Réflexion juridique autours de la notion de désinformation eu égard à la transmission de métavirus

Nicolas VERMEYS*

Lex Electronica, vol.10 n°3, Hiver/Winter 2006
http://www.lex-electronica.org/articles/v10-3/vermeys.htm

* Avocat chez Legault Joly Thiffault.

Introduction

Votre vieille tante, laquelle a votre intérêt à cœur, vous fait suivre un courriel reçu d'une de ses amies, qui l'a elle-même reçue de son gendre, lequel l'a reçu de son beau-frère, et ainsi de suite… Selon ce court message, un nouveau virus informatique[1] des plus destructeurs intitulé *Explorer* vient tout juste de voir le jour. Toujours selon cet avertissement, lequel, semble-t-il, est issu directement de chez Microsoft[2] et IBM[3], ce virus aurait pour effet d'effacer le contenu de votre disque dur le premier jeudi de chaque mois.

Heureusement il y a une façon fort simple d'enrayer cette problématique et l'auteur du message qu'on vous a fait suivre a eu la gentillesse de vous en informer : il suffit d'aller dans votre dossier « Windows » et d'effacer le fichier « Explorer »… Votre PC sera alors sain et sauf. Fort de cette nouvelle information, vous faites donc une vérification pour constater que votre système est effectivement infecté par ce terrible virus et vous vous empressez de l'effacer. Ce qui devait arriver arriva et votre ordinateur commence à afficher un message d'erreur vous annonçant qu'il ne peut accéder au fichier Explorer et procède à la fermeture de Windows. Votre vielle tante, malgré ses bonnes intentions, vous a induit en erreur… Explorer n'est pas un virus, c'est un métavirus !

Les métavirus sont des « virus » fictifs découlant du fruit de l'imagination des internautes, bref, ce sont des canulars[4]. Il ne s'agit donc pas de maliciels[5] au sens propre, puisque les métavirus infectent l'esprit des gens naïfs et non leurs ordinateurs[6]. Cependant, malgré l'inexistence factuelle de ces faux virus, leur impact peut s'avérer tout aussi dommageable que celui d'un véritable maliciel[7].

La question se pose donc : Dans la mesure où la transmission de métavirus peut être la source d'un certain préjudice pour les internautes, l'arsenal législatif devrait-il être mis à contribution pour enrayer cette problématique. En autres termes, l'un des rôles du droit, ou, plus

---

1 Les virus informatiques peuvent être décrits comme étant 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* ». Voir François RICHARD, *Vocabulaire de la sécurité et des virus informatiques*, Ottawa, Groupe Communication Canada, 1995, 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, (« *A virus is a program that can « infect » other programs by modifying them to include a, possibly evolved, version of itself* », Frederick COHEN, *A Short Course on Computer Viruses*, 2e éd., New York, Wiley, 1994, p. 2) d'autres la critiquent comme 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.

2 http://www.microsoft.com

3 http://www.ibm.com

4 ANONYME, *Maximum Security*, 3e éd., Indianapolis, Sams, 2001, p. 336.

5 Les maliciels (*malware*) sont des « *logiciels comportant des instructions malveillantes pouvant entraîner pertes et dommages* ». Voir François RICHARD, *Vocabulaire de la sécurité et des virus informatiques*, Ottawa, Groupe Communication Canada, 1995, p. 133.

6 ANONYME, *op. cit.*, note 4, p. 333.

7 REUTERS « La peur du virus plus destructrice que le virus lui-même », (2001) disponible sur le site *01net* : <http://www.01net.com/article/148435.html> (dernière mise à jour : 14 mai 2001).

particulièrement, de la responsabilité civile, étant la prévention des comportements anti-sociaux[8], pouvons-nous utiliser les outils législatifs à notre disposition pour responsabiliser les émetteurs de métavirus?

Cette question qui, force nous est d'admettre, découle tant d'une problématique sociologique que juridique nécessite tout de même un certain retour au concept de responsabilité et à ses composantes afin d'évaluer leur applicabilité à la problématique des métavirus, mais surtout à leur effectivité dans un tel contexte. Avant de se faire, il importe cependant de se pencher sur le fonctionnement de ces canulars informatiques et le rôle que nous jouons dans leur dissémination.

Il nous faut cependant souligner que le présent exposé ne se veut pas une simple démonstration de l'applicabilité des principes de la responsabilité civile à la problématique des métavirus, mais plutôt un discours soulignant les lacunes de ces principes qui, bien que pouvant trouver application, s'avèrent un remède plus ou moins adapté à la réalité créée par de tels canulars.

Les métavirus : définition et problématique

Les canulars informatiques prennent généralement la forme d'un courriel annonçant l'arrivée 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 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 informatiques[9] 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* ».[10]

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.*

---

8 André TUNC, *La responsabilité civile*, 2e éd., Paris, Economica, 1989, p. 55.

9 « Un ver est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour se propager ». Voir Jean-François PILLOU, « Les vers » (2005) disponible sur le site *Comment ça marche* : <http://www.commentcamarche.net/virus/worms.php3> (date de visite : 30 octobre 2005).

10 Sarah GORDON, « Hoaxes and Hypes », (1997) disponible sur le site *IBM Research* : <http://www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html> (date de visite : 31 octobre 2005).

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 virus est déjà sur votre disque dur car il devrait être activé le 25 mai.
Bien à vous. »[11]

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[12]. Ainsi, l'utilisateur qui suivra les instructions de ce message causera un dommage à son système suite aux indications mensongères d'un tiers.

Le métavirus De ce fait, s'apparente au pourriel[13] ou à l'hameçonnage[14] dans la mesure où il s'agit d'une utilisation du courriel éthiquement répréhensible. Une distinction importante entre ces techniques, laquelle rend le contrôle judiciaire des métavirus plus complexe, réside cependant dans le fait que, contrairement aux pourriels ou aux courriels hameçons, les métavirus ne sont pas des envois massifs dont on peut facilement retracer les auteurs, mais bien des envois uniques se basant sur un mode pyramidal de diffusion pour se répandre. Bref, leurs auteurs sont souvent difficilement identifiables, raison de plus pour se questionner sur la responsabilité de ceux qui ont participé à la diffusion volontaire de ce canular.

Responsabiliser par le droit : l'applicabilité de la responsabilité au principe de la désinformation

Le recours au droit pour limiter la propagation de désinformations n'est pas un phénomène nouveau, voire propre à la problématique des métavirus. La responsabilité de ceux qui propagent des faussetés est spécifiquement visée par de nombreux textes législatifs. C'est ainsi qu'un publicitaire ou un commerçant ne peut propager de fausses informations sur ses biens ou services[15], qu'un avocat « *ne doit pas, directement ou indirectement, publier ou diffuser un rapport ou des commentaires qu'il sait faux ou qui sont manifestement faux à l'égard d'un tribunal ou de l'un de ses membres* »[16] et qu'« *un professionnel ne peut, par quelque moyen que ce soit, faire une représentation fausse, trompeuse ou incomplète à une personne qui recourt à*

---

[11] Source : H*oaxbuster.com* : <http://www.hoaxbuster.com/hliste/juin01/sulfnbk.html>, (Date de visite, 15 septembre 2002).

[12] *Id.*

[13] « Courrier électronique importun et souvent sans intérêt, constitué essentiellement de publicité, qui est envoyé massivement à un grand nombre d'internautes ou à une même adresse de courriel, et que l'on destine habituellement à la poubelle. » OFFICE DE LA LANGUE FRANÇAISE, « Le grand dictionnaire terminologique », (2005) disponible sur le site : <http://www.granddictionnaire.com> (date de visite : 31 octobre 2005).

[14] « Envoi massif d'un faux courriel, apparemment authentique, utilisant l'identité d'une institution financière ou d'un site commercial connu, dans lequel on demande aux destinataires, sous différents prétextes, de mettre à jour leurs coordonnées bancaires ou personnelles, en cliquant sur un lien menant vers un faux site Web, copie conforme du site de l'institution ou de l'entreprise, où le pirate récupère ces informations, dans le but de les utiliser pour détourner des fonds à son avantage. » *Id.*

[15] Voir notamment l'article 221 de la *Loi sur la protection du consommateur*, L.R.Q., c. P-40.1.

[16] Article 2.08 du *Code de déontologie des avocats*, R.Q., c. B-1, r.1.

ses services, notamment quant à son niveau de compétence ou quant à l'étendue ou à l'efficacité de ses services et de ceux généralement assurés par les membres de sa profession »[17].

Si aucun texte particulier ne peut s'appliquer, c'est alors vers les principes généraux de la responsabilité civile et de l'article 1457 du Code civil du Québec[18] que nous devons nous retourner :

> « *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.* »

En effet, dans la mesure où nous tentons d'évaluer s'il est opportun, voire possible, de se référer au droit pour contrôler et tenter d'atténuer la propagation de métavirus, il nous faut d'abord tenter d'établir si l'action de faire suivre un tel canular est source de responsabilité en évaluant si les composantes classiques du régime de responsabilité civile – à savoir : la capacité de discernement, l'existence d'une faute, l'existence d'un préjudice et la présence d'un lien de causalité entre la faute et le préjudice – sont présentes dans l'accomplissement d'un tel geste.

La capacité de discernement

La capacité de discernement qualifiée comme étant l'incapacité, pour un individu, de rendre compte des conséquences des actes qu'il pose[19] ne vient aucunement influencer notre réflexion quant à l'applicabilité du régime de responsabilité civile à celui ou celle qui ferait suivre un métavirus à un tiers. En effet, dans la mesure où un individu privé de raison ne peut être tenu responsable juridiquement de ses actes[20], il va de soi qu'il n'est pas visé par la présente problématique.

Qui plus est, celui ou celle que suivrait les conseils transmis par un individu incapable de discerner ne pourrait argumenter qu'il s'est fié de bonne foi sur ce dernier en supposant qu'il a mis de l'avant les efforts nécessaires pour vérifier la validité des informations transmises. Dans un tel scénario, la faute contributive de la victime[21] serait, à nos yeux, complètement libératrice pour le transmetteur du métavirus.

Que faire toutefois si le destinataire du métavirus ignore l'état d'incapacité du transmetteur ? En effet, comment un internaute dont la nièce de 5 ans utilise l'ordinateur de son père pour lui transmettre des courriels peut-il établir l'identité de son véritable interlocuteur ? Chaque cas étant un cas d'espèce, il s'agira, selon nous d'établir que le destinataire n'avait aucun indice lui

---

17 Article 60.2 du *Code des professions*, L.R.Q., c. C-26.

18 L.Q., c. 64.

19 Jean-Louis BAUDOUIN et Patrice DESLAURIERS, « Les conditions générales de la responsabilité du fait personnel – Généralités » dans *La responsabilité civile*, 6e édition, 2003, EYB2003RES2.

20 *Id.*

21 Voir l'article 1478 C.c.Q.

permettant de croire que son interlocuteur était incapable de discerner les conséquences de ses gestes et que son gardien a été négligent[22] en lui permettant de faire suivre un métavirus sans supervision.

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*. »[23]

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* »[24]. Commet ainsi une faute toute personne faisant défaut de se conformer aux devoirs généraux ou spécifiques de conduite imposés « *à un moment particulier de l'évolution sociale* » [25]. 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 des moyens, plus perfectionnés, de prévisibilité et d'évitabilité du mal, que la science moderne confère à l'agent* »[26].

Ce qui précède nous pousse donc à faire un premier constat, c'est-à-dire qu'un utilisateur d'ordinateur normalement prudent et diligent constitue la norme à laquelle nous devrons nous référer pour apprécier la responsabilité civile[27] de celui qui fait suivre un métavirus. Ce constat débouche cependant sur une première problématique puisqu'il nous est difficile d'évaluer s'il est raisonnable de s'attendre à ce qu'un utilisateur d'ordinateur normalement prudent et diligent tente de confirmer la validité d'un message avant de le faire suivre.

En effet, le comportement reprochable serait celui d'avoir transmis un tel message à un tiers sans avoir fait les vérifications qui s'imposent afin d'en confirmer la validité en se référant, par exemple, à l'un des nombreux sites Web sur le sujet tels www.vmyths.com ou www.hoaxbuster.com. Il nous faut donc d'abord établir si un tel comportement pourrait être considéré fautif en gardant à l'esprit, tel que nous venons de l'énoncer, que le critère applicable est celui d'un utilisateur d'ordinateur normalement prudent et diligent en 2005.

---

22 Voir les articles 1459 et suivants du Code civil du Québec.

23 Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 19.

24 Hubert REID, *Dictionnaire de droit québécois et canadien*, Montréal, Wilson & Lafleur, 1994, p. 239.

25 Jean-Louis BAUDOUIN et Patrice DESLAURIERS, « La faute » dans *La responsabilité civile*, 6e édition, 2003, EYB2003RES4.

26 René SAVATIER, *Traité de responsabilité civile*, Paris, Librairie générale de droit et de jurisprudence, 1951, 2e éd., t. 1, nº 166, p. 208.

27 En effet : « if you don't act like a "reasonably prudent computer owner", you may find yourself at the wrong end of a losing lawsuit. […] The answer is to be a responsible computer owner. ». Mark GROSSMAN, « Liability for you if you've been hacked », (2000) 3 *IT AUDIT* : <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=103> (dernière mise à jour : 1 août 2000).

Selon l'analyse faite par la doctrine[28] et les tribunaux[29] de l'article 1457 C.c.Q., une faute peut être intentionnelle ou résulter d'une négligence, d'une imprudence ou d'une maladresse[30]. 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* »[31] et doit compenser la victime dudit préjudice[32].

Par imprudence ou 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 ne cause de dommage à autrui* »[33].

Il importe par ailleurs de rappeler que, « *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* »[34]. Ainsi, le fait que l'acte négligent se produise en ligne ne viendrait pas contredire les principes fondamentaux du concept de négligence tels qu'ils existent depuis des siècles.

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* »[35].

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* »[36]. Il importe cependant de souligner que la négligence ne constitue une faute que si elle correspond à un devoir n'ayant pas été rempli[37].

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* » [38], l'on peut en déduire que la responsabilité de ces individus sera reconnue.

---

28 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 24.

29 *L'oeuvre de terrains de jeux de Québec* c. *Cannon*, (1940) 69 B.R. 112 (aux pages 114 et 118).

30 Hubert REID, *op. cit.*, note 24, p. 239.

31 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.

32 André TUNC, *La responsabilité civile*, 2e éd., Paris, Economica, 1989, p. 55.

33 Hubert REID, *op. cit.*, note 24, p. 386.

34 Michael D. SCOTT, *Computer Law*, New York, Wiley, 1985, p. 7-14.

35 Jean CARBONNIER, *Droit Civil*, Tome 4, « Les obligations », Paris, Presses universitaires de France, 1996, p. 378.

36 André NADEAU, *Traité de droit civil du Québec*, Tome 8, Montréal, Wilson & Lafleur, 1965, p. 46.

37 *Id.*

38 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, 1997, p. 135, à la page 195.

Ceci nous ramène donc à notre question : est-il négligent de faire suivre un métavirus sans faire de vérifications quant à l'authenticité du message contenu? Ou encore : une telle vérification constitue-t-elle une « précaution ordinaire et usuelle » ?

Dans l'affirmative, il nous faudra alors établir l'étendu des vérifications devant être entreprises afin de contrôler la désinformation avant de la transmettre à un tiers.

Quels sont donc les caractéristiques associées à l'utilisateur d'ordinateur normalement prudent et prévoyant tel que défini par la jurisprudence ?

En considérant la prolifération journalière de métavirus et autres canulars informatiques[39], il nous faut déduire que la majorité des utilisateurs ne font aucune vérification préalable à leur retransmission. Ceci pourrait notamment s'expliquer par le fait qu'ils ne savent simplement pas où faire de telles vérifications ou, comme nous l'avons déjà souligné, qu'ils font simplement confiance à l'individu leur ayant préalablement transmis le métavirus en question.

Ainsi, il serait raisonnable de prétendre que, selon les usages, l'utilisateur d'ordinateur moyen se contente de faire suivre ces messages sans autre précaution.

Cependant, l'usage ne constitue pas toujours un standard de décision approprié puisqu'il n'enregistre que les préférences des parties l'adoptant et non celles des victimes de son application[40]. Ainsi, si la coutume peut être prise en considération lors de l'identification de la « raisonnabilité » d'un comportement, son poids doit demeurer minime[41]. C'est d'ailleurs ce qui fut établi par la Cour suprême dans l'arrêt *Roberge* c. *Bolduc*[42] et par le juge Learned Hand dans l'arrêt américain *T.J. Hopper* c. *Northern Barge*[43] :

> « *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

---

39 Voir une liste non-exhaustive de ces canulars à l'adresse http://hoaxbusters.ciac.org/.

40 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.

41 *Id*.

42 [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* ».

43 60 F. 2d 737 (2nd Cir. C.A., 1932). Bien que cette affaire n'ait pas été citée par la jurisprudence québécoise, son application à notre droit semble appuyée par certains auteurs. Voir notamment Pierre TRUDEL et al., *Droit du cyberespace*, Montréal, Éditions Thémis, 1997, p. 5-38.

technologie de pointe disponible alors que cette même technologie aurait pu empêcher un préjudice[44].

Il en découle que l'existence et la disponibilité d'une technologie quelconque peuvent avoir pour effet d'accroître la responsabilité d'une personne[45]. 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* »[46].

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* »[47]. On pourrait donc être trouvé coupable lorsque l'on néglige d'adopter des outils perfectionnés mettant à profit de nouvelles technologies raisonnablement accessibles[48].

À la lumière de ce qui précède, il importe de rappeler qu'il n'est pas question ici d'une technologie révolutionnaire ou rare ou dispendieuse, mais simplement de faire les vérifications qui s'imposent avant de faire suivre un courriel, de telles vérifications pouvant être faites en quelques secondes sur Internet sans trop d'effort. Pour utiliser un langage économique, les coûts associés à des telles vérifications sont donc minimes, voire inexistants.

Or, 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[49] :

> « *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* »[50].

---

[44] 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 […] ».

[45] Brian R. BAWDEN, « Les dix commandements de l'informatisation », (1993) *CA Magazine* 34, 35.

[46] Monique C. M. LEAHY, « Liability for Mishandled Computer Information », (2001) 49 *Am. Jur. Trials* 281, § 6.

[47] Brian R. BAWDEN, *loc. cit.*, note 45, 35.

[48] *Id.*

[49] Richard A. EPSTEIN, *loc. cit.*, note 40, 1.

[50] Brian R. BAWDEN, *loc. cit.*, note 45, 35. Voir aussi Pierre TRUDEL et al., *op. cit.*, note 43, p. 5-38.

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[51]. Selon lui, trois considérations étaient pertinentes pour constituer un acte négligent : la probabilité d'un événement 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[52]), c'est-à-dire si B<PL.[53] 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* »[54].

Or, dans le cas des métavirus, le coût de la vérification est minime, il suffit de se diriger sur le Web et de consulter l'un des sites mentionnés ci-dessus, alors que les dommages, tel que nous le verrons plus loin, peuvent être assez importants. Les risques quant à eux dépendront de la naïveté du récepteur du métavirus, ou de la confiance dont il témoigne à l'égard du transmetteur.

Malgré son efficacité dans l'établissement de la négligence, le test du juge Hand affiche la lacune de ne pas tenir compte d'un élément très important de la responsabilité civile, à savoir la faute contributive de la victime[55]. 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* »[56]. Si, dans la majorité des situations, 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)[57], ceci amène un nouveau problème dans notre cas puisque, dans les faits, les précautions que pourrait prendre la victime sont exactement les mêmes que celles que pourrait prendre celui ou celle qui lui fait suivre un métavirus, à savoir s'informer sur la véracité du

---

51 *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947). Les principes mis de l'avant par cette décision 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.

52 Il s'agit de la notion de risque. Voir Kevin P. KALINICH et Kristina MCGRATH, « Identifying and Evaluating the Business Impact of Network Risks and Liabilities », (2004) 33 *WTR Brief* 18, 22 : « The classic definition used to calculate risk is Risk = Threat x Probability x Severity, where threat is the frequency of potentially adverse events (i.e., threat rate of computer virus encounters by an organization with 1,000 PCs = 88 per day); probability is the likelihood of success of a particular threat category against a particular organization (i.e., the number of machines of a particular type that exhibit a particular vulnerability); and severity is the total cost of the impact of a particular threat experienced by a vulnerable target. »

53 Ejan MACKAAY, *L'analyse économique du* droit, tome 2, Montréal, Thémis, non publié, p. 15. Voir aussi William M. LANDES et Richard A. POSNER, *The Economic Structure of Tort Law*, Cambridge, Harvard University Press, 1987, p. 85.

54 Ejan MACKAAY, *op. cit.*, note 53, p. 10.

55 William M. LANDES et Richard A. POSNER, *op. cit.*, note 53, p.88-89.

56 Art. 1479 C.c.Q.

57 Voir William M. LANDES et Richard A. POSNER, *op. cit.*, note 53, p. 87.

message. À notre avis, en appliquant le principe de l'article 1478 du Code civil du Québec[58], la responsabilité sera donc partagée entre les deux individus en considérant notamment les connaissances informatiques de chacun.

Ainsi, il appert qu'il soit possible de prétendre que celui ou celle qui fait suivre un métavirus à un tiers commet une faute dans la mesure où l'on peut considérer qu'il est négligent de ne pas vérifier la véracité des directives contenues dans un tel message avant de le transmettre. Cependant, pour en faire la preuve, il sera nécessaire d'établir qu'une personne raisonnable et diligente aurait accès à une telle information à moindre coût. Or, nous ne sommes pas convaincus que l'internaute moyen saurait où vérifier si le message reçu est un métavirus, ce qui pourrait être suffisant pour déresponsabiliser notre transmetteur.

Le dommage

« Les hoaxes coûtent de l'argent, parce que le temps c'est de l'argent, les ressources sont de l'argent. Les travailleurs perdent du temps quand ils diffusent massivement ces messages d'alerte à tous les membres de leur entreprise »[59].

Comme l'indique un auteur, les conséquences des métavirus sont multiples :

L'engorgement des réseaux en provoquant une masse de données superflues circulant dans les infrastructures réseaux ;

Une désinformation, c'est-à-dire faire admettre à de nombreuses personnes de faux concepts ou véhiculer de fausses rumeurs (on parle de *légendes urbaines*) ;

L'encombrement des boîtes aux lettres électroniques déjà chargées ;

La perte de temps, tant pour ceux qui lisent l'information, que pour ceux qui la relayent ;

La dégradation de l'image d'une personne ou bien d'une entreprise ;

L'incrédulité : à force de recevoir de fausses alertes les usagers du réseau risquent de ne plus croire aux vraies. [60]

S'il est vrai que cette énumération vise plutôt des désagréments que des dommages, elle omet de mentionner le préjudice le plus conséquent pour notre exposé, à savoir l'élimination de fichiers ou de données suite à l'application des indications contenues dans le message transmis.

Concrètement, cette liste démontre par ailleurs une nouvelle problématique, soit celle de l'opportunité d'entreprendre un quelconque recours. En effet, dans la mesure ou les dommages causés sont minimes et que la faute contributive de la victime devra être prise en compte, le recours aux tribunaux s'avère être une avenue difficilement envisageable parce que plus coûteuse que la restitution escomptée…

---

[58] « Lorsque le préjudice est causé par plusieurs personnes, la responsabilité se partage entre elles en proportion de la gravité de leur faute respective. La faute de la victime, commune dans ses effets avec celle de l'auteur, entraîne également un tel partage ».

[59] Rob ROSENBERGER dans REUTERS, *loc. cit.*, note 7.

[60] Jean-François PILLOU, « Les canulars (hoax) » (2005) disponible sur le site *Comment ça marche* : <http://www.commentcamarche.net/virus/hoax.php3> (date de visite : 30 octobre 2005).

Le lien de causalité

L'établissement du lien de causalité constitue le talon d'Achille de toute tentative de responsabiliser le transmetteur d'un métavirus. En effet, comme le souligne un auteur :

> « *dans la mesure où, par exemple, dans une instance donnée, la preuve révèle que la victime d'un préjudice a commis une faute plus grave que l'auteur du préjudice, telle une faute lourde, il devient alors possible de plaider que la conduite intempestive de la victime constitue un novus actus dont l'effet est la rupture du lien de causalité existant entre la faute de la personne poursuivie et le préjudice subi par la victime*. »[61]

Or, tel que nous l'avons exposé à maintes reprises, la faute qui est reprochée à celui ou celle qui fait suivre un métavirus est le simple fait d'avoir commis ce geste sans avoir fait de vérifications préalables quant à la validité du message. C'est la victime qui, ayant reçu ce message et se fiant sur l'autorité de son transmetteur, décide d'en suivre les directives et d'elle-même commettre le geste qui, ultérieurement, sera la cause directe du dommage, soit l'élimination d'un fichier important ou utile. N'est-ce pas là une faute plus grave que celle commise par le transmetteur du métavirus ?

Selon le juge Baudouin, la définition du *novus actus interveniens* est toutefois quelque peu différente :

> « Dans sa recherche d'un lien causal ayant un caractère logique, direct et immédiat, la jurisprudence accorde une importance particulière à l'effet du *novus actus interveniens*, c'est-à-dire à l'événement nouveau, indépendant de la volonté de l'auteur de la faute et qui rompt la relation directe entre celle-ci et le préjudice »[62]

La question se pose donc de savoir si le fait de suivre les conseils d'un tiers constitue un événement hors de la volonté de celui-ci. La réponse à cette question semble négative, le fait de conseiller la commission d'un acte dommageable pouvant, dans certains cas, entraîner la responsabilité dudit conseiller.

En effet, pour ne prendre que cet exemple, en droit criminel, le fait de conseiller la commission d'un crime emporte la même peine que le fait de le commettre soi-même :

> Lorsqu'une personne conseille à une autre personne de participer à une infraction et que cette dernière y participe subséquemment, la personne qui a conseillé participe à cette infraction, même si l'infraction a été commise d'une manière différente de celle qui avait été conseillée.
> Quiconque conseille à une autre personne de participer à une infraction participe à chaque infraction que l'autre commet en conséquence du conseil et qui, d'après ce que savait ou aurait dû savoir celui qui a conseillé, était susceptible d'être commise en conséquence du conseil.

---

[61] Pierre DESCHAMPS, « Les conditions générales de la responsabilité civile du fait personnel », dans *Responsabilité*, Collection de droit 2005-2006, École du Barreau du Québec, vol. 4, 2005, EYB2005CDD88.

[62] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, « Le lien de causalité », dans *La responsabilité civile*, 6e édition, 2003, EYB2003RES6.

> Pour l'application de la présente loi, «conseiller» s'entend d'amener et d'inciter, et «conseil» s'entend de l'encouragement visant à amener ou à inciter. [63]

Une telle règle existerait-elle en droit civil ? La réponse semble positive dans la mesure où il semblerait qu'elle ait été appliquée dans au moins une cause récente.

En effet, dans l'affaire *Brazeau* c. *Hanvik*[64], le demandeur a perdu l'usage d'un œil suite à l'utilisation d'un outil mal adapté aux travaux entrepris. L'utilisation de cet outil lui avait été conseillée par le défendeur, lequel fut donc condamné à assumer le tiers des dommages[65].

L'importance de la part de responsabilité de la victime dans cette cause est attribuable au fait qu'il savait que ce qu'il faisait comportait un élément de danger et donc qu'il avait accepté le risque d'accident. Or, selon la théorie de l'acceptation du risque, lorsqu'une personne connaît le danger ou le risque associé à une activité et l'accepte, les tribunaux ont tendance à soit refuser le recours de la victime ou lui attribuer une part contributoire dans la réalisation du dommage[66].

Cependant, dans le contexte qui nous intéresse, les victimes de métavirus ne connaissent pas le danger d'effacer le faux virus, sans quoi ils ne l'effaceraient pas.

Le principe à retenir de l'affaire *Brazeau* serait donc que celui qui se cause soi-même préjudice en suivant les conseils d'un tiers peut exiger compensation dudit tiers si l'expertise de ce dernier est plus grande que la sienne et qu'il n'a pas accepté consciemment les risques associés à l'accomplissement du geste conseillé.

Conclusion

Il appert donc qu'il serait envisageable d'imputer une part de la responsabilité pour la destruction de données suite à l'exécution des conseils contenus dans un métavirus à celui ou celle qui nous l'a fait suivre. Pour se dégager de cette part de responsabilité, cet individu aurait comme obligation de faire certaines recherches afin de confirmer la véracité des informations contenues dans le message. Afin de se faire, il n'aurait qu'à effectuer une vérification sur Internet.

La problématique devient alors celle de trouver ou aller chercher cette information. Le nombre de pages Web se chiffrant dans les millions, il est difficile pour l'internaute de savoir sur quel site se réfugier pour trouver l'information convoitée ; d'autant plus qu'il risque de se retrouver sur l'un des nombreux sites eux-mêmes coupables de propager de la désinformation.

Ainsi, le recours en responsabilité civile pourrait être envisagé par la victime d'un métavirus, mais il semble qu'il s'agisse d'une solution bien mal adaptée au problème encouru. En effet, à moins que celui ayant fait suivre le canular ait des connaissances en informatique, ce qui s'avère fort peu probable puisqu'un tel individu ne tomberait probablement pas dans ce panneau, un juge risque de ne pas retenir sa responsabilité. Qui plus est, même s'il la retenait, les dommages encourus ne justifieraient probablement pas le recours aux tribunaux…

La seule véritable arme demeure donc malheureusement la méfiance. En autres mots, il ne faut pas croire tout ce que l'on lit…

---

63 *Code criminel*, L.R. 1985 ch. C-46, art. 22.

64 REJB 1998-10166 (C.S.)

65 Il importe cependant de souligner que le juge tint en compte le fait que le défendeur avait une meilleure connaissance des outils à utiliser que le demandeur de par sa profession.

66 Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *op. cit.*, note 62.