Compte rendu

Ouvrage recensé :

NICOLAS W. VERMEYS, *Virus informatiques : responsables et responsabilités*, Montréal, Thémis, 2006, 177 p., ISBN-10 2-89400-224-6.

par Silvia Visciano

Les Cahiers de droit, vol. 49, n° 3, 2008, p. 513-516.

Chronique bibliographique

NICOLAS W. VERMEYS, **Virus informatiques : responsables et responsabilités**, Montréal, Thémis, 2006, 177 p., ISBN-10 2-89400-224-6.

L'informatique joue un rôle désormais essentiel dans la vie quotidienne. En effet, le nombre de personnes ayant une connexion à Internet ou travaillant avec leur ordinateur grandit chaque jour, ce qui implique l'expansion à la fois de l'informatisation des données personnelles et de l'exposition au piratage informatique et à la contamination des ordinateurs.

À partir de ce constat, le jeune auteur Nicolas William Vermeys se questionne sur « les multiples incidences des technologies de l'information sur le droit » (p. XIII). Tout particulièrement, il examine en profondeur le thème de « la responsabilité civile des intermédiaires ayant participé à la transmission de virus informatiques sur Internet » (*ibid.*).

Présenté en 2003 comme thèse de maîtrise, cet ouvrage développe deux thèmes principaux : le rapport entre la responsabilité civile et la fabrication de virus informatiques (p. 11-64) et le rapport entre la responsabilité civile et la transmission de virus informatiques (p. 65-145).

Au sujet de la responsabilité civile des intermédiaires, N. Vermeys examine d'abord la « source de la problématique » (p. 12), c'est-à-dire les différents types de codes malicieux (virus, chevaux de Troie, vers informatiques et métavirus), les raisons de leur existence, leur définition technique et les mesures de protection contre eux. Les aspects informatiques laissent ensuite la place aux aspects juridiques, ce qui amène l'auteur à se pencher sur les différentes manières dont le droit se munit, au Québec, en Ontario, au Canada, aux États-Unis, de qualifications et d'outils traditionnels (nous pensons notamment à la faute et à la négligence (p. 30-55), au dommage et au lien de causalité (p. 50-60) et les adapte afin d'évaluer le comportement fautif « des agents à l'origine de la présence des virus informatiques sur Internet » (p. 67-95) et « des agents à l'origine de la diffusion de virus informatiques sur Internet » (p. 96-139).

Quant au comportement fautif, l'auteur constate : *a*) qu'il n'existe pas de droit informatique en tant que tel ; *b*) qu'il n'existe pas de vide juridique : bien au contraire, il y a une multitude des normes applicables à l'informatique. Le cœur de la problématique peut être donc résumé comme un questionnement sur la manière dont le droit de la responsabilité civile prend déjà en considération et pourrait le faire (droit positif / droit prospectif), les situations dans lesquelles un intermédiaire infecte involontairement l'ordinateur d'une victime (*cf.* à ce propos l'affirmation soulignant que « le Code criminel, comme la majorité des législations étatiques étrangères exige qu'un virus soit transmis intentionnellement, malicieusement et sans autorisation pour constituer une infraction punissable. C'est pourquoi, à ce jour, aucun individu n'a été accusé criminellement d'avoir transmis de virus informatiques en sol canadien ») (p. 2-3). Plus particulièrement, N. Vermeys tente une réponse aux questions suivantes (p. 6 et 8) : « De qui la victime d'un virus peut-elle exiger une juste compensation pour le préjudice causé si l'instigateur du dommage est introuvable ? » Y a-t-il des « méthodes à la disposition de ces intermédiaires pour limiter cette responsabilité » ?

La stratégie juridique dans laquelle le circuit des sujets qui ont participé à la propagation d'un virus quelconque est impliqué trouverait, selon l'auteur, ses racines dans l'idée proposée par A.W. Branscomb[1], à savoir que, « 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 » (p. 6). Il s'agit donc d'une mise en œuvre du principe traditionnel de responsabilité délictueuse (dont l'auteur fait mention) pour introduire un questionnement jurisprudentiel spécifique en matière de prévention informatique (*cf.* p. 38-50, affaire *T. J. Hopper* v. *Northern Barge*[2]).

N. Vermeys dévoile subséquemment un champ de recherche doublement transversal : d'un côté, et de manière générale, par le rapport entre droit et technologie (nous pensons même à la tentative de la jurisprudence québécoise et états-unienne d'élaborer une forme de négligence due au manque de technologies disponibles[3]) ; de l'autre côté, par la complexité juridique qui implique le croisement de différentes branches du droit : droit des biens, droit des consommateurs, droit de la responsabilité civile et droit des nouvelles technologies.

De plus, l'auteur cherche les présupposés juridiques de la responsabilité civile dans la transmission involontaire et inconsciente des codes malicieux, pour évaluer les conséquences de ceux-ci sur le marché électronique existant. La prise en considération des contextes factuel, technologique et économique[4] de l'informatique accompagne constamment tant l'analyse générale des institutions juridiques traditionnelles que l'« appréhension des enjeux en droit québécois » (p. XIV ; *cf. Loi concernant le cadre juridique des technologies de l'information*[5].

1. Voir Anne WELLS BRANSCOMB, *Who Owns Information ? : From Privacy to Public Access*, New York, Basic Books, 1994. Comme l'ont souligné Indira CARR et Katherine S. WILLIAMS, « Reflections on Enforcement Measures and Penalty Levels in Computer Misuse Legislation : The Council of Europe Convention on Crime in Cyberspace », dans *Electronic Datasets and Access to legal Information. 15th BILETA Conference*, 14 avril 2000, University of Warwick, p. 2, en citant l'article d'Anne WELLS BRANSCOMB, « Rogue Computer Program and Computer Rogues : Tailoring the Punishment to Fit the Crime », (1990) 16 *Rutgers Computer & Tech. L.J.* 1, « [a]ccording to Branscomb there are six motives where computers are subjects or objects of crime. These are (a) exhibition of technical prowess, (b) highlighting vulnerabilities of computer security systems (c) publishing or retaliating, (d) engaging in computer voyeurism, (e) asserting a philosophy of open access to computer systems and [*sic*] (e) sabotage. » Les six types de violation mentionnés pourraient tous trouver dans un sujet tiers, négligent et inconscient, la source de propagation de l'illicite, ce qui impliquerait pour le droit une prise en charge et une analyse de son comportement, voire de sa responsabilité.
2. *T. J. Hopper* v. *Northern Barge*, 60 F.2d 737 (2e Cir. 1932). Pour un approfondissement du sujet par rapport aux paramètres juridico-économiques de détermination de la négligence, voir Richard A. EPSTEIN, « The Path to *The T. J. Hooper* : The Theory and History of Custom in the Law of Tort », (1992) 21 *J. Legal Stud.* 1.
3. À propos du « duty to adopt technology », voir aussi l'autre jugement fondateur, *United States* v. *Carroll Towing Co.*, 159 F.2d 169 (2e Cir. 1947), mentionné et commenté par Brian R. BAWDEN, « The Ten Commandments of Computerization », dans C.A. Magazine, août 1993, vol. 126, n. 7, p. 32.
4. *Cf.* p. 43-50, le paragraphe portant sur le « calcul économique de la négligence ». À partir des théories économiques de P. Trudel, B.R. Bawden, R. Posner, M. De Villiers et E. Mackkay, l'auteur montre la façon dont l'économie du droit aide la construction du même droit à travers l'observation de l'impact effectif des règles juridiques sur les comportements humains. N. Vermeys approche de cette manière la distinction dont se nourrissent le droit et l'économie, le premier abordant la question rétrospectivement et considérant l'accident produit, la seconde la regardant prospectivement et analysant les niveaux et les chances de l'« option efficace » (p. 46).
5. *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q. 2001, c. C-1.1.

Tout cela n'empêche pas d'approcher cette matière en construction aussi sous l'angle novateur du « rôle de la victime dans la protection contre les attaques virales » (p. 140-148). À partir d'un constat classique (« Le juge Baudouin nous rappelle que "[s]i la victime, par son imprudence, a été le seul artisan de son malheur, elle doit supporter les conséquences de cette situation et assumer sa propre perte". 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" ») (p. 142), l'auteur passe à l'analyse de la faute contributive (« 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 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" ») (p. 146). Cela constitue, par exemple, un attribut de contenu qui signale que ce livre représente également une tentative d'articuler le « droit potentiel ».

Il en va de même pour les enjeux liés à la preuve, à la territorialité[6], à l'applicabilité du droit et à la viabilité financière (p. 84-94) qui ramènent la problématique de la responsabilisation des sujets et des sites de fabrication de virus informatiques à des questions pratiques (« s'il est […] juridiquement possible de poursuivre les gestionnaires de sites 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 » (p. 84)). Dans cette perspective, N. Vermeys approfondit le thème du lien de causalité (p. 56-64) et celui de son appréciation au cas par cas : « 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 » (p. 59).

Cela dit, et bien que le livre paraisse très inspirant dans ses intentions descriptives, nous remarquons à la lecture certaines lacunes qu'il faudrait combler :

— une mention quant aux implications éthiques et sociales des techniques d'information (anonymat, instantanéité, concurrence, volatilité, accès, etc.) ;

— un approfondissement, à notre avis nécessaire, de l'analyse sémantique de certains mots et concepts (virus, Internet, faute, négligence, etc.). Cela aurait été utile pour une introduction conceptuelle à la tractation, et même à la mise à l'épreuve des classifications traditionnelles du droit ;

— une référence, descriptive, de contenu et bibliographique, au « droit du cyberespace[7] », c'est-à-dire au contexte juridique général du thème envisagé ;

— une considération minimale du droit communautaire, de ses jugements et des politiques européennes au sujet de la sécurité, qui composent et complètent désormais la majorité des ouvrages de droit comparé[8] ;

6. À propos du rapport entre territorialité, ordre public et liens d'harmonisation, voir Jean-Jacques Lavenue, « Internationalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyberespace confronté à la notion d'ordre public », automne 2006, [En ligne], [www.lex-electronica.org/articles/v11-2/lavenue.htm] (16 avril 2008).

7. Voir à ce propos : Pierre Trudel et autres, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997 ; Teresa Fuentes-Camacho (dir.), *Les dimensions internationales du droit du cyberespace*, coll. « Droit du cyberespace », Paris, Éditions Unesco, 2000.

8. D'une part, nous pensons, par exemple, à la directive 2000/31/CE (CE, *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »)*, [2001] J.O. L 178/1) sur la responsabilité des hébergeurs ; d'autre

— une compréhension plus exhaustive des principes d'assurance (qui sont réduits dans le livre aux seules pages 146 à 149), de la différence entre assurance informatique et assurance des informations, des enjeux juridiques liant la contamination virale informatique à la perte de données personnelles ou collectives ou encore d'entreprise.

Silvia VISCIANO
Université de Foggia (Italie)
Université Paris I Panthéon-Sorbonne

---

part, nous songeons à la communication de la Commission parue en 2006 : CE, Commission, *Communication au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions – Une stratégie pour une société de l'information sûre – « Dialogue, partenariat et responsabilisation »*, Bruxelles, CE, 31 mai 2006, COM(2006) 251 final.