابة النظام المعلوماتي للطرف الآخر في العقد بفيروس(٨٠).

– خطأ مبرمج برنامج مكافحة الفيروسات

يمكن أن تثور مسؤولية مبرمج برنامج مكافحة الفيروسات إذا كان هناك خلل في البرنامج أدى إلى عدم التصدي للفيروس، أي أن يكون هناك خطأ في التصميم يؤدي لعدم تحقيق البرنامج لهدفه الأساسي في التصدي للفيروسات(٨١).

ولكن لا يكون المبرمج مسؤولاً في حالة عدم تشغيل البرنامج على النظام المعلوماتي للمضرور لعدم ملائمة البرنامج لهذا النظام المعلوماتي؛ لأن شروط ترخيص البرنامج تحدد فيها الأنظمة المعلوماتية المتوائم معها هذا البرنامج، فإذا قام المرخص له بتثبيت البرنامج على الرغم من عدم مواءمة البرنامج للنظام المعلوماتي، فذلك يعتبر خطأ من المرخص له وليس خطأ من المبرمج.

وتطبيقاً لذلك: حكم القضاء الفرنسي بعدم وجود خطأ عقدي في جانب مبرمج برنامج مكافحة الفيروسات لعدم تشغيل البرنامج على نظام معلوماتي مختلف عن النظام المعلوماتي المتوائم مع البرنامج وفقاً لما هو موضح في شروط عقد الترخيص(٨٢).

وإذا كان برنامج حماية الفيروسات لا يعمل، أو لم تتوافر فيه الخصائص التي نص عليها العقد، في هذه الحالة يكون مبرمج البرنامج قد ارتكب خطأً عقدياً لعدم تنفيذ الالتزام المنصوص عليه في العقد(٨٣).

ولكن مجرد عدم قيام البرنامج بالتصدي لكل الفيروسات لا يعتبر خطأً عقدياً؛

---

(٨٠) Cass.Com, 7 juillet 2009, N° 08-14231.

(٨١) - Nicholas VERMEYS, Computer "Insecurity" and Viral attacks, Op.cit.
- Frédéric DUFLOT, Les Infections Informatiques Bénéfiques: Chroniques d'un anathème, DESS de Droit du Numérique et des Nouvelles Techniques, Univ Paris XI, Fac Jean Monnet, 2003-2004, P 57.

(٨٢) - Juridiction de proximité de vanves, 2 septembre 2008, RG N° 91-08-000006.
- CA Montpellier, 9 Mars 2004, RG N° 03/00974.

(٨٣) Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, Op.cit.

لأن التزام مبرمج البرنامج هو التزام ببذل عناية وليس التزام بتحقيق نتيجة، فهو عليه التزام ببرمجة برنامج يستطيع التصدي للفيروسات، ولكن نظراً لتجدد الفيروسات وتطورها وظهور فيروسات جديدة، فلا يشترط أن يكون البرنامج قادراً على التصدي لكل هذه الفيروسات الجديدة(٨٤).

فالتأمين المعلوماتي من الناحية الفنية هو التصدي للفيروسات التي تهدد النظام المعلوماتي، هذا التصدي لا يمكن من الناحية الفنية أن يتحقق بنسبة المائة في المائة، وإنما يفترض دائماً احتمالية حدوث الإصابة(٨٥).

فلا يمكن أن نقرر بسهولة أن برنامج فيروسات معين هو برنامج جيد أم لا، وإنما يخضع الأمر للسلطة التقديرية للقاضي الذي يستطيع الاستعانة بالخبير الذي يقرر ما إذا كان برنامج حماية الفيروسات برنامجاً كفئاً أم لا(٨٦).

ولكن حتى يكون المبرمج قد أوفى بالتزامه، فيجب عليه أن يقوم بعمل تحديث للبرنامج بصورة منتظمة حتى يكون قادراً على مواجهة الفيروسات الجديدة، وأن يتيح هذا التحديث للمستخدم على موقعه على شبكة الإنترنت، بحيث يستطيع المستخدم تحديث البرنامج بمجرد الاتصال بالشبكة(٨٧).

المطلب الثاني
الضرر

الركن الثاني في المسؤولية العقدية هو الضرر، فلا بد من وجود ضرر حتى تترتب هذه المسؤولية في ذمة المدين، ولا يُفترض وجود الضرر لمجرد أن المدين لم يقم بتنفيذ التزامه العقدي، فقد لا ينفذ المدين التزامه ولا يصيب الدائن ضرر من ذلك(٨٨).

---

(٨٤) - Murielle CAHEN, La sécurité et les systèmes informatiques, Art disponible sur: http://www.murielle-cahen.fr, La date de mise en ligne est: 17 mai 2012.
- Frédéric DUFLOT, Les Infections Informatiques Bénéfiques, Op.cit, P 57.

(٨٥) Valérie SEDALLIAN, Légiférer sur la sécurité informatique: la quadrature du cercle?, Etude disponible sur: http://www.juriscom.net/, La date de mise en ligne est: 5 décembre 2003, P 3.

(٨٦) Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, Op.cit.

(٨٧) Murielle CAHEN, La sécurité et les systèmes informatiques, Op.cit.

(٨٨) السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٦٧٩، فقرة ٤٤٢.

حتى تثبت المسؤولية العقدية لشركة تأمين النظام المعلوماتي، أو مبرمج برنامج مكافحة الفيروسات فيجب أن يترتب ضرر عن خطئه العقدي المتمثل في الإخلال بالتزامه، ويقع على عاتق مالك النظام المعلوماتي أو المرخص له – على حسب الأحوال – إثبات هذا الضرر.

ولكن الإخلال بتأمين النظام المعلوماتي يجعل هذا النظام عرضة للإصابة الفيروسية، أي أن وجود الخطأ العقدي يرفع من نسبة تحقق الضرر وهو الإصابة الفيروسية خاصة إذا كان النظام المعلوماتي مرتبطاً بشبكة الإنترنت، فهل الضرر في هذه الحالة هو ضرر محقق الوقوع في المستقبل، ويتم التعويض عنه، أم أنه ضرر احتمالى لا يتم التعويض عنه؟

ومما لا شك فيه أن الإخلال بتأمين النظام المعلوماتي يجعله عرضة لإصابة فيروسية، ولكن هذا الضرر – في رأينا – هو ضرر محتمل، لأن الإصابة الفيروسية للنظام المعلوماتي قد تحدث، ولكن يظل الفيروس خاملاً فلا يصيب النظام بأي ضرر؛ وذلك لعدم فتح الملف الملتصق به الفيروس.

فمجرد دخول الفيروسات للنظام المعلوماتي لا يعتبر ضرراً في رأينا؛ لأن الضرر يتحقق عندما يتم تحفيز الفيروس على العمل، فيقوم بإحداث خلل بالنظام المعلوماتي، أو بمسح ملفات، أو بإيقاف النظام .... الخ.

وهذا التحفيز للفيروس قد لا يحدث إذا لم يقم مالك النظام بفتح الملف الملتصق به الفيروس، وقد يقوم مالك النظام بمسح الملف ومسح الفيروس تبعاً له، فلا يحدث أي ضرر، مما يجعل الإصابة بالفيروس – في حد ذاتها – ضرراً محتملاً لا يُعوض عنه.

ويُتصور أن يترتب على الخطأ ضرر أدبي لمالك النظام المعلوماتي، متمثلاً في الأذى الذي يصيبه نتيجة شعوره بالعجز، لعدم قدرته على استخدام النظام المعلوماتي الخاص به بعد توقفه نتيجة الإصابة الفيروسية، وهو ما يقدر القاضي وجوده من عدمه في كل حالة على حدة.

المطلب الثالث
علاقة السببية

لا يكفي – حتى تقوم المسؤولية العقدية – أن يكون هناك خطأ وضرر، بل يجب أن تكون هناك علاقة سببية بينهما، وذلك بأن يكون الضرر مترتباً على الخطأ.

يقع على عاتق الدائن إثبات أن الضرر الذي أصابه هو نتيجة معقولة لخطأ المدين، فإذا أثبت ذلك قامت قرينة قضائية على علاقة السببية بين خطأ المدين والضرر الذي أصاب الدائن(٨٩).

ويستطيع مالك النظام المعلوماتي إثبات علاقة السببية بسهولة، فإثبات خطأ شركة تأمين النظام المعلوماتي أو خطأ مبرمج برنامج مكافحة الفيروسات، وإثبات الضرر الذي لحق النظام المعلوماتي نتيجة الإصابة بالفيروسات، يؤدي إلى إقامة قرينة قضائية على علاقة السببية.

وإذا أراد المدين أن يدفع المسؤولية عن نفسه، فإنه يستطيع أن يثبت أن الضرر يرجع إلى سبب أجنبي لا يد له فيه، أو يثبت أن الضرر غير مباشر أو غير متوقع.

- السبب الأجنبي:

يستطيع المدين أن ينفي علاقة السببية في المسؤولية العقدية إذا أثبت أن الضرر الذي حدث لا يرجع إلى خطئه، ولكن يرجع إلى سبب أجنبي لا يد له فيه. وفقاً للمادة ١٦٥ من القانون المدني فإن السبب الأجنبي هو الحادث المفاجئ، أو خطأ الغير، أو خطأ المضرور.

وهذه القاعدة العامة تثير عدة تساؤلات وهي:

التساؤل الأول: هل يستطيع مسؤول التأمين المعلوماتي (شركة تأمين النظام المعلوماتي أو مبرمج برنامج مكافحة الفيروسات) الادعاء بأن الضرر قد نشأ عن حادث مفاجئ هو هجوم فيروسي عبر شبكة الإنترنت، ومن ثم لا تقام مسؤوليته العقدية على الرغم من وجود خطأ من جانبه؟

الحادث المفاجئ هو حادث غير ممكن التوقع ومستحيل الدفع، فيجب أن يكون الحادث المفاجئ غير مستطيع التوقع لا من جانب المدعى عليه فقط، بل من جانب أشد الناس يقظة، فالمعيار هنا موضوعي لا ذاتي، وعدم إمكان التوقع في المسؤولية العقدية يكون وقت إبرام العقد(٩٠).

ويجب أيضاً أن يكون الحادث المفاجئ مستحيل الدفع، فإذا أمكن دفع الحادث حتى لو استحال توقعه لم يكن قوة قاهرة أو حادثاً مفاجئاً.

---

(٨٩) أنور سلطان، الموجز في النظرية العامة للالتزام، مرجع سابق، ص ٢٦٨.

(٩٠) السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٩٩٦-٩٩٧.

نرى بأن شروط الحادث المفاجئ السابقة لا تتوافر في أي هجمة فيروسية مهما كانت شدتها، فالشرط الأول الخاص بعدم إمكان التوقع وقت إبرام العقد غير متوافر؛ لأن محل العقد هو تأمين النظام المعلوماتي من أي هجمات فيروسية، فلا يستطيع مسؤول التأمين المعلوماتي أن يدعي بعدم توقعه حدوث الهجمة الفيروسية، فلا يعتبر ذلك حادثاً مفاجئاً ينفي علاقة السببية بين خطئه والضرر.

التساؤل الثاني: هل يستطيع مسؤول التأمين المعلوماتي (شركة تأمين النظام المعلوماتي أو مبرمج برنامج مكافحة الفيروسات) التمسك بخطأ مبرمج الفيروس الذي أصاب النظام المعلوماتي للتخلص من مسؤوليته على الرغم من وجود خطأ من جانبه؟

وفقاً للقواعد العامة فإن المعيار هنا هو مدى استغراق خطأ الغير لخطأ المدعى عليه من عدمه، فإذا استغرق خطأ الغير خطأ المدعى عليه، ففي هذه الحالة لا يعتد بخطأ المدعى عليه، وتقوم مسؤولية الغير كاملة، أما إذا كان خطأ المدعى عليه مستغرقاً لخطأ الغير فلا يعتد بخطأ الغير، وتقوم مسؤولية المدعى عليه كاملة(٩١).

ونرى أن خطأ الغير المتمثل في خطأ مبرمج الفيروس لا يمكن أن يستغرق خطأ مسؤول التأمين المعلوماتي بأي حال من الأحوال، فعلى الرغم من أن خطأ مبرمج الفيروس هو خطأ عمدي، إلا أن محل التزام مسؤول التأمين هو اتخاذ كافة الإجراءات التقنية اللازمة للتوقي من خطأ مبرمج الفيروس، فإن قصر مسؤول التأمين في اتخاذ هذه الاحتياطات، فيكون مخطئاً ولا يستطيع الادعاء بوجود خطأ للغير لقطع علاقة السببية بين خطئه والضرر.

التساؤل الثالث: هل يستطيع مسئول التأمين المعلوماتي (شركة تأمين النظام المعلوماتي أو مبرمج برنامج مكافحة الفيروسات) التمسك بخطأ المضرور نفسه، كأن يدعي أن المضرور كثير الولوج على المواقع الإباحية، وتحميل الملفات التي تحتوي على فيروسات؟

ومما لا شك فيه أن هناك خطأ في هذه الحالة من جانب المضرور؛ لأنه ليس من السلوك المعتاد أن يقوم المستخدم بالولوج إلى المواقع غير المشروعة، وتحميل الملفات التي يعرف بأنها غالباً ما تكون مصابة بالفيروسات، فهناك خطأ من جانب المضرور في هذه الحالة(٩٢).

---

(٩١) أنور سلطان، الموجز في النظرية العامة للالتزام: مصادر الالتزام، مرجع سابق، ص ٣٦٢-٣٦٣.

(٩٢) Nicholas VERMEYS, Virus informatiques: Responsables et responsabilité, Op.cit, P 136.

ففي هذه الحالة على الرغم من وجود خطأ من جانب مسؤول التأمين المعلوماتي، إلا أن هناك خطأ من جانب المضرور، والقاعدة هنا هى مدى استغراق أحد الخطأين للآخر من عدمه، وذلك حسب مدى جسامة كل منهما وفقاً لتقدير القاضي في كل حالة على حدة.

فإذا قدر القاضي أن خطأ المضرور يستغرق خطأ مسؤول التأمين المعلوماتي، فإنه يعفيه تماماً من المسؤولية، وإذا قدر أن خطأ مسؤول التأمين المعلوماتي يستغرق خطأ المضرور، فإنه يلقي بالمسؤولية كاملة على عاتق مسؤول التأمين.

وإذا قدر القاضي أن الخطأين مستقلان، فإنه يقسم المسؤولية بينهما، مما يؤدي إلى التخفيف من مسؤولية مسؤول التأمين المعلوماتي، هذا التخفيف قد يصل إلى النصف أو أكثر أو أقل حسب تقدير القاضي لمدى جسامة خطأ كل منهما.

- الضرر المتوقع:

وفقاً لصريح نص الفقرة الثانية من المادة ٢٢١ من القانون المدني، فلا يلتزم المدين في المسؤولية العقدية إلا بتعويض الضرر المتوقع، وذلك مالم يكن قد ارتكب غشاً أو خطأً جسيماً.

وتثير هذه المسألة إشكالية خاصة فيما يتعلق بتحديد الضرر المتوقع الذي يُسأل عنه المخطئ، والضرر غير المتوقع الذي لا يُسأل عنه، وذلك نظراً لسرعة تعاقب الأضرار المترتبة على الإصابات الفيروسية واتساع انتشارها.

وفقاً للفقرة الثانية من المادة ٢٢١ فإن الضرر المتوقع هو الضرر الذي كان يمكن توقعه عادة عند التعاقد.

وبالتالي فإن المعيار وفقاً للنص هو أن الضرر المتوقع هو الذي يتوقعه الشخص المعتاد في مثل الظروف الخارجية التي وجد فيها المدين عند التعاقد، لا الضرر الذي يتوقعه هذا المدين بالذات(٩٣).

وبالتالي فإن مسؤول التأمين المعلوماتي يجب أن يتوقع أن تكون الأضرار كبيرة ومتسعة، إذا كان النظام المعلوماتي الملتزم بتأمينه هو نظام مملوك لشركة كبيرة، أو لهيئة، أو بنك، أو مؤسسة حكومية، أو جامعة مثلاً، ويتوقع أن تكون الأضرار أقل إذا كان النظام المعلوماتي خاصاً بمستخدم بسيط.

---

(٩٣) السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٦٨٦-٦٨٧، فقرة ٤٥٣.

- **الضرر المباشر:**

من ناحية أخرى فإن المدين لا يُسأل إلا عن الضرر المباشر، والضرر المباشر هو الضرر الذي يكون نتيجة طبيعية لعدم الوفاء بالالتزام أو التأخر فيه، وهو يعتبر كذلك إذا لم يكن في استطاعة الدائن توقيه ببذل جهد معقول(٩٤).

وبالتالي لا يلتزم مسؤول التأمين المعلوماتي سوى بتعويض الأضرار المباشرة المترتبة على خطئه العقدي، وهى الأضرار التي لا يستطيع مالك النظام المعلوماتي أن يتوقاها ببذل جهد معقول، فمثلاً إذا ترتب على الإصابة الفيروسية للنظام المعلوماتي لإحدى الجامعات تدمير هذا النظام، وضياع كل بيانات الطلاب، فهنا يعد تدمير النظام المعلوماتي ضرراً مباشراً لعدم قدرة الجامعة على توقي هذا الضرر، أما ضياع بيانات الطلاب فهو ضرر غير مباشر؛ لأنها بسهولة تستطيع عمل ملف ورقي بجانب الملفات الإلكترونية، وهذا ما يجري عليه العمل في الجامعات، حيث يُعتمد على هذه الملفات في حالة توقف النظام المعلوماتي للصيانة مثلاً.

ويقع على عاتق القاضي تقدير مدى اعتبار الضرر مباشراً من عدمه في كل حالة على حدة حسب تقديره لمدى قدرة الدائن على بذل الجهد المعقول لتوقي الضرر من عدمه.

المبحث الثالث
تعديل قواعد المسؤولية العقدية

حيث إن الأضرار التي تترتب على الفيروسات قد تكون كبيرة، فإن مبرمج برنامج مكافحة الفيروسات يضع دائماً في عقد الترخيص شروطاً تهدف إلى إعفائه من المسؤولية أو التخفيف منها في حالة حدوث الضرر، كالتزامه بتعويض الضرر في حدود مبلغ معين(٩٥).

ومن ناحية أخرى فغالباً ما يتم النص في عقود تأمين النظام المعلوماتي على حدود معينة لالتزام شركة تأمين النظام المعلوماتي بتعويض الضرر الذي أصاب مالك النظام المعلوماتي نتيجة لحدوث الإصابة الفيروسية(٩٦).

---

(٩٤) محمد حسين منصور، النظرية العامة للالتزام، مرجع سابق، ص ٤٠٠.

(٩٥) Richard OWENS, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, Op.cit.

(٩٦) Dana ROSENFELD and Alysa HUTNIK, Data Security Contract Clauses for Service Provider Arrangements, Op.cit, p12.

من ناحية أخرى فقد يتفق المتعاقدان على تشديد المسؤولية العقدية بأن يتفق على أن مسؤول تأمين النظام المعلوماتي مسؤول عن أي أضرار تصيب النظام المعلوماتي، ولو لم يكن هناك خطأ من جانبه.

سنتناول حكم تعديل قواعد المسؤولية العقدية عن تأمين الأنظمة المعلوماتية من خلال تقسيم هذا المبحث إلى:

المطلب الأول: الإعفاء من المسؤولية أو التخفيف منها.

المطلب الثاني: تشديد المسؤولية.

المطلب الأول
الإعفاء من المسؤولية أو التخفيف منها

وفقاً للمادة ٢/٢١٧ من القانون المدني، فإنه يجوز الاتفاق على إعفاء المدين من أية مسؤولية مترتبة على عدم تنفيذ التزامه الوارد بالعقد، ماعدا ما يكون مترتباً على غشه أو خطئه الجسيم.

وبالتالي يُفهم من هذه المادة أن الاتفاق على الإعفاء من المسؤولية العقدية هو اتفاق صحيح، ولكن لا يجوز التخفيف من المسؤولية العقدية إلى حد الإعفاء من الفعل العمد أو ما يلحق بالفعل العمد، وهو الخطأ الجسيم(٩٧).

فلا يطبق شرط الإعفاء من المسؤولية إذا كان الضرر الذي أصاب الطرف الآخر مترتباً على غش أو خطأ جسيم ممن قرر هذا الشرط لمصلحته.

إذا طبقنا القواعد السابقة على عقود تأمين النظام المعلوماتي، فإنه يمكن القول إن شرط إعفاء شركة تأمين النظام المعلوماتي من المسؤولية أو التخفيف منها هو شرط صحيح، ما لم يكن هناك غش أو خطأ جسيم من جانب هذه الشركة.

---

(٩٧) السنهوري، الوسيط في شرح القانون المدني: الجزء الأول: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٦٧٣، فقرة ٤٣٩.
- سمير تناغو، مصادر الالتزام، مرجع سابق، ص ١٧٦-١٧٧، فقرة ١٣٦.
- أنور سلطان، الموجز في النظرية العامة للالتزام، مرجع سابق، ص ٣٨٧، فقرة ٤٥٧.
- محمد حسين منصور، النظرية العامة للالتزام، مرجع سابق، ص ٤١٢.
- حمدي عبد الرحمن، الوسيط في النظرية العامة للالتزامات، مرجع سابق، ص ٥٨١ – ٥٨٥.
- رمضان أبو السعود، مصادر الالتزام، مرجع سابق، ص ٢٣٩.

ونفس الحكم ينطبق على عقود ترخيص برامج مكافحة الفيروسات، فشرط إعفاء المبرمج من المسؤولية هو شرط صحيح إلا إذا كان هناك غش أو خطأ جسيم من جانب المبرمج، ففى هذه الحالة يكون هذا الشرط باطلاً ولا يكون له أي أثر.

ولكن من ناحية أخرى، فإن عقد الترخيص يعتبر – كما ذكرنا سابقاً – عقد إذعان، وبالتالي فالمستخدم يستأهل الحماية المقررة في المادة ١٤٩ من القانون المدني، التي تقضي بأنه إذا تضمن عقد الإذعان شروطاً تعسفية فإنه يجوز للقاضي أن يعدل هذه الشروط، أو أن يعفي الطرف الضعيف منها، وفقاً لما تقتضيه قواعد العدالة.

وتطبيقا لذلك فإنه إذا قدَّر القاضي أن شرط إعفاء المبرمج من المسؤولية الوارد في عقد الترخيص هو شرط تعسفي، فإن له أن يعدل هذا الشرط بما يزيل أثر التعسف، بل وله أن يلغيه ويعفي المستخدم منه، وسيترتب على هذا الإلغاء تقرير مسؤولية المبرمج عن إخلاله بالتزامه التعاقدي الذي أضر بالمستخدم.

المطلب الثاني
تشديد المسؤولية

قد يُتفق في عقد تأمين النظام المعلوماتي على تشديد مسؤولية شركة تأمين النظام المعلوماتي بحيث تكون مسؤولة عن أي أضرار تصيب النظام المعلوماتي من جراء الإصابة الفيروسية، حتى لو بذلت كل العناية المطلوبة منها، وأوفت بالتزامها على أكمل وجه.

هذا الاتفاق الخاص بتشديد المسؤولية ينتشر من الناحية العملية في عقود تأمين النظام المعلوماتي، ولا يتصور عملاً في عقود ترخيص برمجيات مكافحة الفيروسات، إذ جرى العمل في هذه الأخيرة على الإعفاء أو التخفيف من مسؤولية المبرمج.

ويهدف مالك النظام المعلوماتي من وضع مثل هذا الشرط في العقد إلى تأمين نفسه من أي أضرار قد تصيب النظام المعلوماتي، بحيث يُسأل الطرف الآخر عن تعويض هذه الأضرار، وفي مقابل ذلك يلتزم مالك النظام المعلوماتي بدفع مبلغ أكبر من المعتاد في سبيل هذا التأمين.

الأصل في الالتزام بعناية ألا يكون المدين مسؤولاً عن السبب الأجنبي، ولا عن الفعل المجرد من الخطأ، ويكون مسؤولاً عن فعله العمدي، وعن خطئه الجسيم وعن خطئه اليسير، ويجوز الاتفاق على تشديد هذه المسؤولية فيصبح المدين مسؤولاً عن

الخطأ التافه أو عن الفعل المجرد من الخطأ، وهنا ينقلب الالتزام بعناية إلى التزام بغاية، إذ يصبح المدين مسؤولاً عن تحقيق غاية، لا يتخلص من المسؤولية عنها إلا بإثبات السبب الأجنبي، وقد يصل التشديد في المسؤولية إلى مدى أبعد فيصبح المدين مسؤولاً حتى عن السبب الأجنبي(٩٨).

وفقاً لصريح نص الفقرة الأولى من المادة ٢١٧ من القانون المدني، فإنه يجوز الاتفاق على التشديد من المسؤولية حتى تصل إلى تحمل المدين لتبعة الحادث المفاجئ والقوة القاهرة، وبالتالي يكون الاتفاق على تشديد المسؤولية في عقد تأمين النظام المعلوماتي هو اتفاق صحيح حتى لو كان مضمونه التزام مسؤول التأمين على تعويض الأضرار الناشئة عن السبب الأجنبي.

الخاتمة:

تناولت الدراسة التي بين دفتي البحث موضوع (المسؤولية المدنية عن فيرسة النظم المعلوماتية عبر الإنترنت)، وسوف نستعرض ما توصلت إليه من نتائج وتوصيات.

أولاً – النتائج:

١ – مسؤولية مبرمج الفيروس التقصيرية عن الأضرار التي تصيب الأنظمة المعلوماتية لمستخدمي شبكة الإنترنت نظراً لتعمده الإضرار بالغير.

٢ – مسؤولية مالك الموقع الإلكتروني التقصيرية عن الأضرار التي تصيب الأنظمة المعلوماتية لمستخدمي شبكة الإنترنت من جراء تحميل ملفات مصابة بالفيروس من هذا الموقع، وذلك إذا لم يستخدم مالك الموقع وسائل التأمين المعلوماتي المناسبة للكشف عن أي ملف يتم تحميله على موقعه.

٣ – تقوم مسؤولية مستخدم الإنترنت التقصيرية إذا أرسل للغير رسالة إلكترونية

(٩٨) السنهوري، الوسيط في شرح القانون المدني، الجزء الأول: نظرية الالتزام بوجه عام: مصادر الالتزام، مرجع سابق، ص ٦٧٦، فقرة ٤٤٠.
– سمير تناغو، مصادر الالتزام، مرجع سابق، ص ١٧٥-١٧٦، فقرة ١٣٦.
– أنور سلطان، الموجز في النظرية العامة للالتزام، مرجع سابق، ص ٣٨٨، فقرة ٤٥٩.
– محمد حسين منصور، النظرية العامة للالتزام، مرجع سابق، ص ٤٠٩-٤١١.
– حمدي عبد الرحمن، الوسيط في النظرية العامة للالتزامات، مرجع سابق، ص ٥٨٥-٥٨٧.
– رمضان أبو السعود، مصادر الالتزام، مرجع سابق، ص ٢٣٩- ٢٤٠.

محملة بملف مصاب بفيروس، إذا كان هذا المستخدم لا يستعمل أي برامج لمكافحة الفيروسات على نظامه المعلوماتي.

٤ – ضرورة تطبيق نظرية تكافؤ الأسباب في حالة حدوث ضرر للنظام المعلوماتي، ولا يُعرف بدقة أي فيروس موجود على النظام المعلوماتي هو الذي أحدث الضرر فعلاً.

٥ – عقد التأمين المعلوماتي هو العقد الذى يُبرم بين مالك النظام المعلوماتي والمسؤول عن تأمين هذا النظام، وتكون له صورتان: إما عقد تأمين النظام المعلوماتي أو عقد ترخيص برنامج مكافحة الفيروسات.

٦ – التزام شركة تأمين النظام المعلوماتي أو مبرمج برنامج مكافحة الفيروسات هو التزام ببذل عناية، وهو استخدام كل الإجراءات التقنية المتاحة لتأمين النظام المعلوماتي.

ثانياً – التوصيات:

أن يخطو المشرع المصري خطوات واسعة وسريعة في وضع إطار تشريعي لتكنولوجيا المعلومات، ويتمثل هذا الإطار في وضع قانون خاص بتكنولوجيا المعلومات يتضمن المحاور الآتية:

- **المحور الأول:** تنظيم العلاقات الناشئة بين وسطاء شبكة الإنترنت بعضهم البعض وبينهم وبين المستخدمين وتحديد مدى مسؤولية كل وسيط.
- **المحور الثاني:** تنظيم أعمال التجارة الإلكترونية من حيث إبرام العقود إلكترونياً، التزامات من يمارس هذه الأعمال على شبكة الإنترنت، وما يتعلق بحماية المستهلك عبر الشبكة.
- **المحور الثالث:** تجريم الأفعال التي تتضمن اعتداء على شبكة الإنترنت أو الأنظمة المعلوماتية مثل فيرسة الأنظمة المعلوماتية والدخول غير المشروع لها وإتلافها .....الخ.
- **المحور الرابع:** تنظيم عقود ترخيص البرمجيات، وعقود التأمين المعلوماتي، وعقود إنشاء الأنظمة المعلوماتية، من حيث تحديد التزامات وحقوق أطراف العقد.

المراجع

أولاً – باللغة العربية:

- **أنور سلطان**، الموجز في النظرية العامة للالتزام: مصادر الالتزام، دار الجامعة الجديدة للنشر بالإسكندرية، مصر، ٢٠٠٥.
- **جلال علي العدوي**، أصول الالتزامات: مصادر الالتزام، منشأة المعارف بالإسكندرية، مصر، ١٩٩٧.
- **حمدي عبد الرحمن**، الوسيط في النظرية العامة للالتزامات: المصادر الإرادية للالتزام، دار النهضة العربية، الطبعة الأولى، ١٩٩٩.
- روب سميس ومارك سبيكر ومارك تومسون، التجارة الإلكترونية: ترجمة خالد العامري، دار الفاروق للنشر والتوزيع، القاهرة، ٢٠٠٠.
- **رمضان أبو السعود**، مصادر الالتزام، دار الجامعة الجديدة بالإسكندرية، مصر، ٢٠٠٧.
- **سليمان مرقس**، الوافي في شرح القانون المدني، الالتزامات: الفعل الضار والمسؤولية المدنية، الطبعة الخامسة، ١٩٩٢، بدون ناشر.
- **سمير تناغو**:
  - نظرية الالتزام، منشأة المعارف بالإسكندرية، مصر، بدون سنة نشر.
  - مصادر الالتزام، ٢٠٠٠، بدون ناشر.
- **عابد رجا الخلايلة**، المسؤولية التقصيرية الإلكترونية: المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والإنترنت، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، الأردن، ٢٠٠٩.
- **عبد الرزاق أحمد السنهوري**، الوسيط في شرح القانون المدني الجديد، المجلد الثاني، نظرية الالتزام بوجه عام، مصادر الالتزام، منشورات الحلبي الحقوقية، بيروت، الطبعة الثالثة، ٢٠٠٩.
- **عبد الناصر توفيق العطار**، مصادر الالتزام، ١٩٩٠، بدون ناشر.
- **عبد الودود يحيى**، الموجز في النظرية العامة للالتزامات، دار النهضة العربية، مصر، ١٩٩٤.
- **عزة خليل**، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب: دراسة في

القانون المدنى والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق بجامعة القاهرة، ١٩٩٤.

- **محمد حسين منصور**، النظرية العامة للالتزام: مصادر الالتزام، دار الجامعة الجديدة للنشر بالإسكندرية، مصر، ٢٠٠٦.
- **محمود جمال الدين زكي**، نظرية الالتزام في القانون المصري، الجزء الأول: مصادر الالتزام، مطبعة جامعة القاهرة والكتاب الجامعي، الطبعة الثانية، ١٩٧٦.
- **مصطفى الجمال**، مصادر الالتزام، دار المطبوعات الجامعية، الإسكندرية، مصر، ١٩٩٩.

ثانياً - باللغة الإنجليزية:

- **Cheryl MASSINGALE & Faye BORTHICK**, Risk allocation for computer system security breaches: Potential liability for providers of computer services, Western New England Law Rev, Vol 12, Issue 2, 1990.
- **Clive GRINGRAS**, The Laws of the Internet, Londres, Butterworths, 1997.
- **Dana ROSENFELD and Alysa HUTNIK**, Data Security Contract Clauses for Service Provider Arrangements, Practical Law Publishing Limited,USA, 2011.
- **Daniel HANSON**, Easing Plaintiffs' Burden of Proving Negligence for Computer Malfunction, Iowa Law Rev, 69 (1983) 241.
- **Daphyne THOMAS and other**, Legal and social aspects of e-commerce, Art on line at: www.iacis.org http://www.iacis.org, the date of publishing is: 2003.
- **David COHEN & Roberta ANDERSON**, Insurance coverage for cyber-losses, Tort & Insurance Law Journal http://www.jstor.org/action/showPublication?journalCode=tortinslawj, Vol. 35, N°. 4, SUMMER 2000 http://www.jstor.org/stable/10.2307/i25763475.
- **David HARLEY and others**, Viruses Revealed, Berkeley, McGraw-Hill, 2001.

- **Eleanor MCKENZIE**, Computer Viruses and How They Affect Our Economy, Art on the internet at:http://www.ehow.-com, date of publishing: 2011.
- **Jeff TYSON**, How Firewalls Work, Art on the internet at: http://www.howstuffworks.com/virus.htm, the date of reading: 17 April 2013.
- **Jonathan STRICKLAND**, How to Remove a Computer Virus, Art on the internet at: http://www.howstuffworks.-com, the date of reading: 17 April 2013.
- **Jonathan S. http://electronics.howstuffworks.com/how-to-tech/jonathan-strickland-author.htmTRICKLAND**, How to Remove a Computer Virus, Art on the internet at: http://www.howstuffworks.com/virus.htm, the date of reading: 17 April 2013.
- **Katie MATISON**, Liability forbreach of e-commerce security standards, Art on line at: http://www.lanepowell.com/, the date of publishing is: 2001.
- **Lilian EDWARDS**, Dawn of the death of distributed denial of service: How to kill zombies, on the internet at: http://www.cardozoaelj.com/, the date of publishing: 2006.
- **Margaret ROUSE**, virus, Art on the internet at: http://www.searchsecurity.techtarget.com/definition/virus http://www.howstuffworks.com/virus.htm, the date of publishing is: July 2006.
- **Mark COLOMBELL**, The legislative response to the evolution of computer viruses, the Richmond journal of law and technology, vol VIII, Issue 3, spring 2002.
- **Mark GROSSMAN**, Liability for you if you have been hacked, on the internet at: http://www.pdesign.net, the date of publishing: 1 August 2000.
- **Marshall Brain and Wesley Fenlon**, How Computer Viruses

Work, Art on the internet at: http://www.howstuffworks.-com/virus.htm, the date of reading: 17 April 2013.

- **Meiring VILLIERS**, Computer viruses and civil liability: a conceptual framework, Tort trial and insurance practice law journal, fall 2004(40) (1).
- **Meiring VILLIERS**, Information security standards, Journal of internet law, January 2010.
- **Nicholas VERMEYS**, Computer "Insecurity" and Viral attacks: Liability issues Regarding Unsafe Computer Systems under Quebec Law, Lex Electronica, Vol.9, n°1, Hiver 2004.
- **Philip FITES and others**, The Computer Virus Crisis, 2e éd, New York, Van Nostrand Reinhold, 1992.
- **Richard OWENS**, Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections, canadian journal of law and technology, Volume 3 Number 1,March 2004.
- **Robin BROOKS**, Deterring the spread of viruses online: Can tort law tighten the 'net'?, Rev. Litig. 17 (1998) 343.
- **Roland STANDLER**, Possible vicarious liability for computer users in the USA?, on the internet at: http://www.rbs2.com, date of publishing: 17 April 2004.
- **Sarah FAULKNER**, Invasion of the information snatchers: Creating liability for corporations with vulnerable computer networks, The John Marshall Journal of Computer & Information Law, (2000) 18.
- **Vicky ROBBINS**, Vendor liability for computer viruses and undisclosed disabling devices in software, Computer Law, 20 (1993) 10.

ثالثاً – باللغة الفرنسية:

- **Alex WEILL et François TERRE**, Droit civil: les obligations, DALLOZ, 4 éme èd, 1986.

- **Alain BENSOUSSAN**, Virus: combiner l'approche lgale avec l'approche technique, Les Echos N° 17083 du 09 fevrier 1996.
- **Blandine POIDEVIN**, Quelle responsabilité en matière de sécurité informatique?, Art disponible sur: http://www.jurisexpert.net, La date de mise en ligne est: 8 Avril 2002.
- **Christian LARROUMET**, Droit civil: les obligations: le contrat, t.3, 4 éme èd, paris, Economica, 1998.
- **Christiane SCHUHL**, cyber droit: le droit à l'épreuve de l'internet, Dalloz, 2 éme éd, 2001.
- **Eric A CAPRIOLI et Noelle LEBOEUF**, Innovation informatique: Les risques des logiciels open source, Art disponible sur: www.caprioli-avocats.com http://www.caprioli-avocats.com, La date de mise en ligne est: octobre 2007.
- **Eric FLOUR et Jean AUBERT**, Droit civil, les obligations, V.I: l'acte juridique, deuxième éd, 1977, collection u, Armand colin.
- **Frédéric DUFLOT**, Les Infections Informatiques Bénéfiques: Chroniques d'un anathème, DESS de Droit du Numérique et des Nouvelles Techniques, Univ Paris XI, Fac Jean Monnet, 2003-2004.
- **Jean CARBONNIER**, Droit civil: les obligations, presses universitaires de France, 9 ème éd, 1976.
- **Jean-Vasken ALYANAKIAN**, Quels recours en cas de manquement contractuel ou de fraude?, Art disponible sur: www.01net.com http://www.01net.com, La date de mise en ligne est: 06/05/2011.
- **Marie BAREL**, Le point de vue d'une jurist, Revue de sécurité informatique, Sept 2005, N° 54.
- **Michel ZOIA**, La notion de consentement à l'épreuve de l'électronique, Gaz pal, 15-17 juillet 2001, p 16.

- **Michelle BAPTISTE et Xavier STRUBEL**, Creìer et exploiter un commerce électronique, litec, 1998.
- **Murielle CAHEN**, La sécurité et les systèmes informatiques, Art disponible sur: http://www.murielle-cahen.fr http://murielle-cahen.fr/, La date de mise en ligne est: 17 mai 2012.
- **Murielle CAHEN**, Le consentement sur internet, Art disponible sur www.droit-tic.com http://www.Droit-tic.com > , la date de mise en ligne est 15/3/2004.
- **Nicholas VERMEYS**, Virus informatiques: Responsables et responsabilité, Les Éditions Thémis, Canada, 2007.
- **Nicolas VERMEYS**, Réflexion juridique autours de la notion de désinformation eu égard à la transmission de métavirus, Lex Electronica Rev, vol.10 nº3, Hiver/Winter 2006.
- **Philippe HELIS & Philippe MOZAS**, Chronique multimedia, Petites affiches, 18 (1998) 89.
- **Raphael PEUCHOT**, Rudiments juridiques à l'usage des clients de prestations d'intrusion informatique, Lamy Lexel, 26 mars 2002.
- **Stefan MARTIN**, L'exploitation d'un serveur Internet: droits et obligations des institutions à l'égard des créateurs, du public et des étudiants, dans Développements récents en droit de l'éducation, Cowansville, Éditions Yvons Blais, 1996.
- **Sylvette GUILLEMARD**, Le droit international privé face au contrat de vente cyberspatial, thèse de doctorat, fac de droit, univ Paris II, 2003.
- **Valérie SEDALLIAN**, Légiférer sur la sécurité informatique: la quadrature du cercle?, Etude disponible sur: http://www.juriscom.net, La date de mise en ligne est: 5 décembre 2003.

رابعاً – أحكام القضاء:

ا – القضاء الإنجليزي:

- CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).
- Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559 (1996).
- American Guarantee & Liability Insurance Co. V Ingram Micro Inc., No. Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299 (D. Ariz. April 19, 2000).

ب – القضاء الفرنسي:

- Cass.Com, 7 juillet 2009, Nº 08-14231.
- Cass.Com, 25 Nov 1997, Nº 95-14603, Bull 1997 IV Nº308 p. 264.
- Cass.Crim, 12 Décembre 1996, Nº 95-82.198, Bull.crim 1996 Nº465 p. 1353.
- CA Montpellier, 9 Mars 2004, RG Nº 03/00974.
- Juridiction de proximité de vanves, 2 septembre 2008, RG NNº 91-08-000006.

قائمة المختصرات

Al	Alinéa.
Art	Article.
Bull	Bulletin des arrets de la cour do vassation.
Bull.Civ	Bulletin de la cour de cassation (chambre civile).
Bull.Crim	Bulletin de la cour de cassation (chambre criminelle).
C	Contre.
CA	Cour d'appel.
Cass.Civ	Cour de cassation (chambre civile).
Cass.Com	Cour de cassation (chambre commerciale).
Cass.Crim	Cour de cassation (chambre criminelle).
Ch	Chambre.
comm	Commentaire.
DESS	Diplôme d'études supérieures spécialisées
Doc	Document.
doctr	Doctrine.
éd	Edition.
Fac	Faculté.
fév	février
Gaz.pal	Gazette du Palais.
Ibid	Au mêm endroit.
Jan	Janvier.
JORF	Journal officiel des lois et décrets.
Nov	Novembre.
Nº	Numéro.
Oct	Octobre.
Op.cit	Ouvrage précité.
P	Page.
Prec	Precedent.
Rev	Revue
RG	Numéro dau répertoire général.
S	Suivant.
Sec	Section.
sept	Septembre
T	Tome.
Univ	Université.
Vol	Volume.
ص	صفحة