Université de Montréal

La responsabilité civile des intermédiaires ayant participé à la transmission de virus informatiques sur Internet

Par
Nicolas William Vermeys

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de maîtrise en droit (L.L.M.)

décembre 2002

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

La responsabilité civile des intermédiaires ayant participé à la transmission de virus informatiques sur Internet

Présenté par :
Nicolas William Vermeys

a été évalué par un jury composé des personnes suivantes:

Président-rapporteur : M^{e} Pierre Trudel

Directeur de recherche : M^{e} Karim Benyekhlef

Membre du jury : M. Daniel Poulin

"No, Aubie – there are safeguards. The thing is, how much are you willing to pay for them? At what point does the cost of protecting the computer outweigh the efficiency gained by its use?

David Gerrold, *When Harlie Was One*

Année après année, plusieurs entreprises signalent d'énormes pertes économiques attribuables aux agissements de virus informatiques et autres logiciels causant la destruction ou la corruption de données. Confrontées à l'impossibilité de retracer efficacement les auteurs de ces « maliciels », les victimes de telles contaminations se retrouvent trop souvent seules à payer la facture, et ce, nonobstant le fait que leur infection découle souvent du manque de diligence d'une série d'intervenants.

Il devient dès lors important pour une victime de s'interroger sur la possibilité d'intenter certains recours afin d'exiger compensation de ceux dont la négligence a joué un rôle dans la transmission du virus ayant contaminé son système.

Ainsi, en se basant principalement sur le modèle économique de la négligence élaboré par le juge Learned Hand au début du siècle dernier et sur les développement doctrinaux et jurisprudentiels en matière de responsabilité pour la transmission de virus biologiques, cette étude vise l'identification des acteurs ayant joué un rôle dans la transmission de virus informatiques sur Internet, ainsi que la part de responsabilité attribuable à chacun d'eux sous le régime de responsabilité civile québécois.

Mots clés : Droit – Responsabilité civile – négligence – Québec – virus informatique – maliciel – vers – cheval de Troie – ordinateur – Internet

Every year, more and more businesses register tremendous financial losses which can be attributed to the destruction or corruption of valuable data due to computer viruses and other forms of malicious software. Confronted with the difficult task of finding the authors of these "malware", victims are all too often left flipping the bill even though, after consideration, their infection often stems from the lack of diligence demonstrated by third parties.

It therefore becomes essential for victims to contemplate to possibility of taking legal recourse against those whose negligence has permitted the transmission of viruses onto their system.

This study offers a detailed look at all parties involved in the transmission of computer viruses through the Internet and, referring itself to the economic model of negligence established by judge Learned Hand at the beginning of the last century and to the doctrinal and jurisprudential treatment of liability for the transmission of biological viruses, tries to establish when and how each party could be held liable under Quebec law.

Key terms: Law – civil liability – negligence – Quebec – computer virus – malware – worm – Trojan Horse – computer – Internet

Table des matières

Liste des tableaux

Liste des figures

Liste des sigles et abréviations

Termes juridiques

C.c.Q.	Code civil du Québec
C. cr.	Code criminel
L.p.c.	Loi sur la protection du consommateur

Termes informatiques

AOL	America Online
F.A.I.	Fournisseur d'Accès Internet
Ftp	File transfer protocol
HTML	Hypertext Markup Language
MIME	Multi-purpose Internet Mail Extensions
PC	Personal Computer
VX	Virus Exchange

Termes médicaux

M.T.S.	Maladies Transmises Sexuellement
SIDA	Syndrome d'Immuno-Déficience Acquise
V.I.H.	Virus de l'Immuno-déficience Humaine

Autres termes

PME	Petites et Moyennes Entreprises

Introduction

Avoir accès au réseau Internet devient une réalité difficile à contourner pour les entreprises et individus, le Web constituant l'un des piliers de l'économie du savoir dans laquelle nous évoluons. Selon la firme de sondage Nielsen, le nombre global d'internautes atteignait plus de 445 millions en octobre 2001, nombre qui ne cesse de croître. Les échanges d'information en ligne et la création de bases de données informatiques sont eux aussi à la hausse. Les événements du 11 septembre 2001 ont d'ailleurs démontré à quel point il s'avère important pour une entreprise d'avoir un réseau interne rendant possible le transfert des données en lieux sûrs.

Si l'informatisation de données importantes devient de plus en plus répandue, elle comporte l'inconvénient d'exposer ces données aux divers ralentissements du réseau, aux pirates informatiques, mais également aux maliciels ou virus informatiques[1]. En effet, le nombre de cas rapportés d'infection de systèmes informatiques grimpa jusqu'à 52 658 en 2001, soit une augmentation de plus de 150%.

Les maliciels (*malware*) sont des « *logiciels comportant des instructions malveillantes pouvant entraîner pertes et dommages* »[2]. Parmi ceux-ci, les virus informatiques, une « *suite d'instructions ou* [un] *programme doté d'un mécanisme d'auto-reproduction introduit frauduleusement dans un système informatique et se transportant d'un programme à un autre pour le modifier ou le détruire* »[3], composent l'ensemble ayant reçu

---

[1] L'auteure Christiane Féral-Schuhl qualifie les virus informatiques d'« *atteintes les plus usuelles sur le web* ». Christiane FÉRAL-SCHUHL, *Cyber droit : Le droit à l'épreuve de l'Internet*, Parie, Dunod, 2000, p.43.

[2] François RICHARD, *Vocabulaire de la sécurité et des virus informatiques*, Ottawa, Groupe Communication Canada, 1995, p. 133.

[3] *Id.*, p. 51. Il importe de souligner qu'il n'existe aucune définition universellement acceptés du terme « virus informatique ». Bien que plusieurs experts aient recours à la définition adoptée par Frederic B. Cohen, crédité comme ayant inventé la notion de « virus informatique » dans sa thèse de doctorat de 1984, d'autres la critiquent comme

la plus grande couverture médiatique, poussant l'opinion populaire à exprimer une certaine confusion quant à la distinction à apporter entre les deux termes. Quoi qu'il en soit, il importe simplement de comprendre que ces logiciels peuvent avoir des conséquences dévastatrices sur le contenu de systèmes informatiques.

Malgré l'aspect socialement et éthiquement discutable des maliciels, aucun instrument législatif particulier n'interdit la création ou la diffusion de virus informatiques ou autres logiciels dangereux en sol canadien[4]. En effet, le *Code criminel*[5], comme la majorité des législations étatiques étrangères[6] exige qu'un virus soit transmis intentionnellement, malicieusement et sans autorisation pour constituer une infraction punissable[7]. C'est pourquoi, à ce jour, aucun individu n'a été accusé criminellement d'avoir transmis de virus informatiques en sol canadien[8].

Cependant, la présence de dispositions punitives pour l'initiateur d'une attaque virale ne s'avère pas nécessairement réconfortante pour la

---

étant trop incomplète. Voir Robert SLADE, *Robert Slade's Guide to Computer Viruses: How to Avoid Them, How to Get Rid of Them, and How to Get Help*, 2e éd., New York, Springer, 1996, p. 4, ainsi que David HARLEY et al., *Viruses Revealed*, Berkeley, McGraw-Hill, 2001, p. 570 et ss. Voir également la section I (B) du présent mémoire.

[4] *ÉTUDE DES QUESTIONS DE DROIT ENTOURANT LA SÉCURITÉ DES RENSEIGNEMENTS ÉLECTRONIQUES*, Chapitre 7 : « Usage criminel des technologies de l'information », en ligne sur le site du *Ministère de la justice du Canada* : <http://canada.justice.gc.ca/fr/ps/ec/toc.html> (Mise à jour : 2002-06-19)

[5] L.R.C. (1985), c. C-46, article 430(1.1).

[6] Voir PISA, « Virus », (2001) en ligne sur le site de *PISA* : <http://www.pisa.belnet.be/pisa/fr/jur/virus.htm> (date de visite : 25 octobre 2001) pour la situation en Belgique. Voir également Kelly CESARE, « Prosecuting Computer Virus Authors: The Need For An Adequate And Immediate International Solution », (2001) 14 *Transnat'l Law* 135, 141, pour la situation américaine et Christiane FÉRAL-SCHUHL, *op. cit.*, note 1, p.44, pour la situation française. La seule exception notoire à cette règle réside dans la législation Suisse dont l'article 144Bis du Code pénal vise spécifiquement la personne « *qui aura fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de commettre une infraction visée au chiffre 1, ou qui aura fourni des indications en vue de leur fabrication* ».

[7] Frederick COHEN, *A Short Course on Computer Viruses*, 2e éd., New York, Wiley, 1994, p.112.

[8] L'arrêt *R.* c. *M.C.* ([2001] J.Q. no 4318), la seule décision traitant de l'article 430(1.1) C. cr., ne concerne pas les virus informatiques, mais plutôt les DDoS (*Distributed denial of service*).

victime de celle-ci. En effet, les juges des différentes chambres criminelles sont très réticents à l'idée d'accorder un quelconque dédommagement aux victimes d'actes criminels[9], malgré la présence d'une disposition visant cette éventualité dans le Code[10].

Pour les victimes, la possibilité d'être dédommagées pour la perte de données causée par les virus informatiques et autres maliciels se résume donc à poursuivre l'auteur de l'attaque en responsabilité civile[11] selon les dispositions du *Code civil du Québec*. En effet, la responsabilité de l'auteur d'un tel acte est engagée sur le plan civil par l'application des règles traditionnelles de notre régime de responsabilité civile lesquelles énoncent le principe que quiconque a causé un dommage à autrui doit le réparer[12]. Rappelons-nous qu'il suffit alors de prouver un préjudice, une faute et un lien de causalité entre ceux-ci[13]. En effet, comme l'explique le groupe PISA :

> « *L'auteur doit indemniser totalement la victime si un lien de causalité peut être démontré entre le virus et le dommage à un ordinateur ou à un autre système informatique ou à une de leurs parties.* »[14].

---

[9] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *La responsabilité civile*, 5e éd., Cowansville, Éditions Yvon Blais, 1998, p. 41.
[10] Art. 738 C. cr.
[11] Comme l'expliquent les auteurs David Johnston, Sunny Handa et Charles Morgan : « *As it relates to cyberspace* [the tort of conversion] *might apply where a computer virus damages electronic files.* Il est à noter que l'hésitation des auteurs ne concerne pas l'application du régime des « *torts* » à la transmission de virus informatiques, mais bien la catégorie de torts la mieux adaptée à ces maliciels. Voir Sunny HANDA et al., *Cyber Law*, Toronto, Stoddart, 1997, p. 211. Aux États-Unis, certains documents législatifs prévoient explicitement les poursuites au civil du responsable de la dissémination d'un virus. Voir Susan C. LYMAN, « Civil Remedies for the Victims of Computer Viruses », (1992) 11 *Computer/Law Journal*, 607, 612-613.
[12] Alain BLOCH, « Virus : responsabilité juridique », (1989) 114 *Expertises* 52, 52.
[13] C'est ce que nous rappelle le groupe PISA, « *La victime devra donc prouver (1) l'identité de l'auteur, (2) le dommage, qui doit pouvoir être fixé, et (3) le lien de causalité entre la présence du virus et le dommage* ». PISA, *loc. cit.*, note 6.
[14] *Id.*

Le préjudice s'avère évident, à savoir la perte de données[15]. Pour ce qui est de la faute, tout délit pénal constituant également un délit civil[16], celle-ci peut donc être inférée des dispositions du *Code criminel*. Finalement, pour ce qui est du lien de causalité, un informaticien moindrement doué peut facilement établir celui-ci en exposant la fonction du virus, c'est-à-dire pourquoi il a été créé[17].

Or, il était assez simple de retracer l'auteur d'un virus, ou tout au moins celui l'ayant volontairement retransmis, lorsque la transmission ne pouvait se faire que par contact physique, c'est-à-dire lorsque le virus était transmis par le biais d'un support matériel tel une disquette, ou encore s'il était créé directement sur l'ordinateur infecté. Dans tous les cas, il suffisait de savoir qui pouvait avoir accès à un poste pour trouver l'auteur du méfait. Cependant, l'avènement du réseau Internet et les avancés technologiques croissantes ont compliqué la donne[18]. Les maliciels prennent aujourd'hui plusieurs formes[19] et leurs auteurs tirent avantage de l'aspect ouvert du réseau pour transmettre leurs créations destructives.

Sur Internet, les virus peuvent être retransmis plus rapidement[20] et de façon exponentielle, permettant ainsi une plus grande diffusion[21].

---

[15] Il importe d'apporter un bémol à cette affirmation, puisque la doctrine voulant qu'une perte de données puisse être considérée un dommage n'est en soi pas acceptée par tous. Voir Clive GRINGRAS, *The Laws of the Internet*, Londres, Butterworths, 1997, pp. 66 et suivantes.

[16] Olivier ITEANU, « Virus, les implications légales », (1993) 1 *Chaos Digest*.

[17] Quoique le principe de la responsabilité civile n'ait pas encore été abordé dans l'optique du dédommagement de victimes de virus informatiques par la doctrine et les tribunaux québecois, il fut avancé par certains auteurs américains que la transmission volontaire de virus pouvait être incluse dans la doctrine d'« *intentional torts* » en common law. Voir SUSAN C. LYMAN, *loc. cit.*, note 11.

[18] Voir Christiane FÉRAL-SCHUHL, *op. cit.*, note 1, p.44.

[19] Parmi celles-ci, notons les chevaux de Troie, les métavirus, ainsi que les vers, pour n'en nommer que quelques uns.

[20] ANONYME, *Maximum Security*, 3e éd., Indianapolis, Sams, 2001, p. 324-325.

[21] Carey NACHENBERG, « Future Imperfect », (1997) *Virus Bulletin* 6, 6.

Surtout, la décentralisation du réseau et son relatif anonymat[22] permettent une transmission plus sournoise rendant l'identification de l'auteur de l'attaque pratiquement impossible[23] sans efforts considérables et sans investissements majeurs[24]. Il s'ensuit qu'il devient difficile pour la victime d'un virus d'être dédommagée pour les torts causés.

Il va de soi que le particulier dont l'ordinateur personnel est infecté par un virus, supprimant ainsi, par exemple, ses mémoires ou son agenda, ou encore l'entreprise qui perd des données importantes à la suite de l'infection de son réseau, n'a pas les moyens, tant logistiques que financiers, de retrouver l'individu fautif et d'exiger compensation. Cette constatation nous pousse donc à poser la question suivante, à savoir : De qui la victime d'un virus peut-elle exiger une juste compensation pour le préjudice causé si l'instigateur du dommage est introuvable?

La réponse à cette question est amorcée par l'étude du chemin suivi par le virus avant d'arriver à destination, c'est-à-dire avant d'infecter le système informatique de la victime. Comme l'explique un auteur :

> « *One strategy is to impose strict legal liability upon the providers of computer systems, services, networks, and software providers requiring them to put into place adequate technological barriers to unauthorized invasions of their computer networks and products and/or*

---

[22] Comme l'expliquent Steve R. WHITE et al. (« Coping with Computer Viruses and Related Problems », dans Lance J. HOFFMAN, (éd.), *Rogue Programs: Viruses, Worms, and Trojan* Horses, New York, Van Nostrand Reinhold, 1990, p. 7, à la page 11), mis à part certains cas exceptionnels, seuls les auteurs ayant manifesté leur responsabilité pour la création d'un virus sont identifiables.

[23] Eugene H. SPAFFORD et Stephen A. WEEBER, « Software Forensics: Can We Track Code to its Authors? », (1992) disponible à l'adresse <www.cerias.purdue.edu/homes/spaf/tech-reps/9210.pdf> (date de visite : 17 juillet 2002), 2.

[24] Comme l'expliquent Philip Fites et al. : « *The victim rarely knows who the vandal was, and often can determine his identity through the expenditure of considerable time and money* », Philip FITES et al., *The Computer Virus Crisis*, 2e éd., New York, Van Nostrand Reinhold, 1992, p. 139.

> *to carry sufficient insurance to cover any losses which occur* »[25].

Cette « stratégie » implique ainsi la responsabilisation des intervenants ayant participé à la propagation dudit virus. En effet, s'il est difficile de cerner le créateur d'un virus, l'identité de la dernière personne ayant transmis ce logiciel, ou encore de celle ayant permis ladite transmission, est facilement discernable[26]. Il suffirait donc pour la victime de l'infection de se retourner vers le dernier transmetteur du virus[27] ou encore les intermédiaires techniques dont les lacunes sécuritaires ont permis l'infection[28]. Cependant, il faut souligner que ces intervenants ne participent pas volontairement à la transmission de virus informatiques, ils servent simplement de canaux, d'intermédiaires. La question se pose donc de savoir si la diffusion involontaire d'un virus peut constituer une infraction à la norme générale de prudence[29] ; ou plutôt si la participation passive à l'infection virale d'un système informatique constitue une faute en droit civil québécois.

---

[25] Anne W. BRANSCOMB, « Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime », dans Lance J. HOFFMAN, (éd.), *Rogue Programs: Viruses, Worms, and Trojan* Horses, New York, Van Nostrand Reinhold, 1990, p. 80.

[26] Richard B. LEVINE, *The Computer Virus Handbook*, Berkeley, Osborne McGraw-Hill, 1990,, p. 254.

[27] Il s'agit là de la position du groupe belge PISA « *Les devoirs d'une personne privée doivent pour cela impliquer qu'elle se pose sérieusement la question de savoir si l'information qu'elle rentre sur son ordinateur et qu'elle envoie éventuellement plus loin est sans risque. L'utilisation d'un bon et récent scanneur de virus convient également ici. C'est seulement lorsqu'il se tient à cela qu'il ne peut lui être reproché qu'il y ait des virus sur le net* ». PISA, *loc. cit.*, note 6.

[28] Cette théorie portant le nom de « downstream liability » se résume par l'idée que les auteurs de virus informatiques sont rarement économiquement viables, ces derniers étant souvent des étudiants ou encore des « hackers » dont l'actif sera utilisé pour payer les honoraires de leurs avocats. Cette théorie propose donc de poursuivre les intermédiaires Internet qui ont permis, de par leur négligence, la transmission de virus, leurs systèmes de sécurité n'étant pas à la fine pointe de la technologie. Michael RASMUSSEN dans Robyn WEISMAN, « Got a Virus? You're Sued! », (2001) en ligne sur le site *NewsFactor Network* : <http://www.osopinion.com/peri/printer/12529/> (visité le 4 novembre 2001).

[29] PISA, *loc. cit.*, note 6.

Comme l'explique un auteur : « *The computer virus phenomenon is still relatively new, and few legal precedents have been set* »[30]. Il s'avère donc difficile de répondre à notre question sans effectuer une étude exhaustive du contexte législatif et jurisprudentiel pouvant trouver application dans les circonstances.

En effet, si l'hypothèse de dédommagement mentionnée ci-haut, à savoir la poursuite des tiers transmetteurs, semble s'avérer une avenue intéressante pour la victime d'attaques virales puisqu'elle multiplie le nombre de défendeurs potentiels; il appert que les principes sous-tendant la responsabilité civile ne constituent pas toujours la meilleure option lorsque confrontée au bien-être de la société dans son ensemble[31]. Il importe donc de nous questionner sur la portée à accorder à ces principes dans le cas d'infections virales.

Un tel questionnement nécessite inévitablement une étude de la législation, de la jurisprudence et de la doctrine applicables aux virus informatiques en droit québécois. Cependant, les écrits juridiques rédigés au Québec et ayant trait à ces maliciels étant peu nombreux, nous nous référerons, dans le présent mémoire, aux différents développements en droit américain dans ce domaine. En effet, le réseau Internet étant, à la base, sous contrôle américain, sans compter le fait que les États-Unis monopolisent une grande partie dudit réseau de par la taille de leur population informatisée, la majorité de la doctrine et des décisions touchant de près ou de loin les virus informatiques est concentrée dans ce pays. Il devient donc justifié de recourir au droit comparé et de baser notre étude sur les développements américains en la matière et d'envisager leur adaptation au système juridique québécois.

---

[30] Philip FITES et al., *op. cit.*, note 24, p. 139.

[31] Comme l'explique George S. Takach, « *An important question is whether our liability regimes, both contract- and tort-based, are up to the challenge posed by computers* ». George S. TAKACH, *Computer Law*, Toronto, Irwin Law, 1998, p. 34.

Avant toute étude, il nous faut cependant nous pencher sur les différents types de logiciels malicieux afin de mieux comprendre leur méthode de propagation et de diffusion et ainsi voir dans quelles circonstances il devient alors possible de conclure à la négligence d'un tiers ayant servi de canal à ladite transmission.

Nous pourrons ensuite nous pencher sur la notion de responsabilité civile afin de cerner l'origine de cette doctrine, ainsi que les différentes théories nous permettant de déterminer si un comportement est négligent dans le contexte de la diffusion des virus informatiques.

À la lumière de ces recherches, nous saurons alors présenter les situations dans lesquelles un intermédiaire peut entraîner sa responsabilité pour l'infection involontaire de l'ordinateur d'une victime, ainsi que les méthodes disponibles à ces intermédiaires pour limiter cette responsabilité.

Finalement, il nous faudra déterminer les comportements préventifs à adopter afin de protéger son propre réseau contre l'infiltration de logiciels malicieux.

I. La responsabilité civile et la fabrication de virus informatiques : les rouages d'une problématique en émergence

Avant même d'évoquer l'idée d'une quelconque forme de responsabilité civile dans la transmission de maliciels, il importe de se questionner sur l'opportunité d'appliquer le régime de responsabilité civile à ces logiciels. En effet, il peut parfois s'avérer discutable d'adapter les règles de droit existantes à une technologie en émergence. Toutefois, comme l'indique W.H. Murray :

> « *The exposure to computer viruses arises from the desire to share programs and other data. It arises from the desire to communicate, cooperate and coordinate. In short, it arises from the very human desire to live in a community* »[32].

Or, de ce désir de vivre en communauté découle la responsabilité sociale[33] et, avec le développement du régime de responsabilité juridique, la responsabilité civile. En effet, dès qu'il est établi que la transmission de virus informatiques découle d'une quelconque relation sociale, il devient alors apparent que les règles établies pour gérer ces mêmes relations doivent s'appliquer à cette « nouvelle » problématique.

Afin d'explorer plus en profondeur cette prétention, il nous faut cependant nous pencher en premier lieu sur le sens et la portée des termes employés en établissant ce que sont les maliciels (A) puis en examinant les rouages du régime de responsabilité civile et son éventuelle application à ces logiciels malicieux (B).

---

[32] W.H. MURRAY, « The Application of Epidemiology to Computer Viruses », dans H.J. HIGHLAND (éd.), *Computer Virus Handbook*, Oxford, Elsevier Advanced Technology, 1990, p. 15, à la page 22.

[33] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 3.

A. La source de la problématique : les logiciels malicieux (maliciels) – conception, fonction, qualification et protection

À leur origine, les ordinateurs personnels (PC) furent créés afin de satisfaire les besoins d'un seul utilisateur. Les notions de réseau et d'interconnexité n'existant pas encore à cette époque, personne ne pensa à se questionner sur les effets que pourrait avoir l'accès indirect à un système par des tiers[34]. Malgré la création subséquente de réseaux et de logiciels de plus en plus performants, cette réalité demeure : les ordinateurs n'ont jamais été conçus pour être connectés. C'est cette problématique, conjointement avec le manque de savoir des utilisateurs du réseau, qui est à la source de la création de maliciels, une catégorie de logiciels conçus pour se déplacer d'ordinateur à ordinateur et de réseau en réseau, dans le seul but de modifier les systèmes informatiques sans le consentement de leurs propriétaires[35]. Comme l'explique Eugene H. Spafford :

> « *hardware and operating systems are still based on the assumption of single trusted user access, and this allows computer viruses to spread and flourish on those machines. The population of users of PCs further adds to the problem, as many are unsophisticated and unaware of the potential problems involved with lax security and uncontrolled sharing of media* »[36].

Avant d'aborder le régime de responsabilité civile résultant de la propagation de ces logiciels malicieux, encore faut-il comprendre le fonctionnement de ces programmes (1) et connaître les différentes formes de protection pouvant réduire la probabilité de leur transmission involontaire et, par conséquent, la responsabilité des tiers transmetteurs

---

[34] Eugene H. SPAFFORD, « Computer Viruses as Artificial Life », (1994) disponible à l'adresse <http://www.cerias.purdue.edu/coast/archive/data/categ20.html> (date de visite: 17 juillet 2002), 4.
[35] Roger A. GRIMES, *Malicious Mobile Code: Virus Protection for Windows*, Sebastopol, O'Reilly, 2001, p. 2.
[36] Eugene H. SPAFFORD, *loc. cit.*, note 34, 4.

(2). Il est à noter que l'exposé qui suit ne se veut pas une analyse complète sur les maliciels[37], mais bien un aperçu destiné à familiariser le lecteur avec certaines notions extérieures à la sphère juridique.

1. Le fonctionnement des maliciels

Comme nous venons de le souligner, le terme « maliciel » regroupe un ensemble de programmes informatiques visant à causer des dommages. Quoique ceux-ci soient nombreux et incluent une panoplie de programmes tels les parasites[38] et les bactéries[39], nous nous concentrerons sur les représentations les plus courantes des logiciels malicieux[40], à savoir les virus informatiques (a), les chevaux de Troie (b), les vers (c)[41] et, dans une moindre mesure, les métavirus (d).

a) Les virus

Les virus informatiques sont sans aucun doute la forme de maliciel la plus connue et demeurent l'un des problèmes de sécurité les plus terrorisants, mais également les plus incompris du réseau Internet[42]. Le terme « virus » dérivé du latin « poison »[43], fut appliqué à cette catégorie de maliciels de par les ressemblances entre ces deux « organismes »[44].

---

[37] Pour une telle introduction, nous référons le lecteur à l'excellent livre de David HARLEY et al., (*op. cit.*, note 3), dont le chapitre 8 dresse une liste de toute la documentation pertinente en la matière.

[38] « *Un parasite est un court programme informatique non destructeur en une première approche. Il se borne à être présent et à se reproduire sans cesse, tout en se propageant. De ce fait, il occupe de plus en plus de mémoire, aussi bien centrale que sur disque* ». Henri LILEN, et François DAROT, *Virus & protection*, Paris, Radio, 1991, p. 12.

[39] Une bactérie est « *a program that replicates itself and feeds off the host system by preempting processor and memory capacity* ». Peter J. DENNING, « Computer Viruses », dans Peter J. DENNING (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 285, à la page 287.

[40] Sascha SEGAN, « Killer Apps » (2002) 13 *Smart Computing* 54, 54.

[41] Philip FITES et al., *op. cit.*, note 24, p. 7.

[42] ANONYME, *op. cit.*, note 20, p. 324.

[43] Eugene H. SPAFFORD, *loc. cit.*, note 34, 2.

[44] Vicky H. ROBBINS, « Vendor Liability for Computer Viruses and Undisclosed Disabling Devices in Software », (1993) 10 *Computer Lawyer* 20, 20. Voir aussi W.H. MURRAY, *op. cit.*, note 32, p. 17.

Tout comme les virus biologiques, leurs homologues informatiques sont également difficiles à localiser de par leur petite taille, se répandent en s'attachant à d'autres « cellules » (programmes) et se multiplient tout en causant un dommage à l'« organisme » hôte[45]. Il existe néanmoins une différence marquante entre ces deux entités : contrairement aux virus biologiques, les virus informatiques sont des programmes écrits par des programmeurs[46] ; ils ne sont pas simplement apparus suite à une quelconque évolution électronique du réseau Internet[47].

Le terme « virus » fut d'abord employé en relation avec les ordinateurs dans une oeuvre de science-fiction intitulée « *When Harlie Was One* » :

> « [W]ell, *you know what a virus is don't you? It's pure DNA, a piece of renegade genetic information. It infects a normal cell and forces it to produce more viruses – viral DNA chains – instead of its normal protein. Well, the VIRUS program does the same thing* »[48]

Malheureusement, les prédictions de l'auteur de ce livre allaient se révéler plus ou moins exactes. En effet, de tels programmes commencèrent à se retrouver sur les réseaux dès le début des années 80. Mais c'est en 1982 que l'expression « virus informatique » sera officiellement accolée à ces logiciels par David Cohen[49], crédité comme étant le premier à prouver qu'il s'agissait bien d'une menace véritable et donc à faire le pont entre science et science-fiction. Ainsi, la définition de Cohen, encore aujourd'hui utilisée par de nombreux auteurs, désigne les

---

[45] Robert J. MALONE et Reuven R. LEVARY, « Computer Viruses : Legal Aspects », (1994) 4 *U. Miami Bus. LJ* 125, 128.

[46] En effet, les virus informatiques sont de véritables programmes informatiques au même sens qu'un jeu ou un logiciel de traitement de texte et utilisant les mêmes fonctions du système que ceux-ci. Frederic COHEN, « Implications of Computer Viruses and Current Methods of Defense », dans Peter J. DENNING (éd.), *Computers Under attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 381, à la page 382.

[47] Robert SLADE, *op. cit.*, note 3, p. 4.

[48] David GERROLD, *When Harlie Was One*, New York, Nelson Doubleday Inc., 1972, p.154.

[49] David HARLEY et al., *op. cit.*, note 3, p. 570-571.

virus informatiques comme suit : « *A virus is a program that can « infect » other programs by modifying them to include a, possibly evolved, version of itself* ».[50]

Cependant, cette définition est souvent critiquée parce trop peu restrictive[51]. Sera donc qualifié de virus dans la présente étude tout « *antiprogramme dont l'exécution est déclenchée lorsque le vecteur auquel il a été attaché clandestinement est activé, qui se recopie au sein d'autres programmes ou sur des zones systèmes lui servant à leur tour de moyen de propagation, et qui produit les actions malveillantes pour lesquelles il a été conçu* »[52].

Un virus est donc, au sens propre, un logiciel auto-reproductible – comportant du code informatique se copiant explicitement – pouvant « infecter » d'autres programmes en les modifiant ou en modifiant leur environnement, afin que l'accès à un logiciel infecté implique l'accès à une copie évoluée du virus[53]. Les deux caractéristiques fondamentales des virus sont ainsi leur auto-reproductibilité et leur auto-propagation[54]. Lorsqu'ils sont activés, les virus se chargent en mémoire et exécutent les instructions préalablement programmées par leurs auteurs. Les virus se reproduisent donc en infectant les disquettes, systèmes informatiques et réseaux. Cependant, il importe de souligner qu'un virus ne peut agir que s'il est exécuté par l'utilisateur souvent inconscient de son acte[55].

Bien qu'il existerait plus de 57 000 virus différents[56], la plupart de ceux-ci sont en réalité des clones, ou plus exactement des mutants, c'est-à-dire

---

[50] Frederick COHEN, *op. cit.*, note 7, p. 2.
[51] David HARLEY et al., *op. cit.*, note 3, p. 571.
[52] OFFICE DE LA LANGUE FRANÇAISE, « Le grand dictionnaire terminologique », (2002) en ligne sur le site : <http://www.granddictionnaire.com> (date de visite : 25 avril 2002).
[53] David HARLEY et al., *op. cit.*, note 3, p. 571.
[54] Henri LILEN, et François DAROT, *op. cit.*, note 38, p. 10.
[55] Jen HRUSKA, *Virus informatiques et systèmes anti-virus*, Paris, Masson, 1992, p. 16-17.
[56] Voir le site « http://vil.mcafee.com/default.asp? »

des virus ayant été réécrits par d'autres utilisateurs afin de modifier leur comportement ou tout simplement pour changer les messages qu'ils affichent[57]. La mutation s'obtient donc par une programmation intentionnelle à l'opposé des mutations biologiques qui, elles, sont accidentelles[58]. Toutefois, si la majorité des virus se ressemblent du fait qu'ils possèdent pratiquement tous une fonction de multiplication, c'est-à-dire d'insertion dans les fichiers exécutés[59], ils peuvent comporter différentes qualités les rendant plus ou moins dommageables.

Certains virus possèdent un déclencheur, c'est-à-dire une série d'informations lui indiquant où et quand exécuter sa charge (la fonction pour laquelle il a été programmé)[60]. Cette sous-catégorie de virus porte habituellement le nom de « bombe logique »[61]. Le déclencheur pourrait être la mise en œuvre d'une série de conditions comme l'ouverture répétée d'un certain fichier[62], la présence ou l'absence d'une donnée[63], ou encore l'arrivée d'une date ou d'une heure précise. Dans ce dernier cas, le virus portera le nom de « bombe à retardement »[64]. Cependant, certains auteurs précisent que les bombes logiques ne sont pas nécessairement des virus au sens de notre définition, puisque, à la base, ces programmes sont non auto-reproductibles et non auto-propagateurs[65]. Cette distinction s'avère toutefois négligeable dans le

---

[57] Jean-François PILLOU, « Les virus » (2001) en ligne sur le site *Comment ça marche* : <http://www.commentcamarche.net/virus/virus.php3> (date de visite : 25 avril 2002).
[58] Jan HRUSKA, *op. cit.*, note 55, p. 70.
[59] Jean-François PILLOU, *loc. cit.*, note 57.
[60] David HARLEY et al., *op. cit.*, note 3, p. 7.
[61] Les bombes logiques sont des « *dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système* ». Jean-François PILLOU, « les bombes logiques » (2001) en ligne sur le site *Comment ça marche* : <http://www.commentcamarche.net/virus/bomblogi.php3> (date de visite : 25 avril 2002).
[62] David HARLEY et al., *op. cit.*, note 3, p. 100.
[63] Jan HRUSKA, *op. cit.*, note 55, p. 15.
[64] David HARLEY et al., *op. cit.*, note 3, p. 101.
[65] Henri LILEN, et François DAROT, *op. cit.*, note 38, p. 11.

cadre de notre étude, c'est pourquoi nous incluons les bombes logiques dans la classe des virus.

Ensuite, certains virus sont polymorphes ou furtifs. En effet, puisque, comme nous le verrons, les logiciels antivirus détectent les maliciels grâce à l'apparence de leur code, certains créateurs de virus ont pensé leur donner la possibilité de modifier ou camoufler celle-ci[66].

Finalement, les virus ne s'attaquent pas tous aux mêmes types de fichiers. Ainsi, les virus multimodes contaminent à la fois certaines zones du système d'exploitation et des programmes exécutables; les virus d'amorçage attaquent la zone du disque ou de la disquette qui contient le programme d'amorçage, lequel est utilisé pour charger et lancer le système d'exploitation; les virus de partition endommagent l'enregistrement d'amorçage maître en se greffant sur le premier secteur de la première partition du disque dur, laquelle contient la table des partitions du système d'exploitation[67] ; les virus systèmes, attaquent le système informatique dans son entier ; les virus fichiers contaminent et attaquent les fichiers[68], etc.

Néanmoins, le type de virus le plus courant de par sa facilité de fabrication, demeure le virus de macro[69], soit un virus « *programmé dans le langage utilisé par l'application visée, qui se propage dans les fichiers de macrocommandes et qui contamine non pas le programme, comme c'est le cas pour les autres virus, mais les documents créés par celui-ci, en leur ajoutant des macrocommandes dont les actions sont variées, depuis le simple affichage de messages jusqu'à la suppression*

---

[66] Jean-François PILLOU, *loc. cit.*, note 57.
[67] OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[68] Henri LILEN, et François DAROT, *op. cit.*, note 38, p. 53.
[69] Les macros sont des « [i]*nstruction complexe écrite dans un langage d'assemblage ou créée par l'utilisateur, qui représente une suite d'instructions réelles en langage machine et qui est destinée à être remplacée par cette suite chaque fois qu'elle apparaît dans un programme* ». OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.

de fichiers »[70]. Ce type de virus arrive actuellement à infecter les macros[71] de documents *Microsoft Office*, c'est-à-dire qu'il peut être situé à l'intérieur d'un banal document Word ou Excel et exécuter une portion de code à l'ouverture de celui-ci, ce qui lui permet d'une part de se propager dans les fichiers, mais aussi d'accéder au système d'exploitation[72].

b) Les chevaux de Troie

Les chevaux de Troie sont des antiprogrammes qui, suite à leur introduction dans une séquence d'instructions normales, prennent l'apparence d'un programme valide contenant en réalité une fonction illicite cachée, grâce à laquelle les mécanismes de sécurité du système informatique sont contournés[73]. Bref ce logiciel exécute des services ne se limitant pas à ceux énoncés dans ses spécifications[74], permettant ainsi la pénétration par effraction dans un ordinateur pour en consulter, modifier ou détruire les fichiers[75]. Comme l'expliquent David Harley, Robert Slade et Urs E. Gattiker, les chevaux de Troie sont des « *programs that claim to do something useful or desirable, and may do so, but also perform actions that the victim wouldn't expect or want* »[76]. Un cheval de Troie est donc un programme caché à l'intérieur d'un autre qui exécute des commandes sournoises et qui permet l'accès à la machine sur laquelle il est exécuté[77]. Ainsi, si un programme ou un

---

[70] *Id.*
[71] « *A simple macro is series of steps that could otherwise be typed, selected, or configured, but are stored in a single location so they can automated* ». Roger A. GRIMES, *op. cit.*, note 35, p. 131.
[72] Jean-François PILLOU, *loc. cit.*, note 57.
[73] OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[74] Jan HRUSKA, *op. cit.*, note 55, p. 12.
[75] OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[76] David HARLEY et al., *op. cit.*, note 3, p. 13.
[77] Jean-François PILLOU, « Chevaux de troie » (2001) en ligne sur le site *Comment ça marche* : <http://www.commentcamarche.net/virus/trojan.php3> (date de visite : 25 avril 2002).

fichier est contaminé par un virus, il devient lui-même un Cheval de Troie[78].

Pour en arriver aux fins escomptées par leurs créateurs, les chevaux de Troie ouvrent certains ports de l'ordinateur infecté, principe connu sous le nom de « porte dérobée » (*backdoor*). Cette machination permet alors à leurs auteurs de prendre le contrôle de l'ordinateur infecté. Le dommage causé par un cheval de Troie s'effectue donc en deux temps. Premièrement, l'utilisateur ouvre un fichier infecté contenant le « troyen » et, dans un second temps, l'auteur du cheval de Troie accède à l'ordinateur infecté par le port ouvert pour voler des mots de passe ou encore pour copier des données sensibles contenues sur l'ordinateur[79].

Si, tout comme le virus, le cheval de Troie est un logiciel nuisible placé dans un programme sain[80], il demeure qu'il s'agit de deux maliciels distincts dans leur nature. Un cheval de Troie n'est pas un virus dans la mesure où il ne se reproduit pas par lui-même[81], son but n'étant pas nécessairement d'infecter d'autres machines, mais bien d'en prendre le contrôle en se faisant passer pour un logiciel légitime[82].

L'absence du caractère épidémique rend les chevaux de Troie beaucoup plus facile à cerner dans l'optique de la responsabilité civile des intermédiaires, puisque le logiciel en soi demeure plus ou moins inoffensif. Ce n'est que lorsque le pirate informatique l'ayant distribué tente de s'en servir que les dommages peuvent survenir, ceux-ci étant donc normalement directement causés par l'auteur de l'acte illicite. Cette étape étant désintermédiarisée, la recherche d'autres débiteurs potentiels devient inutile. Cependant, dans la mesure où le « troyen » cache également un virus ou encore que l'attaque effectuée passe par

---

[78] Jan HRUSKA, *op. cit.*, note 55, p. 12.
[79] Jean-François PILLOU, *loc. cit.*, note 77.
[80] *Id.*
[81] David HARLEY et al., *op. cit.*, note 3, p. 13.
[82] Roger A. GRIMES, *op. cit.*, note 35, p. 183.

plusieurs réseaux internes, les règles de responsabilité civile s'appliquant aux virus s'appliqueront *mutatis mutandis* aux chevaux de Troie.

c) Les vers

Un ver est un programme informatique autonome pouvant s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes de celui-ci[83]. Les vers ne sont pas des virus au sens stricte, ceux-ci ne faisant pas recours à un support physique pour se propager[84], c'est-à-dire qu'ils ne s'attachent pas à un programme hôte comme le font les virus pour assurer leur épandage[85].

Les vers actuels se propagent via le courrier électronique des utilisateurs grâce à des fichiers attachés[86] contenant des instructions leur permettant de récupérer l'ensemble des adresses de courrier contenues dans les carnets d'adresses de ces derniers[87]. Leur évolution se décrit comme suit :

> « *The user runs the attached file, and the worm invades the user's system and sends itself to recipients on the user's email address book lists. An email arrives in the new victim's inbox, sent by a known acquaintance. It implores the new victim to run the attached file or web link* »[88].

Cette fonctionnalité du logiciel lui permet ensuite de se transmettre à tous les destinataires inscrits dans le carnet d'adresses de la victime de l'infection.

---

[83] Jean-François PILLOU, « Les vers » (2001) en ligne sur le site *Comment ça marche* : <http://www.commentcamarche.net/virus/worms.php3> (date de visite : 25 avril 2002).
[84] Lawrence LESSIG, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, p. 17.
[85] David HARLEY et al., *op. cit.*, note 3, p. 572.
[86] Roger A. GRIMES, *op. cit.*, note 35, p. 183.
[87] Jean-François PILLOU, *loc. cit.*, note 83.
[88] Roger A. GRIMES, *op. cit.*, note 35, p. 183.

Au sens strict, les vers sont donc potentiellement moins dommageables que les virus puisqu'ils infectent l'environnement, c'est-à-dire le système d'opération ou encore le réseau et non les fichiers[89]. C'est donc dire qu'ils ne causent pas forcément de dommages irréparables comme la perte de données.

Il existe deux types de vers, à savoir les vers de station de travail (*host computer worms*) et les vers de réseaux (*network worms*). Les vers de station de travail se limitent à corrompre l'ordinateur dans lequel ils se trouvent[90], c'est-à-dire qu'ils sont entièrement contenus dans les stations de travail sur lesquelles ils tournent[91]. Ils n'utilisent les connections réseaux que pour se déplacer d'un ordinateur à un autre. Ainsi, ce type de ver ne se reproduit pas nécessairement. Il peut simplement migrer via le réseau sans laisser aucune trace de son passage. Dans ces circonstances particulières, le ver sera qualifié de lapin, soit de « [p]*rogramme malveillant qui n'altère pas les ressources d'un réseau et ne s'attache pas à d'autres programmes, mais qui peut épuiser toutes les ressources d'un système informatique en se multipliant à l'infini, ce qui cause généralement une défaillance du système* »[92].

Les vers de réseaux, de leur côté, sont des vers constitués de plusieurs parties ou « segments » tournant chacun sur des systèmes différents et pouvant accomplir des tâches distinctes. Ces vers utilisent le réseau pour communiquer et éventuellement, pour se propager d'un système à un autre[93]. Lorsqu'un ver de réseau comporte un segment dont la fonction consiste à coordonner le travail des autres segments, il sera alors qualifié de pieuvre (*octopus*)[94].

---

[89] ANONYME, *op. cit.*, note 20, p. 326.
[90] David HARLEY et al., *op. cit.*, note 3, p. 572.
[91] OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[92] *Id.*
[93] *Id.*
[94] David HARLEY et al., *op. cit.*, note 3, p. 572.

Malgré ce qui précède, la distinction entre virus et vers s'avère parfois difficile à établir, certains experts hésitant même à tenter l'exploit[95], les maliciels hybrides étant aujourd'hui chose commune[96]. De plus, si la différence au sens logistique peut parfois être perceptible, la différence au sens juridique s'adonne à être futile de par le fait que ces deux formes de maliciels se propagent de façon similaire, c'est-à-dire qu'ils utilisent des tiers comme agents de propagation. Cependant, certains vers qualifiés d'« actifs »[97] offrent une complication absente chez les virus au sens juridique puisque leur propagation est possible sans intervention humaine quelle qu'elle soit[98]. Nous explorerons cette complication dans la section II de la présente étude.

d) Les métavirus

Les métavirus sont des « virus » fictifs découlant du fruit de l'imagination des internautes, bref, ce sont des canulars[99]. Il ne s'agit donc pas de maliciel au sens de notre exposé, puisque les métavirus infectent l'esprit des gens naïfs et non leurs ordinateurs[100]. Cependant, il nous apparaît opportun de souligner l'existence de ces faux virus puisque leur impact peut s'avérer tout aussi dommageable que celui d'un véritable maliciel.

Les canulars informatiques prennent généralement la forme d'un courriel annonçant l'arrivé d'un nouveau virus extrêmement dangereux dont le remède demeure inconnu. Le message invite alors le lecteur à transmettre l'information à toutes ses connaissances afin de restreindre

---

[95] Comme l'explique Sascha SEGAN : « [y]*ou'll often see worms referred to as viruses; most experts consider the word "virus" to include worms, as well* ». Sascha SEGAN, *loc. cit.*, note 40, 54.
[96] David HARLEY et al., *op. cit.*, note 3, p. 12.
[97] Tracy BAKER, « Your Computer Is Worm Food: Thanks to Email, Malicious Code Really Gets Around » (2002) 13 *Smart Computing* 62, 62.
[98] *Id.*
[99] ANONYME, *op. cit.*, note 20, p. 336.
[100] *Id.*, p. 333.

l'épidémie. Heureusement, ces messages sont fictifs et n'ont comme objectif que d'engorger le réseau. Il s'agirait, si l'on veut faire l'analogie, de vers dont l'activation est manuelle. Le succès de tels canulars réside dans le fait que les internautes sont moins sceptiques que lorsqu'ils se retrouvent dans « le monde réel » :

> « *People have a tendency to accept what they read on the Internet without considering whether or not the source is a known trustworthy source. Information from friends is often accepted at face value, as the friend is a known trustworthy person. Evaluation of the qualifications of the friend or co-worker to advise in the areas of computer viruses is often neglected. Application of legitimate scientific scepticism is perhaps our most powerful weapon in the battle against hoaxes* ».[101]

Si, à la base, les métavirus paraissent plutôt inoffensifs de par le fait qu'ils ne peuvent se propager aussi rapidement que les vers et donc qu'ils ne peuvent réellement engorger les différents réseaux informatiques, leur force persuasive s'avère dangereuse. En effet, si, à première vue les canulars causent plus de désagrément que de dommage, certains, s'ils sont mis en application, peuvent être tout aussi virulents que le pire des virus. Prenons l'exemple suivant :

> « *ATTENTION VIRUS !*
>
> *La majorité des utilisateurs d'Internet vont être contaminés, si ce n'est déjà fait, par un virus nommé: sulfnbk.exe qui est redoutable car écrasant votre disque dur je viens de le détruire sur mon propre disque dur, il était déjà là.*
>
> *Procédure: dans menu démarrer: rechercher fichiers ou dossiers et vous saurez si vous l'avez. Dans ce cas, allez le chercher, cliquez une seule fois dessus et supprimez-le. Aller ensuite dans corbeille et supprimer le contenu de la corbeille. Je vous incite très fortement à vérifier si ce*

---

[101] Sarah GORDON, « Hoaxes and Hypes », (1997) en ligne sur le site *IMB Research* : <http://www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html> (date de visite : 11 juillet 2002).

> *virus est déjà sur votre disque dur car il devrait être activé le 25 mai.*
>
> *Bien à vous.* »[102]

Le virus « Sulfnbk.exe » n'existe pas. Cependant, Sulfnbk.exe est un utilitaire de Windows 98 déjà présent dans les fichiers des utilisateurs de ce système d'exploitation[103]. Ainsi, l'utilisateur qui suivra les instructions de ce message causera un dommage à son système suite aux indications mensongères d'un tiers. Bien que la question de la responsabilité des tiers soit pertinente dans la transmission de métavirus – les dommages étant liés non pas à un logiciel, mais bien à une forme de publicité trompeuse – elle s'éloigne considérablement du type de responsabilité attribuable à la transmission d'un véritable virus. Les métavirus, bien qu'ils méritent d'être mentionnés, ne seront donc pas traités subséquemment dans le présent mémoire.

2. Les mesures de protection contre les maliciels

La majorité des virus sont transmis via les services de courrier électronique sous la forme d'un fichier joint[104]. Cependant, ces logiciels peuvent également être transmis par des disquettes contaminées ou téléchargés d'un site Web ou d'un serveur[105]. En effet, « *tout support servant à la transmission de programmes exécutables est un vecteur potentiel de virus parasites* »[106]. C'est donc dire que l'établissement de mesures de protection devra tenir compte de ces diverses possibilités. À

---

[102] Source : H*oaxbuster.com* : <http://www.hoaxbuster.com/hliste/juin01/sulfnbk.html>, (Date de visite, 15 septembre 2002).
[103] *Id.*
[104] PISA, *loc. cit.*, note 6. En effet, « *more than 80 percent of viruses use e-mail as the principal means of propagation* ». « Persistant Viruses Sound Industry Alarm », (2001) en ligne sur le site *ArmourPlate* : <http://www.armourplate.com/news/015.htm> (dernière mise à jour : 14 août 2001). Il existe toutefois quelques rares virus pouvant être activés par l'ouverture du courriel lui-même, sans recours aux pièces jointes. Voir à ce sujet : Roger A. GRIMES, *op. cit.*, note 35, p. 383.
[105] Roger A. GRIMES, *op. cit.*, note 35, p. 440.
[106] Jan HRUSKA, *op. cit.*, note 55, p. 25.

cette fin, les experts s'accordent pour dire qu'il est nécessaire, afin de s'assurer d'avoir le système le plus sécuritaire possible, de combiner les technologies des logiciels antiviraux (a), du coupe-feu (b) et certaines mesures préventives (c).

a) Les logiciels antiviraux

L'utilisation de logiciels antivirus fiables et mis à jour régulièrement devrait être la première étape dans la protection d'un système informatique, puisque ces derniers permettent la détection et l'élimination de logiciels malicieux[107].

Les logiciels antiviraux peuvent être divisés en trois catégories : les moniteurs d'activité[108], les logiciels de détection de changement[109] et les « scanners »[110]. Ces derniers étant les plus communs, ils méritent qu'on les aborde plus particulièrement.

Les scanners étudient l'information contenue sur les disques et en mémoire afin d'y retrouver une structure de code identifiable à une forme virale connue[111]. Ces logiciels peuvent recourir à une technologie générique qui détecte les structures virales sans les identifier[112] ou, plus communément, à une technologie dite spécifique (*virus-specific*), c'est-à-dire selon laquelle chaque fois qu'un nouveau virus est identifié, il est étudié jusqu'à ce qu'un remède soit trouvé et adopté[113].

---

[107] Roger A. GRIMES, *op. cit.*, note 35, p. 441.
[108] « *Activity monitors examine operations as they occur in the computer, sounding the alarm when a possibly dangerous event happen* ». David HARLEY et al., *op. cit.*, note 3, p. 151.
[109] « *Change-detection software takes a snapshot of the details of the system, alerting the user when some modification has been made* ». *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*, p. 15.
[113] *Id.*, p. 15.

Ce second modèle de scanner fait un recensement des fichiers contenus sur le disque sélectionné en comparant le code résidant sur le support à une banque de donnée contenant la structure des virus connus.[114] Ceci implique donc que celui-ci ne détectera que les virus déjà présents dans ses banques[115]. Il devient donc important de mettre ce type de logiciel à jour dès qu'un nouveau virus est découvert sur Internet[116].

De nos jours, ces deux technologies sont cependant souvent jumelées. En effet, certains scanners spécifiques utilisent une technique générique, l'analyse heuristique[117], pour déceler de nouveaux virus non encore répertoriés[118].

L'utilisation d'un logiciel antivirus à jour est donc essentiel à la protection d'un ordinateur. Cependant, il serait irresponsable de prétendre que cette mesure place l'utilisateur dans une situation d'invulnérabilité[119]. En effet, la présence d'antivirus ne saurait en soi être suffisante[120], puisque ces logiciels ne peuvent éliminer qu'un certain pourcentage des nouveaux virus[121]. Il est ainsi primordial d'y ajouter d'autres moyens de protection[122].

---

[114] Roger A. GRIMES, *op. cit.*, note 35, p. 447.
[115] David HARLEY et al., *op. cit.*, note 3, p. 158.
[116] Vicky H. ROBBINS, *loc. cit.*, note 44, 27-28.
[117] « *Méthode de recherche empirique ayant recours aux essais et erreurs pour la résolution de problèmes* ». OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[118] David HARLEY et al., *op. cit.*, note 3, p. 15.
[119] ANONYME, *op. cit.*, note 20, p. 349. Voir aussi Vicky H. ROBBINS, *loc. cit.*, note 44, 27-28.
[120] Roger A. GRIMES, *op. cit.*, note 35, p. 441.
[121] Selon Carey Nachenberg, ce pourcentage se situerait autours de 70 à 80 %. Carey NACHENBERG, *loc. cit.*, note 21, 7.
[122] Sarah GORDON, « Why Computer Viruses Are Not – And Never Were – A Problem » (1994) en ligne sur le site *Commandcom* : <http://www.commandsoftware.com/virus/problem.html> (date de visite : 1 mai 2002).

b) Les coupe-feu

Le coupe-feu est un « [d]*ispositif informatique qui permet le passage sélectif des flux d'information entre un réseau interne et un réseau public, ainsi que la neutralisation des tentatives de pénétration en provenance du réseau public* »[123]. Sous sa forme la plus simple, le coupe-feu bloque la circulation sur le réseau et permet seulement les entrées et sorties pré-autorisées par le propriétaire de l'ordinateur ou le responsable du réseau[124]. Bien que ces logiciels n'empêchent pas la circulation de virus, ils empêchent les tiers d'entrer dans un système sans autorisation, ce qui enraye aussi, par exemple, l'utilisation de chevaux de Troie.

c) Les mesures générales de sécurité préventive

Il n'y a que trois façons de réduire les risques d'infection liés à la transmission de virus informatiques : limiter le partage, limiter la transitivité et limiter la fonctionnalité[125]. Or, il existe une panoplie de mesures de sécurité pouvant être mises en oeuvre par un utilisateur ou encore un gestionnaire de réseau interne afin de mettre en application ces principes sans toutefois rendre leur matériel inutilisable. Notre objectif n'étant pas la rédaction d'une politique de sécurité informatique, mais bien la démonstration de l'existence de mesures pouvant réduire le risque d'infection et donc la responsabilité des tiers transmetteurs de virus informatiques, nous nous limiterons ici à la simple énumération des mesures les plus recommandées et renvoyons le lecteur aux ouvrages en bibliographie portant sur la sécurité informatique pour plus d'information.

---

[123] OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[124] Roger A. GRIMES, *op. cit.*, note 35, p. 465.
[125] Frederic COHEN, *op. cit.*, note 46, p.394.

i) Le contrôle de courrier électronique et des fichiers joints

La règle de base dans le cas du courrier électronique est de ne pas ouvrir les fichiers joints[126], surtout s'ils proviennent d'une source inconnue[127] ou si le sujet du message semble étrange[128], puisque c'est à l'intérieur de ceux-ci que se cachent la majorité des virus. Cependant, il est important de noter que même un fichier envoyer par une connaissance pourrait être infecté à son insu[129]. Il est donc recommandé par les experts de ne pas ouvrir toute pièce jointe pouvant agir comme vecteur à un virus tels les fichiers .EXE, .COM ou .DOC[130] ou, tout au moins, de soumettre ces fichiers à un logiciel antivirus avant de les ouvrir. Comme le souligne Sixto Ortiz Jr. : « *Prevention of file virus infection is simple: Never trust an executable file delivered by email or downloaded from the Internet. Always virus-scan an executable file* before *you run the program* »[131].

ii) Le téléchargement de fichiers

La règle demeure la prudence lors du téléchargement de fichiers sur Internet[132]. Il est recommandé de ne jamais télécharger de fichiers à partir de sites inconnus[133], ou encore de babillards électroniques[134]. Si cela n'est pas possible, il est alors recommandé de soumettre ces fichiers à un logiciel antivirus avant de les ouvrir[135].

---

[126] ANONYME, *op. cit.*, note 20, p. 349.
[127] James STANGER (éd.), *E-Mail Virus Protection Handbook*, Rockland, Syngress, 2000, p. 405.
[128] *Id.*
[129] *Id.*
[130] David HARLEY et al., *op. cit.*, note 3, p. 144.
[131] Sixto ORTIZ Jr., « Twisted Bits : How Computer Viruses Do Their Dirty Work », (2002) 13 *Smart Computing* 58, 59.
[132] James STANGER, *op. cit.*, note 127, p. 405
[133] *Id.*, p. 405. En effet, il est toujours préférable de télécharger les logiciels sur les sites d'entreprises établies puisque celles-ci s'assurent normalement de leur qualité.
[134] H.J. HIGHLAND (éd.), *Computer Virus Handbook*, Oxford, Elsevier Advanced Technology, 1990, p.279.
[135] Vicky H. ROBBINS, *loc. cit.*, note 44, 27-28.

iii) La configuration du système

Il est suggéré d'éviter l'utilisation de logiciels vulnérables aux virus de macro[136]. Cependant, comme ceux-ci incluent tous les logiciels de la suite Microsoft Office, cela peut s'avérer impossible. Il est alors recommandé de désactiver les macros ou encore de s'assurer que celles-ci ne sont pas activées par défaut sur ces programmes[137].

Internet n'étant pas le seul vecteur possible de transmission de virus, il est également suggéré de limiter l'accès de disquettes, soit en désactivant le lecteur lors du démarrage[138], ou de façon permanente[139], soit en éliminant simplement les lecteurs[140]. Si toutes ces options s'avèrent difficiles à adopter, il serrait judicieux de soumettre toute disquette à un logiciel antivirus avant d'y accéder[141].

iv) Le comportement des utilisateurs

Il est conseillé de n'acheter que des logiciels d'entreprises dont la réputation devrait être gage de qualité[142]. Si cela n'est pas possible, il serait approprié de soumettre ces programmes à un logiciel antivirus avant de les utiliser[143]. Quoiqu'il en soit, l'installation de logiciels devrait toujours se faire avec prudence. En effet,

> « *One industry expert claims that salespersons and product demonstrators account for 65 percent of corporate infections, by infecting company computers*

---

[136] David HARLEY et al., *op. cit.*, note 3, p. 144.
[137] ANONYME, *op. cit.*, note 20, p. 349.
[138] Roger A. GRIMES, *op. cit.*, note 35, p. 56. Voir aussi David HARLEY et al., *op. cit.*, note 3, p. 144.
[139] David HARLEY et al., *op. cit.*, note 3, p. 144.
[140] H.J. HIGHLAND, *op. cit.*, note 134, p.280.
[141] Roger A. GRIMES, *op. cit.*, note 35, p. 57.
[142] H.J. HIGHLAND, *op. cit.*, note 134, p.279.
[143] Vicky H. ROBBINS, *loc. cit.*, note 44, 27-28.

> *with their disks. Repair personnel who run infected diagnostic disks also account for many infections. It is best to scan all foreign disks for infection before use* »[144].

Dans le cas d'entreprises, il est également important d'empêcher ses employés d'apporter des logiciels de la maison au bureau[145]. Cependant, lorsque l'application de telles mesures devient difficile, il serait sage de soumettre ces logiciels à un logiciel antivirus avant de les utiliser[146].

L'adoption de ce type de mesures de sécurité, si elle ne peut assurer l'impossibilité d'une infection subséquente, aura cependant pour effet de réduire le risque de contamination. Or, comme nous l'aborderons maintenant, la responsabilité civile repose sur le principe que l'individu ayant pris toutes les précautions qu'aurait pris une personne raisonnable ne peut être tenu responsable du dommage causé à un tiers. Une politique de sécurité adéquate est donc la meilleure façon de se protéger contre d'éventuelles poursuites.

B. La responsabilité civile dans le cadre de la transmission de virus informatiques : fondements et objectifs

La responsabilité civile consiste en l'« *obligation pour une personne de réparer le préjudice qu'elle a causé à autrui par sa faute, par le fait ou la faute d'une autre personne ou par le fait d'un bien qu'elle a sous sa garde* »[147] Pour reprendre une formule bien connue, elle est engendrée « *lorsqu'une personne fait défaut de se comporter de façon*

---

[144] *Id.*
[145] H.J. HIGHLAND, *op. cit.*, note 134, p.280.
[146] Vicky H. ROBBINS, *loc. cit.*, note 44, 27-28.
[147] Hubert REID, *Dictionnaire de droit québécois et canadien*, Montréal, Wilson & Lafleur, 1994, p. 503.

raisonnablement prudente et diligente et cause ainsi un dommage à un tiers »[148]. En effet, comme le soulignait Domat :

> « *Toutes les pertes et tous les dommages, qui peuvent arriver par le fait de quelque personne, soit imprudence, légèreté, ignorance de ce qu'on doit savoir, ou autres fautes semblables, si légères qu'elles puissent être, doivent être réparées par celui dont l'imprudence ou autre faute y a donné lieu. Car c'est un tort qu'il a fait, quand même il n'aurait pas eu l'intention de nuire* »[149].

Depuis ses origines, la responsabilité civile semble avoir servi cinq fonctions distinctes, mais étroitement liées[150], à savoir : le châtiment du coupable, la vengeance, l'indemnisation de la victime, le rétablissement de l'ordre social et la prévention des comportements anti-sociaux[151]. Si toutes ces fonctions continuent à inspirer le droit dans une certaine mesure[152], la responsabilité civile contemporaine ne visant plus à blâmer, ni à punir, mais seulement à compenser une perte[153], il en découle que la fonction première de la responsabilité civile en soit aujourd'hui une de réparation[154].

En effet, la responsabilité civile entraîne l'obligation de rétablir l'équilibre économique rompu et de réparer le dommage causé[155] :

> « *Historiquement, il est vrai, l'indemnisation de la victime n'a probablement pas été la première fonction de la responsabilité civile. Dans les sociétés primitives, la faute apparaît certainement comme une rupture de l'ordre social ou même de l'ordre cosmique. Mais au fur et à mesure que la faute civile se séparait du crime ou du péché et gagnait son identité propre, l'indemnisation de*

---

[148] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 1
[149] Voir André TUNC, *La responsabilité civile*, 2e éd., Paris, Economica, 1989, p. 55.
[150] *Id.*, p. 133.
[151] *Id.*
[152] *Id.*
[153] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 5
[154] *Id.*, p. 3-4
[155] *Id.*, p. 3

> *la victime devenait un de ses objectifs fondamentaux* »[156].

Cela ne veut pas dire pour autant que les autres fonctions n'ont plus d'impact en droit contemporain puisque, encore aujourd'hui, la menace d'une condamnation à des dommages exerce une fonction préventive sur le comportement des individus[157].

En droit québécois, c'est l'article 1457 du *Code civil du Québec* qui établit les principes de la responsabilité civile en précisant que :

> « *Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.*
>
> *Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.*
>
> *Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde.* »

À la lumière de cet article, la doctrine et la jurisprudence ont établi quatre critères devant être démontrés pour engager la responsabilité d'autrui, soit sa capacité de discernement, l'existence d'une faute (1), l'existence d'un préjudice (2) et la présence d'un lien de causalité entre la faute et le préjudice (3)[158]. Le critère de la capacité de discernement de l'individu ayant eu un comportement fautif ne soulève pas de difficultés particulières dans le contexte des virus informatiques. En effet, les principes établis ailleurs sont tout aussi valides et notre sujet ne vient

---

[156] André TUNC, *op. cit.*, note 149, p. 142.
[157] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 4. Voir aussi Ejan MACKAAY, *L'analyse économique du* droit, tome 2, Montréal, Thémis, non publié, p. 8 : « *dans sa conception fondamentale, la responsabilité civile vise à remplir, d'un seul coup, la double fonction de dissuasion et d'indemnisation* ».
[158] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 56 et 57.

en aucun cas modifier la donne[159]. Ce sont donc les trois autres critères qui retiendront notre attention.

1. La faute

Comme l'expliquent Jean-Louis Baudouin et Patrice Deslauriers :

> *Il ne suffit pas de pouvoir relier le dommage subi au comportement reproché* [pour engager la responsabilité civile [d'un tiers], *encore faut-il démontrer que le dommage est dû à une faute, c'est-à-dire à un comportement non conforme aux standards généralement acceptés par la jurisprudence ou* [...] *à la norme de conduite qui, selon les circonstances, les usages ou la loi, s'imposent à elle.* [160]

À la lumière de cet extrait, constitue une faute en droit civil québécois tout « *acte ou omission dont l'auteur est une personne douée de discernement qui a fait défaut de se conformer à une prescription de la loi ou à l'obligation générale de se comporter en personne diligente et raisonnable à l'égard d'autrui* »[161]. Commet ainsi une faute toute personne faisant défaut de se conformer aux devoirs généraux ou spécifiques de conduite imposés par les tribunaux et le législateur « *à un moment particulier de l'évolution sociale* » [162]. En effet, la notion de faute varie, pour reprendre une formule classique, « *selon l'époque et le lieu de la faute prétendue. Il dépend des mœurs et des usages, ainsi que*

---

[159] Comme l'expliquent Jean-Louis Baudouin et Patrice Deslauriers, « *l'individu privé de raison, c'est-à-dire incapable de rendre compte des conséquences des actes qu'il pose, ne peut donc, en principe, être tenu civilement responsable* », Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 56. Ainsi, la raison n'étant pas un facteur influencé par les avancements technologiques, nous ne croyons pas utile d'étudier cet aspect de la responsabilité déjà traité dans plusieurs textes de doctrine.

[160] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 56.

[161] Hubert REID, *op. cit.*, note 147, p. 239.

[162] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 98-99.

des moyens, plus perfectionnés, de prévisibilité et d'évitabilité du mal, que la science moderne confère à l'agent »[163].

La notion de faute peut ainsi reposer sur la transgression du devoir imposé par un texte de loi spécifique. Est donc fautif l'individu qui affiche un comportement social qui ne correspond pas au modèle que la société attend de lui[164]. Lorsque aucune norme particulière de comportement n'a été prévue, il y a faute quand, volontairement ou par simple imprudence, l'individu transgresse le devoir général de ne pas nuire à autrui[165]; critère développé par les juristes romains pour l'application de la loi Aquilia[166]. Selon cette loi, était considérée fautive la conduite n'étant pas conforme à celle qu'aurait eu un bon père de famille[167]. Aujourd'hui, le modèle du « bon père de famille » est remplacé par celui du type abstrait et objectif de la personne raisonnable, prudente et diligente, bref, du bon citoyen[168]. Est donc fautif quiconque a un comportement contraire à celui auquel on peut s'attendre d'une personne raisonnable placée dans les mêmes circonstances[169].

Ce qui précède nous pousse donc à faire un premier constat, c'est-à-dire qu'un utilisateur d'ordinateur normalement prudent et prévoyant constitue la norme à laquelle nous devrons nous référer pour apprécier la responsabilité civile[170] dans la transmission de virus informatiques. Ce constat débouche cependant sur une première problématique. En effet, « [a]*t this point, there is no reliable standard of behavior which can be relied upon in tort litigation. Indeed, there is a certain amount of*

---

[163] René SAVATIER, *Traité de responsabilité civile*, Paris, Librairie générale de droit et de jurisprudence, 1951, 2e éd., t. 1, nº 166, p. 208.
[164] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 105.
[165] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 97.
[166] André TUNC, *op. cit.*, note 149, p. 56.
[167] *Id.*
[168] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 112.
[169] *Id*, p. 98.
[170] PISA, *loc. cit.*, note 6.

controversy over what the "rational computer programmer" would do under the circumstances »[171].

Afin de solutionner cette problématique, il importe donc de nous pencher sur l'analyse de ce qui pourrait constituer un comportement prudent et diligent dans le cas d'un tiers transmetteur de virus informatiques.

a) La négligence comme composante de la faute

Selon l'analyse faite par la doctrine[172] et les tribunaux[173] de l'article 1457 C.c.Q., une faute peut être intentionnelle ou résulter d'une négligence, d'une imprudence ou d'une maladresse[174]. Il n'est donc pas nécessaire d'avoir l'intention de nuire ou de causer un préjudice à autrui ou même d'être conscient d'avoir adopté un comportement différent de celui de la norme, pour commettre une faute. Ainsi, « [t]*oute personne exposant autrui à une situation qu'elle sait ou devrait savoir être une situation susceptible de causer un préjudice* [doit être] *tenue responsable pour motifs d'imprudence et de négligence* »[175] et doit compenser la victime dudit préjudice[176].

Par négligence, nous entendons la « *faute non intentionnelle qui consiste, pour l'auteur du préjudice, à s'abstenir de prendre toutes les précautions normalement requises pour que l'activité à laquelle il se livre*

---

[171] Anne W. BRANSCOMB, *op. cit.*, note 25, p. 81.
[172] Comme l'expliquent Jean-Louis Baudouin et Patrice Deslauriers, « *Est en faute quiconque a un comportement contraire à celui auquel on peut s'attendre d'une personne raisonnable placée dans les mêmes circonstances* », Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 98.
[173] *L'oeuvre de terrains de jeux de Québec* c. *Cannon*, (1940) 69 B.R. 112 (aux pages 114 et 118).
[174] Hubert REID, *op. cit.*, note 147, p. 239.
[175] David J. ROY et al., *VIH et SIDA : Rapport d'étude sur les aspects éthiques et juridiques*, Québec, Ministère de la santé et des services sociaux, 1988, p. 67.
[176] André TUNC, *op. cit.*, note 149, p. 55.

ne cause de dommage à autrui »[177]. Comme le soulignait déjà Carbonnier :

> « [L]*a négligence est le relâchement de l'attention, qu'une tension de l'esprit, effort de volonté, aurait pu combattre; l'imprudence est témérité, qu'aurait pu inhiber la réflexion, autre effort de volonté. Que sa volonté n'ait pas choisi au carrefour où elle le pouvait encore est assez pour que le négligent ou l'imprudent soit responsable* »[178].

Ainsi, comme l'explique un auteur, on ne la relèvera que « *s'il y a eu défaut de prendre les précautions ordinaires et usuelles nécessaires pour parer à des dangers normalement prévisibles* »[179]. Il importe cependant de souligner que la négligence ne constitue une faute que si elle correspond à un devoir n'ayant pas été rempli[180]. Mais peut-on prétendre que « [a] *victim might be accused of faillling to apply "due diligence"* [...] *in the dissemination of a virus* »[181]?

Tout comme l'explique un auteur, « *The basic legal principles of negligence law are not altered simply because a computer is the instrumentality being used. Those who use a computer have a duty to do so with care* »[182]. En effet, le fait que l'acte négligent se produise en ligne ne vient pas contredire les principes déjà établis. Prenons l'exemple suivant :

> « *Suppose a user unknowingly receives an infected program; suppose further that the user could detect the destructive code but neglects to do so, and subsequently*

---

[177] Hubert REID, *op. cit.*, note 147, p. 386.
[178] Jean CARBONNIER, *Droit Civil*, Tome 4, « Les obligations », Paris, Presses universitaires de France, 1996, p. 378.
[179] André NADEAU, *Traité de droit civil du Québec*, Tome 8, Montréal, Wilson & Lafleur, 1965, p. 46.
[180] *Id.*
[181] ANONYME, *op. cit.*, note 20, p.324.
[182] Michael D. SCOTT, *Computer Law*, New York, Wiley, 1985, p. 7-14.

> *passes the program on to a third party whose system is damaged by the code* »[183].

Comme le souligne Philippe Helis, la présence d'un virus est un risque prévisible auquel il est possible de pallier par des vérifications grâce à l'utilisation d'un antivirus. Il ne s'agit donc pas d'un fait irrésistible[184]. L'on peut ainsi prétendre que celui qui transmet un virus de cette façon n'a pas pris les précautions « *ordinaires et usuelles nécessaires* »[185]. Ainsi, pour prouver la négligence dans le contexte informatique :

> « *a potential plaintiff must show that a manager breached his or her duty of reasonable care. A systems manager might be found to have breached a duty of reasonable care for a number of reasons, such as the failure to recognize defects in a system, the failure to correct defects, or the failure to warn of defects.* [...] *Breach of duty might also arise from failure to train and supervise employees, or the failure to use reasonable means to secure the system from unauthorized and unintended use* »[186].

De plus, comme les tribunaux « *montrent une tendance naturelle à imputer la responsabilité à ceux qui étaient raisonnablement en mesure d'agir pour prévenir le dommage* » [187], l'on peut en déduire que la responsabilité de ces individus sera reconnue.

La conduite considérée négligente doit cependant être évaluée en regard de l'activité propre de l'agent au moment où le préjudice a été causé. On doit prendre en considération le contexte professionnel et

---

[183] Richard B. LEVINE, *op. cit.*, note 26, p. 244.
[184] Philippe HELIS et Philippe MOZAS, « Chronique multimédia », (1998) 89 *Petites affiches* 18.
[185] André NADEAU, *op. cit.*, note 179, p. 46.
[186] Cheryl S. MASSINGALE et A. FAYE BORTHICK, « Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services », (1990) 12 *W. New Eng. L. Rev.* 167, 178.
[187] Pierre TRUDEL, « La responsabilité civile : qui répond de l'information », dans *L'espace cybernétique n'est pas une terre sans loi : Études des questions relatives à la responsabilité à l'égard du contenu circulant sur Internet*, Ottawa, Industrie Canada, p. 135, à la page 195.

social de l'individu concerné[188]. Ainsi, dans le cadre de la transmission de virus informatiques, le comportement d'un novice ne sera pas regardé du même œil que celui d'un usager habitué, d'un programmeur ou d'un créateur de logiciels[189]. Dans la même veine, un acte présumé fautif ne le sera pas forcément dans tous les cas. Par exemple, si le maliciel est transmis accidentellement lors d'une urgence (par exemple durant une vidéoconférence entre médecins lors d'une télé-opération) il sera plus difficile de reprocher à l'individu de ne pas avoir pris toutes les précautions nécessaires que si le virus est transmis par une personne lors du téléchargement d'un jeux vidéo piraté[190].

La question à se poser devient donc : « *what are the definitive responsibilities of computer center employees or persons having access to software and information to the public they serve* [...] *in creating an 'environment of security' and in practicing solid ethical standards in regard to the valuable data they use when performing their jobs?* »[191]. Cette interrogation nous pousse maintenant à observer les caractéristiques associées à l'utilisateur d'ordinateur normalement prudent et prévoyant tel que défini par la jurisprudence.

b) L'utilisateur d'ordinateur normalement prudent et prévoyant selon la jurisprudence : L'affaire *T.J. Hopper* c. *Northern Barge*[192].

Comme nous l'avons déjà suggéré, une personne peut être tenue responsable de ne pas avoir mis en œuvre des mesures de sécurité raisonnables et de ne pas avoir veillé à leur respect[193]. En effet, le fait de

---

[188] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 113-114.
[189] Richard B. LEVINE, *op. cit.*, note 26, p. 251.
[190] *Id.*
[191] Karen A. FORCHT, « Ethical Use of Computers », dans L.J. HOFFMAN (éd.), *Rogue Programs: Viruses, Worms, and Trojan Horses*, New York, Van Nostrand Reinhold, 1990, p. 117, à la page 117.
[192] 60 F. 2d 737 (2nd Cir. C.A., 1932).
[193] Brian R. BAWDEN, « Les dix commandements de l'informatisation », (1993) *CA Magasine* 34, 37.

ne pas recourir à une forme de technologie quelconque pour prévenir un dommage peut être considéré comme de la négligence[194]. Cependant, dans un domaine aussi récent que la protection contre les virus informatiques, il peut s'avérer difficile d'établir ce qui constitue des « mesures de sécurité raisonnables » :

> « *there is no way to insure that testing will reveal the presence of a virus. Therefore, the issue becomes how much testing and inspection is enough testing and inspection, such that there can be no finding of negligence* »[195].

Selon un sondage effectué aux États-Unis, environ quatre-vingt-dix pour cent (90%) des entreprises consultées utilisent un logiciel antivirus pour la protection de leur système et quatre-vingt-quatre pour cent (84%) ont également recours à cette technologie pour protéger leurs serveurs de courrier électronique. Finalement, environ cinquante pour cent (50%) des entreprises utilisaient un logiciel coupe-feu[196] et quarante-cinq pour cent (45%) possédaient des antivirus pour leurs serveurs proxy[197]. Il ressort de ces statistiques que la personne raisonnable devrait avoir recours à un logiciel anti-virus pour protéger son système et son serveur courriel. Quant à l'utilisation des autres technologies, il s'avère que celle-ci ne pourrait probablement pas être « raisonnablement exigée » selon la coutume.

Cependant, l'usage ne constitue pas toujours un standard de décision approprié puisqu'il n'enregistre que les préférences des parties

---

[194] *Id.* 35.
[195] Vicky H. ROBBINS, *loc. cit.*, note 44, 26.
[196] Un autre sondage fixe ce taux à 60%. Voir CONSUMERS UNION of U.S., INC., « Cyberspace Invaders », (2002) en ligne sur le site *ConsumerReports.org* : <http://www.consumerreports.org/main/detailv2.jsp?CONTENT%3C%3Ecnt_id=159611&FOLDER%3C%3Efolder_id=18151&bmUID=1038263919040> (dernière mise à jour : juin 2002)
[197] « Persistant Viruses Sound Industry Alarm », (2001) en ligne sur le site *ArmourPlate* : <http://www.armourplate.com/news/015.htm> (dernière mise à jour : 14 août 2001).

l'adoptant et non celles des victimes de son application[198]. Ainsi, si la coutume doit être prise en considération lors de telles décisions, son poids doit demeurer minime[199]. C'est d'ailleurs ce qui fut établi par la Cour suprême dans l'arrêt *Roberge* c. *Bolduc*[200] et par le juge Learned Hand dans l'arrêt américain *T.J. Hopper* c. *Northern Barge*[201] :

> *« Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.* [...] *But here there was no custom at all as to receiving sets; some had them, some did not; the most that can be urged is that they had not yet become general. Certainly in such a case we need not pause; when some have thought a device necessary, at least we may say that they were right, and the others too slack* ».

Dans cette affaire, le capitaine d'un navire a été tenu responsable pour la perte de sa cargaison suite à une tempête parce qu'il avait fait preuve de négligence en n'écoutant pas les prévisions météorologiques alors qu'il était en haute mer et ce, malgré le fait qu'il n'était ni obligatoire, ni même habituel de retrouver des appareils radiophoniques sur les navires à cette époque. Il fut ainsi jugé qu'une entreprise pouvait être tenue civilement responsable de ne pas s'être procuré la technologie de pointe disponible alors que cette même technologie aurait pu empêcher

---

[198] Richard A EPSTEIN, « The Path to the *T.J. Hopper*: The Theory and History of Custom in the Law of Tort » (1992) 21 *Journal of Legal* Studies 1, 5.

[199] *Id.*

[200] [1991] 1 R.C.S. 374. À la page 437 du jugement, la juge L'Heureux-Dubé explique que « [Le] *fait qu'un professionnel ait suivi la pratique de ses pairs peut constituer une forte preuve d'une conduite raisonnable et diligente, mais ce n'est pas déterminant* ».

[201] Précitée, note 192. Bien que cette affaire n'ait pas été citée par la jurisprudence québécoise, son application à notre droit semble appuyée par certains auteurs. Voir Pierre TRUDEL et al., *Droit du cyberespace*, Montréal, Éditions Thémis, 1997, p. 5-38.

un préjudice[202]. Il en découle que l'existence et la disponibilité d'une technologie quelconque peuvent avoir pour effet d'accroître la responsabilité d'une personne[203]. Cette décision a, par la suite, donné naissance au principe doctrinal suivant :

> « *The failure to rapidly adopt generally recognized benefits that may accrue from use of the computer may also result in liability on the basis of fault, possibly even where negligence cannot be shown directly. The question is whether the failure of a business to use a computer may result in liability if it can be shown that harm might have been avoided by use of that computer... a party that fails to make use of available and accepted technology may find itself held liable on the theory that such a failure breaches the obligation (duty) to exercise reasonable care* »[204].

Ainsi, l'obligation d'adopter une solution technologique existe si « *la technologie a un effet positif sur l'équilibre entre la probabilité et la gravité du préjudice d'une part, et le fardeau de la solution d'autre part* »[205]. On pourrait donc être trouvé coupable lorsque l'on néglige d'adopter des outils perfectionnés mettant à profit de nouvelles technologies raisonnablement accessibles[206].

Cependant, l'adoption de technologies n'est pas suffisante, encore faut-il s'en servir, sans quoi il sera également possible d'engager notre responsabilité[207]. Ainsi, comme l'explique Brian R. Bawden, « *si le propriétaire d'un système informatique opérationnel avait pu éviter de*

---

[202] Bien que ce raisonnement n'ai pas été endoctriné par les tribunaux québécois, la juge L'Heureux-Dubé, Dans l'arrêt *Hydro-Québec* c. *Girard* ([1987] R.R.A. 80), concède la possibilité de l'application d'une telle doctrine : « Même en admettant que l'appelante ait été en faute pour ne pas avoir installé le dispositif le plus parfait qui soit sur son réseau électrique afin d'éviter toute possibilité d'accident [...] ».

[203] Brian R. BAWDEN, *loc. cit.*, note 193, 35.

[204] Monique C. M. LEAHY, « Liability for Mishandled Computer Information », (2001) 18 *J. Marshall J. Computer & Info. L.* 1019, § 6.

[205] Brian R. BAWDEN, *loc. cit.*, note 193, 35.

[206] *Id.*

[207] George S. TAKACH, *op. cit.*, note 31, p. 303. Voir aussi *Chute* v. *Bank One of Akron*, N.A., 460 N.E.2d 720 (Ohio App. 1983).

causer un préjudice en utilisant l'ensemble des fonctions disponibles de son système, il pourrait être trouvé coupable de négligence pour avoir fait défaut d'exploiter pleinement le système »[208].

Ces considérations ont menées à un test en cinq étapes pouvant établir le degré de négligence d'un comportement dans le contexte de la sécurité informatique :

1. La technologie est-elle disponible?
2. L'entreprise en question peut-elle raisonnablement se permettre d'acquérir cette technologie?
3. Cette technologie est-elle déjà utilisée, même de façon minimale, dans le domaine de l'entreprise?
4. Les mesures de sécurité sont-elles à ce point essentielles qu'elles nécessitent l'utilisation de cette technologie?
5. L'absence de technologie est-elle la cause directe du préjudice?[209]

L'individu pouvant répondre par la négative à l'une de ces questions verra fort probablement sa responsabilité diminuer.

On peut donc établir que – pour déterminer si un individu peut être trouvé coupable de négligence pour ne pas avoir suivi l'évolution de la technologie – il faut chercher à savoir si une technologie supérieure et fiable était raisonnablement accessible et si le fournisseur du service connaissait ou aurait dû connaître cette technologie[210]. Dans le cas de la transmission de virus informatiques, « *the inquiry will be into the degree of sophistication of the malignant program and the availability of preventative measures that could have been taken to detect the presence of the destructive code and prevent it from actually causing*

---

[208] Brian R. BAWDEN, *loc. cit.*, note 193, 38.
[209] Monique C. M. LEAHY, *loc. cit.*, note 204.
[210] Brian R. BAWDEN, *loc. cit.*, note 193, 35.

damage »[211]. Il nous reste donc à définir la notion de technologie « raisonnablement accessible ».

c) Le calcul économique de la négligence

Comme nous l'avons déjà abordé, les critères dans l'évaluation de la diligence seront la probabilité du préjudice, la gravité des dommages prévisibles et le fardeau des mesures de protection adéquates[212]. En effet, il est souvent avancé que l'on peut évaluer la négligence en établissant si l'auteur du préjudice a pris toutes les précautions dont les coûts étaient justifiés par le risque de dommage[213] :

> « *Si la gravité des dommages prévisibles est faible, ou si les frais associés à la mise en place des précautions sont hors de proportion par rapport au risque et à la gravité du préjudice, il peut ne pas exister d'obligation ; en revanche, si la probabilité et la gravité du préjudice sont relativement élevées et que les frais associés à la mise en place des mesures sont faibles, il pourrait exister une obligation* »[214].

L'énoncé ci-haut découle d'un test mis de l'avant par le juge Learned Hand en 1947 pour concrétiser le concept de négligence en droit américain[215]. Selon lui, trois considérations étaient pertinentes pour constituer un acte négligent : la probabilité d'un événement

---

[211] Richard B. LEVINE, *op. cit.*, note 26, p. 251.

[212] Pierre TRUDEL et al., *op. cit.*, note 201, p. 5-38 et Brian R. BAWDEN, *loc. cit.*, note 193, 35. En effet, comme l'explique Ejan Mackaay : « *Si des moyens de prévention du risque en question sont connus, il faut déterminer s'il convient de les adopter. La réponse est affirmative pour tous les moyens de précaution dont le coût est inférieur à la réduction du coût du risque qu'ils permettent de réaliser. Il s'agit là du « calcul préventif » qui est à la base de la responsabilité pour faute* ». Ejan MACKAAY, *L'analyse économique du droit : I – Fondements*, Montréal, Thémis, 2000, p. 173.

[213] Richard A. EPSTEIN, *loc. cit.*, note 198, 1.

[214] Brian R. BAWDEN, *loc. cit.*, note 193, 35. Voir aussi Pierre TRUDEL et al., *op. cit.*, note 201, p. 5-38 et Cheryl S. MASSINGALE et A. FAYE BORTHICK, *loc. cit.*, note 186, 179.

[215] *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947). Les principes mis de l'avant par cette decision ont depuis trouvé application en droit canadien. Voir Allen M. LINDEN et Lewis N. KLAR, *Canadian Tort Law: Cases, Notes & Materials*, 11e éd., Toronto, Butterworths, 1999, p. 166.

dommageable (P); la gravité du préjudice qui en résulterait, le cas échéant (L); et le fardeau de précautions adéquates pour le prévenir (B). Ainsi, l'individu responsable de l'événement dommageable était négligent, selon le juge Hand, si le fardeau des précautions (B) était moins lourd que le produit de la probabilité de l'événement dommageable et du préjudice en résultant (PL), c'est-à-dire si B<PL.[216] Comme l'explique Ejan Mackaay :

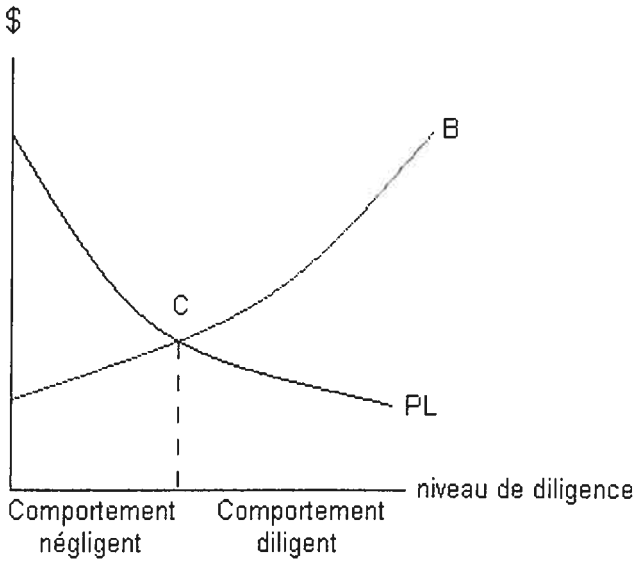
> « *La schématisation de la décision, même intuitive, fait ressortir une considération essentielle. C'est le coût du préjudice appréhendé ou de l'accident qui détermine dans quelle mesure se justifient les mesures de précaution. Vous adoptez toutes les mesures de précaution dont le coût est inférieur aux économies - même entièrement intuitives - que vous comptez ainsi réaliser* »[217].

Schématiquement, le modèle se représente comme suit, où tout individu se retrouvant à la gauche de C est négligent, puisque B est plus petit que PL[218] :

---

[216] Ejan MACKAAY, *op. cit.*, note 157, p. 15. Voir aussi William M. LANDES et Richard A. POSNER, *The Economic Structure of Tort Law*, Cambridge, Harvard University Press, 1987, p. 85.
[217] Ejan MACKAAY, *op. cit.*, note 157, p. 10.
[218] Richard POSNER, *Economic Analysis of Law*, 5e éd., New York, Aspen Law and Business, 1998, p. 181.

Figure 1 : Graphique d'évaluation d'un comportement négligent



Dans le cas des maliciels, les dépenses associées à l'achat de logiciels antiviraux peuvent également être déterminées à l'aide de la formule du juge Hand[219]. Comme l'explique Meiring de Villier :

> « *Scanners, for instance, come in a variety of degrees of sophistication (and cost), ranging from basic systems that detect only known strains, to heuristic artificial intelligence-based systems capable of detecting polymorphic viruses and even unknown strains. The optimal Learned Hand level of investment in scanning technology would be determined by balancing the cost of acquiring and operating the technology against the expected harm avoided* »[220].

En effet, nous pouvons maintenant constater qu'il existe un risqué élevé de dommages causés par une infection virale, alors que la prévention, soit par la programmation, soit par l'achat d'un logiciel antivirus, s'avère être une option efficace[221] et, dans bien des cas, moins dispendieuse[222].

---

[219] Meiring De VILLIERS, « Virus Ex Machina Res Ipsa Loquitur », (2002) non publié, 32.

[220] *Id.*

[221] Comme l'explique Gérard Mannig, « *les protections antivirus résidentes permettent toute manipulation de fichiers avec un bon taux de détection. Des lors, tout envoi de virus, manuel ou automatique sera immédiatement repéré par cette protection et le mécanisme de contamination déjoué. Enfin, un pare-feu personnel anti-virus (personal*

Ainsi, l'individu désirant poursuivre un tiers pour une infection causée par un maliciel devra établir la négligence de ce dernier en prouvant que la technologie antivirale était disponible au moment de l'infection, que celle-ci était fiable et que son coût relatif par rapport aux préjudices potentiels était justifié[223]. Il est présentement possible d'obtenir une licence pour les produits antiviraux des entreprises McAfee et Symantec pour aussi peu que 50 $ (U.S.)[224]. Bien qu'aucun logiciel ne puisse garantir la détection de tous les virus qui seront créés[225], la technologie heuristique actuelle utilisée par ces deux entreprises permet la détection de 70 à 80% des nouvelles créations virales[226]. En considérant que, selon un sondage effectué conjointement par le *Federal Bureau of Investigation* américain (FBI) et le *Computer Security Institute* (CSI), les pertes associées aux infections virales s'élèvent en moyenne à 283 000 $ (U.S.)[227] par entreprise par an et que les risques d'infection sont de 94%[228], il s'avère difficile à nos yeux de contester une poursuite pour cause de négligence si l'on omet de se procurer un tel logiciel. Pour reprendre la formule mathématique du juge Hand :

---

firewall) interdira de la même manière toute connexion sur le Net de programmes non validés par l'utilisateur, validation qui peut être opérée préalablement ou sur l'instant ». Gérard MANNIG, propos transmis à la liste de discussion droit-net@cru.fr le 25 août 2002.

[222] Robbin A. BROOKS, « Deterring the Spread of Viruses Online : Can Tort Law Tighten the 'Net'? », (1998) 17 *Rev. Litig.* 343, 361.

[223] Monique C. M. LEAHY, *loc. cit.*, note 204, § 6.

[224] Voir les sites respectifs des deux entreprises : <www.mcafee.com> et <www.symantec.com>.

[225] Carey NACHENBERG, *loc. cit.*, note 21, 6.

[226] *Id.*, 7.

[227] Ce sondage a été sélectionné selon la renommée des organismes impliqués dans la récolte des données mais, comme le souligne Sascha Segan, « [h]*ow much damage viruses cause depends on whom you ask* ». Ces chiffres peuvent donc varier d'un sondeur à l'autre mais demeurent très élevés quelle que soit la source consultée. Sascha SEAGAN, *loc. cit.* note 40, 55.

[228] Richard POWER, « 2002 CSI/FBI Computer Crime and Security Survey », (2002) 8 *Computer Security Issues & Trends* 1, 15.

Figure 2 : Calcul de l'opportunité d'achat d'un logiciel antivirus

Si :

P (la probabilité d'un événement dommageable) = 0,94 (94 %)
L (la gravité du préjudice en découlant) = 283 000 $ par année
B (le fardeau de précautions adéquates pour le prévenir) = 50 $ par année

Donc :
LP = 0,94 x 283 000 $ = 266 020 $

Et

50 $ < 266 020 $

Ce qui implique qu'il serait négligent de ne pas adopter cette technologie.

Il s'agit ici d'un exemple caricatural, puisque le degré d'informatisation des entreprises sondées ne représente pas celui de la majorité des utilisateurs d'Internet, leurs risques de préjudice étant moins élevés étant donnée leur moins grande informatisation. Cette diminution des dommages probables justifierait le recours à une technologie de base, c'est-à-dire un logiciel acheté à 50$ au magasin d'informatique. Cependant il sera légitime de s'attendre à ce que ceux faisant affaires avec des entreprises dont l'actif est constitué en grande partie de données informatisées, ou encore avec une clientèle très vaste, investissent dans des technologies plus perfectionnées et dont le taux de réussite est plus élevé[229] tant et aussi longtemps que ces mesures coûtent moins de 266 020 $ selon les statistiques retenues. Quoique ces chiffres ne tiennent compte que d'un échantillonnage restreint, il n'en demeure pas moins que, comme l'explique Meiring de Villiers :

> « *The Learned Hand formula, applied to anti-virus precautions, therefore suggests that the high danger level of virus infection, the high (and rapidly increasing) prevalence of viruses, and the modest cost of anti-virus*

[229] Nous vous référons, à cette fin au titre 2. de la section I A du présent mémoire.

> *precautions, create a legal duty to implement sophisticated and effective anti-virus technology that is capable of avoiding a large proportion of all virus strains* »[230].

Le test du juge Hand peut également être utile quant à l'évaluation de la mise à jour des logiciels antiviraux[231]. En effet, l'installation d'un logiciel antivirus demeurera inefficace contre la protection des tiers si celui-ci n'est pas mis à jour périodiquement[232]. La proximité des mises à jour devra dépendre encore ici du risque de contamination. Celui ou celle qui n'utilise Internet qu'une ou deux fois par semaine court un risque de contamination moindre. Il est justifié pour cet individu de ne pas mettre son logiciel à jour de façon quotidienne. Selon les suggestions des experts, une mise à jour hebdomadaire devrait suffire afin de réduire le risque et donc les chances d'être tenu responsable pour sa propre négligence. Cependant, les utilisateurs avides du réseau devraient procéder à la mise à jour de leurs logiciels quotidiennement afin d'éviter tout reproche. Il en va de même pour les entreprises qui, rappelons-le, se doivent de recourir à une technologie de pointe dans le domaine de la sécurité[233], surtout lorsque le coût de cette technologie est négligeable voire nul[234] dans le cas des mises à jour de la majorité des logiciels concernés. Il importe cependant de souligner que les plus récentes versions des logiciels antiviraux comportent maintenant une fonctionnalité de mise à jour automatique dès que l'utilisateur se branche sur le réseau[235]. Ceci élimine donc la problématique reliée à la mise à jour manuelle de l'utilisateur.

Malgré son efficacité dans l'établissement de négligence, le test du juge Hand affiche la lacune de ne pas tenir compte d'un élément très

---

[230] Meiring De VILLIERS, *loc. cit.*, note 219, 51.
[231] « *The optimal frequency of viral database updating is determined similarly* », *Id.*, 32.
[232] CONSUMERS UNION of U.S., INC., *loc. cit.*, note 196.
[233] *T.J.Hopper* c. *Northern Barge*, précitée, note 192.
[234] *United States v. Carroll Towing Co.*, précitée, note 215.
[235] CONSUMERS UNION of U.S., INC., *loc. cit.*, note 196.

important de la responsabilité civile, à savoir la faute contributive de la victime[236]. En effet, « *la personne qui est tenue de réparer un préjudice ne répond pas de l'aggravation de ce préjudice que la victime pouvait éviter* »[237]. Si, dans la majorité des cas, cette lacune peut être corrigée en calculant la valeur marginale des précautions à prendre (c'est-à-dire la valeur des précautions à prendre en calculant celles que devrait prendre une victime potentielle)[238], ceci amène un nouveau problème dans le cas de virus informatiques. En effet, s'il est vrai qu'une victime potentielle peut parfois réduire ses risques de préjudice à moindre coût que l'auteur dudit préjudice (par exemple en portant un casque à vélo), le coût du logiciel antivirus est le même pour la victime que pour l'auteur du préjudice[239]. Nous avançons donc que c'est à la personne ayant causé le préjudice et non à la victime de débourser pour le logiciel en question[240].

À la lumière de ces observations, nous soumettons que la personne responsable de l'infection du système informatique d'un tiers est également responsable des dommages causés si ceux-ci sont le fruit de sa propre négligence, c'est-à-dire si elle n'a pas pris les mesures nécessaires pour empêcher la diffusion dudit virus, soit, à tout le moins, l'achat d'un logiciel antivirus[241]. Découle de cette position le fait que cette personne ne pourra être tenue responsable d'infections causées par des virus ne pouvant être détectés par une personne raisonnable,

---

[236] William M. LANDES et Richard A. POSNER, *op. cit.*, note 216, p.88-89.
[237] Art. 1479 C.c.Q.
[238] Voir William M. LANDES et Richard A. POSNER, *op. cit.*, note 216, p. 87.
[239] Quoique, comme nous l'avons déjà abordé, il existe une série de précautions que l'utilisateur consciencieux peut prendre pour éviter la perte de données due à une infection virale.
[240] Il est à noter, comme nous l'examinerons dans la section II C du présent ouvrage, que le modèle idéal verrait tout individu socialement contraint à posséder un logiciel antivirus. Quoi qu'il en soit, nous soumettons qu'une victime ne peut se faire reprocher de ne pas avoir pris les précautions qui auraient dû être prises par l'auteur du préjudice.
[241] Michael L. RUSTAD, « Private Enforcement of Cybercrime on the Electronic Frontier », (2001) 11 *S. Cal. Interdisc. L.J.* 63, 114.

puisque, comme nous l'avons déjà souligné, il demeure impossible de déceler toute nouvelle forme de contamination informatique[242].

2. le dommage

Comme l'expriment Jean-Louis Baudouin et Patrice Deslauriers, « *un comportement fautif ne suffit pas, en soi, à engager la responsabilité civile s'il ne se matérialise pas dans un préjudice causé à autrui* »[243]. En effet, il faut démontrer la présence d'un dommage pour qu'il y ait responsabilité[244], principe consacré par l'exigence d'une atteinte à *un intérêt légitime juridiquement protégé*[245], c'est-à-dire la violation d'un droit[246]. Comme l'explique Justin Thorens, le dommage peut être défini comme étant la différence existant entre le patrimoine d'une personne avant et après l'acte dommageable[247].

L'auteur du dommage même involontaire se voit donc contraint à indemniser la victime[248], c'est-à-dire rétablir le manque causé à son patrimoine. Cette indemnisation consiste normalement en une exécution par équivalent, soit sous forme monétaire « *représentant la traduction pécuniaire du préjudice subi* »[249].

Pour les victimes d'attaques virales, les formes de dommages peuvent inclure la perte de temps associée au ralentissement du système[250], le

---

[242] Philip FITES et al., *op. cit.*, note 24, p. 142. Comme l'explique Meiring de Villier : « *An example of an unavoidable virus is an unknown, complex strain that could only be detected and eliminated at unreasonably high cost, e.g. through expensive and sophisticated scanning techniques based on artificial intelligence technology* ». Meiring De VILLIERS, *loc. cit.*, note 219, 30.
[243] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 57
[244] Ejan MACKAAY, *op. cit.*, note 157, p. 21.
[245] Jean CARBONNIER, *op. cit.*, note 178, p. 353.
[246] Justin THORENS, *Le dommage causé à un tiers*, Genève, Imprimerie Henri Studer S.A., 1962, p. 12.
[247] *Id.*, p. 26.
[248] André TUNC, *op. cit.*, note 149, p. 55.
[249] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 155.
[250] Comme l'expliquent David Harley et al. : « *Nearly all viruses entail damage in this category* [incidental damage]*, since their presence involves loss of performance due to*

coût de sa remise en marche[251] (élimination du virus et réinstallation des logiciels infectés), le salaire des techniciens engagés pour effectuer les réparations nécessaires[252], les coûts associés à l'implantation de nouvelles mesures de sécurité[253], sans compter les pertes de clientèle et de profits[254] associées à la chute de confiance du public en ses politiques de sécurité. Bref, pour une entreprise dont le réseau est rendu momentanément inutilisable par l'infiltration d'un virus, le ralentissement des activités économiques de celles-ci, soit le « bénéfice d'exploitation manqué »[255], peut s'avérer une méthode efficace pour quantifier le préjudice subi.

Dans certains cas qui, pour l'instant, s'avèrent plutôt rares, quelques virus tels CIH (mieux connu sous le nom de *Chernobyl*) peuvent rendre bon nombre des composantes informatiques inutilisables en effaçant les micrologiciels[256] les opérant[257], causant ainsi de lourdes pertes matérielles.

De plus, avec l'informatisation grandissante de la société et la propension vers l'interconnexité des différentes technologies, il n'est pas difficile d'imaginer un scénario où les dommages ne seront pas uniquement liés au contenu du réseau informatique infecté, mais

---

the theft of memory, disk space, clock cycles, system modification, or a combination of two or more of these ». David HARLEY et al., *op. cit.*, note 3, p. 7. Voir aussi Christiane FÉRAL-SCHUHL, *op. cit.*, note 1, p. 43.

[251] Clive GRINGRAS, *op. cit.*, note 15, p. 66.

[252] Sascha SEGAN, *loc. cit.*, note 40, 55.

[253] SUSAN C. LYMAN, *loc. cit.*, note 11, p. 628. Voir aussi Pamela SAMUELSON, « Can Hackers Be Sued for Damages Caused by Computer Viruses? », dans Peter J. Denning (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990,, p.472, à la page 472.

[254] Clive GRINGRAS, *op. cit.*, note 15, p. 66.

[255] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 211. Le juge Baudouin renvoi à une série de jurisprudences pour appuyer cette position dont *Canadien Pacifique ltée* c. *Henri Inc.*, [1977] C.S. 890.

[256] Les micrologiciels sont un « [e]*nsemble ordonné d'instructions et de données stockées d'une façon qui est fonctionnellement indépendante de la mémoire centrale* ». OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.

[257] ANONYME, *op. cit.*, note 20, p. 324. Voir également Roger A. GRIMES, *op. cit.*, note 35, p. 422 et Martin P.J. KRANTZ et Cruickshank PHILLIPS, « *Legal Vaccines for computer viruses* », (1988) 5 *Canadian Computer Law Reporter* 69, 69.

également aux mauvais fonctionnement des systèmes opérationnels sophistiqués dont il assure la gestion tel la tour de contrôle d'un aéroport[258] ou le bloc opératoire d'un hôpital[259].

Cependant, qu'en est-il de la perte de données due à une attaque virale? La perte ou la modification de données s'avère souvent être la conséquence la plus directe et la plus préjudiciable de toute infection virale[260]. Or, quoiqu'une certaine doctrine soumette que la suppression ou la modification de données devrait être suffisante pour constituer un dommage en soi[261], certains jugements américains n'ont pas considéré l'information contenue dans les fichiers informatiques comme étant une forme de propriété légalement protégée[262]. Comme l'explique un auteur :

> « *it is initially necessary to establish that altering the orientation of magnetic particles, how programs and data are stored, is damage to property.* [...] *To damage a program or data* [...] *is not to cause any physical damage in the way in which it is normally considered: all that is occurring is that the magnetic particles are being altered* »[263].

Les dommages n'étant pas « physiques », puisque le médium n'est pas altéré, il ne s'agirait donc pas de dommages. Heureusement, cette tendance semble aujourd'hui s'estomper[264], mais il n'en demeure pas moins que la qualification juridique des données n'est pas encore établie aux États-Unis. En Angleterre, c'est la position doctrinale énoncée ci-haut qui nous apparaît être mise de l'avant par les tribunaux. Dans

---

[258] C'est ce qu'a fait un jeune pirate informatique du Massachusetts en 1998. Voir Michael L. RUSTAD, *loc. cit.*, note 241, 78.
[259] Cet exploit a déjà été accompli par un groupe de pirates informatiques portant le nom de « *Milwaukee Microkids* ». Voir Anne W. BRANSCOMB, *op. cit.*, note 25, p. 29.
[260] Steve R. WHITE et al., *op. cit.*, note 22, p. 7.
[261] Stephen SAXBY, *Encyclopedia of information technology law*, London, Sweet & Maxwell, 2000, p. 7026. Voir aussi SUSAN C. LYMAN, *loc. cit.*, note 11, p. 628 et Pamela SAMUELSON, *op. cit.*, note 253, p. 472.
[262] Robin A. BROOKS, *loc. cit.*, note 222, 357.
[263] Clive GRINGRAS, *op. cit.*, note 15, p. 66 et 67.
[264] Voir, entre autres, le affaires CompuServe Inc. v. Cyber Promotions, Inc., 1997 WL 109303 (S.D. Ohio Feb. 3, 1997) et Thrifty Tel, Inc. v. Bezeneck, 46 Cal. App. 4th 1559 (1996).

l'affaire *R.* c. *Whiteley*[265], le juge en chef de la Cour d'appel précise, quant à l'applicabilité du *Criminal Damage Act* aux données informatiques :

> « *What the Act required to be proved was that tangible property had been damaged, not necessarily that the damage itself should be tangible. There could be no doubt that the magnetic particles on the metal discs were a part of the discs and if the appellant was proved to have intentionally and without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disc to the owner, there would be damage within the meaning of section 1. The fact that the alteration could only be perceived by operating the computer did not make the alterations any the less real, or the damage, if the alteration amounted to damage, any the less within the ambit of the Act* »[266].

Cette position est également adoptée par le législateur ontarien qui définit les programmes informatiques comme étant des biens meubles corporels[267]. Bien qu'aucune disposition semblable n'existe au Québec, nous soumettons que les tribunaux québécois devraient suivre les positions ontarienne et anglaise, sans nécessairement considérer tangibles les informations contenues sur les supports informatiques, puisque la perte de telles données ne peut être que préjudiciable pour les personnes affectées et ce, malgré l'absence d'altération du support sur lequel ces informations se trouvent. Cette position concorde d'autant plus avec le rôle important que le législateur semble présentement accorder à l'information numérisée[268].

---

[265] (1991) 93 Cr App Rep 25.
[266] *R.* v. *Whiteley*, précitée, à la page 29.
[267] *Loi sur la taxe de vente au détail*, L.R.O. 1990, chap. R.31, art 1. Il faut cependant noter que les lois fiscales ont souvent tendance à donner un sens très large aux termes employés.
[268] En effet, l'adoption de la *Loi concernant le cadre juridique des technologies de l'information* (L.Q. 2000, c. 32) démontre l'intention claire d'accorder plus d'importance aux documents électroniques. Soumettre que la destruction de ces documents ne mène pas à la responsabilité civile de l'initiateur de l'acte s'avère contraire à cette intention.

Quoiqu'il en soit, il peut s'avérer assez contraignant pour la victime d'un virus d'établir le contenu de son système avant l'infection – donc la portée des dommages subis – sans avoir de copies de secours des fichiers s'y trouvant. Si tel est le cas, le dommage est minime, voire nul, puisqu'il n'y a eu aucune perte d'information. Ce cercle vicieux peut ainsi constituer un obstacle considérable pour les victimes, sans compter qu'il s'avère difficile de donner une valeur monnayable à des documents personnels. Cependant, il importe de souligner que cette problématique n'est pas propre aux infections virales puisque le bris mécanique des composantes mnémoniques d'un ordinateur, ou encore la destruction de l'ordinateur suite à un incendie, aura le même effet. Il revient alors à la victime de tenter de prouver l'existence et la valeur de l'information qu'elle prétend avoir perdu suite à l'infection selon les dispositions du *Code civile*.

Une autre problématique pouvant se présenter pour la victime désirant imputer un dommage à un tiers réside dans le fait que ce dommage doit avoir été la conséquence « logique, directe et immédiate » de la faute[269]. Cependant, « *a program infected by a computer virus does not usually execute the ultimate function of the virus immediately* »[270]. Cette exigence pose également problème dans le cas des bombes logiques, qui, rappelons-le, ne s'exécutent pas instantanément, mais attendent un moment précis (le vendredi 13 ou le premier avril) pour agir. Ce moment peut donc arriver plusieurs semaines, voire plusieurs mois après la transmission du maliciel. Comme le précise un auteur :

> « *When a hacker infiltrates a computer system with a "time bomb," this will present a different legal problem. Did the harmful act occur when the hacker first breached the computer's security, when the virus became active, or when the effect was first realized? One author suggests the courts resolve this question by analogy to*

[269] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 349.
[270] SUSAN C. LYMAN, *loc. cit.*, note 11, p. 626.

> *professional malpractice negligence. The statute of limitations in many states does not begin to run in malpractice actions until the "time of discovery"* »[271].

Cette notion de « *time of discovery* » existe également en droit québécois. En effet, l'article 2926 C.c.Q. précise que « [l]*orsque le droit d'action résulte d'un préjudice moral, corporel ou matériel qui se manifeste graduellement ou tardivement, le délai court à compter du jour où il se manifeste pour la première fois* ». Comme le soulignent Pauline Lesage-Jarjoura et Suzanne Philips-Nootens, cette disposition s'explique par le fait qu'on « *ne peut exiger d'une victime qu'elle prenne un recours avant même de savoir qu'elle est atteinte, et qu'elle en connaisse la cause* »[272].

3. Le lien de causalité

Comme l'explique un auteur, « *The more extensive and expensive the damage is, the more appealing (at the least initially) will be the prospect of a lawsuit to seek compensation for the losses incurred* »[273]. Cependant, encore faut-il que ce dommage soit directement relié au comportement négligent de la personne poursuivie.

En effet, « [l]*orsqu'une faute a été commise et que la victime se plaint d'un préjudice, elle doit établir la relation directe existant entre les deux* »[274]. C'est donc dire que la faute « *doit avoir été la cause directe du dommage, ou le dommage l'effet immédiat d'une conduite jugée fautive* »[275]. Ainsi, ce ne sont pas tous les individus ayant, de près ou de loin, participé à la réalisation du dommage qui seront considérés

---

[271] Cheryl S. MASSINGALE et A. FAYE BORTHICK, *loc. cit.*, note 186, 186.
[272] Pauline LESAGE-JARJOURA et Suzanne PHILIPS-NOOTENS, *Éléments de responsabilité civile médicale : Le droit dans le quotidien de la médecine*, 2e éd., Cowansville, Éditions Yvon Blais, 2001, p. 81-82.
[273] Pamela SAMUELSON, *op. cit.*, note 253, p.472.
[274] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 341.
[275] *Id.*, p. 57.

responsables du préjudice, mais seulement ceux ayant rendu « *objectivement possible* » la réalisation de celui-ci[276]. Comme l'expliquent Jean-Louis Baudouin et Patrice Deslauriers :

> « *Le caractère direct de ce lien est apprécié, avant tout, par l'examen de la situation de fait, au cours duquel le juge est amené à peser l'influence respective de tous les événements et circonstances ayant entouré l'accident. Pour lui permettre de se faire une opinion, trois éléments principaux entrent en général en ligne de compte soit conjointement, soit alternativement. D'abord, la possibilité objective de la création du préjudice; ensuite, la prévisibilité raisonnable de celle-ci et enfin la situation dans le temps des divers facteurs à caractère causal* »[277].

Si, suite à cette évaluation un individu est considéré avoir contribué directement à la réalisation du préjudice, « *la jurisprudence applique alors la même règle que pour la faute commune en faveur de la victime*[278]*, et lui permet de réclamer la totalité du préjudice subi de l'un et l'autre des « coauteurs »* »[279].

Concernant l'appréciation à faire du lien plus ou moins direct entre l'infection d'un individu et la faute d'un tiers, Clive Gringras a tenté d'établir une distinction entre ce qu'il qualifie de « dommage primaire » et de « dommage secondaire »[280]. Pour résumer sa position, dont plusieurs éléments sont tirés de la théorie de la causalité immédiate[281], monsieur Gringras explique que la responsabilité d'un tiers n'ayant pas infecté directement la victime (dommage secondaire) sera moindre que celle de celui ayant directement introduit le virus dans son système

---

[276] *Id.*, p. 353.
[277] *Id.*, p. 358.
[278] Article 1478 al. 1er C.c.Q.
[279] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 368.
[280] Clive GRINGRAS, *op. cit.*, note 15, pp. 60 et suivantes.
[281] « *Cette théorie* [...]*retient parmi toutes les causes adéquates l'événement qui s'est produit le dernier dans le temps et qui, à lui seul, a pu suffire objectivement à produire la totalité du dommage* ». Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 346.

(dommage primaire), « *because the law tends to avoid opening the 'floodgates' to too many similar claims* »[282]. Ainsi, comme le soulignent Cheryl S. Massingale et A. Faye Borthick :

> « *The manager of a computer system would have a duty to use reasonable care to secure the system when it is reasonably foreseeable that failure to secure it would result in injury to others. While "others" encompasses a potentially unlimited group, there are limits on how far liability would extend. A duty of care runs only to "foreseeable plaintiffs," any person or class of persons who could reasonably be expected to be injured by the systems manager's negligence* »[283].

Toutefois, la nature même des virus étant de se reproduire exponentiellement, « [i]*t may therefore be alleged that the controller of an infected system is in a sufficient proximate relationship with the owner of* any *equipment which becomes infected by the virus emanating from his system* »[284]. Cette réflexion s'agence d'ailleurs parfaitement avec la recherche, par les tribunaux québécois, des seuls faits rendant objectivement possible la création du préjudice et dont les conséquences étaient normalement prévisibles pour l'agent[285].

Cependant, même s'il est possible d'établir clairement qui a contribué directement à la transmission d'un virus, encore faut-il en faire la preuve ce qui, comme nous le verrons maintenant, peut s'avérer beaucoup plus complexe qu'il n'apparaît au premier abord.

---

[282] Clive GRINGRAS, *op. cit.*, note 15, p. 63.
[283] Cheryl S. MASSINGALE et A. FAYE BORTHICK, *loc. cit.*, note 186, 177.
[284] Clive GRINGRAS, *op. cit.*, note 15, pp. 60 et 61.
[285] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 354. Voir l'arrêt *Deguire Avenue Ltd.* c. *Adler*, [1963] B.R. 101.

a) La composition tripartite des systèmes informatiques et son influence sur l'établissement du lien de causalité

Comme nous l'avons vu, il nous faut établir un lien de causalité entre le virus et les problèmes reliés à notre système informatique pour pouvoir entraîner la responsabilité civile d'un tiers ayant participé à la transmission dudit virus. Afin de comprendre la complexité de l'établissement d'une quelconque responsabilité dans le présent contexte, il importe d'examiner la nature même des systèmes informatiques[286].

Comme l'explique Daniel J. Hanson, un système informatique consiste en l'interaction de trois éléments distincts, à savoir les logiciels, les supports matériaux et les utilisateurs. Chacun de ces éléments possède des failles et certaines faiblesses et le mauvais fonctionnement ou l'erreur de l'un de ces éléments est suffisant pour causer un préjudice[287]. Dans le cas d'un mauvais fonctionnement du système, il est donc souvent difficile d'établir objectivement lequel de ces trois éléments est à la source du problème[288]. Ceci implique qu'il devient ardu d'établir la négligence d'un tiers, puisque l'on ne peut confirmer que le préjudice subi découle directement de l'acte fautif[289]. D'autant plus que, comme chaque système informatique comporte des composantes différentes, le mauvais fonctionnement de l'un ne sera pas toujours attribué à la même source que le mauvais fonctionnement de l'autre[290]. Par conséquent, la victime d'un problème informatique peut être incapable d'établir qu'un quelconque maliciel fut « la cause directe du dommage » et qu'il ne s'agissait pas simplement d'une mauvaise gestion du système[291] :

---

[286] Daniel J. HANSON, « Easing Plaintiff's Burden of Proving Negligence for Computer Malfunction », (1983) 69 *Iowa L. Rev.* 241, 242-243.
[287] *Id.*
[288] *Id.*
[289] Cheryl S. MASSINGALE et A. FAYE BORTHICK, *loc. cit.*, note 186, 178. Voir aussi Daniel J. HANSON, *loc. cit.*, note 286, 259.
[290] Daniel J. HANSON, *loc. cit.*, note 286, 242-243.
[291] *Id.*, 241.

> « *The tripartite composition of the computer system clearly frustrates the search for the actual cause of malfunction. Yet, traditional negligence theory requires proof of the actual cause of an accident in order to establish that the malfunction and resulting damages were proximately caused by a breach of duty. Without proof of a specific act or omission that caused the injurious error, the plaintiff may face summary dismissal for lack of evidence* »[292]

Cependant, l'utilisateur ayant accès aux bons outils, c'est-à-dire un logiciel pouvant identifier la présence de virus sur son système et l'impact qu'ont eu ces derniers, peut clairement identifier si un quelconque maliciel est à la source de ses ennuis. Certains aspects uniques du code viral permettent, au même titre qu'une signature, l'identification de la source du problème si celui-ci est dû a un virus informatique. Ceci facilite donc la preuve du lien de causalité dans le cas d'une attaque virale et rend les possibilités d'erreur dans l'identification de l'élément responsable du préjudice pratiquement nulles[293]. Reste à établir sa source.

b) La multiplicité des sources possibles d'infection

David Roy et al. tiennent les propos suivants quant à l'identification de la source de l'infection d'une victime du SIDA :

> « *Prouver la véritable causalité* [de l'infection] *peut se révéler ardu, sinon impossible, puisque l'infection par le VIH peut aussi être transmise par l'échange d'aiguilles contaminées ou par transfusions sanguines. Le demandeur, qui doit se décharger du fardeau qui lui incombe de démontrer qu'il a contracté le SIDA par voie sexuelle, doit prouver que c'est bel et bien le défendeur qui lui a transmis la maladie. Si le demandeur a eu des relations sexuelles avec de nombreux partenaires, il lui sera peut-être difficile de prouver ce fait. En outre, la*

---

[292] *Id.*, 248-249.
[293] Meiring De VILLIERS, *loc. cit.*, note 219, 40.

> *période d'incubation pouvant durer de 6 mois à 4 ans, les arguments invoqués par le demandeur pourraient être peu convaincants* »[294].

Ce même raisonnement peut être appliqué aux virus informatiques, puisque, dans certains cas, il s'avère difficile d'établir quel défendeur nous a transmis le fichier infecté[295], d'autant plus que les utilisateurs choisissant d'éliminer immédiatement tout fichier infecté afin de limiter la propagation du virus sont nombreux. Ce comportement préventif a malheureusement la fâcheuse conséquence de détruire « *toute preuve matérielle susceptible d'étayer une action en justice* »[296].

De plus, pour reprendre l'exemple des bombes logiques cité ci-haut, la période de latence entre l'arrivée du maliciel dans notre système et son activation peut être significative[297]. En effet, il est possible que le Cheval de Troie ou le fichier utilisé pour transmettre ce logiciel ait depuis été effacé et, de ce fait, toute trace de l'historique du virus se soit volatilisée. De plus, si un logiciel anti-virus est incapable de déceler la présence d'un maliciel, soit parce que celui-ci est dormant[298] ou encore parce qu'il est trop récent, cela pourrait pousser l'utilisateur à en déduire que l'infection a eu lieu plus tardivement que ce qu'il en est réellement. Finalement, plus l'utilisateur télécharge de fichiers distincts, plus les sources possibles d'infection augmentent. Ceci s'avère encore plus problématique si l'ordinateur en question est connecté à un réseau privé où les fichiers sont partagés[299] et donc où les sources d'infections sont multipliées. Se pose alors la question suivante : Comment peut-on établir le lien de causalité lorsque deux courriels distincts nous sont

---

[294] David J. ROY et al., *op. cit.*, note 175, p. 68. Voir aussi Lorne E. ROZOVSKY et Fay A. ROZOVSKY, *AIDS and Canadian Law*, Toronto, Butterworths, 1992, p. 54.
[295] Lorne E. ROZOVSKY et Fay A. ROZOVSKY, *op. cit.*, note 294, p. 53.
[296] Gerard MANNIG, « Après SirCam », (2001) en ligne sur le site http://realites-virus.org/: <http://realites-virus.org/2001-08-16.html> (dernière mise à jour : 16 août 2001)
[297] Robbin A. BROOKS, *loc. cit.*, note 222, 377.
[298] *Id.*
[299] Mary L. BEYER, « A Lawyer's Primer in Feminist Theory and Tort », (1989) 38 *J. of Legal Educ.* 3, 23.

parvenus contenant des fichiers infectés par le même virus? Loin d'être hypothétique, cette situation s'est récemment produite dans le cas du virus SirCam qui a frappé certains internautes plusieurs fois dans la même semaine[300].

Lorsque le lien de causalité s'avère difficile à démontrer, non pas parce que l'on ne peut prouver la présence d'un acte fautif, mais bien parce que l'on ne peut identifier quel acte fautif est réellement à la source de notre préjudice, le législateur est venu établir une présomption de fait visant à engager la responsabilité de tous les auteurs potentiels du dommage[301] :

---

[300] Voir Bertrand SALVAS, « Foulard, virus (bis) et sécurité », (2001) 10 *Entracte* 7.

[301] Certains auteurs américains proposent l'utilisation de la doctrine *res ipsa loquitur* dans la détermination du lien de causalité entre le préjudice subit et la faute de tiers trasmetteurs de virus informatiques (Voir Meiring DE VILLIERS, *loc. cit.*, note 219). Comme l'explique la Cour suprême dans l'affaire *Fontaine* c. *Colombie-Britannique* ([1998] 1 R.C.S. 424), cette maxime est généralement traduite par l'expression « la chose parle d'elle-même » et représente une présomption de négligence lorsque la victime peut démontrer que : « *la chose qui a causé le dommage est uniquement sous la direction et le contrôle du défendeur* » et que « *les circonstances sont telles que l'accident ne se serait pas produit s'il n'y avait pas eu négligence* ». Cependant, une utilisation trop libérale de cette doctrine par les différents tribunaux de *common law* a poussé la Cour suprême à la déclarer obsolète : « *Étant donné que diverses tentatives d'appliquer la maxime res ipsa loquitur ont été plus déroutantes qu'utiles, le droit s'en portera mieux si la maxime est tenue pour périmée et n'est plus utilisée comme une notion distincte dans les actions pour négligence. Son utilisation avait été limitée aux cas où les faits permettaient de déduire la négligence et où on ne disposait d'aucune autre explication raisonnable de l'accident. Il est plus logique que le juge des faits traite de la preuve circonstancielle dont la maxime tentait de traiter, en la soupesant en fonction de la preuve directe, s'il en est, pour décider si le demandeur a établi, selon la prépondérance des probabilités, une preuve prima facie de la négligence du défendeur. Si une telle preuve est établie, le demandeur aura gain de cause à moins que le défendeur ne produise une preuve réfutant celle du demandeur* » (*Fontaine* c. *Colombie-Britannique* [1998] 1 R.C.S. 424. Voir également Peter BURNS, « *Res Ipsa Loquitur*: The Unlamented Demise of a Pleader's Shibboleth » (1999) 57 *The Advocate* 839.). Quoi qu'il en soit, « *la règle res ipsa loquitur n'est pas nécessaire en droit civil, puisque le Code civil du Québec* [à son article 2849] *reconnaît et réglemente la présomption de fait* ». Jean-Claude ROYER, *La preuve Civile*, 2e éd., Cowansville, Yvon Blais, 1995, p. 519. Les auteurs Nadeau et Ducharme en sont arrivé à une conclusion semblable : « *Lorsque les tribunaux font, surtout dans le domaine de la responsabilité civile, appel à la maxime res ipsa loquitur, ils ne font rien d'autre qu'appliquer la règle de l'article 1238 (C.C.B.-C.)* » (article 2846 C.c.Q.). A. NADEAU et L. DUCHARME, « La preuve en matières civiles et commerciales », *Traité de droit civil du Québec*, tome 9e Montréal, Wilson Lafleur, 1965, p. 495-496.). Ceci étant, le débat sur la pertinence de la doctrine *res ipsa loquitur* ne vient donc aucunement remettre en cause notre recours au droit américain puisque les résultats recherchés par son

> « *There are many cases outside of the computer context in which an innocent plaintiff can prove an injury was tortiously inflicted but cannot prove which defendant inflicted the injury. Instead of allowing all defendants to escape liability, many courts have held all defendants jointly and severally liable even though they may have acted independently. Under the theory of joint and several liability, each defendant is allowed an opportunity to exonerate himself or limit his liability by proving responsibility for only a fraction of the harm. Because of their specialized knowledge, programmers and manufacturers are better able to prove themselves blameless than the user is to prove which is the blameworthy party. It seems proper, therefore, to shift the burden of producing evidence explaining the malfunction to the defendants when the plaintiff-user is innocent* »[302].

Cette notion est d'ailleurs reprise à l'article 1480 du *Code civil du Québec* qui précise que si plusieurs personnes: « *ont commis des fautes distinctes dont chacune est susceptible d'avoir causé le préjudice, sans qu'il soit possible, dans l'un ou l'autre des cas, de déterminer laquelle l'a effectivement causé* », elles sont alors tenues solidairement à la réparation dudit préjudice[303].

*

* *

Comme nous l'avons énoncé en introduction, cette première partie visait à identifier le fonctionnement des maliciels et les rouages de l'institution

---

application sont en concordance avec notre Code civil et l'interprétation fait de l'article 2849 par nos tribunaux. Voir à ce sujet l'affaire *RCA Limitée* c. *Lumbermen's Mutual Company*, [1984] R.D.J. 523, à la page 527, où le juge Chouinard explique qu'une présomption de fait est grave lorsque le fait à déterminer s'infère logiquement du fait connu, ce qui renvoi à la définition même de la *res ipsa loquitur*. Voir également Pierre NICOL, « Trépas de la *res ipsa loquitur* », (1999) *La presse juridique* 4.

[302] Daniel J. HANSON, *loc. cit.*, note 286, 260-261.

[303] Le juge Baudouin donne l'exemple d'un accident de chasse où un individu est atteint simultanément par deux projectiles sans qu'il soit possible d'établir lequel a causé sa mort. Dans ce cas, les deux chasseurs seront tenus solidairement responsables. Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, page 348.

de la responsabilité civile afin de mieux comprendre les situations pouvant entraîner la responsabilisation de tiers transmetteurs. Ces individus ne bénéficiant pas tous de ressources similaires et ne jouant pas nécessairement le même rôle dans la transmission de virus informatiques, nous abordons maintenant, dans cette seconde partie, les situations dans lesquelles un intermédiaire identifiable peut entraîner sa responsabilité lors de l'infection involontaire de l'ordinateur d'une victime potentielle, ainsi que les méthodes disponibles à ces tiers pour limiter leur responsabilité.

II. La responsabilité civile et la transmission de virus informatiques : Peut-on engager la responsabilité des intermédiaires?

Dans son livre portant sur les maliciels, Roger A. Grimes décrit ainsi le scénario habituel de transmission d'un virus informatique :

> « *the author writes the rogue program and posts it to a VX site. A spreader downloads the program and sends it to a legitimate, unsuspecting site.* [...] *The unsuspecting users execute the file, which can then infect other files or take control of their systems. The users email the malicious code to another friend or acquaintance and continue the cycle* »[304].

Cet extrait vient établir une liste sommaire des intermédiaires ayant joué un rôle dans la diffusion de virus et donc ceux qui auraient possiblement pu mettre fin à la contamination s'ils avaient pris les mesures de sécurité appropriées. De ce fait, ces personnes pourraient faire l'objet d'une poursuite en responsabilité civile par les individus subséquents dans la liste de diffusion s'il est possible d'établir leur négligence.

Avant d'aborder notre analyse, il importe de souligner que le droit civil ne fait aucune distinction entre « personne physique » et « personne morale » quant à l'imputabilité de la faute. Ainsi, étant donné les termes des articles 300 et 1457 C.c.Q., « *une personne morale peut être tenue responsable, si l'acte fautif qui a causé le dommage provient d'un de ses organes de direction, agissant dans le cadre de ses fonctions, ou d'une personne dont elle est responsable en vertu de la loi* »[305]. C'est donc dire que les intermédiaires techniques, les sites commerciaux et les entreprises pourraient être tenus responsables d'une attaque virale

---

[304] Roger A. GRIMES, *op. cit.*, note 35, p. 19.
[305] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 65.

ayant causé des dommages à un tiers, en supposant, bien sûr, que leur négligence, ou celle de leurs employés[306], puisse être prouvée.

Parallèlement, il nous faut souligner qu'il s'agit bien de la responsabilité des personnes et non de celle du fait des biens telle que décrite à l'article 1465 du Code dont il faut tenir compte. « *A virus cannot run completely of its own volition* »[307], c'est-à-dire qu'un utilisateur doit toujours accomplir un acte pour permettre la diffusion d'un maliciel, même si cet acte ne consiste qu'au démarrage du système[308]. Or, pour tomber sous le régime de la responsabilité des biens, il faut que le préjudice découle du « fait autonome » de ceux-ci, « *ce qui exclut l'intervention humaine et ce qui exclut par conséquent aussi un réseau informatique en ce qu'il ne peut fonctionner sans celle-ci* »[309]. C'est pourquoi les discussions concernant la notion de fait des biens nous semblent non fondées[310].

---

[306] En effet, l'article 1463 C.c.Q. souligne que « [l]*e commettant est tenu de réparer le préjudice causé par la faute de ses préposés dans l'exécution de leurs fonctions* ». Ainsi, « *if an employer makes it possible for its employee to create and disseminate a worm into e-commerce by providing its employee with a computer that has Internet access; and if it was foreseeable that the employee would use the Internet for personal use, the employer may face liability due to its employee's illegal online activity* ». Mark ISHMAN, « Computer Crimes And The Respondeat Superior Doctrine : Employers Beware », (2000) 6 *B.U.J. Sci. & Tech. L.* 6, par. 59. Voir aussi Mary L. BEYER, *loc. cit.*, note 299, 23 et Mark R. COLOMBELL, « The Legislative Response to the Evolution of Computer Viruses » (2002) 8 *Rich. J.L. & Tech.* 18, par. 47.

[307] David HARLEY et al., *op. cit.*, note 3, p. 59.

[308] *Id.*

[309] François THEMENS, *Internet et la responsabilité civile*, Cowansville, Éditions Yvon Blais, 1998, p. 65.

[310] Cette prétention souffre toutefois d'une exception notoire, puisque certains vers se transmettent automatiquement aux individus inscrits dans le carnet d'adresse d'un programme de messagerie dès leur entrée dans le système. Dans de telles circonstances, la personne subséquemment infectée devra faire la preuve d'un manquement au devoir de garde du transmetteur selon l'article 1465 C.c.Q., puisque ce dernier n'est qu'indirectement responsable de la transmission. En renvoyant le lecteur aux mesures de sécurité pouvant être adoptées par les usagés mentionnées à la section I, nous soumettons que celui dont l'ordinateur a transmis un vers sans son intervention demeure responsable de cette transmission dans les limites exposées dans la présente section. Cependant, il importe de souligner que le fardeau risque d'être beaucoup plus élevé pour la victime si ce vers lui a été transmis par un particulier puisque, comme nous le verrons plus loin, le devoir de s'assurer de l'absence de virus doit s'effectuer à la sortie d'un message et non à son entrée. Or, lorsque ces deux moments sont simultanés, seul un logiciel coupe-feu efficacement

Ces considérations étant mises au clair, nous pouvons maintenant étudier le régime de responsabilité applicable aux différents intermédiaires participant à la transmission de virus, à savoir les agents à l'origine de la présence de virus informatiques sur Internet (A), des agents à l'origine de la diffusion de virus informatiques sur Internet (B), ainsi que des agents permettant l'activation de virus informatiques, c'est-à-dire les victimes (C).

A. La responsabilité civile des agents à l'origine de la présence de virus informatiques sur Internet

Comme nous l'avons esquissé en introduction, le transmetteur initial d'un virus n'agit plus seul depuis l'avènement du réseau Internet. Il existe aujourd'hui une panoplie de sites web permettant au « cybervandale » de récolter l'information et les outils nécessaires à la création de virus informatiques[311]. Pour le néophyte, il n'est plus nécessaire de se soumettre à l'exercice fastidieux qu'est l'apprentissage du code informatique, il suffit simplement de disposer de quelques minutes et de taper les bons mots clés dans un outil de recherche pour avoir accès à toute la documentation nécessaire à la création ou l'emprunt de code viral. Mais ces sites de fabrication de virus

---

programmé peut limiter les dommages, mais ce logiciel s'avère fort probablement hors de portée pour la personne moyenne. Quoiqu'il en soit, cette exception risque de disparaître avec les nouvelles versions de *Outlook*, (voir *Microsoft Office XP Security White Paper*, 2002, p. 18) puisque ce logiciel de messagerie, le plus utilisé au Québec, averti automatiquement l'expéditeur à chaque fois que son système tente d'envoyer un message à son insu (Le logiciel antivirus *VirusScan* de *McAfee*, grâce à sa technologie HAWK permet un résultat semblable en alertant l'utilisateur dès que son ordinateur tente de transmettre un message à un pourcentage élevé du nombre d'adresses retrouvées dans son carnet. Voir Myles WHITE, « The Cure: Antivirus Big Guns Help Keep Your PC Squeaky Clean » (2002) 13 *Smart Computing* 67, 69-70). L'expéditeur devant maintenant autoriser tout envoi, il ne s'agit donc plus d'une question de responsabilité du fait des biens. De plus, comme cette fonctionnalité est maintenant activée par défaut, il sera facile d'établir que l'individu normalement diligent y aura recours, ce qui risque de faciliter le fardeau de preuve de la victime éventuelle.

[311] Voir Sarah GORDON, « Who Writes this Stuff? », (1996) en ligne sur le site *Commandcom* : <http://www.commandcom.com/virus/writes.html> (date de visite : 1 mai 2002).

informatiques et les individus les nourrissant ont-ils une quelconque responsabilité civile envers la victime d'une infection virale? Leur contribution à l'acte dommageable est-elle suffisante pour constituer une faute?

Ce sont à ces questions que nous proposons de trouver réponse en abordant le fonctionnement et la légitimité de ces sites de fabrication de virus informatiques (1) pour ensuite étudier la question spécifique de leur responsabilité civile (2). Finalement, nous aborderons les problèmes de pratiques associés à la responsabilisation de ces individus (3).

1. Le fonctionnement et la légitimité des sites de fabrication de virus informatiques

a) Le fonctionnement des sites de fabrication de virus informatiques

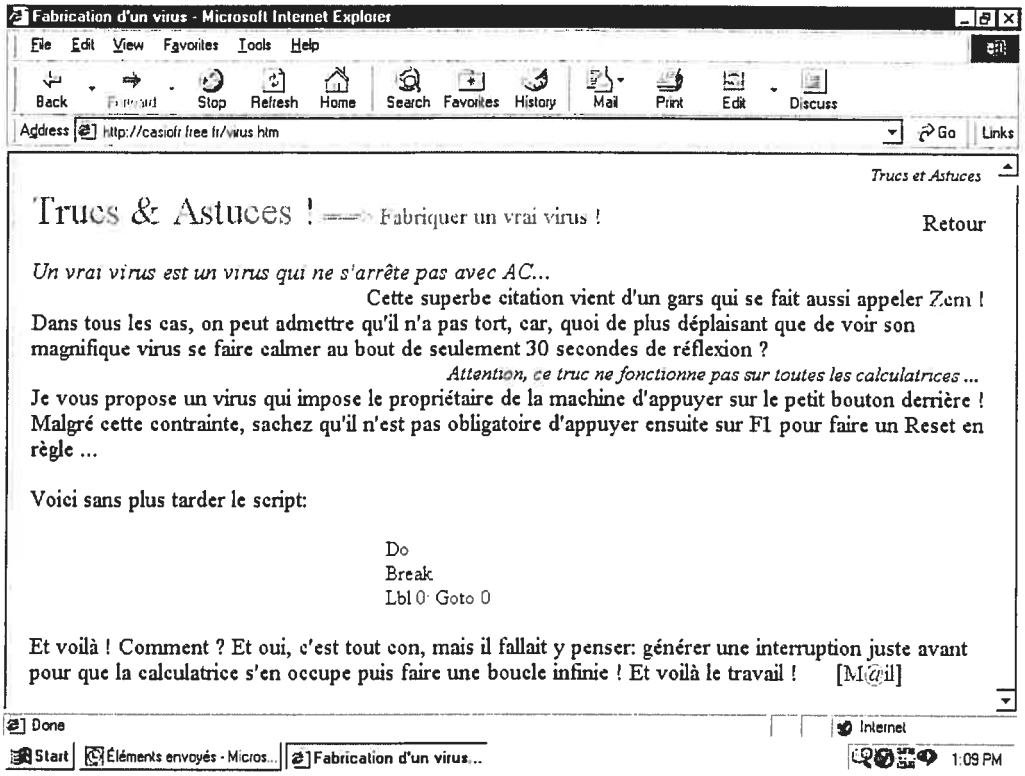
Par « site de fabrication de virus informatique », nous désignons tout site dont le contenu est destiné à diriger un individu dans la création ou la dissémination d'un maliciel tel que défini en introduction. Ainsi, dans la majorité des cas, il s'agit de pages web contenant le code de fabrication d'un quelconque virus ou encore l'hébergement d'un écrit expliquant comment créer son propre code[312]. L'utilisateur n'a donc qu'à copier le script pour le retranscrire dans un dossier et ainsi fabriquer une copie dudit virus comme le démontre la figure 4[313].

---

[312] C'est le cas, par exemple, du site <http://www.infowar.com> qui héberge une copie électronique du livre très controversé *The Little Black Book of Computer Viruses* de Mark A. LUDWIG (American Eagle Publications, 1996, 167 p.).

[313] <http://casiofr.free.fr/virus.htm>

Figure 3 : Script d'un virus informatique



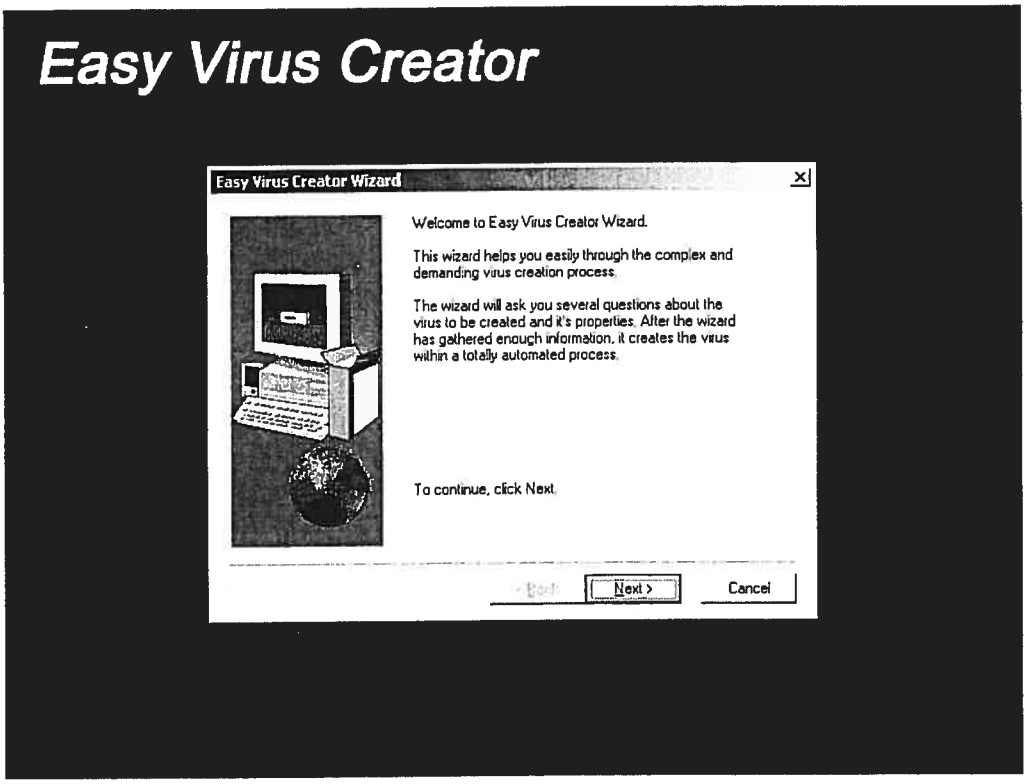
Cette méthode présente cependant l'inconvénient pour l'utilisateur de devoir posséder une base en programmation (quoique le *modus operanti* accompagne souvent code). Pour les néophytes désirant fabriquer leur propre virus sans programmation, il existe également des « générateurs de virus » (*virus generators*)[314], soit des programmes informatiques desquels même l'utilisateur le moins érudit peut se servir pour fabriquer une réelle application virale en quelques instants, comme le démontre la figure 5[315].

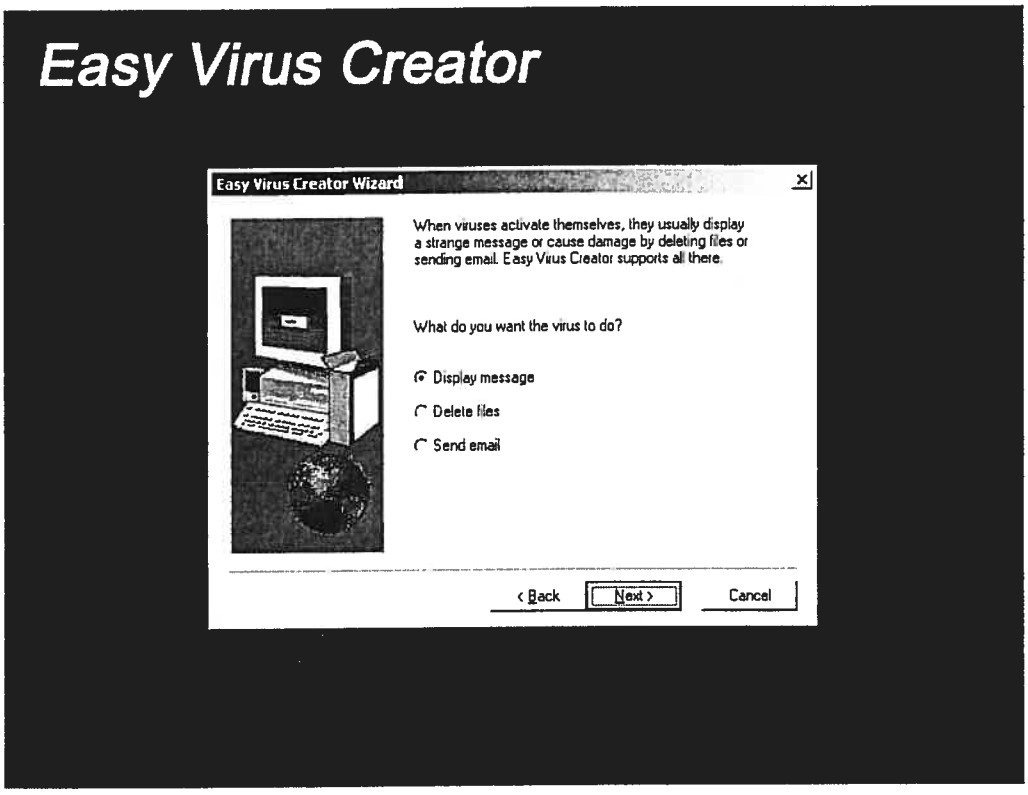
---

[314] ANONYME, *op. cit.*, note 20, p. 330. Voir également David HARLEY et al., *op. cit.*, note 3, p. 65 et 66.

[315] Un liste des logiciels les plus courants est disponible sur le site <http://orbita.starmedia.com/~lautaroml/virus.html>.

Figure 4 : Outil de création de virus informatiques[316]





316 <http://homokaasu.org/evlaunch.asp>.

Quoique ces logiciels possèdent des caractéristiques leur étant propres, ils fonctionnent tous selon le même modèle opérationnel, soit une série de menus permettant à l'utilisateur de créer un virus taillé sur mesure pour ses besoins. Ainsi, l'utilisateur n'a qu'à sélectionner la sorte de dommage visée (destruction de données, apparition de messages, etc.), la période d'infection, la méthode de propagation, etc. Il n'a ensuite qu'à peser sur une touche et le tour est joué, quelques minutes plus tard, il possède une véritable arme technologique pouvant causer des ravages importants comme en témoignent certaines infections récentes[317].

Finalement, l'individu désirant simplement se procurer un virus déjà fonctionnel peut se diriger vers un site d'échange viral (*virus exchange* ou VX)[318] offrant une liste de virus pouvant être téléchargés[319]. Dans un tel cas, le site ne fait qu'héberger les logiciels de tiers auteurs. Il importe donc de nous pencher d'abord sur la responsabilité de ces derniers.

b) Le rôle joué par les auteurs de virus informatiques

Selon Sarah Gordon, ceux qui alimentent les sites de virus informatiques sont motivés soit par l'ambition d'obliger les créateurs d'applications informatiques à générer un meilleur produit, soit par une prétention de « rendre service » en soulignant les limites du réseau ou soit, tout simplement, par un désir de commettre des actes de vandalisme de la même façon qu'un jeune peut faire des graffitis sur le mur d'un

---

[317] Les virus « Anna Kournikova » et « Melissa » auraient tous deux été conçus par des novices ayant eu recours à des logiciels de fabrication de virus informatiques. Voir Steve GOLD, « New Virus Creation Utility Set to Wreak Havoc », (2001) en ligne sur le site *Newsbytes* : <http://www.newsbytes.com/news/01/163077.html> (dernière mise à jour : 13 mars 2001) et John LEYDEN, « Malware by Numbers : Online Virus Creation Tool Spotted », (2002) en ligne sur le site *The Register* : <http://www.theregister.co.uk/content/56/24272.html> (dernière mise à jour : 4 mars 2002)

[318] ANONYME, *op. cit.*, note 20, p. 331

[319] Sarah GORDON, *loc. cit.*, note 311.

commerce[320]. Quoi qu'il en soit, leurs actes sont facilités par l'absence de craintes d'être identifiés en tant qu'auteurs de ces logiciels[321]. Cependant, certains individus refusent de se cacher derrière le couvert de l'anonymat puisque, selon leurs dires, ils ne jouent aucun rôle dans la dissémination de virus informatiques, n'étant point responsables de l'usage délictuel fait de leur code par des tiers[322] :

> « *Some virus writers state that they are not responsible for their virus once it leaves their own computer, justifying the operation of virus exchange bulletin board systems. From these systems, knowing/willing persons can obtain computer viruses. Because the persons receiving the viruses know what they are getting, the viruses are not a problem from the standpoint of their creator. "I'm not saying viruses don't hurt people, but usually when they affect people, it's almost always the person's fault."* » [323]

En autres mots, le problème se logerait chez le distributeur et non chez l'auteur[324] qui n'a plus la garde du bien au moment de l'acte délictuel[325], prétention cohérente avec les dispositions pénales applicables aux virus informatiques[326]. Cependant, l'on pourrait invoquer que le fabricant d'un virus ne se comporte aucunement comme une personne prévoyante et prudente s'il permet la distribution de son logiciel[327] sans contrôler la qualité des usagers potentiels. En effet, la distribution de produits dangereux fait normalement l'objet d'une réglementation au Canada, « [*i*]*l suffit de penser aux armes à feu. Pour des raisons évidentes de sécurité, quiconque ne peut aller dans une armurerie se procurer librement un tel bien. Il doit présenter au commerçant au moins un*

---

[320] Sarah GORDON, « The Generic Virus Writer II » (1994) en ligne sur le site *IBM Research* : <http://www.research.ibm.com/antivirus/SciPapers/Gordon/GVWII.html#NEWAGE> (Date de visite : 1 mai 2002).
[321] Eugene H. SPAFFORD et Stephen A. WEEBER, *loc. cit.*, note 23, 2.
[322] ANONYME, *op. cit.*, note 20, p. 329.
[323] Sarah GORDON, *loc. cit.*, note 122.
[324] ANONYME, *op. cit.*, note 20, p. 329.
[325] Article 1465 C.c.Q.
[326] Voir article 430 C.cr.
[327] PISA, *loc. cit.*, note 6.

certificat d'acquisition, comme le patient doit présenter au pharmacien une ordonnance. »[328] Malgré l'absence de textes législatifs concernant la mise à la disposition du public de virus informatiques, il s'avère raisonnable, considérant l'aspect dommageable des logiciels en question, d'assurer un certain contrôle quant aux individus ayant accès à un tel contenu. C'est d'ailleurs ce que souligne Carbonnier :

> « *La responsabilité de celui qui a mis en circulation les instruments du dommage n'est pas toujours supprimée par la présence des utilisateurs intermédiaires qui l'ont matériellement causé. Une imprudence ou négligence peut lui être imputée dans le choix ou le contrôle de ces utilisateurs. Les tribunaux ont ainsi tenu pour responsable le droguiste qui a vendu des pétards à un gamin si incendie s'ensuit* »[329].

Autrement, comme l'explique Slade, l'auteur d'un maliciel demeure en partie responsable de l'utilisation illicite de son programme : « *No PC is an island – at least not where viral programs are concerned. Therefore, your "right" to study, write, and distribute viral programs carries the responsibility to ensure that your creations do not – ever – run on machines where they are not authorized* »[330].

En conclusion, nous soumettons que, lorsque l'auteur d'un virus consent à ce que son logiciel se retrouve sur un site d'échange viral, ce dernier est conjointement responsable de l'utilisation faite par les tiers de son programme. Ainsi, l'analyse faite de la responsabilité civile des sites de fabrication de virus informatiques dans la présente étude s'applique *mutatis mutandis* aux auteurs des virus s'y retrouvant.

---

[328] *Ciba-Geigy Canada Ltd.* c. *Apotex Inc.*, [1992] 3 R.C.S. 120, chap. 81.
[329] Jean CARBONNIER, *op. cit.*, note 178, p. 365.
[330] Robert SLADE, *op. cit.*, note 3, p. 179.

2. Peut-on imputer une faute aux auteurs de virus informatiques et aux gestionnaires de sites hébergeant leurs créations

Il ne fait aucun doute aux yeux d'une majorité d'observateurs que de mettre de telles armes destructives à la portée de tous témoigne d'un comportement socialement répréhensible. Cependant, le simple fait qu'un acte soit répréhensible ne constitue pas une faute au sens du Code civil, encore faut-il que cet acte soit fait en violation d'une norme de conduite imposée par le législateur[331] (a) ou encore qu'il constitue un comportement déraisonnable (b)[332].

a) Les sites de fabrication de virus informatiques violent-ils une norme de conduite imposée par le législateur

Selon nos recherches, il n'existe à ce jour aucune décision jurisprudentielle mettant en cause la légitimité d'un site de fabrication de virus informatiques et la doctrine canadienne semble muette sur cette question. Cependant, cela ne signifie pas que de tels sites ne pourraient être considérés comme étant illégaux. En effet, depuis 1997, l'article 342.2 (1) du *Code criminel*[333] (C. cr.) précise que :

> « *[q]uiconque, sans justification ou excuse légitime, fabrique, possède, vend, offre en vente ou écoule des instruments, ou des pièces de ceux-ci, particulièrement utiles à la commission d'une infraction prévue à l'article 342.1, dans des circonstances qui permettent de conclure raisonnablement qu'ils ont été utilisés, sont destinés ou étaient destinés à la commission d'une telle infraction, est coupable [...] soit d'un acte criminel [...] soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire* ».

---

[331] « *Rapporté au virus informatique, il est des lors evident que l'ensemble des actes vises par la loi penale peuvent donner lieu a action civile devant les Tribunaux* », Olivier ITEANU, *loc. cit.*, note 16.
[332] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 97.
[333] L.R. 1985, c. C-46.

Or parmi les infractions prévues à l'article 342.1, notons le fait d'utiliser un ordinateur directement ou indirectement dans l'intention de détruire ou modifier des données, dépouiller des données de leur sens, empêcher, interrompre ou gêner l'emploi légitime des données, etc.[334] L'infection virale d'un ordinateur tombant clairement dans les limites de l'article 342.1 et les sites de fabrication de virus étant des « instruments particulièrement utiles » à la conception de ces virus, il en découle donc que ceux-ci peuvent être visés par l'article 342.2 (1) du *Code criminel*. Cependant, c'est le critère d'excuse légitime qui pourrait, dans certains cas, présenter des difficultés pour la poursuite. En effet, le Tribunal de grande instance de Paris a déjà tenté d'interdire la publication du livre « *La naissance d'un virus* » de Mark Ludwig parce que celui-ci comportait des instructions sur la fabrication de virus, mais la Cour d'appel a rapidement rejeté cette décision sous prétexte qu'il s'agissait d'un « procès de la science »[335]. Ainsi, la valeur éducative de certains de ces sites pourrait être plaidée pour légitimer leur existence. Toutefois, les endroits comme *Homokaasu.org*, un site prônant l'anarchie et les génocides[336], auront, à nos yeux, beaucoup de difficulté à prétendre que leurs intentions n'étaient pas malveillantes.

Même si des dispositions propres aux crimes informatiques n'avaient pas été adoptées en 1997, il est de notre opinion que la présence de certains sites de fabrication de virus informatiques peut être interdite par l'application de l'article 21 du *Code* criminel. En effet, cet article stipule que quiconque accomplit ou omet d'accomplir quelque chose en vue d'aider un tiers à commettre une infraction ou encore quiconque encourage la commission de celle-ci est considéré comme participant à

---

[334] Ces infractions sont énumérées à l'article 430 (1.1) C. cr. Auquel renvoi l'alinéa c) de l'article 342.1 C. cr.

[335] Voir la revue *Line noiz*, du 12 juin 1994 disponible à l'adresse <http://www.div8.net/billy/linenoiz/linenoiz-17>.

[336] Le site offre un jeu intitulé « *Kill everyone* » dont l'objectif est d'éliminer le plus d'êtres humains sur terre sous prétexte que le monde est surpeuplé et qu'il est donc « noble » de désirer tuer des innocents.

ladite infraction. La destruction de propriété étant une infraction selon l'article 430 (1) C. cr., les sites de fabrication de virus pourraient donc être visés par cette disposition s'il est possible d'établir une intention de servir à ou d'encourager la commission d'une infraction. Or, malgré le fait que certains sites prétendent avoir une légitimité éducative et donc qu'ils n'opèrent pas « en vue d'aider » la commission d'une infraction, d'autres indiquent clairement leur intention de fournir de l'information destinée à être utilisée malicieusement[337] et expriment une fierté à l'idée de causer des dommages[338]. Il est de notre avis que les gestionnaires de ces sites encouragent et aident de façon proactive à la propagation de virus informatiques et qu'ils tombent donc sous l'empire des articles 21 et 430 (1) C. cr.

Cependant, il est à noter que le terme « bien » utilisé à l'article 430 (1) C. cr. « *s'entend d'un bien corporel immeuble ou meuble* »[339]. Il est donc pertinent de se demander si un logiciel est un bien corporel. Dans *R.* v. *Turner*[340], la Cour suprême d'Ontario refusa d'admettre la prétention de la partie défenderesse qui alléguait « *that as the computer tape remained completely intact and its use as a computer tape was unaffected, there was a complete absence of evidence that the Applicants had in any way obstructed, interrupted or interfered with the lawful use, enjoyment or operation of "property" as currently defined* »[341]. Quoi que l'on puisse penser de cette décision, la position de la Cour a depuis été codifiée avec l'ajout de l'alinéa 1.1 à l'article 430 du Code criminel qui ajoute la destruction ou la modification volontaire de

---

[337] Ainsi l'auteur du site <http://casiofr.free.fr/virus.htm> souligne très clairement son intention de causer des dommages avec son virus « *Je vous propose un virus qui impose le propriétaire de la machine d'appuyer sur le petit bouton derrière !* »

[338] Le site <http://homokaasu.org/evlaunch.asp> va jusqu'à suggérer à l'utilisateur comment rendre son virus le plus dommageable possible.

[339] Art. 428 C. cr.

[340] [1984] O.J. No. 1268.

[341] *Id.*, au paragraphe 7.

données à la liste des méfaits pouvant constituer une infraction, mettant ainsi fin au débat.

Outre les dispositions présentement en vigueur au pays, le Canada est, depuis 2001, signataire[342] de la *Convention sur la cybercriminalité* déposée à Budapest le 23 novembre 2001 par le Conseil de l'Europe, texte criminalisant clairement la présence de tels sites à son article 6 :

> « *Article 6 – Abus de dispositifs*
>
> *1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:*
>
> *a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition*
>
> *i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 – 5 ci-dessus ;* [...]
>
> *2. Le présent article ne saurait être interpréter comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'a pas pour but de commettre une infraction établie conformément à l'Article 2 à 5 de la présente Convention, comme en cas d'essais autorisés ou de protection d'un système informatique.* »[343]

Or parmi les articles 2 à 5 de ladite convention, notons que l'article 4 précise que « *[c]haque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale,*

---

[342] Il importe cependant de souligner que le Canada n'a pas encore ratifié la convention et que celle-ci n'est toujours pas en vigueur.
[343] Convention sur la cybercriminalité, Budapest, 23.XI.2001.

conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques », alors que l'article 5 vise à criminaliser « *l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques* ». Ainsi, à la lecture combinée de ces trois articles, la diffusion d'un logiciel principalement conçu pour entraver le fonctionnement d'un système informatique, ce qui inclut clairement la transmission de virus, constitue un acte criminel. Il est encore une fois nécessaire, selon le paragraphe 2 de l'article 6 de prouver l'intention malicieuse du gestionnaire du site visé, ce qui, comme nous l'avons vu plus haut, peut s'avérer très complexe ou très simple selon les sites concernés.

À la lecture de ce qui précède, il s'avère donc possible de prétendre que la gestion d'un site de fabrication de virus informatiques peut être considérée comme étant un acte criminel si la présence d'une intention malicieuse est démontrée. Or, comme nous l'avons déjà souligné, « la transgression d'une obligation spécifique imposée par la loi [...] constitue en principe une faute civile »[344], ce qui implique que le gestionnaire d'un site de fabrication de virus informatiques reconnu criminellement responsable selon les dispositions énoncées ci-dessus devrait normalement être également reconnu fautif en droit civil.

b) Est-il déraisonnable de permettre l'accès à du code viral à des tiers

Selon Pierre Trudel, « *la personne qui choisit de mettre en ligne une information ou se comporte de manière à exercer un contrôle sur la diffusion de celle-ci assume la responsabilité découlant de son caractère*

[344] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 109.

illicite ou délictueux »[345]. Or un acte illicite ne découle pas obligatoirement d'une action illégale, les activités illicites étant celles pouvant constituer une faute sans être nécessairement contraires à la loi[346]. Ainsi, même s'il n'est pas possible, dans certains cas, de prouver l'illégalité d'un site de fabrication de virus informatiques, cela n'implique pas pour autant que leur responsabilité ne soit pas mise en cause. En effet, si l'on peut établir que le gestionnaire du site n'a pas agi de façon diligente et raisonnable, sa responsabilité peut être entraînée[347].

Comme nous l'avons déjà souligné, afin d'établir la responsabilité civile d'un tiers, il faut d'abord prouver que ce dernier a commis un acte fautif et que celui-ci a contribué au dommage subi. Or, comme l'explique la cour dans l'affaire *Arkwright Boston Manufacturers Mutual Insurance Co. c. Gagnon*[348], le fait d'encourager la commission d'un acte illicite peut en soi constituer une faute en droit québécois :

> *« Cette faute en sera une d'action, par des instructions positives ou un encouragement manifeste à des actions illicites ou, d'omission, par une abstention d'agir dans une situation où il devait le faire. C'est dans ce contexte que les actions et omissions des représentants d'un syndicat feront l'objet d'un examen judiciaire. Aussi, la responsabilité civile du syndicat pour des actes illicites commis au cours d'une grève doit être envisagée, ultimement, à la lumière de l'art. 1053 C.c.B.-C. et, dans*

---

[345] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », dans Vincent GAUTRAIS (dir.) *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 607, à la page 612.

[346] En effet, comme le souligne Hubert Reid, le terme « illicite » a un sens plus large que « illégal » puisqu'il inclut la notion de moralité. Hubert REID, *op. cit.*, note 147, p. 281.

[347] Ici, un parallèle peut être établi avec les entreprises qui entreposent des virus biologiques dans le but de les étudier. En Angleterre, une telle entreprise fut jugée responsable de la propagation du virus : « [T]*he defendant's duty to take care to avoid the escape of the virus was due to the foreseeable fact that the virus might infect cattle in the neighbourhood and cause them to die. The duty is accordingly owed to the owners of cattle in the neighbourhood* ». *Weller and Co.* c *Foot and Mouth Sisease Research Institute* [1965] 3 All ER 560, à la page 570. Voir également Clive GRINGRAS, *op. cit.*, note 15, p. 61 et 62.

[348] [1997] A.Q. no 3704.

> *les faits, le premier juge s'est également imposé cet exercice »*[349].

Les sites de fabrication de virus informatiques offrant des conseils sur la transmission efficace de virus comme *homokaasu.org* commettent donc une « faute d'action ». Cependant, encore faut-il que cette faute soit à l'origine du dommage causé, ce qui n'est pas évident dans le cas d'informations dommageables disponibles sur le web[350].

Un principe jurisprudentiel bien établi en matière de responsabilité civile pose que le préjudice subi par la victime doit être la conséquence logique, directe ou immédiate de la faute[351]. L'utilisation du terme « ou » implique donc qu'il n'est pas nécessaire de satisfaire à ces trois critères, l'un d'eux étant suffisant. Dans le cas des sites de fabrication de virus informatiques, le lien entre un site et le préjudice subi n'étant ni direct, ni immédiat, reste donc à savoir s'il est logique.

Afin de répondre à cette question, les tribunaux ont adopté un processus en deux étapes. D'abord, ils recherchent la causalité adéquate du dommage, c'est-à-dire les conditions ayant rendues possible la réalisation du préjudice[352] et sans lesquelles aucun dommage ne se serait produit. Il va de soi que si le transmetteur du virus ne se l'était pas procuré sur un site, il n'aurait pas pu le transmettre par la suite. Cette exigence semble donc être atteinte dans le cas nous intéressant.

Vient ensuite le test de la prévision raisonnable. Ainsi, comme l'expliquent Jean-Louis Baudouin et Patrice Deslauriers, « *lorsque cet événement se rattache à une conduite fautive, on se demande alors si les conséquences de l'acte ou de l'omission pouvaient être*

---

[349] *Arkwright Boston Manufacturers Mutual Insurance Co. c. Gagnon*, précitée, note 348, par. 29.
[350] François THEMENS, *op. cit.*, note 309, p. 37 et 38. L'auteur donne l'exemple d'informations relatives à la confection de bombes ou à des directives portant sur la procédure à suivre pour se suicider.
[351] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 349.
[352] *Id.*, p. 353.

raisonnablement prévues »[353]. Or, comme l'explique Mark Ludwig dans son écrit sur les virus, « *When I wrote it, it was largely an experiment. I had no idea what would happen. Would people take the viruses it contained and rewrite them to make all kinds of horrificly destructive viruses? Or would they by and large be used responsibly?* »[354]. Il ressort de ce passage que l'hypothèse d'une utilisation malicieuse de son œuvre lui est passée par la tête, ce qui nous laisse supposer que cette possibilité devrait être envisagée par le gestionnaire de site de fabrication de virus diligent et raisonnable.

Afin d'appliquer ce test aux gestionnaires de site de fabrication de virus informatiques, il est intéressant d'étudier les faits de la décision *Dubois* c. *Dubois*[355]. Dans cette affaire, un étudiant est devenu aveugle après avoir consommé une bouteille d'alcool méthylique que lui avait vendu un ami. Ce dernier avait volé la bouteille du chauffeur de son autobus scolaire et ignorait nécessairement la nature de son contenu. Or, malgré le fait que la bouteille lui ait été volée, la Cour d'appel a jugé à l'unanimité que le chauffeur d'autobus était responsable de préjudice subi par l'étudiant.

Cette situation, quoique différente de celle qui se produit lorsqu'un individu se procure un virus sur Internet afin d'infecter un tiers du point de vue des faits, s'avère intéressante et similaire selon le contexte juridique. En effet, dans les deux cas, le défendeur (le chauffeur et le gestionnaire de site) n'exerce aucun contrôle sur le bien une fois que celui-ci a quitté sa charge. Or, si le chauffeur a été condamné à dédommager la victime suite à son manque de prévoyance malgré son ignorance de la possibilité du danger et malgré le fait qu'il n'a pas volontairement confié le contenu de la bouteille à l'étudiant vendeur, le

---

[353] *Id.*, p. 354.
[354] Mark LUDWIG, *op. cit.*, note 312, « Preface to the Electronic Edition ».
[355] [1978] C.A. 569.

gestionnaire de site qui distribue volontairement des logiciels viraux ne saurait plaider avec succès qu'il ne peut se douter de ce qui adviendra de son code malicieux, d'autant plus que, comme le soulignent Jean-Louis Baudouin et Patrice Deslauriers, si la faute est lourde et intentionnelle, ou encore si la situation provoquée est objectivement dangereuse (nous soumettons qu'il est objectivement dangereux de mettre de tels logiciels à la disposition de tous et chacun), la jurisprudence tend à reconnaître plus facilement la présence d'un lien de causalité[356]. Cependant, il importe de souligner que le chauffeur d'autobus est titulaire d'un devoir de diligence plus élevé que le gestionnaire de site puisqu'il a la charge de mineurs durant son trajet.

Dans *Gagnon* c. *Raté*[357], une autre affaire d'intérêt dans le contexte présent, la C.T.C.U.Q., un organisme parapublic, vendait des barils contenant des résidus de substances dangereuses à un tiers du nom de Gauvin. Ce dernier avait, par la suite, vendu l'un desdits barils au voisin du demandeur qui a causé une explosion en essayant de couper le baril à l'aide d'une scie ronde, blessant par le fait même le demandeur. La cour a, dans cette affaire, reconnu la négligence de la C.T.C.U.Q. pour ne pas avoir pris soin de bien informer l'acheteur Gauvin des dangers découlant desdits barils.

Ici, même si c'est Gauvin qui est directement responsable du préjudice subi par le demandeur, la plus grande part de la responsabilité (60% contre 20% pour Gauvin et 20% pour le voisin du demandeur) repose sur les épaules de la personne ayant permis la distribution des biens dangereux. Cet exemple est très parlant dans le contexte d'une infection virale, puisque la chaîne des événements est semblable : 1° mise de produits dangereux à la disposition de tiers (C.T.C.U.Q. ou site de fabrication de virus informatiques), 2° distribution du produit par un tiers

---

[356] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 348 et 355.
[357] [1996] A.Q. no 982

à une victime inconsciente des dangers pouvant en découler (Gauvin ou celui qui utilise illicitement le maliciel), 3° dommages causés à la victime ainsi qu'à d'autres individus entrant en contact avec cette dernière (le demandeur et son voisin).

Il importe de souligner que la responsabilité de Stamchem, l'entreprise ayant vendu les barils (pleins) à la C.T.C.U.Q. en premier lieu, n'a pas été retenue. En effet, le juge Letarte a considéré que les actes négligents de la C.T.C.U.Q. constituaient un *novus actus interveniens* ce qui venait rompre la responsabilité du fournisseur. Les auteurs de virus pourraient donc utiliser cet exemple pour appuyer leur position de non-responsabilité. Cependant, il importe de faire une distinction entre les deux relations. Dans le cas de l'affaire Gagnon, Stamchem a vendu le produit à une entreprise parapublique réputée sans savoir que les déchets causés par ce produit ne seraient pas éliminés selon les normes. Les auteurs de virus qui affichent leur programme sur un site quelconque sont parfaitement conscients de l'utilisation faite de leur logiciel par le gestionnaire du site.

Dans un contexte propre à Internet, l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information*[358] précise que « *le prestataire de service qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication* [...] *peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a la connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité* ». Ceci implique donc que celui-ci est responsable du dommage causé à un tiers par de l'information disponible sur un site qu'il héberge. Il s'agit ici d'une relation tripartite

[358] L.Q. 2001, c. 32.

similaire à celle qui nous intéresse. Ainsi, si l'on peut tenir l'hébergeur responsable pour les accomplissements d'un tiers sur lequel il n'exerce pas de contrôle, le gestionnaire du site qui contrôle le contenu de celui-ci devrait logiquement pouvoir être tenu responsable d'une utilisation illégitime de ce dernier.

c) Les clauses de non-responsabilité

À la lumière de ce qui précède, plusieurs sites de fabrication ou de distribution de virus informatiques ont décidé de prendre certaines mesures afin de limiter leur responsabilité dans le cas d'infections virales causées par l'un de leurs logiciels. Le site coderz.net, par exemple, affiche l'avis suivant sur l'une de ses pages :

> « *IN NO EVENT SHALL THE WEBSITE AUTHORS OR THEIR SUPPLIERS BE LIABLE TO ANY USER OR ANY THIRD PARTY FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, INCIDENTIAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY OR LOST PROFITS) RESULTING FROM THE USE OR INABILITY TO USE THE WEB SITES OR THE MATERIAL, WHETHER BASED ON WARRANTY, CONTRACT, TORT, OR ANY OTHER LEGAL THEORY, AND WHETHER OR NOT THE WEBSITE AUTHORS ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.* »[359] (nous soulignons).

La présence d'une telle clause de non-responsabilité est doublement inefficace. D'abord, la disposition concernant la responsabilité du site envers les tiers (*third party*) n'a aucune valeur juridique et ne saurait être opposable à la victime d'une attaque virale désirant être dédommagée; l'article 1440 C.c.Q. soulignant qu'un contrat n'a d'effet qu'entre les parties contractantes. Ainsi, même en supposant que l'utilisateur du site est réellement lié par la clause de non-responsabilité[360], il ne peut, par son acceptation des risques engager un tiers.

---

[359] <http://www.coderz.net/disclaimer.html>

[360] À cette fin, voir la section II B 2 d) du présent mémoire.

Ensuite, ce type de clause démontre une connaissance des risques associés à la gestion de sites de fabrication de virus informatiques. Elle vient ainsi aider le requérant à prouver qu'il est non seulement raisonnable de s'attendre à ce qu'un individu utilise malicieusement le contenu d'un tel site, mais que l'accusé était conscient de cette possibilité. Ceci vient donc remplir le critère de prévision raisonnable énoncé dans la section précédente.

3. La problématique pratique derrière la responsabilisation des sites de fabrication de virus informatiques

S'il est, tel nous le soumettons, juridiquement possible de poursuivre les gestionnaires de sites de création de virus informatiques ou les auteurs des logiciels de création virale contenus sur ces sites, il n'en demeure pas moins que, pratiquement, cette tâche peut s'avérer trop complexe et inefficace pour la victime désirant être compensée. En effet, celle-ci peut devoir surmonter divers problèmes quant au régime de preuve (a), à la nature extraterritoriale du réseau (b) et à la viabilité financière des participants (c).

a) Le problème de preuve

La problématique liée à la nécessité d'établir la preuve de la responsabilité civile du gestionnaire d'un site de fabrication de virus ou de l'auteur d'un virus ayant affiché son logiciel sur un tel site est double. D'abord il faut établir leur participation à l'acte préjudiciable, ensuite il faut quantifier les dommages subis. Ce second obstacle ayant déjà été traité dans la section I[361] du présent mémoire, nous nous permettons tout simplement de renvoyer le lecteur à celle-ci.

---

[361] Voir le point 2 (Le dommage) de la section I B.

En ce qui concerne la possibilité d'établir la participation d'un site ou d'un individu à la confection d'un virus ayant causé des dommages, la vitesse de transmission de l'information sur Internet prise conjointement avec les différentes mesures de protection de la vie privée des utilisateurs du réseau rendent la source d'un message difficilement identifiable. Cette proposition est d'autant plus véridique dans le cas de virus puisque leurs auteurs et distributeurs n'ont normalement pas l'intention d'êtres retracés. Comme l'expliquent David Harley, Robert Slade et Urs E. Gattiker, « *The undirected nature of virus epidemiological patterns means that tracing an infection back to its original source is a little like tracing your ancestry back through the aeons* »[362]. En effet, il est difficile de retracer les déplacements d'un virus jusqu'à son créateur[363].

Cela ne signifie pas pour autant que l'appréhension des créateurs de virus soit impossible, les individus et les sites responsables de la mise en ligne de « Melissa »[364] ayant chacun été retrouvés par les forces de l'ordre[365]. D'ailleurs, si l'on est porté à penser qu'il est encore plus complexe de retracer le site sur lequel le transmetteur initial du virus a pris l'information nécessaire à la commission de son délit que le

---

[362] David HARLEY et al., *op. cit.*, note 3, p. 442.

[363] Eugene H. SPAFFORD et Stephen A. WEEBER, *loc. cit.*, note 23, 2. Il existe cependant une exception notoire à cette règle : un virus connu sous le nom de *Brain.* Ce dernier affiche le nom, l'adresse et le numéro de téléphone de ses auteurs, les propriétaires d'une boutique informatique située au Pakistan, lorsqu'il est activé par l'utilisateur infecté. Voir Jan HRUSKA, *op. cit.*, note 55, p. 61.

[364] « *Both Codebreakers.org and SourceOfKaos.com have been connected to the Melissa macro virus via an electronic fingerprint derived from a serial number found in documents created with Microsoft Word* », Luke REITER et Robert LEMOS, « FBI hunting for virus writer » (1999) en ligne sur le site zdnet.com : <http://www.zdnet.com.com/2102-11-514208.html> (dernière mise à jour : 31 mars 1999).

[365] Voir Kevin POULSEN, « Justice mysteriously delayed for 'Melissa' author », (2001) en ligne sur le site *The Register* : <http://www.theregister.co.uk/content/archive/20751.html> (dernière mise à jour : 8 janvier 2001) et ASSOCIATED PRESS, « Kournikova virus creator arrested, released », (2002) en ligne sur le site de *USA Today* : <http://www.usatoday.com/life/cyber/tech/2001-02-14-virus-arrest.htm> (dernière mise à jour : 6 février 2002).

cybervandale lui-même, cela n'est pas nécessairement le cas. Premièrement, si le cybervandale est trouvé, la saisie des informations contenues sur son ordinateur risque de mener directement à la source. C'est d'ailleurs ce qui s'est produit dans l'affaire américaine *Rice* v. *Paladin Enterprises, Inc.*[366] – que nous étudierons sous peu – et la raison derrière les accusations portées contre la compagnie. Ensuite, il est souvent possible de retracer l'origine de certains virus en comparant leurs diverses versions ainsi que les « améliorations » apportées par leurs auteurs[367]. Comme l'explique Mark Ludwig dans la préface de son livre « *The Little Black Book of Computer Viruses* », il est plausible, en étudiant la structure d'un virus, d'en déduire la source, c'est-à-dire d'où le code employé est issu :

> « *The Stealth virus described in its pages has succeeded in establishing itself in the wild, and, as of the date of this writing it is #8 on the annual frequency list, which is a concatenation of the most frequently found viruses in the wild. I am sorry that it has found its way into the wild [...] Next round at the printer, I updated the Stealth virus to work more like the Pakistani Brain, hiding its sectors in areas marked bad in the FAT table, and to infect as quickly as Stoned. [...] it would appear that Stealth has done nothing but climb the wild-list charts. Combining aggressive infection techniques with a decent stealth mechanism has indeed proven effective...* »[368]

Cette science baptisée « software forensics » par les auteurs Eugene H. Spafford et Stephen A. Weeber, se base sur la notion que, tout comme un texte écrit en prose, un logiciel comporte des segments reflétant un style particulier attribuable à son auteur. Tout comme il serait difficile de confondre les ouvrages de Hugo et de Camus, « Melissa » et « Anna Kournikova » ne pouvaient être l'œuvre d'un même programmeur.

---

[366] 128 F.3d 233.
[367] Jan HRUSKA, *op. cit.*, note 55, p. 61.
[368] Mark LUDWIG, *op. cit.*, note 312, « Preface to the Electronic Edition ».

> « *The keys to identifying the author of suspect code are selection of an appropriate body of code and identification of appropriate features for comparison. This may not be easy to do if the programmer has attempted to hide his authorship, or if appropriate sample code is not available. Nonetheless, our personal experience is such that we believe important features might still be present for analysis, in some cases. At the least, analysis of the characteristics of the code might well lead to the identification of suspects to examine further* ».[369]

C'est ainsi que l'on a pu remonter jusqu'à l'I.U.T. de Turin pour cerner l'auteur du virus *Italian* et à l'Université hébraïque de Jérusalem pour le virus *Jerusalem*.[370] Même si le « software forensics » ne permet pas d'établir hors de tout doute l'origine d'un virus, il ne faut pas perdre de vue qu'en droit civil la responsabilité d'un individu est établie selon la balance des probabilités[371]. Ainsi, il n'est pas nécessaire de prouver qu'un site ou un individu ait inévitablement participé à la propagation d'un virus, il suffit de démontrer qu'il soit plus plausible de prétendre à l'implication de ceux-ci que l'inverse[372].

b) Le problème de territorialité

Les juristes ne se font plus d'illusions quant à l'effectivité des lois dans le cyberespace. Toute solution juridique à un problème découlant d'Internet doit tenir compte de l'aspect transfrontalier du réseau et donc de l'applicabilité, au sein de la communauté internationale, des dispositions législatives adoptées[373]. Cependant, comme la problématique de la responsabilité civile n'est pas propre à Internet,

---

[369] Eugene H. SPAFFORD et Stephen A. WEEBER, *loc. cit.*, note 23, 3.
[370] Jan HRUSKA, *op. cit.*, note 55, p. 61.
[371] Article 2804 C.c.Q.
[372] *C'est par la prépondérance de la preuve que les causes doivent être déterminées, et c'est à la lumière de ce que relèvent les faits les plus probables, que les responsabilités doivent être établies* ». *Parent* c. *Lapointe*, [1952] 1 R.C.S. 376, p. 380 (juge Taschereau).
[373] À ce sujet, voir l'article « Réflexions pour une approche pragmatique des conflits de juridictions dans le cyberespace » de Karim BENYEKHLEF dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p.137.

certaines dispositions du code concernant le droit international privé peuvent trouver application dans le cas de la responsabilisation des gestionnaires de sites de fabrication de virus informatiques :

> « *3126. L'obligation de réparer le préjudice causé à autrui est régie par la loi de l'État où le fait générateur du préjudice est survenu. Toutefois, si le préjudice est apparu dans un autre État, la loi de cet État s'applique si l'auteur devait prévoir que le préjudice s'y manifesterait.*
>
> *Dans tous les cas, si l'auteur et la victime ont leur domicile ou leur résidence dans le même État, c'est la loi de cet État qui s'applique* ».
>
> « *3148. Dans les actions personnelles à caractère patrimonial, les autorités québécoises sont compétentes dans les cas suivants:*
>
> *[...]*
>
> *3. Une faute a été commise au Québec, un préjudice y a été subi, un fait dommageable s'y est produit ou l'une des obligations découlant d'un contrat devait y être exécutée* ».

A la lecture de ces articles, il apparaît possible d'appliquer les dispositions du C.c.Q. tant que l'on peut démontrer l'existence d'un préjudice en sol québécois, ainsi que le fait que gestionnaire du site devait prévoir qu'un tel préjudice puisse se manifester au Québec. Cependant, comme l'affirme la juge McLaughlin dans l'affaire *Zippo* :

> « *At the opposite end are situations where a defendant simply posted information on a Internet website which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercis(ing) of personal jurisdiction* »[374].

---

[374] *Zippo Manufacturing Co.* c. *Zippo Dot Com. Inc.*, (952) F.Supp. 1119 (United States District Court W.D. Pennsylvania), p. 1124.

Quoique cette explication n'ait pas été fournie dans un contexte de responsabilité civile, il n'en demeure pas moins qu'il risque d'être difficile pour une victime de prouver que le gestionnaire du site visait une clientèle québécoise, même si l'aspect international du réseau devrait être un fait notoire.

Cela implique donc que la victime québécoise risque de devoir recourir à un droit étranger pour demander compensation, ce qui en soit, n'est pas nécessairement défavorable[375] pour le demandeur. Toutefois, comme la distribution de matériaux viraux n'est pas prohibée dans la majorité des États en autant que le récipiendaire est conscient de la nature du programme et que le site de distribution n'incite pas à la commission d'un crime[376], la victime peut se retrouver sans droits. De plus, même en admettant la commission d'une faute en sol québécois, encore faut-il que l'État d'où est issu le site négligeant soit conciliant. En effet, l'arrêt *Yahoo !*[377] explique que :

> « *the Internet in effect allows one to speak in more than one place at the same time. Although France has the sovereign right to regulate what speech is permissible in France, this Court may not enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders* »[378].

Comme la majorité des sites de fabrication de virus informatiques que nous avons visités pour cette étude semblent être hébergés aux États-Unis, c'est donc vers nos voisins du sud qu'il importe de se retourner pour évaluer les chances de réussite d'une poursuite intenté par un demandeur québécois en sol américain.

---

[375] Voir affaire Amozo
[376] David HARLEY et al., *op. cit.*, note 3, p. 495.
[377] *Yahoo!, Inc.* c. *La Ligue contre le racisme et l'antisémitisme*, 169 F.Supp.2d 1181.
[378] *Id.*, p. 1192.

D'abord, il faut savoir qu'aux États-Unis, comme au Québec, toute poursuite pénale peut donner lieu à une poursuite civile[379]. C'est donc dire que s'il est possible d'établir l'illégalité des sites de fabrication de virus informatiques, il est également possible d'établir leur responsabilité, en supposant, bien sur, qu'ils causent un dommage[380].

Aux États-Unis, c'est la *National Information Infrastructure Protection Act*[381] (NIIPA) qui régit la transmission de virus informatiques[382]. Ainsi, selon cette loi, quiconque « *knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer* »[383] est passible d'une amende et/ou d'une période d'emprisonnement. Cependant, ce document législatif ne semble pas aborder la responsabilité de celui qui donne à l'individu fautif les outils nécessaires à la création d'un virus.

De plus, la rédaction de la section 1030 pousse certains auteurs comme Kelly Cesare à prétendre que la simple rédaction d'un virus (*malicious code*) n'est pas criminelle si elle n'est pas accompagnée d'une intention d'accéder à un ordinateur sans autorisation. Pour être considéré comme un acte délictuel, le virus doit être transmis volontairement sur un autre ordinateur par courriel, par disquette ou par tout autre moyen de propagation[384].

Ceci ne veut pas pour autant dire que la poursuite du gestionnaire d'un site de fabrication de virus informatique au criminel est impossible. En

---

[379] SUSAN C. LYMAN, *loc. cit.*, note 11, p. 623.
[380] En effet, les principes à la bases du « tort of negligence » américain sont les même que ceux régissant la responsabilité civil, à savoir la présence d'une faute, d'un dommage et d'un lien de causalité entre les deux. Voir Monique C. M. LEAHY, *loc. cit.*, note 204, § 6.
[381] 18 U.S.C. § 1030.
[382] Kelly CESARE, *loc. cit.*, note 6, 147.
[383] Section 1030(a)(5).
[384] Kelly CESARE, *loc. cit.*, note 6, 139.

effet, la doctrine de la facilitation criminelle (*criminal facilitation*) vient criminaliser la publication d'information si l'on peut établir qu'il est loisible de penser que l'information ainsi transmise sera utilisée à des fins illicites[385]. Selon le droit penal américain, « [a] *person is guilty of criminal facilitation* [...] *when, believing it probable that he is rendering aid* [...] *to a person who intends to commit a crime, he engages in conduct which provides such person with means or opportunity for the commission thereof and which in fact aids such person to commit a felony* »[386]. Le cas classique de la facilitation criminelle était celui de l'épicier fournissant de la farine et du sucre à des individus lors de la prohibition[387]. Bien que la vente de farine et de sucre était bel et bien légale à cette époque, certains épiciers furent reconnus coupables parce qu'ils savaient que leurs vivres servaient à l'exploitation d'une activité illicite. Cependant, pour qu'un site de fabrication de virus informatiques tombe sous l'empire de la doctrine de la facilitation criminelle, encore faut-il établir que l'intérêt principal d'une grande partie du public ciblé par le site soit la commission d'un crime[388], ce qui, comme nous l'avons déjà vu, ne devrait causer aucun problème.

Une autre doctrine de *Common law*, la doctrine de l'incitation (*incitement*) pourrait également s'appliquer aux gestionnaires de certains sites de création virale. Selon cette thèse, le fait d'encourager un tiers dans la commission d'un acte illicite constitue en soi un comportement criminel. Ainsi, selon certains auteurs, « *making virus-related material available, such as actual viruses, virus code, information on writing viruses, and virus engines* »[389] pourrait être qualifié d'incitation en *Common law*.

---

[385] Christopher E. CAMPBELL, « Murder Media – Does Media Incite Violence and Lose First Amendment Protection? », (2000) 76 *Chi.-Kent L. Rev.* 637, 647.
[386] N.Y. Penal Law § § 115.00
[387] *Falcone v. United States*, 109 F.2d 579 (2nd. Cir., 1940), aff'd, 311 U.S. 205 (1940).
[388] Christopher E. CAMPBELL, *loc. cit.*, note 385, 647.
[389] David HARLEY et al., *op. cit.*, note 3, p. 494.

Il est également à noter que les États-Unis sont eux aussi signataires de la Convention sur la Cybercriminalité et qu'ils n'ont, à ce jour, soumis aucune rétraction concernant les différentes dispositions du traité. L'analyse faite des articles 4 à 6 de la convention dans la section précédente devrait donc être également valable en droit américain.

Cependant, toute tentative de criminalisation du contenu de sites Internet, aussi malicieux soient-ils, demeure difficile selon l'interprétation particulièrement large qu'ont fait les tribunaux du premier amendement à la Constitution américaine qui, rappelons-le, précise que :

> « *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances* »[390].

Ainsi, comme il en fut le cas dans l'affaire *Yahoo !*[391], les tribunaux pourraient refuser d'admettre l'illégalité de tels sites sous prétexte qu'il s'agit là de la simple manifestation de la liberté d'expression de leurs auteurs. Afin d'établir la responsabilité civile des sites de fabrication de virus informatiques en sol américain, il est donc préférable de démontrer que le contenu de ceux-ci ne peut faire l'objet d'une protection constitutionnelle comme le suggèrent certains auteurs[392].

En 1969, dans l'arrêt *Brandenburg v. Ohio*[393], la cour a établi que la liberté d'expression « *does not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such*

---

[390] U.S. Const. Amend. 1.
[391] *Yahoo!, Inc.* c. *La ligue contre le racisme et l'antisémitisme*, 169 F.Supp.2d 1181 (2001).
[392] Comme l'explique Sarah Gordon, « there are those who argue that virus writing and distribution are not pure speech », ce qui implique que cette « forme d'expression » ne serait donc pas protégée par le premier amendement. Voir Sarah GORDON, *loc. cit.*, note 122.
[393] 395 U.S. 444 (1969).

advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action »[394].

Comme la protection accordée à toute forme d'expression est excessivement large aux États-Unis, la cour exige, pour qu'une quelconque régulation des discours ait lieu, que le gouvernement respecte trois exigences. D'abord, l'orateur ne doit pas seulement promouvoir un acte illicite, mais celui-ci doit être imminent. Ensuite la probabilité de la réalisation de cet acte imminent doit être très forte. Finalement, l'orateur doit avoir l'intention de produire de tels actes illicites[395].

Récemment, c'est dans l'arrêt *Rice* v. *Paladin Enterprises, Inc.*[396] que la responsabilité d'un orateur pour les actes de son auditoire a été rappelée. Dans cette affaire, Paladin, une maison d'édition a été tenue civilement responsable pour la mort d'une dame exécutée selon les directives du livre « *Hit Man: A Technical Manual for Independant Contracters* » publié chez la défenderesse. Le juge a alors établi qu'un jury raisonnable pouvait conclure que la défenderesse était responsable civilement du meurtre de la victime en aidant l'assassin dans sa préparation[397]. Pour ce qui est d'un possible recours au premier Amendement de la constitution, Christopher E. Campbell explique que :

> « *Arguing that Hit Man should be afforded protection under democratic self-government theories of the First Amendment, however, does not work. Hit Man is not espousing contract killings because of a political belief but, instead, is helping would-be assassins get away with murder* »[398].

---

[394] Cass SUNSTEIN, « Is Violent Speech a Right? », (1995) en ligne sur le site *The American Prospect* vol. 6, no. 22 : <http://www.prospect.org/print/V6/22/sunstein-c.html> (dernière mise à jour : 23 juin 1995).
[395] *Id.*.
[396] 128 F.3d 233.
[397] *Id.*, par. 17.
[398] Christopher E. CAMPBELL, *loc. cit.*, note 385, 651.

La décision dans *Rice* a ouvert la porte à une discussion sur le degré de protection constitutionnelle à accorder à d'autres contenus illicites, notamment aux sites de confection de bombes[399]. Comme l'explique Cass Sunstein :

> « *The Brandenburg test was designed to protect unpopular points of view from government controls; it does not protect the publication of bomb manuals. Instructions for building bombs are not a point of view, and if government wants to stop the mass dissemination of this material, it should be allowed to do so. A lower court so ruled in a 1979 case involving an article in the Progressive that described how to make a hydrogen bomb, and the court's argument is even stronger as applied to the speech on the Internet, where so many people can be reached so easily* » [400].

Cette position a, depuis, donné naissance à une nouvelle loi[401] stipulant qu'une recette de confection de bombe ne peut faire l'objet d'une quelconque protection constitutionnelle si celle-ci est rédigée dans un but autre qu'éducatif. Ainsi, dans le cas de sites de confection de bombes, « *a content provider who knew such information could be used in a crime could be prosecuted as an accomplice to a crime* »[402]. Or, les ressemblances entre une recette de confection de bombe et la distribution de code viral sont évidentes, le produit étant, dans les deux cas, dédié à la destruction de biens. De plus, ces deux exemples sont en fait des instructions, des modes d'emploi, il ne s'agit aucunement de textes d'opinion dénonçant le monopole de Microsoft ou le rôle du gouvernement dans l'affaire. Ainsi, il est de notre opinion qu'un tribunal

---

[399] Voir Steven G. GEY, « Fear Of Freedom : The New Speech Regulation In Cyberspace », (1999) 8 *Tex. J. Women & L.* 183 et Ian A. KASS, « Regulating Bomb Recipes on the Internet : Does Frist Amendment Law Permit the Government to React to the Most Egregious Harms? », (1996) 5 *S. Cal. Interdisciplinary L. J.* 83.

[400] Cass SUNSTEIN, *loc. cit.*, note 394.

[401] Nom de la loi

[402] « Bombs on the Internet: New fears about free speech vs. public safety », en ligne sur le site *CNN.com* : <http://www.cnn.com/TECH/science/9805/29/t_t/bombs.on.internet/> (dernière mise à jour : 29 mai 1998).

confronté à la légalité des sites de fabrication de virus informatiques en sol américain n'aura d'autre choix que de se référer à la doctrine et à la jurisprudence disponibles concernant les recettes de bombes.

À la lumière de ce qui précède, nous soumettons donc que les sites de fabrication de virus informatiques ne peuvent bénéficier d'une quelconque protection constitutionnelle pour les exempter de l'application des dispositions pénales quant à leur apport dans la commission d'un crime.

Comme la *National Information Infrastructure Protection Act*, criminalise la diffusion de virus et que la mise en ligne de code viral constitue une « facilitation criminelle » de ce comportement, c'est donc dire que la gestion d'un site de fabrication de virus informatiques peut être considérée criminelle et ce, nous tenons à le souligner, nonobstant la Constitution qui ne peut trouver application dans les circonstances. Or, est-il nécessaire de le rappeler, toute poursuite pénale peut donner lieu à une poursuite civile en droit américain. C'est donc dire qu'il est également possible pour une victime de poursuivre le gestionnaire du site de fabrication de virus en droit civil selon le régime des « *torts* ».

Cependant, selon la jurisprudence, la victime n'a pas besoin d'avancer la notion de facilitation criminelle dès qu'il est établi que celui ayant transmis un virus volontairement est criminellement et donc civilement responsable de ses actes. En effet, comme l'explique la cour dans l'affaire *Paladin*, « *a defendant may be liable in tort if he by any means encourages, incites, aids or abets the act of the direct perpetrator of the tort* »[403]. Cette position est cohérente avec une décision plus récente[404] établissant que le gestionnaire d'un site peut être tenu responsable de l'usage fait de l'information disponible via ses serveurs s'il est

---

[403] *Rice* v. *Paladin Enterprises, Inc.*, précitée, note 366, p. 251.
[404] *A&M Records, Inc.* c. *Napster, Inc.*, 239 F.3d 1004 (Cal., C.A., 2001).

raisonnable de penser que ce dernier avait connaissance du fait que ce contenu était utilisé à des fins illégitimes. Or, comme nous l'avons déjà souligné, cette connaissance s'avère être présente chez les gestionnaires de sites de fabrication de virus informatiques qui prennent la peine d'afficher des clauses de non-responsabilité pour de telles circonstances[405].

c) Le problème de viabilité du gestionnaire de site

Le virus « Melissa » aurait causé plus de 80 millions[406] de dollars de dommages, « InterNet » en aurait causé pour plus de 98 millions[407] ; même si les créateurs de ces virus sont connus, et même si l'on réussit à établir leur responsabilité, il est peu probable qu'ils puissent assumer les coûts associés à la réparation du préjudice causé en plus de leurs frais juridiques[408]. En effet, « *the typical virus writer is young, almost invariably male, and tends to "grow out" of the virus writing game as soon as he gets a real life* »[409]. De plus, ces individus agissent normalement seul, sans affiliation quelconque à un organisme ou une communauté pouvant débourser pour réparer les dommages causés[410]. C'est donc dire que, dans la majorité des cas, les auteurs de virus sont insolvables.

Cette présomption semble également s'appliquer à la plupart des sites de création de virus informatiques qui sont, plus souvent qu'autrement, situés sur des serveurs gratuits ou dont les frais sont négligeables[411], ce qui laisse supposer qu'ils ne bénéficient pas nécessairement de moyens

---

[405] Voir la sous-section 2 c) de la présente section.
[406] Kevin POULSEN, *loc. cit.*, note 365.
[407] MUND, A.J., « Organisational Liability Exposure : A Conceales Virus Threat », (1990) en ligne sur le site <http://www.cmcnyls.edu/papers/VIRUSES.TXT> (date de visite : 10 janvier 2002).
[408] *Id.*
[409] David HARLEY et al., *op. cit.*, note 3, p. 441. Voir également ANONYME, *op. cit.*, note 20, p. 327.
[410] ANONYME, *op. cit.*, note 20, p. 327-328.
[411] C'est la cas, par exemple, du site <http://casiofr.free.fr/virus.htm>.

suffisants pour obtenir leur propre domaine, encore moins pour dédommager leurs victimes.

Selon plusieurs experts, les gestionnaires de tels sites sont souvent d'anciens ou de futurs pirates informatiques (*hackers*), c'est-à-dire des « *criminels informatiques qui exploitent les failles dans une procédure d'accès pour casser un système informatique, qui violent l'intégrité de ce système en dérobant, altérant ou détruisant de l'information, ou qui copient frauduleusement des logiciels* »[412]. Or, « *[a] hacker is probably a kid or a criminal, somebody who's going to spend all his money on a lawyer, not somebody from whom you can recoup* »[413], ce qui implique que les coûts juridiques dépasseront souvent la valeur d'un quelconque règlement[414], agent dissuasif important pour les victimes.

Ainsi, la responsabilisation des gestionnaires de sites de création de virus informatiques ou des individus dont les logiciels nourrissent ces sites, quoiqu'une avenue intéressante pour les juristes, ne s'avère pas des plus prometteuses d'un point de vue pratique, puisque des problèmes de ressources peuvent décourager la majorité des victimes, d'autant plus qu'ils risquent de se retrouver devant un défendeur insolvable ou, du moins, qui ne possède pas de moyens financiers suffisants pour assurer un quelconque dédommagement[415].

En effet, celui qui poursuit un site de fabrication de virus informatiques dans le but d'obtenir une pleine restitution des dommages causés s'aventure dans une entreprise sans réelle chance de réussite. C'est

---

[412] OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[413] Jennifer Stisa GRANICK, dans Robyn WEISMAN, *loc. cit.*, note 28.
[414] Pamela SAMUELSON, *op. cit.*, note 253, p.473.
[415] Il s'agit là d'une démonstration du fait que la fonction première de la responsabilité civile, à savoir la réparation du préjudice subi par la victime est inefficace dans le cas de tels sites. Ici, c'est la fonction seconde de la responsabilité civile, c'est-à-dire la fonction préventive qui s'avère la plus intéressante puisqu'elle s'avère être la seule raison concrète pouvant expliquer l'application du régime de responsabilité civile aux gestionnaires de tels sites.

pourquoi nous nous proposons maintenant d'étudier d'autres avenues de restitution pour les victimes de virus informatiques, à savoir la poursuite de tiers dont l'absence de diligence a permis l'infection.

B. La responsabilité civile des agents à l'origine de la diffusion de virus informatiques sur Internet

Comme nous venons de l'aborder, la poursuite des individus à l'origine de la création et de la diffusion de virus informatiques peut s'avérer ardue et peu bénéfique économiquement. C'est pour cette raison que de plus en plus d'auteurs suggèrent plutôt de recourir aux principes[416] établis dans l'arrêt *T.J. Hopper* c. *Northern Barge*[417] et de poursuivre les intermédiaires dans la transmission dont le refus d'adopter les technologies nécessaires à la protection de leur réseau équivaut à une faute au sens du *Code civil du Québec*[418], puisque ces intermédiaires (surtout lorsqu'ils sont commerciaux) sont normalement plus viables financièrement que les auteurs des virus et leurs collaborateurs[419]. Comme l'explique Perritt, il ne devrait pas incomber à la victime d'une attaque de supporter seule le fardeau des dommages causés par celle-ci[420]. La responsabilisation des intermédiaires reste alors la seule option viable :

> « *Tort liability imposed on an intermediary is a kind of default rule or safetynet, recognizing that there may be instances in which the person with fault - the originator of*

---

[416] Voir la section I B du présent mémoire pour une analyse de ces principes.
[417] Précitée, note 192.
[418] Voir PISA, *loc. cit.*, note 6, Brian R. BAWDEN, *loc. cit.*, note 193, 34, Robyn WEISMAN, *loc. cit.*, note 28. et Rob GALLAGHER, « Victim or Vilain? Viral Liability: Guard against viruses or face legal action », (2001) en ligne sur le site *FAB IT Solutions* : <http://www.fabit.com/antivirus/businesliab.asp> (dernière mise à jour : 17 août 2001).
[419] Richard B. LEVINE, *op. cit.*, note 26, p. 254.
[420] Henry H. PERRITT Jr., « Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction », (1995) en ligne sur le site du *Chicago-Kent College of Law Cyberlaw Jurisdiction* : <http://www.kentlaw.edu/cyberlaw/resources/interjuris.html> (dernière mise à jour : 12 octobre 1995).

> *the harmful message or file - would be unavailable, beyond the jurisdiction of any tribunal available to the victim, or judgment proof. Thus, the policy question for intermediary liability is whether the victim should bear the loss when the originator cannot be found, or conversely when the intermediary should bear the loss* »[421].

Comme nous l'avons déjà souligné à maintes reprises, encore faut-il que ces individus aient été négligents. Plus encore, la loi doit autoriser leur responsabilisation ce qui, dans le cas des intermédiaires techniques, n'est pas nécessairement le cas. Nous nous pencherons donc sur la responsabilité de ces derniers (1), mais également sur celle des gestionnaires de sites Web contaminés (2), ainsi que les personnes – tant morales que physiques – qui propagent inconsciemment les virus par courriel (3).

1. Les intermédiaires techniques

Comme le souligne Pierre Trudel, les intermédiaires techniques représentent « *des personnes, entreprises ou organismes qui interviennent dans l'accomplissement d'une tâche effectuée entre le point d'expédition d'une transmission de document et le point de réception final* »[422]. Le professeur Trudel souligne également que ces intervenants ont en commun le fait qu'ils n'exercent aucun droit de regard sur l'information qui transite via leurs « environnements technologiques »[423]. C'est cette dernière spécificité des intermédiaires techniques qui complique leur responsabilisation dans le cadre de la transmission de virus informatiques. Toutefois, comme nous le verrons, ceux-ci pourraient, s'ils le désiraient, mettre sur pied certains dispositifs relatifs à la sécurité de leur clientèle sans modifier leur rôle

---

[421] *Id.*
[422] Pierre TRUDEL, « La responsabilité civile sur Internet selon la *Loi concernant le cadre juridique des technologies de l'information* », (2001) 160 *Développements récents en droit de l'Internet* 107, 114.
[423] *Id.*

d'intermédiaire neutre. La question de la responsabilité civile de ces intervenants nous ramène donc à l'éternel débat entre le devoir de protection des intermédiaires et les différents droits des utilisateurs[424]. Pour relancer ce débat, nous aborderons les intermédiaires techniques les plus aptes à participer à la transmission de virus sur Internet, à savoir les transmetteurs (a), les hébergeurs (b) et les intermédiaires offrant des services de références à des documents technologiques (c).

a) Les transmetteurs

Par l'expression transmetteur, nous renvoyons à la notion de « *prestataire de services qui agit à titre d'intermédiaire pour fournir les services d'un réseau de communication exclusivement pour la transmission de documents technologiques sur ce réseau* »[425]. Sont ainsi considérés des « transmetteurs » pour les propos qui suivent les fournisseurs d'accès Internet (F.A.I.) et les services de messagerie.

Il importe d'abord de souligner que la transmission d'un virus mettra nécessairement en cause la participation d'un minimum de deux transmetteurs, à savoir celui du diffuseur du virus et celui de la victime :

---

[424] Comme l'expliquent Pierre Trudel et Robert Gérin-Lajoie : « [p]*uisque les gestionnaires des réseaux sont les portiers donnant accès aux environnements électroniques ouverts, c'est autour des relations qu'ils entretiennent avec leurs usagers qu'émergent certaines normes et processus de régulation susceptible de procurer un équilibre entre la liberté d'expression et la protection des droits des personnes et des autres valeurs fondamentales. Dans un tel contexte, les administrateurs de réseaux apparaissent comme les portiers à qui on demande parfois de devenir gendarmes afin de protéger les droits de propriété intellectuelle ou les valeurs morales.* [...] *Se pose alors la question du cadre de leur intervention et des limites qu'il conviendrait de fixer à leurs pouvoirs et prérogatives. Les régulations qui s'observent dans ce genre de contextes sont souvent liées aux missions assignées aux réseaux.* [...] *C'est au nom de la protection de* [ces missions] *du réseau et aussi de la garantie de son intégrité que les administrateurs de réseaux justifient leur intervention* ». Pierre TRUDEL et R. GÉRIN-LAJOIE, « La protection des droits et des valeurs dans la gestion des réseaux ouverts », dans Daniel POULIN, Pierre TRUDEL et Ejan MACKAAY (dir.), *Les autoroutes électroniques : usages, droits et promesses*, Montréal, Éditions Yvon Blais, 1995, p. 279 , aux pages 303 et 304.

[425] Article 36 de la *Loi concernant le cadre juridique de technologies de l'information.*

> « *L'auteur ou l'offreur de virus informatiques fera usage d'un fournisseur de service pour amener son information sur internet. Le consommateur reçoit également un accès via son fournisseur de service au réseau et donc aux virus* »[426].

Bien qu'il est fort probable que ces deux transmetteurs soient réunis dans une même entité – lorsque les deux intervenants font affaires avec le même F.A.I. ou le même service de messagerie – il demeure que les recours intentés n'auront pas les mêmes assises juridiques.

En effet, la victime d'une attaque virale désirant poursuivre son propre transmetteur pour la transmission d'un virus informatique ne devra pas forcément recourir aux principes de l'article 1457 C.c.Q. puisqu'elle est contractuellement liée à celui-ci. Elle devra dans certains cas invoquer un manquement au contrat[427], ce qui s'avère évident lorsque le transmetteur offre un service de balayage des documents[428], mais impossible lorsque le transmetteur limite sa responsabilité quant aux infections virales dans le cadre du contrat. Concernant ce dernier point, il importe cependant de préciser que, si la victime de l'infection est un consommateur, toute clause contractuelle limitant la responsabilité du transmetteur malgré sa faute sera réputée non écrite[429].

Mais qu'en est-il lorsque le contrat ne fait pas mention de la responsabilité du transmetteur dans le cas d'infections virales? Peut-on supposer qu'une garantie de sécurité des documents fait implicitement partie du contrat? Bien que ces questions demeurent sans réponse, notons que le législateur prévoit qu'un contrat de transport d'un bien matériel implique nécessairement la responsabilité du préjudice résultant

---

[426] PISA, *loc. cit.*, note 6.
[427] Article 1458 C.c.Q.
[428] C'est l'opinion de Gerard MANNIG: « *devien*[t] *coupable de propagation de virus par negligeance* [...] *le FAI qui pretend - grande mode actuelle, concurrence oblige - offrir un filtre antivirus* ». Gérard MANNIG, propos transmis à la liste de discussion droit-net@cru.fr le 25 août 2002.
[429] Article 10 L.p.c.

du transport[430], mais ne mentionne aucune forme de responsabilité quant aux préjudices subséquents. Imposer implicitement un fardeau plus volumineux aux transmetteurs sur Internet serait donc difficilement conciliable avec les dispositions du code concernant les contrats de transport.

Que l'on se situe dans un contexte contractuel ou extracontractuel, il n'en demeure pas moins que la question reste la même, c'est-à-dire « *dans quelle mesure les* [transporteurs] *peuvent être rendus responsables pour l'information qui est diffusée par leurs services* »[431].

Afin d'établir la portée de la responsabilité des transmetteurs dans le cas de la transmission de virus informatiques, il est proposé par certains auteurs de recourir aux règles déjà applicables à ces entreprises dans le cadre des lois régissant la propriété intellectuelle et la diffamation et de les appliquer *mutatis mutandis* à la diffusion de virus informatiques via Internet[432].

Cette proposition a pour mérite de rendre la situation plus facile à discerner. Aux États-Unis, par exemple, l'état du droit sur cette question devient clair. En effet, selon la législation en vigueur, toute poursuite en responsabilité civile à l'encontre de F.A.I. est proscrite[433], il suffirait donc d'étendre cette proscription aux virus informatiques de façon jurisprudentielle.

Pour ce qui est de la situation au Québec, c'est la *Loi concernant le cadre juridique des technologies de l'information* qui régit la part de

---

[430] Article 2049 C.c.Q.
[431] PISA, *loc. cit.*, note 6.
[432] *Id.*
[433] Communications Decency Act, 47 U.S.C. §230. Voir Sarah FAULKNER, « Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks », (2000) 18 *J Marshall J. Computer and Info. L.* 1019, 1045.

responsabilité à accorder aux fournisseurs d'accès Internet. Les dispositions pertinentes du texte de loi sont reproduites ci-après :

> **27.** Le prestataire de services qui agit à titre d'intermédiaire pour fournir des services sur un réseau de communication ou qui y conserve ou y transporte des documents technologiques n'est pas tenu d'en surveiller l'information, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités à caractère illicite.
>
> **36.** Le prestataire de services qui agit à titre d'intermédiaire pour fournir les services d'un réseau de communication exclusivement pour la transmission de documents technologiques sur ce réseau n'est pas responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité.
>
> Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui :
>
> 1° en étant à l'origine de la transmission du document;
> 2° en sélectionnant ou en modifiant l'information du document;
> 3° en sélectionnant la personne qui transmet le document, qui le reçoit ou qui y a accès;
> 4° en conservant le document plus longtemps que nécessaire pour sa transmission.
>
> **37.** Le prestataire de services qui agit à titre d'intermédiaire pour conserver sur un réseau de communication les documents technologiques que lui fournit son client et qui ne les conserve qu'à la seule fin d'assurer l'efficacité de leur transmission ultérieure aux personnes qui ont droit d'accès à l'information n'est pas responsable des actions accomplies par autrui par le biais de ces documents.
>
> Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui :
>
> 1° dans les cas visés au deuxième alinéa de l'article 36;

> 2° en ne respectant pas les conditions d'accès au document;
> 3° en prenant des mesures pour empêcher la vérification de qui a eu accès au document ;
> 4° en ne retirant pas promptement du réseau ou en ne rendant pas l'accès au document impossible alors qu'il a de fait connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau, du fait qu'il n'est pas possible aux personnes qui y ont droit d'y avoir accès ou du fait qu'une autorité compétente en a ordonné le retrait du réseau ou en a interdit l'accès.

À la lecture de ces articles, il serait donc impossible de prétendre à la responsabilité civile des transporteurs lorsqu'ils n'adoptent aucun rôle supplémentaire. À première vue, cette position s'avère logique puisqu'il n'est pas du rôle du transporteur de contrôler le contenu visité ou téléchargé par ses utilisateurs. S'il le faisait, ces derniers pourraient prétendre à une violation de leur vie privée[434]. Cependant, les dispositions de la loi citée ci-haut n'ayant pas été rédigées dans l'optique de la transmission de virus informatiques, leur application à cette problématique ne peut être considérée comme étant automatique, les virus ne constituant pas, à nos yeux, des « documents » au sens de la loi.

Afin d'établir si les dispositions de la *Loi concernant le cadre juridique des technologies de l'information* pourraient trouver application dans le contexte de la transmission de virus informatiques et donc exonérer les F.A.I. et les exploitants de services de messagerie, il importe, comme le suggère Pierre-André Côté, de tenter de cerner l'intention du législateur lors de la rédaction de ces dispositions[435]. Ainsi, en lisant la version annotée de la loi[436], on peut y lire que l'un des objectifs visés par la déresponsabilisation des intermédiaires techniques est de protéger la

---

[434] Article 36 2° C.c.Q.
[435] Pierre-André CÔTÉ, *Interprétation des lois*, 3e éd., Montréal, Thémis, 1999, p. 7.
[436] CRDP, 2001.

liberté d'expression[437]. Or, comme nous l'avons déjà mentionné dans la section précédente, un virus informatique peut difficilement être considéré comme une forme d'expression. Un autre des objectifs de la loi, celui-ci découlant des notes explicatives du texte, est d'assurer la protection de la vie privée des utilisateurs du réseau. En effet, tenir les exploitants de services de messagerie responsables du contenu des courriels transmis par leur entremise reviendrait à obliger ces derniers à lire les messages de leurs clients, ce qui va à l'encontre de l'article 36 (2°) du *Code civil du Québec*. Précisons toutefois que le balayage de courriels à l'aide d'un logiciel antivirus ne nécessite ni l'ouverture du message, ni le contrôle de son contenu. En fait, les virus informatiques étant des programmes distincts des fichiers auxquels ils se rattachent, leur repérage et subséquente destruction ne viendraient en aucun cas affecter le contenu du message, pas plus que son intégrité, qualité également exigée par la loi.

À la lumière de ce qui précède, il est de notre opinion que les dispositions de la *Loi concernant le cadre juridique des technologies de l'information* concernant la responsabilité civile des F.A.I. et des exploitants de services de courriel ne peuvent être appliquées pour limiter la responsabilité de ces intervenants dans le cadre d'une infection virale, auxquels cas il importe d'aménager un cadre juridique propre à cette problématique. Voyons en premier lieu la situation des fournisseurs d'accès Internet.

i. Les fournisseurs d'accès Internet (F.A.I.)

Comme l'explique un auteur, on ne peut raisonnablement rendre le serveur responsable des dommages causés par la simple utilisation du

---

[437] *Id.*, p. 21.

réseau[438]. Cette présomption ne saurait cependant relever le F.A.I. de toute obligation de diligence, puisque ce dernier doit tout au moins prendre toute mesure appropriée pour sévir et éventuellement exclure un usager indélicat[439]. En effet, les F.A.I. « *clearly have a duty to avoid foreseeable, unjustified harm to others. Sysops should take action to prevent criminal or tortious conduct, once they have notice of the risk* »[440].

C'est pourquoi certains auteurs suggèrent tout de même la mise en cause des F.A.I. dans le cadre d'infections virales accentuées par leur négligence :

> « *Ne pas oublier d'y mettre en cause le Internet Service Provider* [...] *utilisé pour lancer une telle attaque si la preuve démontre qu'une tierce partie devrait raisonnablement avoir dû prendre certaines mesures pour se protéger de ces attaques et empêcher une telle attaque ce qu'elle n'a manifestement pas réussi à faire* »[441].

Cette position, comme l'explique Michael Geist, peut être reliée au fait que, contrairement aux croyances populaires, les F.A.I. ne sont pas nécessairement aussi passifs qu'ils pourraient le prétendre :

> « *The information possessed by ISPs appears to belie their claims of helplessness. For example, in a two week span in early April 1999, two suspects were apprehended for virus and stock hoaxes. In each instance, it was an ISP (AOL) that played an integral role in the investigation by providing law enforcement officials with access data records. The ISP's ability to cooperate under*

---

[438] 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, 167, 205.
[439] *Id.*
[440] David R. JOHNSON et Kevin A. MARKS, « Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let our Conscience (and our Contracts) Be our Guide? », (1993) 38 *Vill. L. Rev.* 487, 497.
[441] A GAGNON, « Que faire en cas d'attaque de vos systèmes informatiques par un pirate », (2002) 13 *Le monde juridique* 29, 33.

> *circumstances mandated by legal necessity suggests that they may possess greater access to data than they might have the public believe* »[442].

En effet, « *If AOL does not like a certain behaviour, then in at least some cases it can regulate that behaviour by changing its architecture* [...] *if there is a virus problem caused by people uploading infected files, it can run the files automatically through virus checkers* »[443]. Cette possibilité est d'autant plus viable qu'elle est mise de l'avant par un nombre grandissant de F.A.I. qui y voient une façon d'offrir un meilleur service à leur clientèle sans compter qu'ils y trouvent une opportunité d'augmenter leurs tarifs[444]. Cependant, si un F.A.I. offre de tels services et, par leur entremise, détruit ou modifie un fichier, il pourrait alors engager sa responsabilité en vertu de l'article 36 (2°) de la *Loi sur le cadre juridique des nouvelles technologies de l'information*. Ce cercle vicieux s'étend d'ailleurs aux services de messagerie lesquels nous abordons maintenant.

ii. Les services de messagerie

La responsabilité civile de l'exploitant d'un service de messagerie électronique pourrait être engagée, aux yeux de certains, si la victime d'un virus peut établir que le maliciel lui a été transmis par un courriel reçu via ce serveur de messagerie[445]. Cependant, nous nous retrouvons alors avec une problématique identique à celle des fournisseurs d'accès, d'autant plus que ces deux services sont normalement assurés par une même entité.

---

[442] Michael GEIST, *Internet Law in Canada*, North York, Captus Press, 2000, p. 69-70.
[443] Lawrence LESSIG, *op. cit.*, note 84, p. 71.
[444] « The Anti-Virus Can of Worms », (2001) en ligne sur le site *ISP-Planet* : <http://www.isp-planet.com/services/2001/av_bol.html> (dernière mise à jour : 13 décembre 2001).
[445] Alain BLOCH, *loc. cit.*, note 12, 52.

Si la problématique est la même, la solution proposée est également identique, c'est-à-dire l'utilisation d'un outil de filtrage situé sur le serveur permettant ainsi l'élimination de tout virus attaché à un message[446]. Cette technologie aurait en effet l'avantage de réduire la responsabilité attribuable au gestionnaire du service de messagerie[447]. De plus, grâce à l'efficacité des logiciels actuels, le balayage d'un courriel peut être exécuté en quelques secondes, ce qui n'aurait pratiquement aucun impact sur la vitesse de transmission des messages[448].

Cependant, permettre la responsabilité des services de messagerie soulève une autre problématique. En effet, que se produira-t-il lorsqu'un logiciel antivirus obtiendra un faux-positif – c'est-à-dire lorsqu'il identifiera un virus qui n'en est pas un – ou lorsqu'il éliminera un message contenant un virus dont l'utilisation était légitime[449]. Une telle situation pourrait se produire, par exemple, lorsque la victime d'un nouveau virus transmet celui-ci à l'entreprise lui ayant vendu son logiciel antivirus dans le but de développer un remède et d'éviter une épidémie. En effet, il ne faudrait pas perdre de vue le fait qu'un virus en soi n'est pas un logiciel interdit et donc que son transfert entre deux personnes consentantes et éclairées n'est ni illégal, ni illégitime.

La meilleure solution présentement en application est, à nos yeux, celle mise de l'avant par le service de messagerie Yahoo! Mail. Sans effectuer mécaniquement un balayage de tous les messages reçus, ce service de messagerie offre à ses abonnés un service antivirus gratuit et

---

[446] James STANGER, *op. cit.*, note 127, p. 399. Un système semblable est d'ailleurs mis de l'avant par le service de messagerie en ligne *Hotmail* de *Microsoft* (<http://www.hotmail.com>). Comme il est indiqué sur le site du service : « *MSN Hotmail a développé la fonctionnalité de détection des virus GRATUITE. Hotmail utilise la solution de détection McAfee.com pour analyser les pièces jointes dans les messages entrants ! Maintenant, vous pouvez profiter d'une meilleure expérience en ligne parce que Hotmail analyse automatiquement toutes les pièces jointes que vous recevez* ».

[447] James STANGER, *op. cit.*, note 127, p. 401.

[448] *Id.*, p. 404-405

[449] *Loc. cit.*, note 444.

rappelle que le balayage est de mise avant l'ouverture de tout fichier reçu par courriel. L'utilisateur ne désirant pas soumettre ses fichiers à un balayage n'est pas tenu de le faire, mais il sera alors bien mal venu de poursuivre le service de messagerie en cas d'infection causée par ce même fichier.

Nonobstant tout ce qui précède, la situation entourant la responsabilité des F.A.I. et des services de messagerie demeure nébuleuse et, bien qu'il soit pour l'instant difficile d'établir ce qui peut constituer un comportement négligent dans le cas de telles entreprises, nous soumettons qu'un transmetteur offrant systématiquement un service d'antivirus sans toutefois obliger le balayage de fichiers ne pourrait se faire reprocher l'infection d'un de ses utilisateurs, en supposant, bien sûr, que cet antivirus soit maintenu à jour.

iii) Pourquoi poursuivre les transmetteurs?

Puisque la faute des transmetteurs semble, pour l'instant, difficile à établir dans le contexte de la transmission de virus informatiques, il importe de se questionner sur l'opportunité d'enclencher une quelconque procédure à leur encontre. Or, malgré les incertitudes soulevées, une poursuite des transmetteurs en responsabilité civile offre des avantages notoires pour la victime comparativement à un éventuel recours contre tout autre débiteur potentiel. D'abord, ces entreprises sont normalement solvables et assurées, ce qui facilitera le dédommagement de la victime. De plus, le fardeau de preuve concernant le lien de causalité entre la faute et le dommage devient beaucoup moins imposant lorsque le défendeur est un transmetteur.

Un virus ne peut s'infiltrer sur un système informatique que de trois façons distinctes : par support matériel (disquette), il peut naître sur l'ordinateur, c'est-à-dire y être directement programmé ou, finalement, il

peut y migrer via le réseau Internet. Dans toute poursuite en responsabilité civile concernant un intermédiaire, il faudra donc, en tout premier lieu, établir le vecteur employé. Une telle preuve devient aisée si l'on est capable de démontrer que seul un nombre restreint d'individus ont eu accès au poste et que ceux-ci n'ont pas créé le virus. Cette preuve sera d'autant plus simple à faire s'il est possible de retrouver le fichier infecté et d'associer celui-ci à un site Web ou à un courriel reçu par la victime. Même lorsqu'il est difficile, voire impossible, de retracer le fichier hôte, il demeure que, statistiquement, les chances que l'infection découle du réseau sont très élevées[450], ce qui peut s'avérer être un argument très persuasif pour faire pencher la balance des probabilités en faveur de la victime.

L'accès à Internet devant nécessairement impliquer la présence d'un transmetteur, le lien de causalité entre l'infection de la victime et le comportement du transmetteur devient incontestable. Il n'est alors guère nécessaire de pousser plus loin l'étude de la preuve contrairement à tout autre intervenant dont le rôle ne saurait être présumé. Néanmoins, puisque, comme le soulignent Baudouin et Deslauriers, la preuve du lien de causalité est souvent plus facile à faire que celle de la faute du défendeur de par la latitude normalement accordée au demandeur par les tribunaux[451], nous soumettons que toute action contre un transmetteur, même envisageable, entraîne nécessairement un fardeau de preuve plus lourd qu'une action contre un tiers ayant participé plus directement à la transmission.

---

[450] En effet, « *more than 80 percent of viruses use e-mail as the principal means of propagation* ». *Loc. cit.*, note 97.

[451] Voir Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 347 et 348.

b) Les hébergeurs

Au premier coup d'œil, établir la responsabilité civile de l'hébergeur ou plutôt l'absence d'une telle responsabilité est beaucoup moins problématique que pour les services de messagerie et les F.A.I. En effet, selon la *Loi concernant le cadre juridique des technologies de l'information*,

> « *Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci.*
>
> *Cependant, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité* »[452].

En appliquant la logique découlant de cet article aux virus informatiques, l'hébergeur n'engage sa responsabilité civile que s'il est avisé de la présence d'un virus informatique sur l'un des sites qu'il héberge et qu'il omet de procéder promptement à l'élimination de ce programme[453]. Ceci s'avère une solution efficace lorsqu'il est question, par exemple, d'un virus ayant été inclus dans les fichiers à télécharger sur un site « respectable » par un pirate informatique. Mais qu'en est-il des entreprises qui hébergent des sites de fabrication de virus informatiques

---

[452] Article 22 al. 1 et 2 de la *Loi concernant le cadre juridique des technologies de l'information.*

[453] . C'est d'ailleurs la solution prônée par Éric Labbé et al. : « *l'hébergeur n'est pas responsable des intrusions de pirates informatiques. Il doit néanmoins faire preuve de bonne foi et de diligence. En général, sa responsabilité sera rejetée s'il met en place des mesures de surveillance des serveurs et agit dans un délai raisonnable pour remédier à l'intrusion et à ses conséquences* ». Éric LABBÉ et al., *Le guide juridique du commerçant électronique*, Version préliminaire pour distribution au Symposium International 2001 : Internet, commerce électronique, droit et arbitrage, 26 au 28 avril 2001, Gammarth, Tunisie, p. 73.

tels que définis préalablement[454]? Bien que, comme nous l'avons mentionné dans la section précédente, nous croyons qu'une majorité de ces sites devraient remplir le critère d'« apparence illicite » de par leurs propres prétentions, nous ne pouvons pour l'instant que spéculer au sujet de ce même critère pour d'autres sites plus « scientifiques ». Cette problématique représente d'ailleurs un dilemme tant éthique que juridique pour les hébergeurs[455], comme le souligne l'un d'eux :

> « *Viruses and information relating to viruses are not, at this time, controlled code. We allow users to make available via anonymous FTP any and all data as long as it is legal, which viruses, viral source code, and newsletters published by virus groups are* »[456].

Cependant, les hébergeurs nord-américains adoptant cette position semblent peu nombreux. En effet, il n'est pas rare de voir les sites de fabrication de virus informatiques changer d'adresse périodiquement, soit à chaque fois que l'hébergeur est avisé du caractère illicite ou socialement inacceptable de certaines informations contenues sur ses pages[457]. C'est donc dire que si leur responsabilité juridique est contestable, leur responsabilité sociale – guidée par leur image commerciale – semble établie.

c) Les intermédiaires offrant des services de références à des documents technologiques[458]

Les intermédiaires visés ici sont, comme le souligne la *Loi concernant le cadre juridique des technologies de l'information*, tous ceux offrant « *des services de référence à des documents technologiques, dont un index,*

---

[454] Voir la section II A du présent mémoire.
[455] Sarah GORDON, *loc. cit.*, note 122.
[456] *Id.*
[457] Le site coderz.net, par exemple, s'est souvent plaint de devoir changer d'hébergeur de façon périodique, ce qu'il a fait à au moins une reprise durant la présente étude.
[458] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 607. à la page 628.

des hyperliens, des répertoires ou des outils de recherches »[459]. Il est ainsi question des sites offrant des hyperliens vers d'autres sites, ou encore d'engins ou moteurs de recherches. Q'en est-il de la responsabilité des gestionnaires de tels sites lorsqu'ils créent un lien vers un fichier infecté. L'exemple idéal de cette problématique est le moteur de recherche *Google*[460] qui permet d'accéder directement à des documents *Word* (.doc), fichiers utilisés, entre autres, pour la transmission de macrovirus. Bien que le fichier infecté n'est pas situé sur les serveurs de *Google*, il n'en demeure pas moins que le site est directement responsable de la mise en contact avec le fichier infecté.

Dans le cadre de la *Loi concernant le cadre juridique des technologies de* l'information, tout comme les hébergeurs, les intermédiaires offrant des services de références à des documents technologiques ne sont pas responsables des activités accomplies par leur biais, mais peuvent engager leur responsabilité dans le cas où ils sont informés du fait que leurs services « *servent à la réalisation d'une activité à caractère illicite* » et qu'ils ne cessent pas de fournir ces services[461]. Il serait convenable d'utiliser cette même logique lors de l'évaluation de leur responsabilité civile dans le contexte de la transmission de virus informatiques puisqu'il demeure que l'élimination du fichier infecté n'est pas de leur ressort. En effet, avant d'engager la responsabilité de tels intermédiaires, encore faut-il prouver une faute de leur part. Puisqu'ils n'ont aucun contrôle sur le contenu des documents infectés, il devient difficile de souligner un quelconque manquement à leur obligation de diligence.

---

[459] Article 22 de la *Loi concernant le cadre juridique des technologies de l'information.*
[460] <http://www.google.com>.
[461] Article 22 de la *Loi concernant le cadre juridique des technologies de l'information.*

2. Les ressources Internet

Ce serait un cliché de rappeler l'aspect commercial du réseau Internet et d'en souligner les conséquences. Mentionnons simplement qu'il existe actuellement de multiples moyens d'obtenir de l'information via le réseau Internet, comme, par exemple, les milliers de sites Web permettant le téléchargement de fichiers soit à titre gratuit, soit contre compensation. Or, ces fichiers sont souvent la cible de pirates informatiques qui viennent leur annexer un maliciel quelconque dans le but d'infecter un plus grand nombre d'internautes. Peut-on reprocher aux propriétaires de tels sites d'avoir été victimisés?

Selon certains experts, la réponse à cette question doit être affirmative. En effet, comme le souligne A. Gagnon, la victime d'un virus lui ayant été transmis via un site Web ne devrait pas oublier de mettre en cause :

> « *le propriétaire du site web (à son insu) utilisé pour lancer une telle attaque si la preuve démontre qu'une tierce partie devrait raisonnablement avoir dû prendre certaines mesures pour se protéger de ces attaques et empêcher une telle attaque ce qu'elle n'a manifestement pas réussi à faire* »[462].

Cette position, comme nous le verrons sous peu, est conforme à la jurisprudence française en la matière. Nous aborderons ainsi, dans la présente section, les sites Web utilisés dans la transmission de virus informatiques, à savoir les sites offrant le téléchargement de fichiers (a) et les babillards électroniques (b), mais également les autres ressources accessibles grâce à une connexion au réseau Internet pouvant permettre la transmission de virus informatiques, à savoir les listes de diffusion et les groupes *Usenet* (c). Nous survolerons par la suite les possibilités de déresponsabilisation contractuelle des gestionnaires de telles ressources (d).

---

[462] A. GAGNON, *loc. cit.*, note 441, 33.

a) Les sites Web permettant le téléchargement de fichiers

Comme nous l'avons déjà établi, le régime de responsabilité civile exige que la victime fasse la preuve d'une faute ou, tout au moins, d'un acte négligent de la part d'un tiers pour être dédommagée. Cependant, dans le contexte de la diffusion de virus informatiques via un site Web alors que le distributeur du logiciel ou du programme infecté ne sait pas que son fichier a été corrompu, la faute sera plus difficile à établir[463] que dans le contexte d'une diffusion par courrier électronique, puisque l'infection aura normalement lieu suite à la mise en ligne du fichier et non conjointement à celle-ci.

Il est possible de trouver une solution à cette problématique dans la jurisprudence. Dans l'une des rares décisions portant sur la responsabilité civile dans le cadre de la transmission de virus informatiques, l'affaire française *Exa publications*[464], il a été établi par le tribunal que le distributeur d'un logiciel était responsable des dommages causés par un virus subséquemment glissé dans celui-ci par un tiers. Dans cette affaire, la société défenderesse était éditrice d'une revue intitulée « Soft & Micro » à laquelle fut incorporée une disquette gratuite infectée malencontreusement par le virus Fredo. Bien que les responsables de la revue n'étaient pas conscients de l'infection, la cour les obligea tout de même à indemniser toutes les victimes dudit virus l'ayant contracté par le biais de leur disquette[465].

Découle de cette décision qu'une société de service ou un distributeur qui transmet un virus à l'un de ses clients peut être tenue civilement

---

[463] Raymond T. NIMMER, *The Law of Computer Technology: rights, licenses, liabilities*, 3e éd., St-Paul, West Group, 1997, § 6:31.
[464] Cour de cassation, Chambre commerciale, 25 novembre 1997 (France).
[465] « L'éditeur de Soft & Micro responsable des conséquences de l'infection », (1998) 112 *Expertises des systèmes d'information* 414.

responsable et condamnée aux dommages et intérêts[466]. De plus, comme le souligne la cour dans cette affaire, « *le risque de contamination par un virus est un fait connu dans le domaine informatique, ayant suscité une abondante littérature ainsi que la mise au point de logiciel de détection et de suppression des virus et d'une véritable stratégie de défense à l'égard de ces risques d'invasion* »[467].

Ainsi, le fait pour une entreprise produisant ou distribuant des logiciels de ne pas prendre les mesures de sécurités adéquates pour prévenir l'infection – par sa faute – de ses clients, constitue une faute au sens de l'article 1457 du Code[468]. Or, comme le souligne Meiring de Villiers, l'opérateur d'un site Web n'est en fait qu'un distributeur, ce qui laisserait sous-entendre qu'un tel site aurait les mêmes responsabilités envers la victime et qu'il pourrait être tenu responsable au même titre que l'auteur du fichier ou du logiciel infecté[469]. Concernant le distributeur de logiciels, Alain Bloch soumet la réflexion suivante :

> « *Étant directement à l'origine de la diffusion du logiciel infecté, il ne saurait échapper à une responsabilité civile l'obligeant à réparer le préjudice dont il est directement à l'origine. Le fait qu'il n'en ait pas été informé apparaît sans incidence sur la responsabilité financière qui en découle, d'autant qu'on pourrait faire valoir à son encontre le fait qu'en bon professionnel il devait, ou aurait dû, s'assurer de l'absence de virus* »[470].

En effet, puisque ces individus permettent l'accès à certains logiciels ou fichiers dans un but commercial ou publicitaire et qu'ils sont ou devraient

---

[466] Henri LILEN, et François DAROT, *op. cit.*, note 38, p. 17.
[467] Philippe HELIS et Philippe MOZAS, *loc. cit.*, note 184.
[468] Comme l'explique Beyer: « *Under a tort theory of liability, the provider and its employees may be held liable if an employee negligently or intentionally placed a virus in software. This risk is best minimized through employee education and through careful management of the software development environment. The provider should limit access to software development systems to those who need to have access, provide regular system maintenance, including viral protection checks, and backup development systems regularly* ». Mary L. BEYER, *loc. cit.*, note 299, 23-24.
[469] Meiring De VILLIERS, *loc. cit.*, note 219, 4.
[470] Alain BLOCH, *loc. cit.*, note 12, 52.

être conscients de la problématique des virus informatiques « *they have an additional duty to the user/consumer to take reasonable steps to preclude virus contamination* »[471]. Ce raisonnement est d'autant plus intéressant qu'il se glisse dans la même lignée que l'article 1473 al. 2 C.c.Q., ce dernier imposant au distributeur du bien le fardeau de prouver que le défaut ne pouvait être connu. Dans le cas de virus informatiques :

> « *Même si le virus était indécelable (s'il est nouveau par exemple), l'éditeur ne pouvait pas s'exonérer, car la présence d'un virus dans une disquette est toujours prévisible en raison de la fréquence de ce type d'anomalie. Il est alors à craindre pour les éditeurs que la force majeure ne sera retenue que dans de rares cas. Il est vrai qu'ils sont les mieux placés pour prendre les précautions pour éviter ce genre de problèmes* »[472].

Ainsi, afin de limiter sa responsabilité et celle de son employeur, le gestionnaire d'un site Web « *should therefore operate a strict regime of checking all the material on the site and where possible attempt to disclaim, to some extent, liability for infecting viewers* »[473]. Nous reviendrons sur ce dernier point dans la sous-section c) du présent chapitre.

b) Les babillards électroniques

Les babillards électroniques sont des « *services informatisés d'échange d'information gérés par un organisme ou une entreprise, auxquels on accède par modem, et qui permettent aux utilisateurs d'afficher des messages et d'y répondre, d'échanger des fichiers, de communiquer avec des groupes thématiques et parfois de se connecter à Internet* »[474].

---

[471] Philip FITES et al., *op. cit.*, note 24, p. 141-142. Le professeur de Villiers donne, à cette fin, l'exemple suivant : « *A web site controller, for instance, may face liability for a Java applet on her home page which deletes data on a particular type of browsing computer* ». Meiring De VILLIERS, *loc. cit.*, note 219, 4.
[472] Philippe HELIS et Philippe MOZAS, *loc. cit.*, note 184.
[473] Clive GRINGRAS, *op. cit.*, note 15, p. 62.
[474] OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.

L'aspect de ces sites pouvant causer problème réside donc dans l'échange de fichiers, puisque ceux-ci peuvent devenir des vecteurs dans la transmission de virus informatiques :

> « *Une fois qu'un virus a envahi un babillard électronique, il peut se propager aux ordinateurs des autres utilisateurs du babillard, à leur insu, et même à l'insu des exploitants des babillards électroniques. Ces derniers autorisent habituellement les gens à télécharger des renseignements (y compris des messages et des programmes qui peuvent être infectés par des virus) vers le babillard ou vers leur ordinateur personnel* » [475].

La question quant à la responsabilité civile des opérateurs de tels babillards devient donc double. D'abord, il importe de se demander si, lorsqu'un opérateur autorise les téléchargements de fichiers en aval, il ne se retrouve pas à distribuer *sciemment* des virus[476]? Ou plutôt, l'exploitant d'un tel service est-il responsable des infections causées par des fichiers téléchargés sur son site? Ensuite, si le virus est caché dans un message électronique, appartient-il à l'exploitant du babillard de vérifier le contenu de chaque courriel[477]? En ce qui concerne cette seconde problématique, nous référons le lecteur à la section sur les intermédiaires techniques puisque les règles applicables à ceux-ci devraient, à nos yeux, s'appliquer *mutatis mutandis* aux opérateurs de babillards électroniques puisque leur fonction est alors assimilable à celle des F.A.I. qui, rappelons-le, ne font l'objet d'aucune protection législative propre aux virus informatiques. Il en découle que la responsabilité de ces individus peut être engagée si elle n'est pas préalablement écartée de façon contractuelle.

Pour ce qui est de la problématique liée au contenu des fichiers disponibles sur les sites, celle-ci doit être dissociée de celle des sites

---

[475] *Op. cit.*, note 4.
[476] *Id.*
[477] *Id.*

commerciaux puisque les fichiers disponibles ne sont pas placés sur le site par le propriétaire du babillard.

Pourtant, la doctrine semble majoritairement en faveur de l'attribution du même régime de responsabilité à ces deux entités. En effet, si certains limitent la responsabilité des opérateurs de babillards électroniques à l'omission d'agir lorsqu'ils sont conscients qu'un virus se situe sur leur site[478], d'autres avancent qu'ils pourraient avoir l'obligation de balayer tous les fichiers contenus sur leurs sites afin de s'assurer qu'ils ne sont pas contaminés[479] :

> « *solutions obviously include ensuring that no files can be uploaded before passing through the site's anti-viral program first. This will probably be sufficient to extinguish the controller's duty to his visitors, although it would be legally safer if a contractual disclaimer is also provided* »[480].

Cette position peut s'expliquer par le fait que, même si l'exploitant du babillard n'est pas le créateur des fichiers contaminés, il en demeure le diffuseur[481] et exerce donc un contrôle sur l'individu ayant diffusé le virus, ainsi qu'un certain contrôle sur ceux qui en deviennent infectés[482].

Quoi qu'il en soit, l'exploitant d'un babillard électronique devrait avoir tout au moins l'obligation d'avertir ses utilisateurs du risque associé au téléchargement de fichiers[483]. Bien qu'il soit peu probable qu'un tel avertissement soit suffisant pour enrayer complètement sa responsabilité[484], il permettra tout au moins de limiter celle-ci.

---

[478] Robbin A. BROOKS, *loc. cit.*, note 222, 369.
[479] Philip FITES et al., *op. cit.*, note 24, p. 142. Voir également Vicky H. ROBBINS, *loc. cit.*, note 44, 27.
[480] Clive GRINGRAS, *op. cit.*, note 15, p. 62.
[481] Nous renvoyons le lecteur à la section portant sur les sites commerciaux pour les explications quant au rôle du distributeur.
[482] Clive GRINGRAS, *op. cit.*, note 15, p. 62.
[483] Philip FITES et al., *op. cit.*, note 24, p. 142. Voir également Vicky H. ROBBINS, *loc. cit.*, note 44, 27.
[484] Clive GRINGRAS, *op. cit.*, note 15, p. 62.

c) Les listes de diffusion[485] et les groupes de nouvelles *Usenet*

Comme le souligne Roger A. Grimes, « [b]*oth newsgroups and list servers have been involved in spreading email attacks and exploits* »[486] Il devient donc important d'évaluer la responsabilité des tenanciers de ces services dans le cas d'infection des tiers.

Par liste de diffusion, nous désignons toute « [l]*iste d'adresses électroniques identifiée par un pseudonyme et à laquelle on a attribué une adresse de courrier électronique en propre, de telle sorte qu'un message expédié à cette adresse sera automatiquement réexpédié à toutes les autres* »[487]. Ces listes diffèrent quelque peu des groupes de nouvelles, puisque, si ces premières nécessitent l'utilisation du courrier électronique[488], ces derniers requièrent l'accès à un réseau mondial (*Usenet*) « *constitué d'un ensemble de serveurs où sont centralisés des articles traitant de sujets particuliers et auxquels les internautes ont accès sur demande* » [489]. Néanmoins, la responsabilité du transfert de l'information reposant, dans les deux cas, sur les épaules du médiateur chargé d'évaluer l'opportunisme de la transmission d'un message ou d'un texte donné, il devient opportun de traiter de ces deux services simultanément.

À la lumière de ce qui précède, le rôle du médiateur de la liste ou du groupe est assimilable à celui d'un gestionnaire de site puisqu'il effectue

---

[485] Le terme plus commun de « *liste de discussion* » (*discussion list*), sans doute né de la confusion entre la liste de diffusion et le forum de discussion, n'a pas été retenue pour ne pas augmenter davantage la confusion. Voir OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[486] Roger A. GRIMES, *op. cit.*, note 35, p. 387.
[487] Voir OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.
[488] « *Les listes de diffusion se distinguent notamment des forums par leur mode de diffusion. Lorsque l'on s'abonne à une liste de diffusion, on reçoit les messages dans sa boîte aux lettres électronique plutôt que par l'intermédiaire d'un serveur de nouvelles* ». *Id.*
[489] *Id.*

un contrôle sur l'information transmise. En effet, si la responsabilité de la transmission d'un virus revient d'abord à celui qui a introduit le maliciel dans une liste ou sur un serveur *Usenet*, il demeure que le modérateur ayant autorisé le passage du fichier infecté garde un part de responsabilité[490].

Mais qu'en est-il s'il n'y a pas de médiateur, c'est-à-dire si la transmission est automatique et qu'elle n'est aucunement censurée[491]?

Dans le cas des listes, il demeure que le message reçu par les tiers est transmis non pas par l'individu ayant créé le fichier infecté, mais bien par la liste, ce qui implique, comme il en était le cas pour les babillards électroniques, que le propriétaire de la liste a une obligation de diligence envers ses membres. Afin d'honorer cette obligation qui, rappelons-le, en est une de moyen, il est conseillé aux propriétaires de listes d'interdire tout type de pièce jointe si le sujet de la liste ne le justifie pas[492]. Ainsi, les MIME[493], les fichiers HTML, les documents et les

---

[490] Propos tenus par Michel ARBOI sur la liste de discussion droit-net@cru.fr le 30 octobre 2002. En effet, puisque « [f]*or the moderated newsgroups, all messages to the newsgroup are forwarded to one person who can screen them for relevance to the topics under discussion* » (*American Civil Liberties Union* c. *Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), réaffirmée dans *Reno* v. *American Civil Liberties Union*, 117 S. Ct. 2329 (1997)), ce médiateur a également l'opportunité de vérifier la presence de virus. De plus, une telle vérification n'aura pas les même conséquences problématiques que celle effectuée par les F.A.I., puisque, dans le cas des listes de discussion et des groupes *Usenet*, le consentement à l'ouverture et à la lecture des fichiers est implicite de par le désir de participer à un échange contrôlé.

[491] En effet, comme l'explique la cour dans *American Civil Liberties Union* c. *Reno*, (précitée, note 490), « [*s*]*ome USENET newsgroups are "moderated" but most are open access* ».

[492] Propos tenus par Michel ARBOI sur la liste de discussion droit-net@cru.fr le 29 octobre 2002.

[493] Le protocole MIME (Multi-purpose Internet Mail Extensions) est un « *Protocole de communication permettant d'inclure autre chose que du texte dans le courrier électronique, c'est-à-dire des caractères spéciaux, des illustrations, des photos en couleur, des images vidéo ou du son haute-fidélité.* [...] *L'originalité du protocole Mime consiste à convertir tous les éléments qui ne sont pas du texte en un format reconnu par toutes les passerelles de messagerie, surtout celles qui ne supportent pas cette norme.* » OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.

images sont à proscrire[494]. De plus, certaines listes possédant un filtre antivirus, le recours à une telle technologie ne peut que réduire les chances de responsabilisation. En effet, quoique cette technologie ne soit pas efficace à 100%[495], il demeure que son utilisation témoigne d'un comportement diligent.

Dans le cas des groupes de nouvelles *Usenet*, l'absence d'un médiateur rend la situation plus complexe puisque « [t]*he dissemination of messages to USENET servers around the world is an automated process that does not require direct human intervention or review* »[496]. Le rôle du propriétaire d'un serveur *Usenet* devient alors assimilable à celui de l'hébergeur : il ne fait que permettre à des tiers d'utiliser ses ressources pour distribuer de l'information. Nous renvoyons donc le lecteur à la sous-section traitant de la responsabilité de l'hébergeur.

Malgré le fait que la responsabilité des gestionnaires de listes de discussion soit plus facile à établir que celle des propriétaires de serveurs *Usenet*, leur déresponsabilisation est également plus aisée. En effet, les listes de discussion nécessitant forcément une inscription[497], tout propriétaire a donc la possibilité de limiter contractuellement sa responsabilité pour les dommages causés par une éventuelle infection. Comme nous le verrons maintenant, cette possibilité doit toutefois respecter certaines limites imposées par le législateur.

---

[494] Propos tenus par Michel ARBOI sur la liste de discussion droit-net@cru.fr le 29 octobre 2002.
[495] *Id.*
[496] *American Civil Liberties Union* c. *Reno*, précitée note 490.
[497] Comme le souligne Éric Labbé : *l'utilisation des listes de distribution est précédée d'une inscription auprès de l'administrateur de la liste. Dans le cas des listes dites ouvertes, cette requête est acceptée automatiquement. Cependant, lorsqu'une liste de distribution est dite fermée, certaines inscriptions peuvent être refusées, les requérants ne correspondant pas au type d'interlocuteur recherché.* » Éric LABBÉ, « Spamming en Cyberespace : à la recherche du caractère obligatoire de l'autoréglementation », (1999) en ligne sur le site *Lex Electronica* : <*http://www.lex-electronica.org/articles/v6-1/labbe.htm*> (dernière mise à jour : printemps 2000).

d) Les clauses de non-responsabilité

La présence de clauses d'exonération de responsabilité dans le cas d'infections virales comme celle-ci est de plus en plus commune sur les sites web :

> « *Bien que **** fasse tout son possible pour que les documents pouvant être téléchargés à partir de son site Web soient exempts de virus, elle ne peut garantir leur innocuité totale. **** décline toute responsabilité pour toute perte ou dommage causé par le logiciel et les codes correspondants, et notamment par des virus ou des vers* »[498].

Il est présentement difficile d'évaluer l'étendue de la protection accordée par de telles clauses[499] puisqu'il est déjà reconnu qu'on ne peut s'exonérer de sa responsabilité délictuelle par un avis général à la société, quand bien même cet avis serait connu de tous[500]. La problématique devient donc celle d'établir si nous nous situons ici dans un cadre contractuel ou si le fait de visiter un site Web n'engage les parties à aucune obligation autre que celles déjà établies par la loi.

En effet, aucune disposition du code n'empêche catégoriquement la contractualisation d'une limitation ou d'une exonération de responsabilité si le consentement des parties est véritablement donné et découle d'une décision libre et éclairée[501]. Ainsi, comme l'explique Alain Gagnon, une

---

[498] Pour ne pas porter préjudice à l'entreprise dont nous nous servons dans l'exemple suivant, nous avons choisi d'éliminer toute référence à celle-ci.

[499] Rob GALLAGHER, *loc. cit.*, note 418.

[500] Article 1476 C.c.Q. Voir également Jacques PERREAULT, *Des stipulations de non-responsabilité*, Montréal, Imprimerie modèle limitée, 1939, p. 149, Benoît MOORE, « À la recherche d'une règle générale régissant les clauses abusives en droit québécois », (1994) 28 *R.J.T.* 177, 211 et *Garage Touchette Limitée* c. *Metropole Parking inc.*, [1963] C.S. 231.

[501] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 117. En effet, le *Code civil du Québec*, par l'entremise de son article 1474, interdit uniquement la présence de clauses contractuelles ayant pour objet la limitation de la responsabilité du cocontractant dans le cas de fautes intentionnelles ou lourdes, ou encore d'un préjudice corporel ou moral. *A contrario* cette disposition du code permet donc l'existence de telles clauses dans le cas de dommages matériels liés à la simple négligence du cocontractant. Il s'agit d'ailleurs de l'interprétation adoptée par le

telle clause d'exonération dans le cadre d'infections virales, pour être valide, doit faire l'objet d'une « *mention précise inscrite sur la page web d'accueil* »[502] de l'entreprise « *déclinant toute responsabilité à l'égard de dommages que pourraient encourir clients et autres utilisateurs du site web causée par* [...] *un virus transmis par inadvertance ou ignorance* »[503]. Cette position est appuyée par Clive Gringras :

> « *It is an obvious and important point that any disclaimer of damage from the site must be shown on the home page and throughout the site. If the disclaimer is buried at the 'back' of web pages there is a risk that the viewer's computer becomes infected before liability is disclaimed* »[504].

Cependant, ces propos ne tiennent pas compte de la réalité d'Internet. En effet, outre les sites offrant un contenu pouvant être jugé offensant, rares sont ceux qui affichent visiblement un contrat sur leur première page. Un lien en bas de page vers les politiques d'utilisation du site constitue la norme. Comme l'expliquent Pierre Trudel et al., « [l]*a question se pose alors à savoir si une clause de non-responsabilité est valide même si elle ne se trouve pas dans un contrat* »[505].

Bien qu'il soit possible de prétendre que le simple fait de visiter un site « *emporte la formation d'un contrat implicite* » [506], encore faut-il que celui qui invoque la présence d'une clause d'exonération « *démontre que l'autre partie en a eu effectivement connaissance au moment de la formation du contrat* »[507]. Par contre, le contrat étant alors déjà formé, et ces clauses ne faisant pas nécessairement partie intégrante de

---

Barreau du Québec. Voir Nathalie VÉZINA et Louise LANGEVIN, « L'exécution de l'obligation » dans F. BOUSQUET (dir.), *Obligations et contrats*, « Collection de droit » vol. 5, Cowansville, Éditions Yvon Blais, 2002, à la page 96.

[502] A. GAGNON, *loc. cit.*, note 441, 32-33.

[503] *Id.*

[504] Clive GRINGRAS, *op. cit.*, note 15, p. 63.

[505] Pierre TRUDEL et al., *op. cit.*, note 201, p. 5-63.

[506] *Id.*

[507] Jean-Louis BAUDOUIN, *Les Obligations*, 4e éd., p. 460

l'engagement puisque, comme nous l'avons déjà souligné, elles sont normalement absentes de la page principale du site, elle ne peuvent plus être imposées unilatéralement après coup et ne lient donc pas le contractant[508].

De plus, dans le cas de contrats de consommation ou d'adhésion, la clause d'exonération sera nulle si « *elle n'a pas été expressément portée à la connaissance du consommateur ou de la partie qui y adhère* » au moment de la formation du contrat, « *à moins que l'autre partie ne prouve que le consommateur ou l'adhérent en avait par ailleurs connaissance* »[509].

Il est donc suggéré, lorsqu'un site offre la possibilité de télécharger un document ou un programme quelconque, d'avertir le consommateur *avant* le début du téléchargement que, malgré toutes les précautions prises par le gestionnaire du site, il est possible que ledit fichier soit infecté[510] et que, s'il décide de procéder tout de même au téléchargement, il ne pourra tenir le gestionnaire ou l'entreprise propriétaire du site responsable des dommages causés. Une telle clause devrait suffire pour répondre aux critères de l'article 1435 C.c.Q. puisque « [t]*he controller of a web site does not need to show a court that a viewer understood such a notice, or even that it was read; the controller must, however, show that he took reasonable steps to bring it to the plaintiff's notice* »[511].

Quoi qu'il en soit, l'appréciation du degré de la faute commise par le gestionnaire d'un site web variera suivant les circonstances et, comme le souligne un auteur, « *ce sera au tribunal à décider si la faute*

---

[508] BAUDOUIN, Les Obligations, Cowansville, Yvon Blais, 1993, p. 459.
[509] Article 1435 al. 2 C.c.Q.
[510] Clive GRINGRAS, *op. cit.*, note 15, p. 87 et 89.
[511] *Id.*, p. 89.

involontaire, personnelle, est assez légère pour qu'on puisse s'en exonérer par une convention »[512].

3. Les utilisateurs du réseau

La dernière catégorie de transmetteurs potentiels de virus informatiques est celle dont la responsabilité entrera en ligne de compte le plus souvent. En effet, puisque la majorité des virus informatiques sont transmis par courrier électronique[513], il va de soi que les personnes à l'origine de ces transmissions soient tenues responsables de leurs envois. L'étendue de cette responsabilité sera cependant différente s'il s'agit d'un message issu de l'employé d'une personne morale (a), ou d'un courriel envoyé par une personne physique (b).

a) Les personnes morales

Comme nous l'avons déjà abordé dans la première partie de la présente étude, « [t]*here exists a strong need to create liability for companies who do not maintain adequate security on their computer networks* »[514]; c'est-à-dire lorsque ces entreprises n'appliquent pas une politique informatique sécuritaire, pouvant ainsi causer préjudice à des tiers[515]. Pour une entreprise désirant limiter sa responsabilité civile, la problématique des virus informatiques en est une des plus complexe puisqu'elle doit être envisagée selon l'optique de la protection des différents ordinateurs personnels, mais également dans la visée des réseaux locaux d'entreprise (*local access network*) et de la gestion des réseaux Internet, intranet[516], extranet[517], etc.[518] De plus, contrairement

---

[512] Jacques PERREAULT, *op. cit.*, note 500, p. 163.
[513] PISA, *loc. cit.*, note 6.
[514] Sarah FAULKNER, *loc. cit.*, note 433, 1028.
[515] *Id.*, 1028.
[516] L'intranet est un « [r]*éseau informatique privé qui utilise les protocoles de communication et les technologies du réseau Internet* ». OFFICE DE LA LANGUE FRANÇAISE, *op. cit.*, note 52.

aux personnes civiles, notion que nous aborderons plus loin, les personnes morales « *also have a duty of care to create reasonable safeguards against unauthorized access to the computing system or to some parts of the computer system because the penchant of hackers to seek unauthorized entry is well known in the computing community* »[519]. En effet, la responsabilité d'une personne morale n'est pas uniquement vis-à-vis les tiers, mais également vis-à-vis sa clientèle pour qui la sécurité des informations contenues sur les serveurs de l'entreprise est essentielle. À cette fin, les articles 19 et 25 de la *Loi concernant le cadre juridique des technologies de l'information* précisent que :

> 19. Toute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné.
>
> 25. La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

À la lumière de ces articles, l'opérateur d'un serveur et, par le fait-même, son employeur, a le devoir d'assurer un niveau de sécurité raisonnable à son système informatique[520]. En effet, comme l'expliquent Cheryl S. Massingale et A. Faye Borthick :

---

[517] L'extranet est un « [r]*éseau informatique à caractère commercial, constitué des intranets de plusieurs entreprises qui communiquent entre elles, à travers le réseau Internet, au moyen d'un serveur Web sécurisé* ». *Id.*
[518] David HARLEY et al., *op. cit.*, note 3, p. 172.
[519] Pamela SAMUELSON, *op. cit.*, note 253, p.475.
[520] Cheryl S. MASSINGALE et A. FAYE BORTHICK, *loc. cit.*, note 186, 173.

> « *if valuable property is left unguarded and exposed to the public view, it may be anticipated that it will be stolen; if the key is left in the lock of a jewelry store over a holiday, it is not at all unlikely that there will be a burglary."* [...] *Similarly, if a computer system is left unprotected, it is likely that information in that system will be stolen, altered, or lost. With the risk of misconduct clearly foreseeable, the manager must use reasonable means to restrict access to the system* »[521].

Ainsi, la demande d'un client fondant sa plainte à l'encontre de l'opérateur d'un serveur sur le fait que ce sont les failles techniques de ce dernier qui ont permis à un tiers de lui causer un dommage, c'est-à-dire d'introduire un virus sur le serveur[522], risque fort bien d'être accueillie par les tribunaux. Par « niveau de sécurité raisonnable », nous renvoyons le lecteur à la notion de l'usager raisonnable, en tenant compte, bien sûr, du niveau d'expertise normalement exigé des individus occupant les postes d'opérateur dans les entreprises :

> « *The provider's liability will depend upon the scope of the original foreseeable risk that the manager created through lax security practices. "If the intervening cause is one which in ordinary human experience is reasonably to be anticipated, or one which the defendant has reason to anticipate under the particular circumstances, the defendant may be negligent, among other reasons, because of failing to guard against it* »[523].

Ainsi, dès qu'il sera possible, pour une victime, d'établir qu'il existait certaines mesures qui auraient permis à l'opérateur de diminuer considérablement la chance d'infiltration d'un virus[524], ou dès que l'opérateur aura omis de restreindre l'accès à son serveur[525], elle pourra alors recourir aux dispositions de la *Loi concernant le cadre juridique des technologies de l'information* énoncées ci-haut, ainsi qu'aux

---

[521] *Id.* 181.
[522] Stefan MARTIN, *loc. cit.*, note 438, 205.
[523] Cheryl S. MASSINGALE et A. FAYE BORTHICK, *loc. cit.*, note 186, 180.
[524] *Id.*, 174.
[525] *Id.*, 179.

principes établis dans *T.J. Hopper c. Northern Barge*[526], pour autant qu'il soit possible d'établir que ces mesures étaient économiquement viables[527].

En effet, la simple prétention, de la part de l'opérateur du serveur, qu'il employait certaines mesures de sécurité n'est, en soi, pas suffisante. Ces mesures doivent être aussi complètes que possible et ne doivent pas contenir de failles apparentes. Comme l'exprimait la cour dans l'affaire *Audet* c. *Fréchette*[528], un individu ne peut s'acquitter de son obligation de prudence en installant une clôture invitante, c'est-à-dire facile à contourner.

Cependant, « [c]*orporations must work to not only protect against outside hackers breaking into secure networks, they must work to protect the information that comes into the network via e-mail. This is done through content filtering* »[529]. En effet, la personne morale étant connectée au réseau Internet détient également l'obligation de surveiller le comportement de ses employés et d'exercer un contrôle sur le contenu des messages qu'ils envoient via leur compte courriel. Bien qu'il soit, comme nous l'avons déjà souligné, impossible de créer un programme pouvant identifier tout virus informatique sans erreur[530], il n'en demeure pas moins que l'utilisation d'un logiciel de filtrage offrira une excellente protection contre toute infection potentielle, sans compter qu'elle réduira sa responsabilité dans le cas de l'infection de l'interlocuteur de l'un de ses employés[531]. Tout au moins, l'opérateur du

---

[526] Précitée, note 192.
[527] Voir la section portant sur la faute.
[528] J.E. 83-866 (C.S.). Dans cette affaire, un propriétaire avait fait installer une clôture autours de sa piscine afin d'en limiter l'accès. Cependant, des enfants on réussi à escalader celle-ci pour être retrouvés noyés quelques instants plus tard. La cour a jugé que, malgré la présence de la clôture, le fait que cette dernière rendait l'escalade si facile de par sa conception (les poteaux avaient l'apparence d'échelles) entraînait la responsabilité du propriétaire.
[529] James STANGER, *op. cit.*, note 127, p. 398.
[530] Eugene H. SPAFFORD, *loc. cit.*, note 34, 13.
[531] James STANGER, *op. cit.*, note 127, p. 398

serveur d'une entreprise qui apprend que le réseau est infecté par un virus informatique a l'obligation, *ipso facto*, d'en aviser les tiers pouvant avoir été en contact avec celui-ci via courrier électronique[532].

Quoi qu'il en soit, comme le souligne A. Gagnon, les entreprises désirant maintenir leur actif devront se protéger à plus d'un titre contre les attaques virales et ainsi se prémunir contre les éventuelles poursuites en dommages-intérêts qui pourraient s'ensuivre[533]. En effet, comme nous l'avons déjà esquissé, les risques de poursuite fructueuse sont plus faibles lorsqu'une entreprise est vigilante[534].

b) Les personnes physiques

Si les principes énoncés dans *T.J. Hopper* c. *Northern Barge*[535] peuvent entraîner la responsabilité civile des personnes morales ne possédant pas la toute dernière technologie antivirale, un pareil investissement ne pourrait être exigé des personnes physiques dont les connaissances et l'actif sont normalement moins importants. Les personnes physiques ne sont pas pour autant exemptées de toute responsabilité puisque, comme les personnes morales, « *users clearly have a duty to avoid foreseeable, unjustified harm to others.* [They] *are not free to disregard potential consequences of their activities online* »[536]. Il importe donc d'employer une autre méthode d'analyse pour établir le degré de responsabilité des tiers transmetteurs qui sont des personnes physiques.

Nous proposons, comme l'ont fait plusieurs auteurs[537], de procéder par analogie en comparant les virus informatiques aux organismes dont ils

---

[532] Meiring De VILLIERS, *loc. cit.*, note 219, 4.
[533] A. GAGNON, *loc. cit.*, note 441, 29.
[534] Rob GALLAGHER, *loc. cit.*, note 418.
[535] Précitée, note 192.
[536] David R. JOHNSON et Kevin A. MARKS, *loc. cit.*, note 440, 497.
[537] Comme l'expliquent Philip Fites et al. : « The name "virus" is used because many of the characteristics of these programs may find a biological metaphor in the characteristics of disease viruses », Philip FITES et al., *op. cit.*, note 24, p. 28. Voir

ont hérité du nom, à savoir les virus biologiques. En effet, « *given a new situation, the typical legal response is always to find an analogy to a situation the law has already treated* »[538]. Cette tendance s'explique par le fait qu'il existe « *substantial utility in asking ourselves how particular online environments are similar to or different from other environments where the rights and duties of participants have been analyzed more fully in the past* »[539].

Ainsi, il paraît utile de faire l'analogie entre les virus informatiques et les virus biologiques puisque l'étude doctrinale concernant ces derniers abonde. De fait, les points de comparaison entre ces deux éléments sont multiples : « *Just as a biological virus uses 'the biochemical mechanisms of a host cell to' replicate, a computer virus produces new copies of itself by using other software* »[540]. De plus, comme dans le cas de maladies, le terme « virus » caractérise le mode de dissémination du logiciel malicieux, soit l'infection de tous les « organismes » avec lesquels il entre en contact[541] :

> « *Like real viruses, these ones carry a genetic code, recorded in this case in machine language. The code tells a "host" system to insert the virus into its main logic, usually on a hard disk. Once established, the virus silently infects every other program it can reach. For example, a floppy disk that is formatted in an infected computer will itself be infected and may carry the virus to other hosts* »[542].

Les ressemblances entre les virus informatiques et leurs homologues biologiques peuvent être résumés ainsi :

---

aussi SUSAN C. LYMAN, *loc. cit.*, note 11, p. 626, ANONYME, *op. cit.*, note 20, p. 326 et W.H. MURRAY, *op. cit.*, note 32, p. 17.

[538] Sunny HANDA et al., *op. cit.*, note 11, p. 204.

[539] David R. JOHNSON et Kevin A. MARKS, *loc. cit.*, note 440, 488.

[540] SUSAN C. LYMAN, *loc. cit.*, note 11, p. 626. Voir aussi ANONYME, *op. cit.*, note 20, p. 326 et W.H. MURRAY, *op. cit.*, note 32, p. 17.

[541] W. H. MURRAY, *op. cit.*, p. 15.

[542] Eliot MARSHALL, « The Scourge of Computer Viruses », (1988) 240 *Science* 133, 133.

Tableau 1 : Comparaison entre les virus informatiques et les virus biologiques[543]

Virus biologiques	Virus informatiques
• Attaquent certaines cellules du corps	• Attaquent certains programmes
• Transforment l'information héréditaire de la cellule	• Manipulent un programme en lui faisant exécuter des tâches différentes de celles prévues à l'origine
• Les cellules touchées produisent de nouveaux virus	• Le programme touché génère lui-même des programmes viraux
• Une cellule infectée n'est jamais infectée plusieurs fois par le même virus	• Un programme n'est en général infecté qu'une seule fois par la plupart des virus
• Un organisme touché peut ne présenter aucun symptôme pendant un temps très long	• Le programme infecté peut fonctionner longtemps sans erreur
• Toutes les cellules entrant en contact avec le virus ne sont pas infectées	• Les programmes peuvent être immunisés contre certains virus
• Les virus peuvent muter et ne sont pas toujours facilement reconnaissables	• Les programmes de virus peuvent se transformer et échapper aux procédures de détection

Il importe cependant de souligner qu'aucune analogie n'est parfaite et qu'elle peut, dans certains cas, porter à confusion.[544] En effet, comme l'explique le juge Mahoney dans l'affaire *Apple Computer*[545], « *La difficulté principale que j'ai rencontrée en l'espèce procède du caractère anthropomorphique de presque tout ce qui est pensé, dit ou écrit au sujet des ordinateurs.* [...] *Les métaphores et analogies que nous utilisons pour décrire leurs différentes fonctions ne demeurent que des métaphores et des analogies* »[546]. Cette tendance anthropomorphique a,

---

[543] Ralf BURGER, *Virus : La maladie des ordinateurs*, Paris, Micro Application, 1989, p. 18.
[544] ANONYME, *op. cit.*, note 20, p. 326.
[545] Apple Computer, Inc. c. Mackintosh Computers Ltd., (1987) 18 C.P.R. (3d) 129.
[546] *Id.*, par. 38.

dans le cas des virus informatiques, possiblement porté à une certaine confusion quant à la nature de ces logiciels[547] et à leurs modes de dissémination. Ainsi, il ne faudrait pas pousser l'analogie trop loin puisque, contrairement à certains virus biologiques, les virus informatiques ne peuvent être transmis que par contact physique et échange de données entre les hôtes du virus. Nous nous pencherons donc uniquement sur les virus biologiques ayant une méthode de dissémination semblable à celle des virus informatiques, à savoir les maladies transmises sexuellement telles l'herpès[548] ou le SIDA[549].

En effet, tout comme toute relation sexuelle non protégée ou toute transfusion sanguine peut causer l'infection d'une victime, « *any sharing of writable memory or communications with any other entity introduces the possibility of virus transmission* »[550]. Nous soumettons donc que le régime de responsabilité civile applicable aux transmetteurs de M.T.S. s'avère être un guide utile dans la mise en place d'un régime de responsabilité civile pour les transmetteurs de virus informatiques.

Puisque le V.I.H. ne peut se répandre que par un contact humain physique et – normalement – volontaire, il est présumé que le SIDA est transmis soit délibérément, soit par négligence, ce qui implique la présence d'une faute et donc d'un devoir de compenser la victime de l'infection pour les dommages causés[551]. En effet, « [*a*]*ny person who is infected with AIDS, at least anyone who knows or ought to know that he*

---

[547] Eugene H. SPAFFORD, *loc. cit.*, note 34, 5.
[548] SUSAN C. LYMAN, *loc. cit.*, note 11, p. 626-627.
[549] Comme l'expliquent Philip Fites et al. : « *Many commentators have used the disease AIDS as an analogy to create some awareness of the concept of the spread and results of computer viruses in computer systems* », Philip FITES et al., *op. cit.*, note 24, p. 135. Voir aussi Charles CRESSON WOOD, « The Human Immune System as an Information Systems Security Reference Model », dans HOFFMAN, L.J. (éd.), *Rogue Programs: Viruses, Worms, and Trojan Horses*, New York, Van Nostrand Reinhold, 1990, p. 50, à la page 57, ainsi que Martin P. J. KRANTZ et Cruickshank PHILLIPS, *loc. cit.*, note 257, 72.
[550] Eugene H. SPAFFORD, *loc. cit.*, note 34, 13.
[551] Lorne E. ROZOVSKY et Fay A. ROZOVSKY, *op. cit.*, note 294, p. 53.

or she is infected, has a duty to any other person whom he or she could infect »[552]. Cette présomption s'avère cependant problématique lorsque le porteur du virus, le transmetteur, n'a pas conscience de sa propre infection. Il ne peut alors prévoir les risques associés à ses actes envers une tierce partie[553]. L'ignorance de son état séropositif n'exonère cependant pas automatiquement le porteur d'un virus de toute responsabilité, l'ignorance et le comportement en découlant pouvant être dus à une faute personnelle.[554]

En effet, comme l'expliquent David Roy et al. :

> « *Si la personne qui transmet le virus est un porteur asymptomatique qui ignore qu'il est infecté par le VIH, les arguments permettant de démontrer sa responsabilité civile pourraient être inexistants, puisque chacun des deux partenaires sexuels est au même titre responsable de limiter ses pratiques à celles qui réduisent les risques de contracter le virus. Cependant, si l'un des partenaires appartient à un groupe très exposé à la maladie et que son infection est probable, même s'il n'a subi aucun test de dépistage du SIDA, il pourrait être tenu civilement responsable, surtout si l'autre personne ignore ces faits. On pourrait peut-être parler de "connaissance par déduction"* »[555].

Ainsi, le toxicomane partageant ses seringues[556], l'individu ayant des relations homosexuelles ou hétérosexuelles avec des partenaires multiples sans protection[557], les prostitué(e)s ayant des relations sexuelles non protégées[558], etc., devraient être conscients des risques de contamination associés à leur comportement et informer leurs

---

[552] *Id.*, p. 58.
[553] *Id.*, p. 54.
[554] Thierry VANSWEEVELT, *Le sida et le droit : une étude de droit de la responsabilité et de droit des assurances*, Bruxelles, CED-Samsom, 1990, p. 98.
[555] David J. ROY et al., *op. cit.*, note 175, p. 65.
[556] Thierry VANSWEEVELT, *op. cit.*, note 554, p. 98.
[557] Lorne E. ROZOVSKY et Fay A. ROZOVSKY, *op. cit.*, note 294, p. 54.
[558] Thierry VANSWEEVELT, *op. cit.*, note 554, p. 98.

partenaires de ces circonstances[559], s'agissant incontestablement de risques prévisibles.[560] Or, l'individu qui devrait normalement savoir qu'il souffre d'une M.T.S. se rendant néanmoins coupable d'un comportement à risque menant à la contamination d'un tiers, est considéré comme responsable par la jurisprudence dans divers juridictions européennes de droit civil.[561]

Ces mêmes types de risques prévisibles sont, comme le soulignent d'anciens pirates informatiques, également présents dans le cas des virus informatiques :

> « *If you frequent the back alleys of the Internet, you should exercise caution in downloading any file (digitally signed or otherwise). Usenet newsgroups are places where viruses might be found, especially in those newsgroups where hot or restricted material is trafficked. Examples of such material include warez (pirated software) or pornography. Similarly, newsgroups that traffic in cracking utilities are suspect* »[562].

Nous soumettons donc que l'Internaute visitant de tels sites adopte un comportement à risque et qu'il devrait en subir les conséquences[563].

Selon certains auteurs, la responsabilité de la personne porteuse du virus peut être écartée si celle-ci insiste pour utiliser des moyens de protection efficaces (le port du condom), rendant ainsi la communication du virus moins probable[564]. À l'opposé, celui qui, ayant un comportement à risque, refuse tout de même d'utiliser une protection quelconque, est responsable du dommage causé :

---

[559] Lorne E. ROZOVSKY et Fay A. ROZOVSKY, *op. cit.*, note 294, p. 54.
[560] Thierry VANSWEEVELT, *op. cit.*, note 554, p. 98.
[561] *Id.*, p. 97.
[562] ANONYME, *op. cit.*, note 20, p. 344-345.
[563] À l'opposé, comme l'explique Roger A. Grimes, « *Avoiding some malicious Internet code is as simple as avoiding nonlegitimate sites. For the most part, surfing at well-known, commercial sites, is a great way to prevent malicious code attacking your browser* ». Roger A. GRIMES, *op. cit.*, note 35, p. 257.
[564] Lorne E. ROZOVSKY et Fay A. ROZOVSKY, *op. cit.*, note 294, p. 58.

> « *Dans les cas cités ci-dessus, il est question du problème de la responsabilité, parce que, en dépit de leur comportement à risques, des gens ne prennent pas de mesures de précaution pour éviter un dommage prévisible. Étant données la gravité du dommage causé par une contamination au virus-IH et la simplicité des mesures de précaution, il nous semble justifié de placer le standard de prudence et de prévoyance suffisamment haut* »[565].

En suivant ce raisonnement, l'individu transmetteur d'un virus informatique ayant un comportement à risque devrait également hériter d'un devoir de prudence élevé puisque les dommages associés à la dissémination peuvent être importants[566], alors que les mesures de précaution – l'achat d'un logiciel antivirus – sont simples et peu dispendieuses[567].

Mais qu'en est-il si l'individu infecté, quoique conscient du fait qu'il – ou plutôt son ordinateur – est porteur du virus, n'est pas au courant des modalités de transmission du logiciel, ou encore des moyens de protection disponibles? Cette question, nous l'espérons, n'est plus vraiment d'actualité dans le cas de la transmission du virus du SIDA ; mais, comme le soulignait la campagne de publicité de *Microsoft* pour son produit *Windows XP*[568], certains individus demeurent très mal informés quant aux modes de transmission des virus informatiques. Ainsi, comme il en fut le cas pour les virus biologiques, « [much will] *depend on what information is available, and on the mental and social sophistication of the infected person, in order to hold that person*

---

[565] Thierry VANSWEEVELT, *op. cit.*, note 554, p. 99.
[566] Le rapport conjoint du CSI et du FBI avance que certaines entreprises ont perdu des millions suite à des infections virales en 2002. Voir Richard POWER, *loc. cit.*, note 228, 10.
[567] Environ 40 à 50$.
[568] Durant l'été 2002, l'entreprise américaine Microsoft faisait circuler des dépliants publicitaires avec l'entête « Personne ne m'a dit qu'il y avait un virus attaché à ce courriel ».

accountable »[569]. La « sophistication mentale » de l'individu ne causant aucune problématique particulière à la transmission de virus informatiques dans la mesure où une personne qui n'est pas douée de raison ne peut être tenue responsable civilement[570], il nous faut donc nous pencher sur la disponibilité de l'information et la « sophistication sociale » de l'individu dont l'ordinateur est infecté.

En ce qui concerne la disponibilité de l'information, il y a abondance de sites d'information sur les virus informatiques sur Internet[571] et les livres traitant de ces logiciels sont nombreux[572]. Ainsi, l'information est disponible, encore faut-il vouloir s'en servir. Pour ce qui est de la « sophistication sociale » de l'individu dont l'ordinateur est infecté, comme le souligne le groupe belge PISA :

> « *Étant donné la connaissance générale actuelle d'Internet, la présence d'un software de prévention et de traitement de virus n'est pas un produit de luxe, mais un instrument indispensable pour chaque utilisateur d'ordinateur prévoyant et prudent* » [573].

Ainsi, nous soumettons que l'individu ne pratiquant pas de « s*afe hex* »[574] comme celui ne pratiquant pas de « *safe sex* » s'expose à une part de responsabilité s'il adopte un comportement à risque. Si certains prétendent qu'il appartient à la victime potentielle de s'informer si son partenaire est porteur de virus, ce transfert du fardeau s'avère inefficace[575]. En effet, tant dans le cas de virus biologiques que dans

---

[569] Lorne E. ROZOVSKY et Fay A. ROZOVSKY, *op. cit.*, note 294, p. 55.
[570] En effet, l'alinéa 2 de l'article 1457 C.c.Q. souligne qu'une personne doit être douée de raison pour engager sa responsabilité.
[571] Voir, par exemple, le site <www.viruswatch.com> et les sites des entreprises McAfee (<www.mcafee.com>) et Symantec (<www.symantec.com>).
[572] À Cette fin, nous dirigeons le lecteur vers la section monographies de notre bibliographie.
[573] PISA, *loc. cit.*, note 6.
[574] Cette expression fut adoptée par les experts de l'industrie pour designer l'utilisation de techniques de sécurité préventives sur Internet. Voir Philip FITES et al., *op. cit.*, note 24, p. 105. Voir aussi ANONYME, *op. cit.*, note 20, p. 345.
[575] David J. ROY et al., *op. cit.*, note 175, p. 67.

celui de virus informatiques, c'est le porteur du virus qui est le mieux placé pour avertir son partenaire des ramifications possibles de leurs activités[576] puisqu'un individu s'attendant à ce que son/sa partenaire n'ait pas de comportement à risque, n'est pas censé prendre des mesures de précaution. [577] L'acceptation du risque de contamination par le V.I.H. suppose donc que la victime est ou devrait être au courant d'un risque possible et l'accepte en toute liberté. [578]

Nous soumettons également qu'un internaute fréquentant les ruelles (*back alleys*) du réseau (sites de pirates, de pornographie, de jeux craqués, etc.), ou échangeant régulièrement des fichiers avec plusieurs tiers, adopte *un comportement à risque*[579] et qu'une personne raisonnable devant la même situation utiliserait un logiciel antivirus avant d'envoyer un fichier à une tierce partie, tout comme un homme raisonnable porte le condom lors de relations sexuelles s'il fréquente plusieurs partenaires différent(e)s. Ainsi, un juge devrait reconnaître la responsabilité d'une telle personne si elle contribue à l'infection de l'ordinateur d'un tiers.

Dans le cas d'un individu qui n'adopte pas de comportement à risque mais dont l'ordinateur est tout de même atteint d'un virus informatique – tout comme le cas du porteur du V.I.H. prudent qui ignore son infection[580] –, nous soumettons qu'un tribunal québécois reconnaîtra l'absence de faute[581] si aucun symptôme de l'infection n'était décelables au moment de la transmission[582]. Il reviendra alors au demandeur de

---

[576] *Id.*
[577] Thierry VANSWEEVELT, *op. cit.*, note 554, p. 105.
[578] *Id.*, p. 103.
[579] *Id.*, p. 98.
[580] Nous référons ici aux victimes de transfusions viciées.
[581] David J. ROY et al., *op. cit.*, note 175, p. 68.
[582] En effet, « *Depending upon the susceptibility of the target and the satisfaction of necessary triggering conditions, the subject may manifest symptoms. Even when no symptoms appear, the subject may manifest sub-clinical evidence of infection. Independent of such evidence of infection, the virus may still replicate or be expelled* ». W.H. MURRAY, *op. cit.*, note 32, pp. 17 et 18.

démontrer que le défendeur « aurait dû être au courant » de son infection[583].

Cependant cette proposition met de l'avant une nouvelle problématique, puisque « *the nature of the virus threat means that you are far likelier to receive an infection from someone you know, someone with no malicious intention, than from a known or anonymous virus author/distributor* »[584]. Or, si tel est le cas, alors tout individu utilisant le courrier électronique adopte un comportement à risque. Ce ne sera en effet pas toujours chose simple d'établir avec exactitude quand quelqu'un doit savoir qu'il risque de contaminer un tiers. Le juge devra ainsi confronter chaque comportement litigieux aux règles de conduite en usage dans la société[585], en tenant compte du fait que le droit exige des utilisateurs du réseau qu'ils restent raisonnablement au courant des développements technologiques[586]. Comme le souligne Gérard Mannig :

> « *Que tout ou partie de ces outils/stratégies* [les logiciels antiviraux et les coupe-feux] *ne soient pas mis en oeuvre par l'utilisateur ou que ce dernier les paramètre mal nous replace en plein dans le problème de la compétence générale informatique appliquée au Net. Il faudra, tôt ou tard, que l'utilisateur y arrive, poussé ou pas par une jurisprudence coercitive* ».[587]

Qu'en est-il de l'évolution de cette « compétence générale informatique appliquée au Net »? Peut-on avancer, comme le suggère le groupe PISA[588] pour le peuple belge, que l'utilisation d'un logiciel anti-virus est également devenue d'usage en sol québécois? Selon un sondage effectué par l'entreprise *Symantec*, seulement 52% des répondants

---

[583] David J. ROY et al., *op. cit.*, note 175, p. 68.
[584] ANONYME, *op. cit.*, note 20, p. 344-345.
[585] Thierry VANSWEEVELT, *op. cit.*, note 554, p. 99-100.
[586] George S. TAKACH, *op. cit.*, note 31, p. 303.
[587] Gérard MANNIG, propos transmis à la liste de discussion droit-net@cru.fr le 25 août 2002.
[588] PISA, *loc. cit.*, note 6.

nord-américains utilisent un logiciel anti-virus[589], quoique ces chiffres aient tendance à croître à chaque année puisque ces logiciels viennent pré-installés sur de plus en plus d'ordinateurs[590]. De plus, l'efficacité de ces logiciels repose, comme nous l'avons déjà souligné, sur leur mise à jour régulière. Or, « *most home and office PC users who have anti-virus software don't update it at least weekly, leaving themselves vulnerable to newly minted viruses* »[591]. En effet, entre 24%[592] et 40%[593] des internautes ne mettent pas à jour leurs logiciels antivirus. Encore une fois, avec les nouvelles technologies de mises à jour automatiques disponibles avec certains logiciels, ces chiffres risquent de diminuer. Quoiqu'il en soit, à la lueur de ces statistiques, il semble difficile d'établir si l'utilisation de logiciels antivirus peut constituer un usage.

Ainsi, quoi qu'il soit impossible d'établir substantiellement que l'internaute raisonnable et diligent doit utiliser un logiciel antivirus même si ce dernier n'adopte aucun comportement « à risque », il demeure que la personne désirant s'assurer qu'elle ne court aucune chance d'être tenue responsable n'a qu'à se poser « *sérieusement la question de savoir si l'information qu'elle rentre sur son ordinateur et qu'elle envoie éventuellement plus loin est sans risque* » [594]. L'une des méthodes privilégiées pour trouver réponse à cette question consiste en l'utilisation d'un logiciel anti-virus mis régulièrement à jour :

> « *il ne peut pas être fait de reproche à l'adresse de l'utilisateur d'un ordinateur qui à chaque fois que des supports externes se relient à son système, les laisse d'abord passer par un scanneur de virus avant de*

---

[589] « Symantec's Free Web-Hosted Security Check Analyses Computer Vulnerabilities For More Than 2 Million Pc Users » (2002) en ligne sur le site Symantec.com : <http://www.symantec.com/PressCenter> (date de visite : 6 juillet 2002).
[590] CONSUMERS UNION of U.S., INC., *loc. cit.*, note 196.
[591] CommSPEED, « *CommSpeed* Introduces Revolutionary Virus Protection and Spam Filtering Services » (2002) en ligne sur le site *CommSPEED*: <http://www.commspeed.com> (dernière mise à jour : 11 mars 2002).
[592] *Loc. cit.*, note 589.
[593] CONSUMERS UNION of U.S., INC., *loc. cit.*, note 196.
[594] PISA, *loc. cit.*, note 6.

> *continuer à travailler, ou qui avant de transmettre de l'information à un tel support externe, se convainc que son information est sans risque* »[595].

C'est seulement lorsqu'une personne remplit ces critères qu'il ne pourra lui être légalement reproché d'avoir participé à l'infection d'un tiers[596].

*

* *

Ainsi, les tiers intervenant dans la distribution de virus informatiques involontairement et, dans la majorité des cas, inconsciemment, peuvent tout de même être tenus responsables des dommages subis par la victime d'une infection virale. Toutefois, la victime réclamant un quelconque dédommagement de la part de ces derniers se devra de prouver leur participation à l'acte et, il va de soi, la commission d'une faute de leur part. À cette fin, il importe de souligner que l'obligation des tiers transmetteurs en est une de moyen[597]. Ces derniers n'ont donc qu'à prouver qu'ils ont pris tous les moyens qu'aurait utilisés une personne prudente et diligente placée dans la même situation[598].

Un autre aspect important que rencontrera la victime est celui du droit applicable et des tribunaux compétents à entendre le litige, puisque, comme nous l'avons souligné lors de notre discussion sur les sites de fabrication de virus informatiques, il est possible que les responsables de l'acte soient situés à l'extérieur du pays. Bien que, outre les frais de déplacement et les autres problèmes associés aux recours en droit international privé, cette situation ne soit pas particulièrement problématique, il importe de rappeler que, en ce qui a trait, entre autre,

---

[595] *Id.* Sixto Ortiz abonde dans le même sens : « *Deploying dependable antivirus software, keeping it updated, and following safe computing practices is a more-than-adequate defense against current and future viruses* ». Sixto ORTIZ, *loc. cit.* note 131, 60.

[596] PISA, *loc. cit.*, note 6.

[597] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 108.

[598] *Id.*, p. 768.

aux États-Unis, il se peut que les dommages associés à la perte de données soient refusés puisque ces dernières ne sont pas reconnues comme étant des formes de propriété dans tous les états[599].

Il serait cependant erroné de prétendre que les intermédiaires responsables de la transmission d'un virus n'aient aucun moyen de se déresponsabiliser outre l'utilisation de mesures de sécurité adéquates. En effet, il leur sera également possible de souligner la faute contributive de la victime qui elle-même n'aurait pas agi de façon diligente lors de l'exécution d'un fichier ou d'un programme infecté. C'est donc sur le rôle de la victime que nous nous pencherons maintenant.

C. Nul n'est mieux servi que par soi-même : Le rôle de la victime dans la protection contre les attaques virales

La victime d'un virus disposera donc, selon ce qui précède, d'un recours contre celui qui est à l'origine de l'introduction du virus[600], celui qui lui a lui-même transmis le logiciel infecté[601] ou tout intermédiaire ayant participé à la transmission et dont il peut prouver la négligence. Toutefois, « [a]*lthough recovering damages may be the most satisfying remedy,* [...] *bringing a civil action can be expensive and time consuming for the person affected by a virus* »[602], d'autant plus qu'aucune compensation monétaire ne peut remplacer un travail durement rédigé et subséquemment détruit par un virus. Le vieux proverbe « mieux vaut prévenir que guérir » trouve ici tout son sens. En effet, considérant l'efficacité des mesures préventives et leurs moindres coûts, il s'avère préférable pour une victime potentielle, à nos yeux, de débourser quelques dollars par année que de devoir recourir aux tribunaux et demander d'être compensée. Cette prévoyance, de la part

---

[599] Mark R. COLOMBELL, *loc. cit.*, note 306, par. 46.
[600] Martin P. J. KRANTZ et Cruickshank PHILLIPS, *loc. cit.*, note 257, 77.
[601] Alain BLOCH, *loc. cit.*, note 12, 52.
[602] SUSAN C. LYMAN, *loc. cit.*, note 11, p. 633.

de l'utilisateur viendra également augmenter ses chances de réussite lors d'une éventuelle poursuite en responsabilité civile dans les rares cas où un virus aura réussi à l'infecter malgré ses précautions. C'est ce que nous rappelle Vicky H. Robbins :

> « *The risk of contracting a computer virus can be greatly reduced by the end user that institutes a comprehensive virus-control program. Furthermore, if a virus is contracted, the presence of such a program will greatly enhance the customer's chances of prevailing in a claim against a vendor as relative liability of the parties is explored. Consider the following in establishing such a program* »:[603]

En effet, « [a] *customer may have certain responsibilities as well, with respect to adequately protecting its computer system from the intrusion of erroneous information in the form of undisclosed or unknown features* »[604]. Cette observation n'a pas pour objet d'aller à l'encontre des derniers chapitres, mais il importe de comprendre que l'utilisateur du réseau demeure lui-même responsable de l'intégrité de ses documents technologiques[605]. S'il ne prend aucune précaution, ce dernier pourrait se faire reprocher d'avoir simplement accepté les risques associés à l'utilisation du réseau (1) et, de ce fait, avoir consenti à son infection ou, pire encore, avoir contribué à celle-ci. Dans un tel cas, il devra lui-même débourser pour réparer les dommages causés ou, comme le font de plus en plus d'entreprises, diriger la réclamation vers son assureur (2).

---

[603] Vicky H. ROBBINS, *loc. cit.*, note 44, 27-28.
[604] *Id.*, 25. Robbin A. Brooks porte cette réflexion encore plus loin: « *Where suppliers are liable for providing a technologically sound means for prevention of virus transmission, consumers and users of software or data should be held to a reasonable standard for preventing the negligent entry of a virus into their systems* ». Robbin A. BROOKS, *loc. cit.*, note 222, 380.
[605] *Loc. cit.*, note 444.

1. La responsabilité de la victime

Le juge Baudouin nous rappelle que « [s]*i la victime, par son imprudence, à été le seul artisan de son malheur, elle doit supporter les conséquences de cette situation et assumer sa propre perte* » [606]. Il poursuit, par contre, en soulignant que si « *son acte n'a fait que contribuer pour partie à la réalisation du préjudice, elle a droit alors de réclamer du tiers responsable une portion de l'indemnité totale, puisque celui-ci doit également être tenu comptable de la partie du dommage qu'il a causé* »[607]. Il importe donc d'aborder ces deux scénarios dans le contexte d'une infection virale via Internet.

a) La seule faute de la victime : l'acceptation des risques

Comme le souligne Brooks, « *It is hardly reasonable to maintain that connecting to the Internet implies consent to intentional infection by rogue code, or a rebuttable presumption thereof* »[608]. Ceci implique donc que, lorsqu'un usager se connecte au réseau, le seul consentement donné implicitement concerne les permissions accordées au site visité. Le gestionnaire de ce site peut logiquement supposer qu'il possède l'autorisation d'accéder à certains secteurs du système de l'usager, sans quoi une quelconque interaction serait impossible. Cette autorisation ne saurait toutefois s'étendre à l'acceptation des risques associés à l'introduction d'un virus, puisque ce geste est accessoire à l'interaction, il n'y est pas implicite[609].

Cependant, comme le précise le juge Baudouin, « [l]*orsqu'une personne s'engage en toute connaissance de cause dans une activité qui comporte certains dangers ou certains risques, peut-elle encore se*

---

[606] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 362.
[607] *Id.*
[608] Robbin A. BROOKS, *loc. cit.*, note 222, 379.
[609] *Id.*, 380.

plaindre si elle subit un préjudice découlant précisément de la réalisation de ceux-ci »[610]? Si la victime était dûment avisée de tels risques, la réponse à cette question doit être négative. Ainsi, si le site visité affiche clairement, comme nous l'avons déjà abordé, une clause précisant qu'il ne saura être tenu responsable d'un quelconque dommage associé à la transmission d'un virus lors du téléchargement d'un fichier et que l'usager décide de tout de même télécharger ledit fichier il ne pourra pas, par la suite, plaider la négligence du site[611].

Un raisonnement semblable doit être adopté dans le cas d'individus consultant des sites de fabrication de virus informatiques. Il serait, comme l'exprime l'exemple suivant, probable qu'un juge considère ce type de comportement comme constituant une acceptation des risques d'infection puisque, comme l'indique le vieux proverbe, « *if you play with matches, you're going to get burned* » :

> « *A ftp site acts as a depository of* [...] *viral code. A plaintiff downloads one of the latest viruses with a view to writing an anti-viral program as an antidote.* [T]*he plaintiff's computer becomes infected forcing him to lose one day's working time. On poor advice he sues. Putting aside the inherent difficulties of establishing negligence, a court will probably allow the full defense of volenti: dealing with virus code is tantamount to dealing with unexploded bombs* »[612].

Cet exemple fait ressortir une autre complication : si un logiciel téléchargé d'un site Web peut être considéré illicite ou même illégal (nous n'avons qu'à penser aux logiciels piratés), l'usager peut-il toujours plaider la négligence du gestionnaire du site alors qu'il a lui-même commis un acte répréhensible ou même illégal ayant contribué à

---

[610] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 362.
[611] En supposant que le site puisse faire la preuve que l'usager n'a pas pu télécharger ledit document sans prendre connaissance du message en question. Voir la section II B 2 d) de la présente étude.
[612] Clive GRINGRAS, *op. cit.*, note 15, p. 81

l'infection[613]? Selon la théorie des « mains propres » (*clean hands*), la victime d'un préjudice ne peut demander compensation lorsque ce préjudice découle, entre autres, de son propre comportement illégal[614]. Dans *Long* c. *Adams*[615], la cour devait trancher quant à la responsabilité d'un individu ayant transmis l'herpès à un tiers. Cette transmission eut lieu lors de relations sexuelles entre conjoints non mariés, un acte criminel en Georgie. Après discussion, le tribunal conclut qu'il était plus important de protéger le public contre les M.T.S. que de respecter les « bonnes mœurs » et refusa de recourir à la doctrine des mains propres. Il importe donc de se questionner sur l'importance proportionnelle des droits en jeu, soit la protection contre les virus informatiques et la protection des droits d'auteurs. Malgré l'importance de la problématique des virus informatiques, il ne fait aucun doute que le volume de doctrine et de jurisprudence concernant la violation des droits d'auteur témoigne d'un intérêt particulièrement important pour la communauté juridique. Cette constatation nous pousse à soumettre que la doctrine des mains propres doit être appliquée dans la transmission de virus informatiques.

b) La faute contributive

Le *Code civil du Québec* prévoit que, lorsqu'une victime contribue à son propre préjudice, elle doit assumer une partie des pertes entraînées[616]. Il s'agit du régime du partage de la responsabilité. Selon ce régime, le fardeau du dommage subi par la victime doit être réparti en proportion des fautes respectives des intervenants[617]. Ceci n'implique pas qu'un

---

[613] Philip FITES et al., *op. cit.*, note 24, p. 142.
[614] Mark WIKERSON, « Tort Law: Long v. Adams The Dirt on the Clean Hands Doctrine », (1988) 56 UMKC L. Rev. 791, 791. Bien que cette doctrine soit issue de la common law, les tribunaux québécois n'ont pas hésité à y recourir. Voir *Brasserie Labatt Ltée* c. *Ville de Montréal*, [1987] R.J.Q. 1141 (C.S.) et *L'Excellence, cie d'assurance-vie c. Conseil régional de l'âge d'or de la Rive-Sud métropolitaine Inc.*, [1997] A.Q. no 1646.
[615] 175 Ga. App. 538, 333 S.E. 2d 852 (1985).
[616] Article 1478, al. 2 C.c.Q.
[617] Ejan MACKAAY, *op. cit.*, note 157, p. 29.

défendeur négligent pourra se disculper complètement en alléguant simplement que le demandeur aurait dû utiliser un logiciel antivirus[618], mais bien que « [o]*ne must examine how easily the person harmed could have avoided the harm* »[619] et comparer ces lacunes à la négligence du tiers. Ainsi, à supposer que les fautes soient jugées d'égale gravité, « *la victime pourrait recouvrer la moitié des dommages et devrait assumer l'autre moitié* »[620].

Il importe d'abord de souligner que les logiciels antiviraux ne sont pas encore présents par défaut sur les nouveaux ordinateurs[621] et qu'aucune loi n'oblige un utilisateur à se procurer un tel logiciel. En effet, il découle de notre étude que, bien que le balayage de fichiers informatiques doive être exécuté machinalement à la sortie du système pour éviter d'engager sa responsabilité, il ne peut être exigé d'une personne d'agir de même à l'entrée du système, même si ce comportement est, sans l'ombre d'un doute, plus prudent. Il est donc difficilement envisageable de reprocher à une victime d'avoir consulté un fichier sans précaution, surtout dans les rapports entre professionnels et consommateurs[622], et ce même si elle devrait être en mesure de réduire le risque de perte, par exemple par l'enregistrement de copies de sauvegarde[623]. Ainsi, une position comme celle-ci, bien que compréhensible, n'a aucune assise juridique :

> « *A network user recently sent out a message to a large distribution saying "I have found this program that just says "BOOM." Does anyone know what it could be?" Such naiveté deserves the potential result* »[624].

---

[618] Clive GRINGRAS, *op. cit.*, note 15, p. 77.
[619] Richard B. LEVINE, *op. cit.*, note 26, p. 251.
[620] Ejan MACKAAY, *op. cit.*, note 157, p. 29.
[621] Clive GRINGRAS, *op. cit.*, note 15, p. 78.
[622] Philippe HELIS et Philippe MOZAS, *loc. cit.*, note 184.
[623] H.J. HIGHLAND, *op. cit.*, note 134, p.284-285. Voir aussi Vicky H. ROBBINS, *loc. cit.*, note 44, 27-28.
[624] James A. SCHWEITZER, *Managing Information Security: Administrative, Electronic, and Legal Mesures to Protect Business Information*, 2e éd., Stoneham, Butterworths, 1990, 197.

S'il est vrai qu'un tel comportement est naïf, le principe de la réparation intégrale exige que l'auteur d'une faute prenne la victime dans l'état où elle se trouve au moment où le dommage est causé. Comme l'explique le juge Baudouin, « [c]*ette règle, connue en common law sous le nom de « thin skull rule », signifie simplement que l'auteur du dommage assume les risques inhérents à la qualité et à la personnalité de sa victime* »[625]. Ceci démontre à quel point il devient important de limiter sa responsabilité contractuellement autant que faire se peut. En effet, « [l]*es professionnels, entre eux, pourront toujours contractuellement limiter, voire exclure, leur responsabilité civile. En revanche, vis-à-vis des utilisateurs/consommateurs, le professionnel ne pourra exclure sa responsabilité civile et il devra, en conséquence, faire montre de la plus grande prudence* »[626].

Toutefois, si l'utilisateur/consommateur n'a aucune obligation d'empêcher les dommages, il se doit d'être diligent et de les limiter. L'article 1479 du C.c.Q. vient restreindre la responsabilité des tiers en précisant que « [l]*a personne qui est tenue de réparer un préjudice ne répond pas de l'aggravation de ce préjudice que la victime pouvait éviter* ». Ainsi, comme l'explique Clive Gringras, « *a plaintiff who became infected by a virus but attempted to continue working with that computer without cleaning it first would not have mitigated his damages* »[627]. Ce dernier ne pourrait donc poursuivre pour les dommages subséquents à la découverte de l'infection[628].

---

[625] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 9, p. 199.
[626] Olivier ITEANU, *loc. cit.*, note 16.
[627] Clive GRINGRAS, *op. cit.*, note 15, p. 69.
[628] À cette fin, il est intéressant de souligner le commentaire de Gérard Mannig : « *Que notre homme, donc, ne soit pas un informaticien peut très bien se concevoir, qu'il ne fasse appel a aucune compétence extérieure devient en revanche répréhensible compte-tenu des conséquences en matière de virus qui, je tiens a le rappeler, perdurent depuis 1989. Par analogie, j'ai le droit de conduire une voiture sans être mécanicien mais deviendrais responsable si je ne faisais pas opérer des contrôles réguliers d'entretien du véhicule, lacune qui viendrait a terme a rendre ledit véhicule*

2. L'assurance est-elle la solution à la problématique des virus informatiques?

Bien que cela soit quelque peu extérieur à notre propos, il importe de souligner qu'une alternative au régime de responsabilité civile est l'obtention, pour la victime, d'une police d'assurance couvrant les risques associés aux virus informatiques[629]. Cependant, il est à noter qu'une majorité des polices conventionnelles d'assurance ne couvrent pas de telles pertes[630] et que certains assureurs sont peu enclins à inclure les virus dans leurs contrats puisque, comme l'explique l'équipe « Assurances et responsabilité professionnelle » du bureau Ogilvy Renault :

> « *L'assuré qui, par sa négligence, permettrait la diffusion d'un virus informatique risquerait d'être tenu civilement responsable des dommages qu'il a causés. S'il a répandu ce virus par Internet, le montant des indemnités que son assureur serait appelé à payer pourrait être énorme* »[631].

Il faut néanmoins rappeler que, bien que l'assurance soit un remède efficace pour la victime, elle ne limite pas la responsabilité du tiers. Ainsi, la compagnie d'assurance ayant indemnisé son assuré pourra alors recourir aux tribunaux en vertu de l'article 2474 C.c.Q. qui précise que

---

incontrôlable sur route ». Gérard MANNIG, propos transmis à la liste de discussion droit-net@cru.fr le 25 août 2002.

[629] SUSAN C. LYMAN, *loc. cit.*, note 11, p. 634.

[630] Voir Brian D. BROWN, « Emerging Insurance Products in the Electronic Age », (2001) 31 *Fall Brief* 28, Anna LEE, « Why Traditional Insurance Policies are not Enough: The Nature of Potential E-Commerce Losses & Liabilities » (2001) 3 *Vand. J. Ent. L. & Prac.* 84 et Paula M. YOST et al., « In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Ensure Lost or Corrupted Computer Data », (2001) 54 *SMU l. Rev.* 2055.

[631] ÉQUIPE ASSURANCES ET RESPONSABILITE PROFESSIONNELLE, « Le commerce de l'assurance dans le cyberespace », (1998) en ligne sur le site www.ogilvy-renault.com: <http://www.ogilvyrenault.com/fr/data/pu/107f_e.pdf> (date de visite : 26 juillet 2002).

l'assureur est subrogé dans les droits de l'assuré contre l'auteur du préjudice.

Conclusion

L'augmentation constante du nombre d'internautes, mais surtout du volume de correspondance par courriel depuis les dix dernières années ont fait passer les virus informatiques du stade de simple phénomène nuisible, à celui d'épidémie[632]. En effet, Internet a accru les possibilités de déclencher un chaos généralisé par l'insertion de codes malveillants[633]. Comme l'expliquent Froehlich et al. :

> « *The computer virus may just be the modern plague that afflicts the upcoming millennium. The "infection" numbers are staggering. The annual damage cost associated with viruses was estimated at over $1 billion for last year and is expected to rise to $2 to $3 billion in the upcoming year. One survey found that 98 percent of North American businesses have been infected by the over 6,000 types of viruses that are currently cataloged. One virus, Concept, is believed to have infected nearly one half of all companies nationwide within one year* »[634].

Bien qu'ils doivent être traités avec une certaine méfiance, ces chiffres viennent démontrer à quel point il est primordial pour la victime d'un virus informatique de pouvoir réclamer une indemnisation de celui ou celle ayant causé l'infection. Malheureusement, comme l'expliquent Pierre Trudel et al. :

> « *Dans le cyberespace comme ailleurs, la personne ayant personnellement posé le geste fautif dommageable est évidemment la première à en assumer la responsabilité. Cependant, dans les environnements électroniques, ces acteurs ne sont pas toujours identifiables ou peuvent se trouver hors d'atteinte. D'où l'intérêt de déterminer la responsabilité des autres*

---

[632] ANONYME, *op. cit.*, note 20, p. 324. Voir aussi Martin P. J. KRANTZ et Cruickshank PHILLIPS, *loc. cit.*, note 257, 69.
[633] *Op. cit.*, note 4.
[634] Joseph N. FROEHLICH et al., « Computer Viruses : Making the Time Fit the Crime », (1997) en ligne sur le site de Ford Marrin Esposito Witmeyer & Gleser, L.L.P. : <http://www.fmew.com/archive/virus/> (dernière mise à jour : mars 1997).

> *intervenants dans la chaîne de transmission de l'information* »[635].

La question se pose alors des fondements de l'attribution de la responsabilité aux intermédiaires[636]. Tel qu'il le fut démontré dans notre mémoire, puisque tout internaute doit se comporter comme une personne prévoyante et prudente, la norme de prudence requiert qu'il tente de prévoir et de prévenir les conséquences nuisibles de ses actes[637]. Or, il est essentiel pour tout usager de comprendre que, de par la structure du réseau, ses actes affectent un nombre grandissant d'individus envers lesquels il a donc un devoir de diligence. Ainsi, le transmetteur d'un virus pourra encourir une responsabilité civile s'il est prouvé qu'il a fait preuve de négligence en ne s'assurant pas de l'absence dudit virus[638], comportement qu'adopterait une personne raisonnable et diligente.

Certains prétendront qu'il existe des problèmes inhérents à l'utilisation de la responsabilité civile comme outil de renforcement des mesures de sécurité dans le domaine informatique[639]. En effet, il est possible d'avancer que le modèle du juge Hand met un fardeau économique trop élevé sur les petites et moyennes entreprises et favorise donc les multinationales telles Microsoft et AOL[640]. Les coûts associés à l'établissement de mesures de sécurité raisonnablement efficaces n'étant ni exorbitants, ni même excessifs, cet argument nous semble irrecevable. Il serait plutôt approprié de souligner que ces outils sont non seulement à la portée des PME, mais également à celle des consommateurs.

---

[635] Pierre TRUDEL et al., *op. cit.*, note 201, p. 5-13.
[636] *Id.*.
[637] PISA, *loc. cit.*, note 6.
[638] Olivier ITEANU, *loc. cit.*, note 16.
[639] Voir, entres autres, Robyn WEISMAN, *loc. cit.*, note 28.
[640] *Id.*

Nous avons, pour cette étude, abordé les seuls cas des intermédiaires ayant participé à la propagation de virus informatiques. Il importe cependant de souligner, comme l'ont fait certains auteurs, qu'il existe d'autres individus dont la responsabilité civile pourrait être engagée dans le cas d'une infection virale. Le premier cas est celui des manufacturiers de logiciels et de systèmes d'exploitation. En effet, « [t]*he possibility exists that a manufacturer of a computer or the developer of an operating system might be held liable if the computer or software contained defects that rendered the system unreasonably vulnerable to damaging software* »[641]. De plus, le fabricant d'un logiciel antivirus pourrait également engager sa responsabilité s'il omet d'aviser l'acheteur potentiel des limites de son produit, si ce produit échoue dans la détection d'un virus ou s'il tarde dans ses mises à jour[642]. Cette responsabilité sera d'autant plus importante si le logiciel prétend être efficace à 100%[643], transformant sa simple obligation de moyen en obligation de résultat ou même de garantie.

Nonobstant ce qui précède, il demeure que les utilisateurs du réseau devraient être méfiants lors de chaque opération pouvant les exposer à un virus informatique puisqu'il sera toujours possible pour un nouveau virus de franchir les barrières de sécurité des entreprises les plus consciencieuses, d'autant plus qu'il ne faudrait jamais oublier qu'un virus peut se propager à l'extérieur du réseau, soit par le biais d'un support matériel tel une disquette[644]. Pour conclure, comme l'explique un expert dans le domaine des virus informatiques :

---

[641] Richard B. LEVINE, *op. cit.*, note 26, p. 253.
[642] Robbin A. BROOKS, *loc. cit.*, note 222, 359-360. Il faut cependant souligner, comme le fait judiciairement Christiane Feral-Schuhl, que, dans la majorité des cas, « *le fournisseur d'un détecteur de virus a prévu contractuellement qu'il n'était tenu que dans la limite de son engagement contractuel et a pris la précaution d'énumérer les virus susceptibles d'être éradiqués par le détecteur* ». Christiane FERAL-SCHUHL, *op. cit.*, note 1, p. 44.
[643] Robbin A. BROOKS, *loc. cit.*, note 222, 381.
[644] *Loc. cit.*, note 444.

> « *The best way to protect yourself, and your personal computers against malicious mobile code is to be aware of what rogue code can do, use and antivirus scanner, close known security holes, and be aware of what runs on your computer. Malicious mobile code is not going away, and the best we can do is to manage it effectively, like any risk, and be prepared* »[645].

Bien sûr, tout recours à ces mesures de protection demeure, dans plusieurs cas, facultatif et nul ne peut être juridiquement contraint à utiliser une quelconque technologie antivirale s'il est prêt à en subir les conséquences économiques. Comme le souligne Lord Denning, « *Everyone is free to* [use] *it or not, as he pleases... Free in the sense that everyone is free to run his head against a brick wall, if he pleases. He can do it if he likes without being punished by the law. But it is not a sensible thing to do* »[646].

---

[645] Roger A. GRIMES, *op. cit.*, note 35, p. 492.
[646] *Froom* c. *Butcher*, [1975] 3 All ER 520 à la page 525.

Table de la législation

Textes canadiens

Textes fédéraux

Code criminel, L.R. 1985, c C-46.

Textes québécois

Code civil du Québec, L.Q. 1991, c. 64

Loi concernant le cadre juridique des technologies de l'information, L.Q. 2000, c. 32.

Loi sur la protection du consommateur, L.R.Q., c. P-40.1

Textes ontariens

Loi sur la taxe de vente au détail, L.R.O. 1990, chap. R.31

Textes américains

U.S. Const.

Communications Decency Act, 47 U.S.C. §230

Digital Millenium Copyright Act, 17 U.S.C. §512

Textes suisses

Code pénal suisse du 21 décembre 1937.

Table des jugements

Jurisprudence canadienne

Roberge c. *Bolduc*, [1991] 1 R.C.S. 374.

Jurisprudence américaine

A&M Records, Inc. c. *Napster, Inc.*, 239 F.3d 1004 (Cal., C.A., 2001).

American Civil Liberties Union c. *Reno*, 929 F. Supp. 824 (E.D. Pa. 1996).

Brandenburg c. *Ohio*, 395 U.S. 444 (1969).

Chute v. *Bank One of Akron*, N.A., 460 N.E.2d 720 (Ohio App. 1983).

CompuServe Inc. v. *Cyber Promotions, Inc.*, 1997 WL 109303 (S.D. Ohio Feb. 3, 1997).

Froom c. *Butcher*, [1975] 3 All ER 520.

Long c. *Adams*, 175 Ga. App. 538, 333 S.E. 2d 852 (1985).

Reno v. *American Civil Liberties Union*, 117 S. Ct. 2329 (1997).

Rice c. *Paladin Enterprises, Inc.*, 395 U.S. 444 (1969).

Thrifty Tel, Inc. v. *Bezeneck*, 46 Cal. App. 4th 1559 (1996).

T.J. Hooper c. *Northern Barge*, 60 F. 2d 737 (2nd Cir. C.A., 1932).

United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

Yahoo!, Inc. c. *La ligue contre le racisme et l'antisémitisme*, 169 F.Supp.2d 1181 (2001).

Zippo Manufacturing Co. c. *Zippo Dot Com. Inc.*, (952) F.Supp. 1119 (United States District Court W.D. Pennsylvania).

Jurisprudence française

Com. 25 nov. 1997, Bull. civ., n° 95-14.603.

Jurisprudence anglaise

R. c. *Whiteley*, (1991) 93 Cr App Rep 25.

Weller and Co. c *Foot and Mouth Sisease Research Institute* [1965] 3 All ER 560.

Bibliographie

Monographies et recueils

ÉTUDE DES QUESTIONS DE DROIT ENTOURANT LA SÉCURITÉ DES RENSEIGNEMENTS ÉLECTRONIQUES, Chapitre 7 : « Usage criminel des technologies de l'information », en ligne sur le site du *Ministère de la justice du Canada* : <**http://canada.justice.gc.ca/fr/ps/ec/toc.html**> (Mise à jour : 2002-06-19).

ANONYME, *Maximum Security*, 3e éd., Indianapolis, Sams, 2001, 896 p.

BAUDOUIN, J.-L., *Les obligations*, 4e éd., Cowansville, Yvon Blais, 1993, 805 p.

BAUDOUIN, J.-L. et P. DESLAURIERS, *La responsabilité civile*, 5e éd., Cowansville, Éditions Yvon Blais, 1998, 1684 p.

BENYEKHLEF, K., « Réflexions pour une approche pragmatique des conflits de juridiction dans le cyberespace », dans GAUTRAIS, V. (éd.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 137.

BRANSCOMB, A.W., « Rogue Computer Programs and Computer Rogues : Tailoring the Punishment to Fit the Crime », dans HOFFMAN, L.J. (éd.), *Rogue Programs: Viruses, Worms, and Trojan Horses*, New York, Van Nostrand Reinhold, 1990, p. 61.

BURGER, R., *Virus : La maladie des ordinateurs*, Paris, Micro Application, 1989, 322 p.

CALABRESI, G., *The Cost of Accidents*, New Haven, Yale University Press, 1970, 340 p.

CARBONNIER, J., *Droit Civil*, Tome 4, « Les obligations », Paris, Presses universitaires de France, 1996, 610 p.

COHEN, F.B., *A Short Course on Computer Viruses*, 2e éd., New York, Wiley, 1994, 250 p.

COHEN, F., « Implications of Computer Viruses and Current Methods of Defense », dans DENNING, P.J. (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 381.

CÔTÉ, P.-A., *Interpretation des lois*, 3e éd., Montréal, Thémis, 1999, 1035 p.

DIRECTOR, D., « Law and Order for the Personal Computer », dans DENNING, P.J. (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 528.

DENNING, P.J. (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, 554 p.

DENNING, P.J., « The Internet Worm », dans DENNING, P.J. (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 193.

DENNING, P.J., « Computer Viruses », dans DENNING, P.J. (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 285.

FÉRAL-SCHUHL, C., *Cyber droit : Le droit à l'épreuve de l'Internet*, Paris, Dunod, 2000, 323 p.

FITES, P., et al., *The Computer Virus Crisis*, 2e éd., New York, Van Nostrand Reinhold, 1992.

FORCHT, K.A., « Ethical Use of Computers », dans HOFFMAN, L.J. (éd.), *Rogue Programs: Viruses, Worms, and Trojan Horses*, New York, Van Nostrand Reinhold, 1990, p. 117.

GAUTRAIS, V., *Le contrat électronique international*, 2e éd., Louvain-La-Neuve, Bruylant-Academia, 2002, 427 p.

GEIST, M., *Internet Law in Canada*, North York, Captus Press, 2000, 747 p.

GERROLD, D., *When Harlie Was One*, New York, Nelson Doubleday Inc., 1972, 247 p.

GRIMES, R.A., *Malicious Mobile Code : Virus Protection for Windows*, Sebastopol, O'Reilly, 2001, 522 p.

GRINGRAS, C., *The Laws of the Internet*, Londres, Butterworths, 1997, 399 p.

HANDA, S. et al., *Cyber Law*, Toronto, Stoddart, 1997, 282 p.

HARLEY, D. et al., *Viruses Revealed*, Berkeley, McGraw-Hill, 2001, 683 p.

HIGHLAND, H.J., *Computer Virus Handbook*, Oxford, Elsevier Advanced Technology, 1990, 375 p.

HOFFMAN, L.J. (éd.), *Rogue Programs: Viruses, Worms, and Trojan Horses*, New York, Van Nostrand Reinhold, 1990, 384 p.

HRUSKA, J., *Virus informatiques et systèmes anti-virus*, Paris, Masson, 1992, 149 p.

JACOBSON, R.V., *The PC Virus Control Handbook*, 2e éd., San Francisco, Miller Freeman Publications, Inc., 1990, 162 p.

LABBÉ, E., et al., *Le guide juridique du commerçant électronique*, Version préliminaire pour distribution au Symposium International 2001 : Internet, commerce électronique, droit et arbitrage, 26 au 28 avril 2001, Gammarth, Tunisie, 277 p.

LANDES, W.M. et R.A. POSNER, *The Economic Structure of Tort Law*, Cambridge, Harvard University Press, 1987, 329 p.

LESAGE-JARJOURA, P. et S. PHILIPS-NOOTENS, *Éléments de responsabilité civile médicale : Le droit dans le quotidien de la médecine*, 2e éd., Cowansville, Éditions Yvon Blais, 2001, 518 p.

LESSIG, L., *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, 297 p.

LEVINE, R.B., *The Computer Virus Handbook*, Berkeley, Osborne McGraw-Hill, 1990, 411 p.

LILEN, H. et F. DAROT, *Virus & protection*, Paris, Radio, 1991, 172 p.

LINDEN, A.M. et L.N. KLAR, *Canadian Tort Law: Cases, Notes & Materials*, 11e éd.Toronto, Butterworths, 1999, 766 p.

LOSCOCCO, P.A. et al., « The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments », dans *Proceedings of the 21st National Information Systems Security Conference*, 1998, p. 303.

LUDWIG, M., *The Giant Black Book of Computer Viruses*, American Eagle Publications, 1998, 490 p.

LUDWIG, M., *The Little Black Book of Computer Viruses*, American Eagle Publications, 1996, 167 p.

MACKAAY, E., *L'analyse économique du droit*, tome 1, Montréal, Thémis, 2000, 319 p.

MACKAAY, E., *L'analyse économique du droit*, tome 2, Montréal, Thémis, non publié.

MICROSOFT COORPORATION, *Microsoft Office XP Security White Paper*, 2001, 37 p.

MURRAY, W.H., « The Application of Epidemiology to Computer Viruses », dans HIGHLAND, H.J. (éd.), *Computer Virus Handbook*, Oxford, Elsevier Advanced Technology, 1990, p. 15.

NADEAU, A., *Traité de droit civil du Québec*, tome 8, Montréal, Wilson & Lafleur, 1965, 664 p.

NADEAU, A. et L. DUCHARME, *Traité de droit civil du Québec*, tome 9, Montréal, Wilson & Lafleur, 1965, 643 p.

NEUMANN, P.G., « A Perspective From the RISKS Forum », dans DENNING, P.J. (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 535.

NIMMER, R.T., *The Law of Computer Technology : rights, licenses, liabilities*, 3e éd., St-Paul, West Group, 1997.

PERREAULT, J., *Des stipulations de non-responsabilité*, Montréal, Imprimerie modèle limitée, 1939, 232 p.

POSNER, R., *Economic Analysis of Law*, 5e éd., New York, Aspen Law and Business, 1998, 802p.

REID, H., *Dictionnaire de droit québécois et canadien*, Montréal, Wilson & Lafleur, 1994, 769 p.

RICHARD, F., *Vocabulaire de la sécurité et des virus informatiques*, Ottawa, Groupe Communication Canada, 1995, 333 p.

ROY, D.J. et al., *VIH et SIDA : Rapport d'étude sur les aspects éthiques et juridiques*, Québec, Ministère de la santé et de services sociaux, 1988, 121 p.

ROYER, J., « La preuve civile » 2e éd., Cowansville, Yvon Blais, 1995, 1290 p.

ROZOVSKY, L.E. et F.A. ROZOVSKY, *AIDS and Canadian Law*, Toronto, Butterworths, 1992, 147 p.

SAMUELSON, P., « Can Hackers Be Sued for Damages Caused by Computer Viruses? », dans DENNING, P.J. (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 472.

SAMUELSON, P., « Computer Viruses and Worms: Wrong, Crime, or Both? », dans DENNING, P.J. (éd.), *Computers Under Attack: Intruders, Worms, and Viruses*, New York, ACM Press, 1990, p. 479.

SAVATIER, R., *Traité de la responsabilité civile*, tome 1, Paris, Librairie générale de Droit et de Jurisprudence, 1951, 2 v.

SAXBY, S., *Encyclopedia of information technology law*, London, Sweet & Maxwell, 2000.

SCHWEITZER, J.A., *Managing Information Security: Administrative, Electronic, and Legal Mesures to Protect Business Information*, 2e éd., Stoneham, Butterworths, 1990, 197 p.

SCOTT, M.D., *Computer Law*, New York, Wiley, 1985.

SLADE, R., *Robert Slade's Guide to Computer Viruses: How to Avoid Them, How to Get Rid of Them, and How to Get Help*, 2e éd., New York, Springer, 1996, 422 p.

SPAFFORD, E.H. et al., « What Is a Computer Virus? », dans HOFFMAN, L.J. (éd.), *Rogue Programs: Viruses, Worms, and Trojan Horses*, New York, Van Nostrand Reinhold, 1990, p. 29.

STANGER, J., (éd.), *E-Mail Virus Protection Handbook*, Rockland, Syngress, 2000, 476 p.

TAKACH, G. S., *Computer Law*, Toronto, Irwin Law, 1998, 478 p.

THEMENS, F., *Internet et la responsabilité civile*, Cowansville, Éditions Yvon Blais, 1998, 152 p.

THORENS, J., *Le dommage causé à un tiers*, Genève, Imprimerie Henri Studer S.A., 1962, 135 p.

TRUDEL, P., « La responsabilité civile : qui répond de l'information? », dans *L'espace cybernétique n'est pas une terre sans loi : Études des questions relatives à la responsabilité à l'égard du contenu circulant sur Internet*, Ottawa, Industrie Canada, 1997, p.135.

TRUDEL, P., « La responsabilité des intermédiaires techniques sur Internet », Exposé présenté lors de la journée d'étude sur la *Loi concernant le cadre juridique des technologies de l'information*, Montréal, 27 septembre 2001.

TRUDEL P., « La responsabilité des acteurs du commerce électronique », dans GAUTRAIS, V. (éd.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 607.

TRUDEL, P. et al., *Droit du cyberespace*, Montréal, Éditions Thémis, 1997.

TRUDEL, P. et R. GÉRIN-LAJOIE, « La protection des droits et des valeurs dans la gestion des réseaux ouverts », dans Daniel POULIN, Pierre TRUDEL et Ejan MACKAAY (dir.), *Les autoroutes électroniques : usages, droits et promesses*, Montréal, Éditions Yvon Blais, 1995, p. 279.

TUNC, A., *La responsabilité civile*, 2e éd., Paris, Economica, 1989, 200 p.

VANSWEEVELT, T., *Le sida et le droit : Une étude de droit de la responsabilité et de droit des assurances*, Bruxelles, CED-Samsom, 1990, 158 p.

VÉZINA, N. et L. LANGEVIN, « L'exécution de l'obligation » dans F. BOUSQUET (dir.), *Obligations et contrats*, « Collection de droit » vol. 5, Cowansville, Éditions Yvon Blais, 2002, p. 63.

WHITE, S.R. et al., « Coping with Computer Viruses and Related Problems », dans HOFFMAN, L.J. (éd.), *Rogue Programs: Viruses, Worms, and Trojan Horses*, New York, Van Nostrand Reinhold, 1990, p. 7.

WILLIAMS, R.D. et B.T. SMYTH, *Computer and Internet Liability: Strategies, Claims and Defenses*, 2e éd., Gaithersburg, Aspen Law & Business, 2001.

WOOD, C.C., « The Human Immune System as an Information Systems Security Reference Model », dans HOFFMAN, L.J. (éd.), *Rogue*

Programs: Viruses, Worms, and Trojan Horses, New York, Van Nostrand Reinhold, 1990, p. 50.

Articles de revue

« Bombs on the Internet: New fears about free speech vs. public safety », en ligne sur le site *CNN.com* : <http://www.cnn.com/TECH/science/9805/29/t_t/bombs.on.internet/> (dernière mise à jour: 29 mai 1998).

« L'éditeur de Soft & Micro responsable des conséquences de l'infection », (1998) 112 *Expertise des systèmes d'information* 414.

« The Anti-Virus Can of Worms », (2001) en ligne sur le site *ISP-Planet* : <http://www.isp-planet.com/services/2001/av_bol.html> (dernière mise à jour : 13 décembre 2001).

« Persistant Viruses Sound Industry Alarm », (2001) en ligne sur le site *ArmourPlate* : <http://www.armourplate.com/news/015.htm> (dernière mise à jour : 14 août 2001).

« Symantec's Free Web-Hosted Security Check Analyses Computer Vulnerabilities For More Than 2 Million Pc Users », (2002) en ligne sur le site Symantec.com : <http://www.symantec.com/PressCenter> (date de visite : 6 juillet 2002).

ASSOCIATED PRESS, « Kournikova virus creator arrested, released », (2002) en ligne sur le site de *USA Today* : <http://www.usatoday.com/life/cyber/tech/2001-02-14-virus-arrest.htm> (dernière mise à jour : 6 février 2002).

BAKER, T., « Your Computer Is Worm Food : Thanks To Email, Malicious Code Really Gets Around », (2002) 13 *Smart Computing* 62.

BALBO-IZARN, N., « Le professionnel face aux risques informatiques », (2001) 34 *Les petites affiches* 4.

BAWDEN, B.R., « Les dix commandements de l'informatisation », (1993) *CA Magazine* 34.

BENDER, L., « A Lawyer's Primer in Feminist Theory and Tort », (1989) 38 *J. of Legal Educ* 3.

BEYER, M.L., « Managing the Risk of Virus Liability », (1993) 12 *Computer Law* 22.

BLOCH, A., « Virus : responsabilité juridique », (1989) 114 *Expertises* 52.

BRANSCOMB, A.W., « Rogue Computer Programs And Computer Rogues: Tailoring the Punishment to Fit the Crime » (1990) 16 *Rutgers Computer & Tech. L.J.* 1.

BROOKS, R.A., « Deterring the Spread of Viruses Online : Can Tort Law Tighten the 'Net'? », (1998) 17 *Rev. Litig.* 343.

BROWN, B.D., « Emerging Insurance Products in the Electronic Age », (2001) 31 *FALL Brief* 28.

BURNS, P., « *Res Ipsa Loquitur*: The Unlamented Demise of a Pleader's Shibboleth » (1999) 57 *The Advocate* 839.

CADEN, M.L. et S.E. LUCAS, « Accidents on the Information Superhighway : On-Line Liability And Regulation », (1996) 2 *RICH. J.L. & TECH.* 3.

CAMPBELL, C.E., « Murder Media – Does Media Incite Violence and Lose First Amendment Protection? », (2000) 76 *Chi.-Kent L. Rev.* 637.

CESARE, K., « Prosecuting Computer Virus Authors : The Need For An Adequate And Immediate International Solution », (2001) 14 *Transnat'l Law* 135.

COHEN, G.M., « The Negligence-Opportunism Tradeoff in Contract Law », (1992) 20 *Hofstra L. Rev.*, 941.

COLE, G.S., « Tort Liability for Artificial Intelligence and Expert Systems », (1990) *Comp/Law jour.* 127.

COLOMBELL, M.R., « The Legislative Response to the Evolution of Computer Viruses » (2002) 8 *Rich. J.L. & Tech.* 18.

CommSPEED, « *CommSpeed* Introduces Revolutionary Virus Protection and Spam Filtering Services » (2002) en ligne sur le site *CommSPEED*: <http://www.commspeed.com> (dernière mise à jour : 11 mars 2002).

CONSUMERS UNION of U.S., INC., « Cyberspace Invaders », (2002) en ligne sur le site *ConsumerReports.org* : <http://www.consumerreports.org/main/detailv2.jsp?CONTENT%3C%3Ecnt_id=159611&FOLDER%3C%3Efolder_id=18151&bmUID=1038263919040> (dernière mise à jour : juin 2002).

COSTES, L., « Assurez vos risques de sinistres sur Internet », (1999) 112 *Lamy droit de l'informatique et des réseaux*, 13.

DAILEY, E., « Rice v. Paladin Enterprises, Inc. : Does the First Amendment Protect Instruction Manuals On How To Commit Murder? », (1999) 6 *Vill. Sports & Ent. L.J.* 79.

De VILLIERS, M., « Virus Ex Machina Res Ipsa Loquitur », (2002) 73 p.

ÉQUIPE ASSURANCES ET RESPONSABILITE PROFESSIONNELLE, « Le commerce de l'assurance dans le cyberespace », (1998) en ligne sur le site de *Ogilvy Renault* : <http://www.ogilvyrenault.com/fr/data/pu/107f_e.pdf> (date de visite : 26 juillet 2002).

EPSTEIN, R.A., « The Path to the *T.J. Hopper*: The Theory and History of Custom in the Law of Tort » (1992) 21 *Journal of Legal Studies* 1.

FAULKNER, S., « Invasion of the Information Snatchers : Creating Liability for Corporations with Vulnerable Computer Networks », (2000) 18 *J Marshall J. Computer and Info. L.* 1019.

FORD, R. et al., « Hoaxes & Hypes » (1997) en ligne sur le site *IBM Research* : <http://www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html> (date de visite : 10 juin 2002).

FROEHLICH, J.N. et al., « Computer Viruses : Making the Time Fit the Crime », (1997) en ligne sur le site de Ford Marrin Esposito Witmeyer & Gleser, L.L.P. : <http://www.fmew.com/archive/virus/> (dernière mise à jour : mars 1997).

GAGNON, A., « Que faire en cas d'attaque de vos systèmes informatiques par un pirate », (2002) 13 *Le monde juridique* 29.

GALLAGHER, R., « Victim or Villain? Viral Liability: Guard against viruses or face legal action », (2001) en ligne sur le site *FAB IT Solutions* : <http://www.fabit.com/antivirus/businesliab.asp> (dernière mise à jour : 17 août 2001).

GEY, S.G., « Fear Of Freedom : The New Speech Regulation In Cyberspace », (1999) 8 *Tex. J. Women & L.* 183.

GOLD, S., « New Virus Creation Utility Set to Wreak Havoc », (2001) en ligne sur le site *Newsbytes* :

<http://www.newsbytes.com/news/01/163077.html> (dernière mise à jour : 13 mars 2001).

GOLDSTEIN, M.P., « Service Provider Liability for Acts Committed by Users: What You Don't Know Can Hurt You », (2000) 18 *J. Marshall J. Computer & Info. L.* 591.

GORDON, S., « Hoaxes and Hypes » (1997) en ligne sur le site *IMB Research* : <http://www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html> (date de visite : 11 juillet 2002).

GORDON, S., « Rx for AV » (1999) en ligne sur le site *Information Security* : <http://www.infosecuritymag.com/articles/1999/gordon.shtml> (dernière mise à jour : Novembre 1999).

GORDON, S., « The Generic Virus Writer II » (1994) en ligne sur le site *IBM Research* : <http://www.research.ibm.com/antivirus/SciPapers/Gordon/GVWII.html#NEWAGE> (Date de visite : 1 mai 2002).

GORDON, S., « Who Writes this Stuff? », (1996) en ligne sur le site *Commandcom* : <http://www.commandcom.com/virus/writes.html> (date de visite : 1 mai 2002).

GORDON, S., « Why Computer Viruses Are Not – And Never Were – A Problem », (1994) en ligne sur le site *Commandcom* : <http://www.commandsoftware.com/virus/problem.html> (date de visite : 1 mai 2002).

HANSON, D.J., « Easing Plaintiff's Burden of Proving Negligence for Computer Malfunction », (1983) 69 *Iowa L. Rev.* 241.

HELIS, P. et MOZAS, P., « Chronique multimedia », (1998) 89 *Petites affiches* 18.

ISHMAN, M., « Computer Crimes And The Respondeat Superior Doctrine : Employers Beware », (2000) 6 *B.U.J. Sci. & Tech. L.* 6.

ITEANU, O., « Virus, les implications légales », (1993) 1 *Chaos Digest.*

JOHNSON, D.R. et K.A. MARKS, « Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let our Conscience (and our Contracts) Be our Guide? », (1993) 38 *Vill. L. Rev.* 487.

KASS, I.A., « Regulating Bomb Recipes on the Internet : Does Frist Amendment Law Permit the Government to React to the Most Egregious Harms? », (1996) 5 *S. Cal. Interdisciplinary L. J.* 83.

KRANTZ, M.P.J. et C. PHILLIPS, « *Legal Vaccines for computer viruses* », (1988) 5 *Canadian Computer Law Reporter* 69.

LABBÉ, E., « Spamming en Cyberespace : à la recherche du caractère obligatoire de l'autoréglementation », (1999) en ligne sur le site *Lex Electronica* : <http://www.lex-electronica.org/articles/v6-1/labbe.htm> (dernière mise à jour : printemps 2000).

LAMONTAGNE, C., « Aménagement d'une piscine privée : contraintes juridiques et responsabilité », (1990) 92 *R. du N.* 586.

LEAHY, M.C.M., « Liability for Mishandled Computer Information », (2001) 18 *J. Marshall J. Computer & Info. L.* 1019.

LEAHY, M.C.M., « Tort Liability for Failure to Provide Computer Disaster Recovery Measures », (1995) 29 *Am. Jur. Proof of Facts 3d* 53.

LEE, A., « Why Traditional Insurance Policies Are Not Enough : The Nature of Potential E-Commerce Losses & Laibilities », (2001) 3 *Vand. J. Ent. L. & Prac.* 84.

LEYDEN, J. « Malware by Numbers : Online Virus Creation Tool Spotted », (2002) en ligne sur le site *The Register* : <http://www.theregister.co.uk/content/56/24272.html> (dernière mise à jour : 4 mars 2002).

LYMAN, S.C., « Civil Remedies for the Victims of Computer Viruses », (1992) 11 *Computer/Law Journal* 607.

MANNIG, G. « Après SirCam », (2001) en ligne sur le site réalités-virus.org: <http://realites-virus.org/2001-08-16.html> (dernière mise à jour : 16 août 2001).

MASSINGALE, S. et A. FAYE BORTHICK, « Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services », (1990) 12 *W. New Eng. L. Rev.* 167.

MALONE, R.J et R.R. LEVARY, « Computer Viruses : Legal Aspects », (1994) 4 *U. Miami Bus. LJ* 125.

MARSHALL, E., « The Scourge of Computer Viruses », (1988) 240 *Science* 133.

MARTIN, S., « 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, 167.

MICHELI, F.R., « La répression de la propagation de virus informatiques en droit pénal suisse », (2000) en ligne sur le site de *Python Schifferli Peter & Partners* : <http://www.psplaw.ch/Publications/Virus.html> (date de visite, 21 juillet 2002).

MOORE, B., « À la recherche d'une règle générale régissant les clauses abusives en droit québécois », (1994) 28 *R.J.T.* 177.

MUND, A.J., « Organisational Liability Exposure : A Conceales Virus Threat », (1990) en ligne sur le site <http://www.cmcnyls.edu/papers/VIRUSES.TXT> (date de visite : 10 janvier 2002).

NACHENBERG, C., « Future Imperfect », (1997) *Virus Bulletin* 6.

NICOL, P., « Trépas de la *res ipsa loquitur* », (1999) *La presse juridique* 4.

NICOLEAU, P., « La protection des données sur les autoroutes de l'information », (1996) *Recueil Dalloz* 111.

ORTIZ, S., « *Twisted Bits : How Computer Viruses Do Their Dirty Work* » (2002) 13 *Smart Computing* 58.

PERRITT, H.H. Jr., « Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction », (1995) en ligne sur le site du *Chicago-Kent College of Law Cyberlaw Jurisdiction* : <http://www.kentlaw.edu/cyberlaw/resources/interjuris.html> (dernière mise à jour : 12 octobre 1995).

PICARD, R., « Problèmes de juridiction dans le cyberespace », (2001) 160 *Développements récents en droit de l'Internet* 1.

PISA, « Virus », (2001) en ligne sur le site de *PISA* : <http://pisa.belnet.be/pisa/fr/jur/virus.htm> (date de visite 25 octobre 2001).

POULSEN, K. « Justice mysteriously delayed for 'Melissa' author », (2001) en ligne sur le site *The Register* :

<http://www.theregister.co.uk/content/archive/20751.html> (dernière mise à jour : 8 janvier 2001).

POWER, R., « 2002 CSI/FBI Computer Crime and Security Survey », (2002) 8 *Computer Security Issues & Trends* 1.

REITER, L. et R. LEMOS, « FBI hunting for virus writer » (1999) en ligne sur le site zdnet.com : <http://www.zdnet.com.com/2102-11-514208.html> (dernière mise à jour : 31 mars 1999).

ROBBINS, V.H., « Vendor Liability for Computer Viruses and Undisclosed Disabling Devices in Software », (1993) 10 *Computer Lawyer* 20.

RUSTAD, M.L., « Private Enforcement of Cybercrime on the Electronic Frontier », (2001) 11 *S. Cal. Interdisc. L.J.* 63.

SALVAS, B., « Foulard, virus (bis) et sécurité », (2001) 10 *Entracte* 7.

SEGAN, S., « Killer Apps », (2002) 13 *Smart Computing* 54.

SUNSTEIN, C., « Is Violent Speech a Right? », (1995) en ligne sur le site *The American Prospect* vol. 6, no. 22 : <http://www.prospect.org/print/V6/22/sunstein-c.html> (dernière mise à jour : 23 juin 1995).

SCHWARTZ, E.I., « Trust Me, I'm Your Software », (1996) 17 *Discover* 78.

SPAFFORD, E.H., « Computer Viruses as Artificial Life », (1994) disponible à l'adresse : <http://www.cerias.purdue.edu/coast/archive/data/categ20.html> (date de visite: 17 juillet 2002).

SPAFFORD, E.H. et S.A. WEEBER, « Software Forensics: Can We Track Code to its Authors? », (1992) disponible à l'adresse <www.cerias.purdue.edu/homes/spaf/tech-reps/9210.pdf> (date de visite : 17 juillet 2002).

TRUDEL, P., « La responsabilité civile sur Internet selon la *Loi concernant le cadre juridique des technologies de l'information* », (2001) 160 *Développements récents en droit de l'Internet* 107.

WEISMAN, R., « Got A Virus? You're Sued ! », (2001) en ligne sur le site *Newsfactor.com* :

<http://www.newsfactor.com/perl/story/12529.html> (date de visite 4 novembre 2001).

WHITE, M., « The Cure: Antivirus Big Guns Help Keep Your PC Squeaky Clean », (2002) 13 *Smart Computing* 67.

WIKERSON, M., « Tort Law: Long v. Adams The Dirt on the Clean Hands Doctrine », (1988) 56 UMKC L. Rev. 791.

YOST, P.M. et al., « In Search of Coverage in Cyberspace : Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Computer Data », (2001) 54 *SMU L. Rev.* 2055.

Sites Internet

ACBM : <http://www.virus.ldh.org/>

Coderz.net : <http://www.coderz.net>

Comment ça marche : <http://www.commentcamarche.net

Google : <http://www.google.com>

Hoaxbuster : <http://www.hoaxbuster.com/>

HotMail : <http://www.hotmail.com>

Le grand dictionnaire terminologique :
<http://www.granddictionnaire.com/>

McAfee : <http://www.mcafee.com>

Symantec : <http://www.symantec.com>

Yahoo! Mail : <http://www.yahoomail.com>