Les Cahiers de droit

La responsabilité bancaire à l'ère du commerce électronique : impact des autorités de certification

Marc Lacoursière

Volume 42, Number 4, 2001

URI: https://id.erudit.org/iderudit/043684ar
DOI: https://doi.org/10.7202/043684ar

See table of contents

Publisher(s)

Faculté de droit de l'Université Laval

ISSN

0007-974X (print)
1918-8218 (digital)

Explore this journal

Cite this article

Lacoursière, M. (2001). La responsabilité bancaire à l'ère du commerce électronique : impact des autorités de certification. *Les Cahiers de droit*, *42*(4), 961–1012. https://doi.org/10.7202/043684ar

Article abstract

Certification authorities provide the keystone to electronic commerce by authenticating information sent via the Internet. The use of these third-party certificators is without any doubt beneficial for e-trading since they offer transaction security. Yet seen from a legal perspective, the arrival of this new player in the banking arena raises a number of issues. The evolution of Canadian and American banking law now assimilates certification services offered by banks into the concept of business of banking. It is fitting to consider, however, the pervasive trend on the part of banks to sidestep their responsibilities that originate in their increasingly automated operations through exclusion of liability clauses. In the first part of this paper, the author examines the concept of certification authority, including a presentation of its nature, role, hierarchic structure, as well as the government policies underlying it. In the second part, he analyzes the legal environment of electronic signatures and proposes the frameworking of banking responsibilities when banks offer certification authority services.

La responsabilité bancaire à l'ère du commerce électronique : impact des autorités de certification*

Marc LACOURSIÈRE**

Les autorités de certification incarnent la pierre angulaire du commerce électronique, en attestant l'authenticité des informations transmises par un support informatisé. L'utilisation de ces tiers certificateurs est certes bénéfique pour le commerce électronique, car elle permet de sécuriser les transactions. Vu sous une perspective juridique, l'arrivée de ce nouveau joueur dans l'arène bancaire soulève cependant quelques interrogations. L'évolution du droit bancaire canadien et américain assimile maintenant les services de certification offerts par les banques au concept d'opérations bancaires. Il convient de considérer, toutefois, la forte tendance des banques à contourner leurs responsabilités dans le contexte de leurs opérations de plus en plus informatisées, habituellement par l'entremise de clauses exonératoires de responsabilité. Dans la première partie du texte, l'auteur examine le concept d'autorité de certification, incluant une présentation de sa nature, de son rôle, de sa structure hiérarchique, de même que des politiques gouvernementales qui le sous-tendent. Dans la seconde partie, il analyse l'environnement juridique des signatures électroniques et en vient à proposer d'encadrer la responsabilité des banques lorsqu'elles exploitent des services d'autorités de certification.

* Professeur, Faculté de droit, Université Laval.

** L'auteur tient à remercier M^me^ Nicole L'Heureux, professeure à la Faculté de droit de l'Université Laval, pour ses commentaires, ainsi que M^me^ Lina Lalancette pour sa collaboration. Sous réserve d'une indication contraire quant à la date d'accès, la consultation des sites Internet cités dans le présent article est à jour au 1^er^ novembre 2001.

Certification authorities provide the keystone to electronic commerce by authenticating information sent via the Internet. The use of these third-party certificators is without any doubt beneficial for e-trading since they offer transaction security. Yet seen from a legal perspective, the arrival of this new player in the banking arena raises a number of issues. The evolution of Canadian and American banking law now assimilates certification services offered by banks into the concept of business of banking. It is fitting to consider, however, the pervasive trend on the part of banks to sidestep their responsibilities that originate in their increasingly automated operations through exclusion of liability clauses. In the first part of this paper, the author examines the concept of certification authority, including a presentation of its nature, role, hierarchic structure, as well as the government policies underlying it. In the second part, he analyzes the legal environment of electronic signatures and proposes the frameworking of banking responsibilities when banks offer certification authority services.

Les autorités de certification représentent la pierre angulaire du commerce électronique. Elles attestent que des informations n'ont pas été interceptées ni modifiées lors d'une transmission par l'entremise d'un support informatisé. D'un point de vue technique, l'utilisation de ces tiers certificateurs est certes bénéfique pour le commerce électronique, car elle permet de sécuriser les transactions. À cet égard, la tendance des récentes années s'oriente vers la cryptographie à clé publique, laquelle permet une forme d'encryptage de données hautement sécurisée, comme en témoigne son utilisation par les grands réseaux interbancaires. D'autres formes de protection techniques sont également à l'essai. D'un angle juridique, la situation est cependant ambiguë. À nos yeux, le concept d'opération bancaire permet aux banques d'offrir des services de certification à leurs clients soit directement, par l'intermédiaire d'un service bancaire interne, soit indirectement, par celui d'une filiale. Au Canada, un nouveau projet de loi portant sur la réforme des institutions financières ouvre la porte à de telles pratiques. Aux États-Unis, l'Office of the Comptroller of the Currency (OCC) opine également en ce sens. Toutefois, il existe une forte propension de la part des banques à éluder leurs responsabilités au regard du volet informatique de leurs opérations, ainsi que le dénotent les ententes relatives aux cartes de crédit et de débit, aux paiements préautorisés et, plus récemment, aux activités bancaires dans Internet.

D'une part, l'état du droit permet maintenant à une banque d'exploiter les services d'une autorité de certification ; pour rehausser la confiance des usagers, il importe de créer une structure hiérarchique. Dans la première partie du texte, nous mettons en relief le concept d'autorité de certification, incluant une présentation de sa nature, de son rôle et de sa structure hiérarchique ainsi que des politiques gouvernementales sous-jacentes. D'autre part, il convient de tenir la banque responsable des erreurs commises par une autorité de certification agissant sous sa tutelle, tout en tentant de circonscrire la portée des clauses d'exonération de responsabilité. Dans la seconde partie, nous présentons l'environnement juridique des

signatures électroniques et proposons d'encadrer la responsabilité des banques lorsqu'elles agissent en tant qu'autorités de certification.

1 Concept d'autorité de certification

1.1 Définition, nature et fonction

Les tiers certificateurs jouent un rôle clé dans le commerce électronique. Ils peuvent agir en tant que réseau de communication afin de permettre aux usagers de se brancher sur la grande toile que représente Internet. Ils peuvent également intervenir en tant qu'autorités de certification, auquel cas leur rôle est plus actif : transmission de documents, délivrance de certificats, vérification de signatures et conservation des certificats[1].

Dans l'hypothèse où une signature électronique est sécurisée par la cryptographie à clé publique[2], les autorités de certification, parfois appelées « réseaux à valeur ajoutée », ont pour rôle essentiel de certifier l'ori-

---

1. H.H. PERRITT, Jr., *Law and the Information Superhighway : Privacy, Access, Intellectual Property, Commerce, Liability*, New York, J. Wiley & Sons, 1996, p. 396 et 397.
2. Seule cette hypothèse est considérée aux fins du présent texte. La science de la cryptographie remonte au XVII^e^ siècle, alors qu'elle était principalement utilisée à des fins militaires, tandis que la version moderne du premier système de cryptographie à clé publique — ou cryptographie asymétrique — a été mise au point en 1976. Pour une analyse historique de ce système, voir notamment : C.M. ELLISON, « Certification Infrastructure Needs for Electronic Commerce and Personal Use », (1998) 2 (2) *Elec. Banking L. & Com. Rep.* 9 ; L. ELDRIDGE, « Internet Commerce and the Meltdown of Certification Authorities : Is the Washington State a Good Model ? », (1998) 45 *UCLA L. Rev.* 1805, 1818 et 1819. En pratique, le fonctionnement de la cryptographie à clé publique s'apparente à ceci : pour qu'un message soit transmis, deux clés — une publique et l'autre secrète — sont générées par un logiciel. Chaque clé est conservée dans un fichier séparé, appelé « porte-clés », lequel est détenu par chaque usager. Deux partenaires qui désirent communiquer ensemble doivent échanger leur clé publique. L'expéditeur peut utiliser la clé publique du récepteur pour chiffrer le message, et ce dernier va le déchiffrer au moyen de sa clé privée ; ainsi, l'expéditeur s'assure que le récepteur a bel et bien reçu un message intact. À l'inverse, l'expéditeur peut chiffrer le message au moyen de sa clé privée, et le récepteur le déchiffrer avec sa clé publique, ce qui permet d'assurer la confidentialité de l'expéditeur. Enfin, la situation idéale est que les deux partenaires utilisent des clés secrètes, auquel cas il s'agit d'un système de cryptographie à clé privée, ce qui n'est pas transposable dans un réseau ouvert comme Internet. L'avantage majeur du système de cryptographie à clé publique est qu'il permet à deux personnes de conserver la confidentialité dans leurs communications : la clé privée est conservée par le détenteur, tandis que la clé publique est distribuée ouvertement ; de plus, il est mathématiquement impossible pour quiconque de découvrir la clé privée à partir de la clé publique, ce qui représente un avantage majeur. Voir : J.K. WINN, « Couriers Without Luggage : Negotiable Instruments and Digital Signatures », (1998) 49 *S.C. L. Rev.* 739, 763 et 764 ; A.M. FROOMKIN, « The Essential Role of Trusted Third Parties in Electronic Commerce », (1996) 75 *Oregon L. Rev.* 49, 51-53.

gine du détenteur d'une clé. Ainsi, une autorité de certification peut être définie comme une personne physique ou une organisation remplissant les fonctions suivantes : 1) authentifier les documents et les messages ; 2) s'assurer du contenu des messages ; 3) déterminer le moment et le lieu des messages ; 4) garantir la sécurité des messages ; et 5) assurer la préservation du message[3]. La délivrance d'un certificat représente également une fonction importante. Celui-ci se définit comme un « document électronique dont l'objet est d'établir un lien entre une personne et une paire de clés asymétriques[4] ». Il fournit une variété d'informations au sujet du détenteur[5]. D'autres fonctions ont trait à la conservation des documents ainsi qu'à la création et à la détention des clés[6].

Toujours selon Franken, l'exécution des fonctions ci-dessus mentionnées dépend de plusieurs conditions, dont l'indépendance de l'autorité de certification par rapport aux intérêts des partenaires, ainsi que la participation, financière ou non, d'une chambre de commerce[7].

En pratique, il est préférable pour les parties de spécifier dans leur contrat de base qu'elles entendent utiliser les services d'une autorité de certification. L'importance de celle-ci est particulièrement notable dans les environnements ouverts, comme le mentionnent deux auteurs : « However, [Trusted Third Parties] services in the financial sector will not only be useful in pure financial EDI environments, but also within electronic banking relationships (already widespread in Europe), cash withdrawals via ATM's, insurance and use of electronic purses and (international) payment systems between banks[8]. »

1.2 Énoncés de politiques entourant les autorités de certification

Dès le début des années 90, l'Organisation de Coopération et de Développement Économiques (OCDE) s'est consacrée à l'examen de politiques et de réglementation d'infrastructure et de technologies de l'information et

3. H. FRANKEN, « Position and Liabilities of Trusted Third Parties », (1995) 2 *EDI L. Rev.* 85.
4. S. PARISIEN et P. TRUDEL, *L'identification et la certification dans le commerce électronique — droit, sécurité, audit et technologies*, Cowansville, Éditions Yvon Blais, 1996, p. 125.
5. *Infra*, section 2.1.
6. *Ibid.*
7. Au surplus, il serait intéressant d'y retrouver une « free position facing bankruptcy situations of EDI-partners and the tax authorities », de même qu'une protection contre les recours judiciaires : A.M. FROOMKIN, *loc. cit.*, note 2, 85 et 86. En pratique, nous croyons que ces deux conditions peuvent difficilement être réalisées.
8. A.-M.C. KEMNA et H. ROSS, « Results from TEDIS EDIPLAY : The Role and Future of Trusted Third Parties in Payment Systems », (1995) 2 *EDI L. Rev.* 89, 91.

des communications[9]. Vu la croissance du commerce électronique au milieu des années quatre-vingt-dix, l'OCDE a convoqué une conférence ministérielle en 1997, qui visait à déterminer les obstacles à la croissance du commerce électronique[10]. Cette rencontre était préparatoire à la conférence ministérielle d'Ottawa de 1998, intitulée « Un monde sans frontières : Concrétiser le potentiel du commerce électronique mondial » (aussi appelée « Conférence d'Ottawa »)[11].

La Conférence d'Ottawa a proposé des éléments de solution aux divers problèmes engendrés par l'éclosion du commerce électronique. Notamment, les participants ont focalisé leur attention sur trois thèmes généraux : protection de la vie privée, protection du consommateur et authentification pour le commerce électronique[12]. La *Déclaration des*

---

9. OCDE, *Lignes directrices régissant la sécurité des systèmes d'information*, [En ligne], 1992, Paris, [http ://www.oecd.org/dsti/sti/it/secur/index.htm] et OCDE, *Lignes directrices régissant la politique de cryptographie*, [En ligne], 1997, Paris, [http ://www.oecd.org/dsti/sti/it/secur/index.htm].

10. OCDE, *Dismantling the Barriers to Global Electronic Commerce*, [En ligne], 19-21 novembre 1997, Turku (Finlande), [http ://www.oecd.org/dsti/sti/it/ec/index.htm] (ci-après citée : « Conférence de Turku »). Plus précisément, les conférences ministérielles de l'OCDE remontent à février 1995 à Bruxelles lors d'une réunion du G-7 sur la société d'information, suivie par la réunion de Bonn en juillet 1997 au sujet des réseaux d'information. La Conférence de Turku avait pour objet l'atteinte de trois objectifs, à savoir : 1) la détermination de principes généraux, ce qui a notamment mené les participants à déclarer que les forces du marché devraient réguler le commerce électronique ; 2) les discussions concernant la désignation de domaines où une intervention gouvernementale — minimale — est requise, tel le domaine de la fiscalité ; 3) l'identification des organisations pouvant implanter et développer ces solutions, telle la Commission des Nations Unies pour le droit commercial international (CNUDCI) — signatures électroniques —, l'Organisation mondiale du commerce — accords de télécommunication — et l'Organisation mondiale de la propriété intellectuelle — droits de la propriété intellectuelle —, par exemple. Cette conférence a été caractérisée par le niveau général des débats, excluant les prises de position sur des points précis. Il a alors été convenu d'aborder de telles discussions l'année suivante, lors de la conférence ministérielle d'Ottawa : *infra*, note 11.

11. OCDE, *Un monde sans frontières : Concrétiser le potentiel du commerce électronique mondial*, 7-9 octobre 1998, Ottawa, [En ligne], [http ://www.oecd.org/dsti/sti/it/ec/index.htm]. La Conférence d'Ottawa a été marquée par son ampleur : environ 1 000 participants venant des 29 pays membres de l'OCDE et de 12 pays non membres, de 12 organisations internationales et non gouvernementales et d'autres organisations à caractère privé — patronales, syndicales, associations de consommateurs, par exemple — y ont assisté.

12. *Déclaration des ministres relative à la protection de la vie privée sur les réseaux*, *Déclaration des ministres sur la protection des consommateurs dans le contexte du commerce électronique* et *Déclaration des ministres sur l'authentification pour le commerce électronique* : Conférence ministérielle de l'OCDE, « Un monde sans frontières : Concrétiser le potentiel du commerce électronique mondial », conclusions de la conférence,

ministres sur l'authentification pour le commerce électronique a reconnu non seulement l'importance du développement sans cesse croissant des technologies et des mécanismes d'authentification, mais également — pour des raisons d'efficacité — la liberté des parties de choisir des mécanismes d'authentification adaptés à leurs besoins, de même que la préférence vers l'élaboration de codes de conduite par le secteur privé au détriment de normes gouvernementales. En d'autres termes, cette déclaration favorisait une attitude attentiste, laquelle est justifiée dans les circonstances.

En février 1998, le gouvernement canadien a présenté un document de travail intitulé « Politique cadre en matière de cryptographie aux fins du commerce électronique : Pour une économie et une société de l'information au Canada[13] », ayant pour objet l'instauration de la confiance dans le commerce numérique. Après maintes discussions et consultations, un résumé de celles-ci a été produit en février 2001[14]. Le gouvernement a notamment entériné la nécessité d'établir un ensemble de principes et de « normes d'assurance volontaires » de niveau général et supérieur afin d'en garantir la souplesse lors de la mise en œuvre[15]. À cet égard, un groupe de travail devrait être établi rapidement. Par ailleurs, un consensus s'est

---

[En ligne], 7-9 octobre 1998, Ottawa, [http ://www.oecd.org/dsti/sti/it/ec/index.htm]. En plus de ces thèmes, il y a également été question du problème de l'imposition des activités commerciales dans Internet.

13. INDUSTRIE CANADA, *Politique cadre en matière de cryptographie aux fins du commerce électronique : Pour une économie et une société de l'information au Canada*, [En ligne], février 1998, Ottawa, [http ://www.e-com.ic.gc.ca/francais/crypto/cryptf.pdf] (ci-après citée : « Politique canadienne »). Ce document de travail s'inscrit dans la vision du gouvernement fédéral au regard du commerce électronique : INDUSTRIE CANADA, *Stratégie canadienne sur le commerce électronique*, [En ligne], 23 février 1998, Ottawa, [http :// www.e-com.ic.gc.ca/francais/ecom_fr.pdf].

14. INDUSTRIE CANADA, *La suite du programme visant à instaurer la confiance : Authentification électronique*, [En ligne], février 2001, Ottawa, [http ://www.e-com.ic.gc.ca/ francais/documents/authen_sommaire.pdf] (ci-après cité : « Programme visant à instaurer la confiance »). Industrie Canada a effectué une série de discussions bilatérales avec des acteurs du secteur privé de mai à octobre 1999 afin, notamment, de repérer les problèmes éventuels et d'examiner la nécessité d'élargir les consultations futures : GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE, *Authentification électronique : Consultations bilatérales — Sommaire des conclusions*, [En ligne], octobre 1999, Ottawa, [http :/ /e-com.ic.gc.ca/francais/documents/bilat-fr.pdf]. Par la suite, Industrie Canada a tenu un atelier en décembre 1999, dont les réflexions ont été cristallisées quelques mois plus tard : INDUSTRIE CANADA, *Instaurer la confiance à l'égard du commerce électronique : Cadre pour l'authentification électronique au Canada*, [En ligne], juillet 2000, Ottawa, [http :// ecom.ic.gc.ca/francais/documents/cadre.pdf]. Les observations recueillies dans ce document sont présentées dans le Programme visant à instaurer la confiance, précité, lequel a pour objet d'établir le processus futur.

15. Programme visant à instaurer la confiance, précité, note 14, p. 5.

dégagé pour s'assurer que les principes sont « compatibles avec les orientations prises par les diverses tribunes internationales » visées par l'authentification[16].

À l'instar de la situation au Canada, la souplesse réglementaire caractérise la politique américaine du commerce électronique. Depuis juillet 1997, les grands enjeux du commerce électronique aux États-Unis se fondent sur les politiques suivantes : 1) le secteur privé devrait être à l'origine du développement ; 2) les gouvernements devraient éviter les restrictions indues ; 3) lorsqu'une intervention gouvernementale est requise, elle devrait être très limitée ; 4) les gouvernements devraient reconnaître les qualités uniques d'Internet ; et 5) le commerce électronique dans Internet devrait être facilité sur une base globale[17]. En particulier, ces politiques insistent sur le fait que, en ce qui concerne les services financiers, l'élaboration d'un système de paiement virtuel doit être réglementée à long terme par l'entremise des autorités gouvernementales et non uniquement par les forces du marché[18].

De son côté, la politique européenne à l'égard de la certification est essentiellement orientée vers le problème de l'authenticité et de l'intégrité de l'information — plutôt que vers une politique néo-libérale du type nord-américaine —, ainsi que vers la nécessité de rehausser la confiance des usagers à l'égard des signatures électroniques[19]. En particulier, la Commission européenne note que l'authenticité d'une information doit s'appuyer sur le principe de la reconnaissance mutuelle — vu la globalité du commerce électronique —, lequel doit être reconnu par les États membres[20]. La Commission ajoute que chaque État membre doit bénéficier d'une autorité de certification — autorité de niveau supérieur[21] — qui « contrôle de manière

16. *Id.*, p. 4 et 5.
17. W.J. CLINTON et A. GORE Jr., *Framework for Global Electronic Commerce*, p. 2-3, [En ligne], juillet 1997, Washington (DC), [http ://iitf.doc.gov/eleccomm/ecomm.htm] ; U.S. DEPARTMENT OF COMMERCE, *The Emerging Digital Economy II*, [En ligne], juin 1999, Washington (DC), [http ://www.ecommerce.gov/ede/report.html]. Pour de plus amples renseignements, voir généralement : UNITED STATES, *Electronic Commerce Policy*, [En ligne], Washington (DC), [http ://www.ecommerce.gov].
18. W.J. CLINTON et A. GORE Jr., *op. cit.*, note 17, p. 5 et 6.
19. COMMISSION JURIDIQUE ET DES DROITS DES CITOYENS, *Rapport sur la communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions : Assurer la sécurité et la confiance dans la communication électronique — Vers un cadre européen pour les signatures numériques et le chiffrement (COM(97)0503 — C4-0648/97)*, par. 2, p. 5, A4-0189/98 (20 mai 1998) (rapporteur : M. Wolfgang Ullmann) (ci-après cité : « rapport Ullmann n° 1 »).
20. *Id.*, p. 10.
21. *Infra*, section 1.4.

objective, non discriminatoire et transparente » le respect des principes, afin de répondre à l'impératif de l'indépendance[22].

Puisque le chiffrement électronique permet de se prémunir contre les intrusions, dont les ingérences gouvernementales d'écoute électronique, les politiques relatives à l'exportation de logiciels de chiffrement posent un sérieux problème pour certains pays. Ainsi, les politiques du Canada, de l'Union européenne et des États-Unis diffèrent sensiblement à cet égard.

Bien que le Canada ait signé l'Entente de Wassenaar[23], la politique canadienne à l'égard de l'exportation de logiciels de chiffrement tend à se caractériser par son aspect très libéral par rapport à l'Europe, et surtout aux États-Unis[24]. À la suite de la séance de discussion de février 1998[25], le point de vue du gouvernement fédéral n'est toutefois pas encore fixé[26].

Tout en rappelant que les « services de recherche et de sécurité plaident en faveur de règles légales en matière d'accès aux clés de chiffrement, et ce par souci de sécurité nationale et pour assurer la lutte contre la criminalité et le terrorisme[27] », le rapport Ullmann suggérait aux États membres de l'Union européenne, au regard de l'Entente de Wassenaar, de réduire les restrictions à l'exportation des produits de chiffrement au minimum[28].

---

22. Rapport Ullmann n° 1, précité, note 19, n° 17, p. 6.
23. L'Entente de Wassenaar, aussi connue sous le nom de « Règlement sur les marchandises et technologies à double usage », a été signée en 1995 par 31 pays — dont le Canada, les États-Unis et les pays européens — afin de contrôler les exportations d'armes et autres biens — notamment les logiciels — à des fins militaires et civiles : *L'Entente de Wassenaar relative au contrôle des exportations d'armes conventionnelles et de biens à double usage, dans le groupe Australie, dans le régime de contrôle de la technologie des missiles et dans le groupe de fournisseurs nucléaires*, [En ligne], 12 juillet 1996, Vienne (Autriche), [http ://fas.org/nuke/control/wassenaar/docs/wassenr4toc.htm]. Pour plus de renseignements sur cette entente, voir : [http ://www.wassenaar.org].
24. Plus précisément, le Canada a évoqué les deux scénarios possibles — mesures libérales et restrictives —, mais il n'a pris aucune décision pour le moment. Par ailleurs, il n'impose aucune restriction à l'égard des produits exportés aux États-Unis — ce dernier agit de même à l'égard des produits vendus au Canada — et permet aux compagnies d'obtenir des licences d'exportation : *Licence générale d'exportation n° 39 — Logiciel de cryptographie de très grande diffusion*, (1999) 133 Gaz. Can. II, 1513 (n° 13, 1999-06-23), modifiée par *Décret modifiant la Liste des marchandises d'exportation contrôlées*, (2001) 13 Gaz. Can. II, 134 (n° 3, 2001-01-17).
25. Politique canadienne, précitée, note 13.
26. *Id.*, p. 33 et 34. Lors des discussions d'octobre 1999 et de février 2001, le gouvernement est demeuré silencieux sur cette question : GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE, *op. cit.*, note 14, et Programme visant à instaurer la confiance, précité, note 14.
27. Rapport Ullmann n° 1, précité, note 19, p. 15.
28. *Id.*, n° 21, p. 7.

Ces recommandations ne sont point restées lettre morte, car la réglementation de 1994[29] a été adoucie en 2000. Elle n'impose maintenant que peu de restrictions envers les États membres et facilite une exemption à la loi pour la plupart des autres pays industrialisés — dont le Canada et les États-Unis[30].

Toutefois, à l'inverse des approches canadienne et européenne, les politiques américaines entourant la cryptographie font l'objet d'une sérieuse controverse, car le gouvernement des États-Unis contrôle sévèrement l'usage et l'exportation de la cryptographie, tant techniquement[31] que

---

29. COMMUNAUTÉ EUROPÉENNE (CE), *Règlement (CE) nº 3381/94 du Conseil, du 19 décembre 1994, instituant un régime communautaire de contrôle des exportations de biens à double usage*, [1994] J.O. L. 367/1, et CE, *Décision du Conseil, du 19 décembre 1994, relative à l'action commune, adoptée par le Conseil sur la base de l'article J.3 du traité sur l'Union européenne, concernant le contrôle des exportations de biens à double usage*, [1994] J.O. L. 367/8, modifiés par (au sujet du contrôle des exportations des logiciels de chiffrement) : CE, *Décision du Conseil du 9 mars 1999 modifiant la décision 94/942/PESC relative à l'action commune, adoptée par le Conseil sur la base de l'article J.3 du traité sur l'Union européenne, concernant le contrôle des exportations de biens à double usage*, [1999] J.O. L. 73/1, et CE, *Index des biens énumérés à l'annexe I de la décision 1999/193/PESC du Conseil du 9 mars 1999 modifiant la décision 94/942/PESC relative à l'action commune, adoptée par le Conseil sur la base de l'article J.3 du traité sur l'Union européenne, concernant le contrôle des exportations de biens à double usage*, [1999] J.O. C. 230/1. En vertu de l'article 113 du *Traité instituant la Communauté européenne*, 25 mars 1957, 298 R.T.N.U. 11 (entrée en vigueur : 1er janvier 1958), modifié par le *Traité sur l'Union européenne*, [1992] J.O. C. 224/1, la Communauté européenne a compétence exclusive en ce domaine : *Fritz Werner Industrie-Austrüstungen GmbH* c. *Bundesrepublik Deutschland*, C-70/94, [1995] Rec. C.E. I-3189, et *Procédure pénale* c. *Peter Leifer e.a.*, C-84/94, [1995] Rec. C.E. I-3231.

30. CE, *Règlement (CE) nº 1334/2000 du Conseil du 22 juin 2000 instituant un régime communautaire de contrôles des exportations de biens et technologies à double usage*, [2000] J.O. L. 159/1.

31. Les producteurs américains d'ordinateurs, particulièrement Microsoft, comprennent l'importance pour les gens de se protéger contre toute intrusion externe. Ils incluent depuis quelque temps dans leurs ordinateurs, un logiciel de sécurité, habituellement très efficace et fonctionnant au moyen de la cryptographie. Or, le gouvernement américain ne partage pas le point de vue que l'on puisse se protéger contre n'importe qui. En agissant ainsi, il devient notamment impossible aux représentants des forces de l'ordre de pouvoir faire de l'« écoute électronique » ou tout autre genre d'espionnage. Le gouvernement a donc trouvé une solution à cet épineux problème. Les spécialistes de la National Security Agency ont conçu une puce électronique du nom de *Clipper* que les constructeurs américains d'ordinateurs doivent installer dans leurs produits. Le principe d'utilisation est simple : deux clés dépendantes l'une de l'autre sont détenues par des organismes gouvernementaux indépendants pour empêcher les abus d'utilisation, soit le Department of Treasury et le National Institute of Standards and Technology. Ce logiciel est donc aussi efficace que ceux que les constructeurs d'ordinateurs utiliseraient

légalement[32]. Est-ce nécessaire de mentionner que le milieu de l'informatique et les associations des droits et libertés civils américains ne partagent pas ce point de vue ? En 1996, un mathématicien américain a contesté la constitutionnalité des restrictions gouvernementales qui l'empêchaient d'exporter un logiciel d'encryptage de données[33]. La Cour d'appel du neuvième circuit a donné raison au requérant, jugeant que les mesures étaient trop restrictives et violaient le Premier Amendement — liberté d'expression — et le Quatrième Amendement — droit à la sécurité et à la protection contre les fouilles abusives — de la Constitution américaine[34]. Cette décision a été à l'origine de quelques modifications législatives ultérieures[35].

1.3 Infrastructure des autorités de certification

Les services fournis par une autorité de certification s'étendent au-delà de simples relations contractuelles et intéressent évidemment le secteur bancaire. En particulier, les systèmes de paiement, tels que les transferts électroniques de fonds, l'informatisation des lettres de crédit et, bien sûr, les nouveaux modes de paiement par Internet, représentent un potentiel de développement pour la certification. En vue de réglementer les relations entre l'émetteur d'un document informatisé et une autorité de certification, il est nécessaire de déterminer de quelle manière celle-ci doit être constituée lorsqu'elle est à l'œuvre dans le secteur bancaire ; dans une telle

---

normalement, mais il permet au gouvernement de vérifier si quelque chose de louche s'y trame. Voir au sujet du fonctionnement de *Clipper* : K.M. LUI-KWAN, « Recent Developments in Digital Signature Legislation and Electronic Commerce », (1999) 14 *Berkeley Tech. L.J.* 463, 478 et 479 ; M. GODWIN, « A Chip over my Shoulder : The Problems with Clipper », *Internet World*, juillet-août 1995, p. 92 ; M. GODWIN, « Keys to Kingdom », *Time*, printemps 1995, p. 64 ; D. WISEBROD, « Controlling the Uncontrollable : Regulating the Internet », (1993-95) 4 *Media & Communications Law Review* 331, 343 et suiv.

32. *Computer Security Act of 1987*, Pub. L. No. 100-235, 101 Stat. 1724, 40 U.S.C. 759n, 15 U.S.C. 278h et 15 U.S.C. 278g-3 — 278g-4. À la suite de l'Entente de Wassenaar, le gouvernement américain a formellement interdit les exportations de logiciels de cryptographie dans le monde entier, sauf au Canada : 15 C.F.R. § 742.15 (1996).
33. *Bernstein* c. *United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999), conf. 974 F.Supp. 1288 (U.S.D.C. 1997) (ci-après cité : « *Bernstein* »).
34. U.S. Const. Amend. I et IV ; *Bernstein*, précité, note 33, 1145 et 1146. La *ratio decicendi* de l'affaire *Bernstein* a été suivie dans l'arrêt *Junger* c. *Daley*, 209 F.3d 481, 484 et 485 (6th Cir. 2000). Voir également le commentaire suivant : N.A. CAIN, « Bernstein, Karn, and Junger : Constitutional Challenges to Cryptographic Regulations », (1999) 50 *Ala. L. Rev.* 869.
35. Voir notamment les récentes modifications de 1998 : 63 Fed. Reg. 55121 et de 1999 : *Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999*, S. 798, 106 Congr., 1re sess. (1999).

situation, nous croyons que l'autorité de certification peut se manifester sous la tutelle d'une banque (section 1.3.1) et sous la forme d'une chambre de compensation (section 1.3.2).

1.3.1 Banques

À l'origine, les tiers certificateurs étaient conçus pour agir en tant qu'entités indépendantes afin de gagner la confiance du public envers les nouvelles technologies[36]. Tant d'un point de vue technique que juridique, les autorités de certification peuvent maintenant agir sous la tutelle des banques pour les raisons suivantes.

D'abord, en 1997, l'OCC a reçu une demande de la part de la Zions First National Bank au sujet de l'établissement d'une filiale agissant en tant qu'autorité de certification pour la vérification de signatures électroniques et de dépositaire pour les certificats[37]. L'OCC a émis l'opinion que « [t]he ability of banks to act as certificate authorities for digital signatures is expected to be vital to their role in the evolving electronic payments systems[38] », avant de conclure que les services d'autorité de certification représentent une partie accessoire des activités bancaires. En particulier, elle note que « [t]he concept that the "business of banking" can evolve to reflect logical outgrowths from the special skills, expertise, and competencies of banks is not new[39] ». L'approbation a été sujette à deux conditions[40].

---

36. *Supra*, note 7, ainsi que le texte correspondant.
37. OCC, *Conditional Approval n° 267*, [En ligne], 2 janvier 1998, p. 1, Washington (DC), [http ://www.occ.treas.gov/netbank/ibi.htm].
38. *Id.*, p. 16.
39. *Id.*, p. 13. Pour une discussion plus approfondie du concept d'opération bancaire, voir notamment au Canada : *Canadian Pioneer Management Ltd.* c. *Le Conseil des relations de travail de la Saskatchewan*, [1980] 1 R.C.S. 433, (1979) 31 N.R. 361 ; *R.* c. *Milelli*, (1989) 51 C.C.C. (3rd) 165, 45 B.L.R. 209 (C.A. Ont.), permission d'appeler à la Cour suprême du Canada rejetée, 53 C.C.C. (3rd) viii, 38 O.A.C. 160n ; aux États-Unis : *Merchants' Bank* v. *State Bank*, 77 U.S. 604, 19 Law. Ed. 1008 (1871) ; *American Insurance Association* v. *Clarke*, 865 F.2d 278 (D.C. Cir. 1988) ; *Farmers Bank of Northern Missouri, Unionville* v. *Erpelding*, 555 N.W.2d 222 (Iowa S.C. 1996) ; *Mercantile National Bank of the City of New York* v. *Mayor, Etc. of the City of New York*, 121 U.S. 138, 154-156, 30 Law. Ed. 895 (1886) ; au Royaume-Uni : *United Dominions Trust Ltd.* v. *Kirkwood*, [1966] 2 Q.B. 431, 453-456, [1966] 1 All E.R. 968 ; *In Re Shield's Estate*, [1901] 1 Ir. R. 172 (Ch.D.).
40. Le requérant devait fournir une description complète du système d'information proposé à l'OCC avant le début des opérations et également informer les vendeurs potentiels que le contrat était sujet à une supervision par l'OCC : OCC, *op. cit.*, note 37, p. 20.

Ensuite, en mai 1999, l'OCC a produit des lignes directrices servant de bases aux discussions entre les autorités de supervision des banques et ces dernières au sujet des risques d'exploiter un système d'autorité de certification[41]. Pour Douglas et Cocker, « [b]anks are well suited to be certificate authorities, due to their relationship with their customers[42] », ce qui confirme notre point de vue selon lequel les banques peuvent remplir efficacement et légalement le rôle d'autorité de certification pour la vérification des signatures et des documents électroniques.

Enfin, la *Loi sur les banques* permet depuis 1997 l'utilisation par les banques canadiennes — Annexe I — de services d'autorité de certification[43]. En vertu du nouvel article 468 (2) (a), une banque a maintenant le droit d'« acquérir ou [d']augmenter un intérêt de groupe financier dans une société d'opérations immobilières », soit dans n'importe quel type d'entité avec laquelle elle fait affaire en conformité avec l'article 410[44]. Il est donc clair que le projet de loi C-8 avantage les banques en leur permettant d'ac-

41. OCC, *OCC Bulletin 99-20 : Certification Authority Systems*, [En ligne], 4 mai 1999, Washington (DC), [http ://www.occ.treas.gov/netbank/ibi.htm] (19 mars 2000) (ci-après cité : « OCC Bulletin 99-20 »). Voir de plus les bulletins suivants relatifs à ces lignes directrices : OCC, *OCC Bulletin 98-38 : Technology Risk Management : PC Banking*, [En ligne], 24 août 1998, Washington (DC), [http ://www.occ.treas.gov/netbank/ebguide.htm], et OCC, *OCC Bulletin 98-3 : Technology Risk Management*, [En ligne], 4 février 1998, Washington (DC), [http ://www.occ.treas.gov/netbank/ebguide.htm].

42. J.L. DOUGLAS et T.R. COCKER, « A Decision Letting Bank Subsidiaries Act as Certification Authorities for Digital Signature Verification Will Increase Bank Forays into Electronic Commerce », *Nat'l L.J.* 16 février 1998 B4 (col. 1).

43. *Loi sur les banques*, L.C. 1991, c. 46, modifiée par la *Loi modifiant la législation relative aux institutions financières*, L.C. 1997, c. 15, art. 42. Plus précisément, les banques peuvent agir de la sorte en vertu de l'article 410 (1) (c.1) — avec l'obtention préalable de l'accord du ministre —, qui leur permet de détenir une « société d'information », laquelle est définie à l'article 468 (1) comme une personne morale travaillant dans le secteur : *a*) de la conception, du développement et de la commercialisation de services de gestion de d'information ou *b*) ou de logiciel.

44. Selon l'article 100 (1) de la *Loi constituant l'Agence de la consommation en matière financière du Canada et modifiant certaines lois relatives aux institutions financières*, Projet de loi C-8 (adopté le 2 avril 2001), 1re session, 37e législature (Can.) (ci-après cité : « Projet de loi C-8 »), modifiant l'article 410 (1) (c.1) de la *Loi sur les banques*, précitée, note 43, une banque peut, avec l'accord préalable du ministre, « s'occuper, notamment en les concevant, les développant, les détenant, les gérant, les fabriquant ou les vendant, de systèmes de transmission de données, de sites d'information, de moyens de communication ou de plates-formes informatiques ou de portails d'information » utilisés dans les cas suivants : « (i) soit pour la fourniture d'information principalement de nature financière ou économique ; (ii) soit pour la fourniture d'information relative à l'activité commerciale des entités admissibles, au sens du paragraphe 464 (1) ; (iii) soit à une fin réglementaire ou dans des circonstances réglementaires ». L'approche du projet de loi

quérir un « intérêt de groupe financier[45] », leur autorisant le contrôle *de jure* sur l'entité détenue[46].

À l'instar des banques américaines, certaines banques canadiennes exploitent maintenant des services de certification. Par exemple, la Banque canadienne impériale de commerce (ou Canadian Imperial Bank of Commerce (CIBC)) fournit des services de certification électronique à sa clientèle en collaboration avec l'autorité de certification VeriSign inc.[47] — sous la bannière « Centre CIBC VeriSign » à titre de société affiliée[48]. Des services, tels que la confirmation de l'identité d'une entreprise et la fourniture de codes de sécurité permettant l'accès aux intranets et extranets, sont maintenant disponibles[49].

1.3.2 Chambres de compensation

Les chambres de compensation présentent un avantage majeur par rapport aux banques dans la certification des signatures et des documents

---

C-8 sur cette question s'éloigne du projet de loi C-67, sanctionné le 17 juin 1999 : *Loi modifiant la Loi sur les banques, la Loi sur les liquidations et les restructurations et d'autres lois relatives aux institutions financières et apportant des modifications corrélatives à certaines lois*, L.C. 1999, c. 28.

45. Selon l'article 10 (1) de la *Loi sur les banques*, une banque possède un « intérêt de groupe financier » lorsqu'elle possède : *a)* plus de 10 p. 100 des actions comportant un droit de vote, ou *b)* plus de 25 p. 100 de l'avoir des actionnaires.

46. L'article 3 (1) (a) énonce que le contrôle est *de jure* lorsque les actions comportant un droit de vote détenues par une banque excèdent 50 p. 100. Toutefois, le paragraphe *d)* établit une présomption de contrôle de fait « quand elle-même et les entités qu'elle contrôle détiennent la propriété effective d'un nombre de titres de la première tel que, si elle-même et les entités contrôlées étaient une seule personne, elle contrôlerait l'entité en question ».

47. VeriSign est un fournisseur de services de certification numérique dans Internet. Pour plus de détails, voir : [http ://www.verisign.com].

48. CIBC, *CIBC devient l'autorité de certification VeriSign au Canada — La Banque CIBC émettra des certificats numériques à l'intention des entreprises et des consommateurs du Canada*, [En ligne], 18 août 1999, Toronto, [http ://www.cibc.com/french/noteworthy/verisign_news_main.html].

49. *Id.* De son côté, la Banque Royale du Canada offre un service de certification — *WebTrust-ISP* — en collaboration avec la SET Secure Electronic Transaction LLC, mieux connue sous le nom de SET. Pour plus de détails sur les *webtrusts*, voir : *infra*, notes 64 et 65, ainsi que le texte correspondant. SET est une plate-forme permettant les transactions par cartes de crédit par l'entremise d'Internet ; à ce sujet, voir le portail de SET : [http ://www.setco.org]. Soulignons finalement que BCE Emergis, qui se concentre notamment sur le secteur des services financiers, collabore également avec e-Scotia ainsi qu'avec la Banque Nationale du Canada pour l'hébergement et la gestion de services de certification : BCE EMERGIS, *Unités d'affaires*, [En ligne], 2001, Montréal, [http ://www.emergis.com/fr/company/company_profiles/business_units.asp].

électroniques : l'indépendance par rapport aux parties en cause, soit l'émetteur et le récepteur du message[50]. Pour cette raison, nous approuvons qu'elles agissent ainsi. Techniquement, les chambres de compensation interbancaires peuvent agir en tant qu'autorité de certification. D'ailleurs, le réseau interbancaire américain de paiements de moindre valeur Automated Clearing House (ACH) permet le transfert de données accompagnant un paiement entre institutions financières[51]. Toutefois, les réseaux interbancaires de transferts électroniques de fonds de grande valeur situés au Canada et aux États-Unis expriment une forte réticence à l'idée de transférer des données autres que des ordres de paiement[52].

Au Canada, une interprétation libérale de la *Loi sur la compensation et le règlement des paiements*[53] permet à une chambre de compensation d'agir en tant qu'autorité de certification. L'article 2 de cette loi définit une chambre de compensation comme une société « qui offre les services d'un système de compensation et de règlement ». Ce concept inclut « des ordres de paiement et de toute autre communication afférente à un paiement [...] Y est assimilé [...] toutes autres opérations pour lesquelles le système ou l'arrangement pratique le règlement ou la compensation des obligations de paiement découlant de ces opérations[54]. » Ainsi, nous croyons que l'expression « autre communication » implique la vérification d'une signature élec-

---

50. A.M. FROOMKIN, *loc. cit.*, note 2, 55-58 ; C. PERREAULT, « Droit, commerce électronique et nouvelles technologies de l'information », [1996] *Meredith Mem. Lect.* 507, 531-533 ; S. PARISIEN et P. TRUDEL, *op. cit.*, note 4, p. 132 et 133.

51. NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION, *Operating Rules*, New York, Nacha, 1998, art. 2.1.2 (ci-après citées : « ACH Rules »). Voir également : B.K. STONE, « Corporate Trade Payments : Hard Lessons in Product Design », *Ec. Rev. Fed. Res. Bank of Atlanta*, vol. 71, avril 1986, p. 9, 20 ; B. GEVA, *The Law of Electronic Funds Transfer*, New York, Matthew Bender, 1999, § 5.02[4][b][ii], p. 5-23–5-30.

52. Contrairement au réseau ACH, non seulement les réseaux interbancaires de transferts de fonds de grande valeur n'offrent pas cette possibilité, mais aucun projet n'est en route à ce sujet.

53. *Loi sur la compensation et le règlement des paiements*, L.C. 1996, c. 6, art. 162.

54. *Id.*, art. 2 : « Système ou arrangement visant le règlement ou la compensation des obligations monétaires, des ordres de paiement et de toute autre communication afférente à un paiement comportant au moins trois établissements participants dont au moins une banque, utilisant le dollar canadien pour au moins une partie de ses opérations et donnant lieu, une fois le règlement ou la compensation [fait], à l'ajustement du compte des parties détenu à la banque. Y est assimilé le système ou l'arrangement pour le règlement ou la compensation des valeurs mobilières, des opérations utilisant des devises étrangères ou toutes autres opérations pour lesquelles le système ou l'arrangement pratique le règlement ou la compensation des obligations de paiement découlant de ces opérations. » La version anglaise est également très claire : « a system [...] for the clearing or settlement of [...] other transactions where the system [...] also clears or settles payment obligations arising from those transactions ».

tronique et la délivrance d'un certificat, étant donné que l'obligation de paiement est la conséquence de cette transaction. Malheureusement, le *Règlement administratif nº 7 sur le système de transfert de paiements de grande valeur*[55] est très limitatif et ne gouverne que la compensation et le règlement des paiements. Cette approche est regrettable, car les règles du Système automatisé de compensation et de règlement (SACR)[56], dont la Règle E3[57] gouvernant la compensation et le règlement des items par l'échange de documents informatisés (EDI), seraient susceptibles de permettre à une chambre de compensation d'agir en tant qu'autorité de certification.

Aux États-Unis, les réseaux interbancaires Clearing House Interbank Payments System (CHIPS)[58] et Fedwire[59], gouvernant les virements électroniques de fonds de grande valeur, sont également très restrictifs, à

---

55. *Règlement administratif nº 7 sur le système de transfert de paiements de grande valeur*, (1985) 132 Gaz. Can. I, 871 (nº 16, 1998-04-18).

56. Les règles SACR régissent la compensation des paiements autres que les transferts électroniques de fonds de grandes valeurs, tels les chèques ou les paiements préautorisés. L'ensemble des règles est maintenant disponible en ligne sur le site de l'Association canadienne des paiements (ACP) : [http ://www.cdnpay.ca/fre/rules/acss-f.htm].

57. ACP, *Règle E3 — Règles applicables aux opérations d'échange de données informatisées (EDI)*, [En ligne], 2001; Ottawa, [http ://www.cdnpay.ca/eng/rules/E3-RULE.ENG.htm]. Plus précisément, la « présente Règle régit la compensation et le règlement des effets de paiement par échange de données informatisées (EDI) en dollars canadiens, à base de crédit, entre institutions financières canadiennes. La Partie I expose les règles générales touchant la compensation et le règlement de ces effets, alors que la Partie II expose des spécifications techniques pour l'échange des effets de paiement EDI entre institutions financières canadiennes. »

58. CHIPS représente un réseau privé américain de communication et de transmission électronique de fonds. En service depuis 1970, CHIPS est détenu par la New York Clearing House Association (NYCHA) et transfère plus d'un milliard de dollars par jour, soit environ 95 p. 100 des transactions commerciales mondiales. Ces transferts de fonds sont régis par les *CHIPS Rules and Administrative Procedures*, New York, NYCHA, 1998 (ci-après citées : « CHIPS Rules ») et la compensation a lieu le jour même : B. GEVA, *op. cit.*, note 51, § 3.03[1][a], p. 3-31 ; N. L'HEUREUX et É. FORTIN, *Droit bancaire*, 3e éd., Cowansville, Éditions Yvon Blais, 1999, p. 452 et 453 ; H.F. LINGL, « Risk Allocation in International Interbank Fund Transfers : CHIPS & SWIFT », (1981) 22 *Harv. Int'l L.J.* 621, 621 et 626 et suiv. Il n'existe aucune disposition précise dans les CHIPS Rules qui traite de la certification, mais l'interprétation de l'ensemble des règles permet d'opiner en ce sens. Les règles ne sont disponibles que pour les institutions financières ; voir toutefois la vitrine Internet de CHIPS pour des renseignements de nature générale : [http ://www.chips.org].

59. FEDERAL RESERVE BANK OF NEW YORK (FRBNY), *Operating Circular, nº 4*, art. 1.1, [En ligne], 2 janvier 1998, New York, [http ://www.ny.frb.org/bankinfo/operating/oc4.pdf]. Tirant son origine du code Morse en 1918, afin d'accélérer les messages,

l'image du Système de transfert des paiements de grande valeur (STPGV), ne permettant que les ordres de paiement[60]. Le réseau SWIFT travaille présentement à l'élaboration d'un projet de cryptographie à clé publique,

---

Fedwire est devenu complètement automatisé en 1973. Des améliorations ont suivi par la suite, par exemple au début des années 80 avec le Federal Reserve Communications System — connu sous le nom de FRCS80. Le réseau a été amélioré en 1993 par l'entremise du Telecommunications Service Priority : D.I. BAKER et R.E. BRANDEL, *The Law of Electronic Funds Transfers Systems*, Boston, Warren, Gordham & Lamont, 1997, paragr. 11.02, p. 11-3. Voir de plus : A.M. GILBERT, D. HUNT et K.C. WINCH, « Creating an Integrated Payment System : The Evolution of Fedwire », *FRBNY Ec. Pol'y Rev.*, juillet 1997, p. 1, 1-4. À l'instar de CHIPS, Fedwire représente de nos jours un réseau américain d'envergure nationale destiné à la compensation et au règlement des paiements de grande valeur. Il est détenu par douze banques membres de la Réserve fédérale, qui compte plus de 11 000 membres — incluant certaines banques canadiennes et la Banque du Canada — et est réglementé par la *Regulation J*, 12 C.F.R. part 210, Subject B, ainsi que par : FRBNY, *Operating Circular n° 6*, New York, 2 janvier 1998. Fedwire effectue la transmission et la compensation, qui ont lieu le jour même : B. GEVA, *op. cit.*, note 51, § 3.04[1], p. 3-72 ; N. L'HEUREUX et É. FORTIN, *op. cit.*, note 58, p. 453 ; FEDERAL RESERVE BANK OF NEW YORK, *Fedwire : The Federal Reserve Wire Transfer Service*, New York, New York Federal Reserve Board, 1995, p. 10. Voir également les portails virtuels des banques composant le réseau de la Réserve fédérale américaine — Board of Governors of the Federal Reserve System, [En ligne], [http ://www.federalreserve.gov] ; Réserve fédérale d'Atlanta, [En ligne], [http ://www.frbatlanta.org] ; Réserve fédérale de Boston, [En ligne] [http ://www.bos.frb.org] ; Réserve fédérale de Chicago, [En ligne], [http ://www.chicagofed.org] ; Réserve fédérale de Cleveland, [En ligne], [http ://www.clev.frb.org] ; Réserve fédérale de Dallas, [En ligne], [http ://www.dallasfed.org] ; Réserve fédérale de Kansas City, [En ligne], [http ://www.kc.frb.org] ; Réserve fédérale de Minneapolis, [En ligne], [http ://woodrow.mpls.frb.fed.us] ; Réserve fédérale de New York, [En ligne], [http ://www.ny.frb.org] ; Réserve fédérale de Philadelphie, [En ligne], [http ://www.phil.frb.org] ; Réserve fédérale de Richmond, [En ligne], [http ://www.rich.frb.org] ; Réserve fédérale de San Francisco, [En ligne], [http ://www.frbsf.org] ; Réserve fédérale de St-Louis, [En ligne], [http ://www.stls.frb.org].

60. Le réseau STPGV a été conçu par l'ACP en 1997 afin de remplacer le Système de paiements interbancaires internationaux (SPII). Le STPGV accepte les paiements de toutes tailles, mais les transferts de paiements de grande valeur sont de loin plus abordables : D.A. CHAMBERLAND, « Canada's New Large-Value Payments System », [1998] 6 *J.I.B.L.* 199, 200 ; P.-L. MCPHERSON, « The Canadian Payments Association : Large Value Transfer System », dans *Electronic Commerce : The Impact of the Digital Age on Commercial Law, Toronto, 25 mars 1997*, Toronto, Osgoode Hall Law School, 1997, non publié : Tab VII, 1, 24. Le principal avantage du STPGV découle de son mode de compensation en temps réel, ce qui garantit la finalité du règlement et répond ainsi aux critiques entourant le SPII quant à la gestion des risques systémiques. Cette garantie est également fournie par des sûretés accordées par toutes les institutions financières à la Banque du Canada, de même que par l'utilisation du réseau Society for Worldwide Interbank Financial Telecommunication — mieux connu sous le nom de SWIFT — pour le transferts des messages de paiement : P.-L. MCPHERSON, *loc. cit.*, 25. Sur le STPGV, voir généralement : B. GEVA, *op. cit.*, note 51, § 4.04[2], p. 4-69 — 4-76 ; P.-L. MCPHERSON, *loc. cit.* ; D.A. CHAMBERLAND, *loc. cit.*

mais le projet ne concerne que l'envoi des messages de paiement, excluant les autres types de données[61].

Il appert donc que les chambres de compensation de grande valeur sont très réticentes à permettre la transmission de données autres que les ordres de paiement, et donc, à offrir des services de certification à cette fin ; seules les chambres de compensation de moindre valeur semblent permettre de telles possibilités. Toutefois, l'Association canadienne des paiements (ACP) travaille actuellement sur un tel projet[62].

1.4 Hiérarchie des autorités de certification

Nous avons déjà précisé qu'une autorité de certification devrait jouir d'une certaine indépendance pour acquérir la reconnaissance et la notoriété[63]. Une structure hiérarchique précise permet d'atteindre cet objectif. Celle-ci consiste en une superposition de plusieurs niveaux verticaux : par exemple, une autorité de certification de base — celle dont nous avons

---

61. SWIFT, *SWIFTNet PKI (Public Key Infrastructure) : Reinforcing SWIFT's Leadership in Security*, [En ligne], 2001, La Hulpe (Belgique), [http ://www.swift.com/index.cfm ?item_id=2306]. Voir de plus : SWIFT, *SWIFT User Handbook — FIN Service Description*, La Hulpe (Belgique), SWIFT, 1997, ch. 9. Organisme sans but lucratif, SWIFT a été incorporé en 1973 par 239 banques provenant de quinze pays — incluant le Canada — et a commencé ses opérations quatre années plus tard. En 2000, SWIFT possédait 7 125 institutions financières provenant de 192 pays — incluant 2 263 banques — qui ont transféré plus d'un milliard de messages pour une moyenne de cinq billions de dollars américains. Pour un historique de SWIFT, voir : SWIFT, « About SWIFT : Our History », [En ligne], 2000, La Hulpe (Belgique), [http ://www.swift.com/index.cfm ?item_id=1243] ; E.U. »BYLER et J.C. »BAKER, « S.W.I.F.T. : A Fast Method to Facilitate International Financial Transactions », (1983) 17 *J.W.T.L.* 459, 460 et suiv. ; E.P. ELLINGER, *Modern Banking Law*, Oxford, Clarendon Press, 1987, p. 343. Le Canada se situe au quatorzième rang avec 15,3 millions de messages : SWIFT, *Fast Facts*, [En ligne], 2000, La Hulpe (Belgique), [http ://www.swift.com/index.cfm ?item_id=1242] (1er décembre 2000). À l'inverse des réseaux STPGV, CHIPS et Fedwire, SWIFT n'est qu'un réseau de communication et n'effectue pas le règlement des ordres de paiement. Les relations entre SWIFT et ses membres sont régies par la loi belge : *SWIFT FIN Policy*, art. 5.3 (11). SWIFT est disponible jour et nuit, sept jours par semaine ; les messages sont standardisés ; c'est un moyen de communication rapide, abordable et très sécuritaire : G. TEDESCHI, « SWIFT : Le message financier éclair », (1992) 1015 *MOCI* 76 ; J. STUDER-LAURENS, « SWIFT : accélérer la vitesse des virements bancaires internationaux », (15 février 1993) *MOCI* 20 ; I. DE LAMBERTERIE et J. HUET, *Les conséquences juridiques de l'informatisation*, Paris, LGDJ, 1987, n° 10, p. 215. Depuis quelques années, SWIFT est utilisé pour des applications intérieures, par exemple en collaboration avec le réseau canadien STPGV : B. GEVA, *op. cit.*, note 51, § 4.04[2], p. 4-71.

62. *Infra*, section 1.4.

63. *Supra*, notes 7 et 50, ainsi que le texte correspondant.

discuté plus haut — se situerait au premier niveau ; une autorité régionale — supérieure — logerait au deuxième niveau ; par la suite, une autorité provinciale ou nationale serait positionnée au troisième niveau ; finalement, une autorité de certification internationale nicherait au quatrième niveau. Bien qu'elle soit attrayante au premier regard, une telle hiérarchie soulève cependant quelques interrogations.

D'abord, cette infrastructure est coûteuse en temps et en argent, et surtout il faut déterminer quels renseignements contenus dans la base de données de l'autorité de certification peuvent être consultés. Une tentative de résolution du problème repose sur la création d'un *webtrust*, c'est-à-dire que « [e]very participant [...] is able to issue notices about whom they know and trust, and there is no central authority[64] ». La base de données pourrait comprendre un bottin des adresses électroniques et des clés publiques, et chacune des représentations devrait être effectuée d'après l'authenticité de l'émetteur. Ce *webtrust* aurait également l'avantage d'éviter une infrastructure rigide et serait indépendant de toute autorité centralisée. En ce sens, l'émetteur devrait non seulement établir un lien de confiance avec les partenaires étrangers, mais aussi accepter qu'il y ait de nombreuses personnes avec qui il ne pourrait communiquer en toute sécurité[65].

Ensuite, il est nécessaire de déterminer qui peut agir en tant qu'autorité de certification aux niveaux supérieurs de la hiérarchie. Il est important, sinon crucial, de désigner des organismes qui jouissent d'une indépendance et d'une notoriété. À titre d'exemple, les chambres de commerce, le gouvernement et les notaires[66] peuvent très bien remplir ce rôle. En fait, les « [c]ybernotaries will play an essential role in the digital communications process [...] because the cryptographic system relies upon an

64. A.M. FROOMKIN, *loc. cit.*, note 2, 56 et 57, n. 26. Au Canada, l'Institut canadien des comptables agréés (ICCA) a proposé un projet commun de *webtrust* avec l'American Institute of Certified Public Accountants (AICPA). Ces principes et critères, tels que de saines relations d'affaires, l'intégrité des transactions et la protection de l'information, s'adressent aux fournisseurs de services Internet qui désirent obtenir un sceau de certification : WebTrust-ISP, CAWebTrust-ISP ou CPAWebTrust-ISP. Le sceau représente une sorte d'assurance pour les usagers de services fournis dans Internet. Voir : AICPA-ICCA, *Principes et critères* Webtrust-ISP^{SMIMD} *pour les fournisseurs de services Internet dans le domaine du commerce électronique*, version 2.0, [En ligne], 15 octobre 1999, [http ://www.webtrust.fr/Apropos/refenrec/criteres %20WebTrust %20pour %20ISPvf.PDF]. Il est intéressant de noter que VeriSign a indiqué sur son site le nom des entreprises ayant reçu le sceau WebTrust-ISP : VERISIGN, *VeriSign Secure Server Ids for the WebTrust Program*, [En ligne], 2000, Mountain View (Californie), [http ://www.verisign.com/webtrust/siteindex.html].

65. A.M. FROOMKIN, *loc. cit.*, note 2, 56 et 57, n-26.

66. C. PERREAULT, *loc. cit.*, note 50, 531-533.

impartial third party to verify the authenticity of electronic transactions[67] ». Toutefois, il ne faut pas négliger la possibilité qu'un cybernotaire certifie une fausse application en vue d'obtenir un certificat[68]. Au Canada, le Centre de la sécurité des télécommunications pilote un projet proposé par le Comité consultatif sur l'autoroute de l'information[69], appelé l'« Infrastructure à clé publique du gouvernement du Canada[70] ». Le gouvernement fédéral désire ainsi régler plusieurs questions, telles que la protection de la vie privée, le contrôle de l'accès, l'intégrité, l'authentification et la non-répudiabilité. Cette démarche devrait aider à résoudre, partiellement du moins, les problèmes liés à la sécurité et ainsi faciliter le commerce électronique. D'autres organisations, telles les associations bancaires ou de paiement, pourraient également assumer ce rôle.

En ce sens, l'ACP propose de devenir une autorité de certification principale — de niveau supérieur[71]. Elle affirme que cela fait partie intégrante de son mandat, qui est « d'établir et de mettre en œuvre un système national de compensation et de règlement et de planifier le développement du système national de paiement[72] ». Le conseil d'administration de l'ACP considère que la réalisation de ce projet permet une « évolution rapide de l'environnement mondial du commerce électronique et de la nécessité d'intervenir rapidement pour donner au Canada une infrastructure de paiement par Internet ». L'ACP croit de plus que sa réputation bien établie pourrait susciter « l'expansion et l'acceptation du commerce électronique

---

67. M.L. CLOSEN et R.J. RICHARDS, « Notaries Public — Lost in Cyberspace, or Key Business Professionals of the Future ? », (1997) 15 *J. Marshall J. Computer & Info. L.* 703, 739.

68. CERTIFICATION AUTHORITIES WORKING GROUP (INTERNET LAW & POLICY FORUM), *The Role Of Certificate Authorities In Consumer Transactions*, [En ligne], 14 avril 1997, nº 4.44, Montréal, [http ://www.ilpf.org/groups/ca/drafts.htm].

69. Pour le rapport définitif du comité, voir : COMITÉ CONSULTATIF SUR L'AUTOROUTE DE L'INFORMATION, *Préparer la Canada au monde numérique*, [En ligne], septembre 1997, Ottawa, [http ://strategis.ic.gc.ca/SSGF/ih01650f.html].

70. CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Infrastructure à clé publique du Gouvernement du Canada, Livre blanc*, [En ligne], 1998, Ottawa, [http ://www.cse-cst.gc.ca/fr/documents/services/mg15af.pdf].

71. ACP, *CPA PKI Business Strategy*, [En ligne], 16 février 2000, Ottawa, [http ://www.cdnpay.ca/fre/pub/PKI310.pdf] (ci-après citée : « Business Strategy »).

72. ACP, *L'Association canadienne des paiements facilitera la croissance des paiements par Internet au Canada*, p. 1, [En ligne], 20 mai 1999, Ottawa, [http ://www.cdnpay.ca/fre/whatsnew/communiqué.htm]. Voir de plus : Business Strategy, précitée, note 71. L'article 224 du nouveau projet de loi C-8, précité, note 44, prévoit un nouveau mandat pour l'ACP :

5. (1) L'Association a pour mission :

(a) d'établir et de mettre en œuvre des systèmes nationaux de compensation et de règlement, ainsi que d'autres arrangements pour effectuer ou échanger des paiements ;

au Canada, et [protéger] la position du Canada à l'avant-scène du commerce électronique mondial[73] ».

Le projet de l'ACP a pour objet d'offrir à ses membres[74] des méthodes de paiement sécuritaires[75]. L'ACP a établi quelques principes fondamentaux[76] qui seront mis en œuvre par l'entremise de plusieurs stratégies[77]. Il est intéressant de noter que les stratégies d'utilisation du certificat — de niveau supérieur — présentent des analogies avec les certificats délivrés par les autorités de certification subalternes. Par exemple, les caractéristiques permettant la sécurité — authenticité, intégrité, confidentialité et non-répudiation — s'y retrouvent, de même qu'un répertoire des transactions[78].

(b) de favoriser l'interaction de ses systèmes et arrangements avec d'autres systèmes et arrangements relatifs à l'échange, la compensation et le règlement de paiements ;
(c) de favoriser le développement de nouvelles technologies et méthodes de paiement.
(2) Dans la réalisation de sa mission, l'Association favorise l'efficacité, la sécurité et le bien-fondé des systèmes de compensation et de règlement et tient compte des intérêts des usagers.

73. ACP, *op.cit.*, note 72. Un récent sondage a confirmé que les usagers canadiens sont très anxieux à l'idée de fournir leur numéro de carte de crédit en ligne, de même qu'ils sont fort inquiets au sujet de la sécurité des transactions dans Internet en général, bien qu'ils soient au troisième rang des usagers d'Internet au monde (60 p. 100) derrière la Norvège (64 p. 100) et le Danemark (63 p. 100), et devant les Américains (57 p. 100) : R. MACKIE et W. IMMEN, « Canada 3rd in World for Use of Net », *The Globe & Mail* (2 juillet 2001) p. A1.

74. Un membre de l'ACP se caractérise par une institution de dépôt qui permet les dépôts par chèques : B. CRAWFORD, *Crawford and Falconbridge — Banking and Bills of Exchange*, Aurora, Canada Law Book, 1986, n° 4401.3(a), p. 1110 et 1111. Parmi les 130 membres de l'ACP, environ 30 p. 100 des institutions sont incorporées au niveau provincial et 60 p. 100 sont des quasi-banques. Les membres peuvent être des adhérents ou des non-adhérents. Seul un adhérent — détenant au moins 0,5 p. 100 du volume total national des effets de paiement — peut détenir un compte à la Banque du Canada en vue d'effectuer le règlement d'effets tirés sur lui ou payables par lui, tandis qu'un sous-adhérent doit utiliser les services d'un membre adhérent pour ce faire : art. 1.01(d), *Règlement n° 3 — Règlement de compensation*, (1983) 117 Gaz. Can. I, 494 (n° 3, 1983-01-15), modifié par le *Règlement administratif modifiant le Règlement n° 3 — Règlement de compensation*, (1998) 132 Gaz. Can. I, 867 (n° 16, 1998-04-18).

75. Business Strategy, précitée, note 71, p. 6.

76. Ce sont, notamment, l'élaboration d'un environnement de confiance, la flexibilité, l'efficience du coût, la neutralité technologique, l'adhérence aux standards, le contrôle, la sécurité, la responsabilité et la résolution des conflits : *Business Strategy*, précitée, note 71, p. 7-10.

77. L'ACP, *op. cit.*, note 72, p. 11-28, a élaboré les stratégies suivantes : 1) stratégies d'affaires ; 2) stratégies organisationnelles ; 3) stratégies axées sur les participants ; 4) stratégies de services de confiance ; 5) stratégies d'utilisation de certificat ; 6) stratégies de livraison.

78. *Id.*, p. 25-28.

Toutefois, l'ACP note que les certificats ne seront utilisés qu'aux fins d'authentification et d'identification de ses membres[79].

Un exemple concret de l'approche de l'ACP a été rendu public en avril 2001 alors que celle-ci a conclu une entente avec une filiale de la Banque de Nouvelle-Écosse (e-Scotia[80]) pour y héberger son autorité de certification principale, laquelle permet d'agréer les institutions membres de l'ACP qui désireront devenir des autorités de certification subalternes. L'ACP opine que l'« initiative nourrira la croissance du commerce électronique au Canada pour les quelques prochaines années, compte tenu des possibilités qu'elle présente de mettre des certificats logiciels à la disposition de presque toutes les entreprises et de tous les consommateurs du Canada, par le truchement de leurs relations bancaires existantes avec les membres de l'ACP ». D'ailleurs, l'ACP poursuit en affirmant, avec justesse, que son expérience en matière de sécurité et d'efficience des systèmes de paiement de même que ses relations de confiance avec ses membres, le gouvernement et les milieux financiers mondiaux la positionnent avantageusement pour remplir ce rôle[81].

2 Signatures électroniques

Nous avons vu que la signature électronique est nécessaire pour l'identification de l'émetteur d'un document informatisé, de même que pour la protection de sa transmission. La chapitre 2 présente les aspects juridiques entourant la délivrance (2.1), la gestion des certificats (2.2), la responsabilité de l'autorité de certification (2.3) et les dommages-intérêts (2.4).

2.1 Délivrance des certificats

Lorsqu'une autorité de certification reçoit un document accompagné d'une signature digitale, elle doit d'abord vérifier l'authenticité de l'émetteur et ensuite délivrer un certificat. L'OCC mentionne que « [v]erifying the identity of subscribers exposes [certification authority(ies)] to transaction, strategic, and reputation risk[82] ». Plus précisément, elle indique qu'une fausse identification, résultant d'une erreur ou d'une fraude, peut donner

79. *Id.*, p. 24.
80. E-Scotia représente une entité qui gère le commerce électronique de la Banque Scotia ; voir la vitrine de l'e-Scotia : <http ://www.e-scotia.com/index.html>.
81. ACP, *L'Association canadienne des paiements et e-Scotia annoncent la conclusion d'une convention d'hébergement de l'autorité de certification principale de l'ACP*, [En ligne], 5 avril 2001, Ottawa, [http ://www.cdnpay.ca/fre/whatsnew/escotia-release-f.htm] ; *supra*, notes 72 et 73, ainsi que le texte correspondant.
82. OCC Bulletin 99-20, précité, note 41, p. 6.

lieu à des risques transactionnels et de réputation. Ces risques peuvent également se produire au moment de la création d'un certificat, lorsque le système synchronisera automatiquement l'« appropriate certificate limitations to each subscriber's unique signing capabilities[83] ». Un risque de réputation peut aussi être soulevé si un logiciel qui permet la création d'une signature électronique est déficient. Au surplus, une carence de sécurité mènera certainement vers une source importante d'exposition aux risques transactionnels et de réputation[84]. Les problèmes de sécurité sont plus susceptibles d'engendrer des questions relatives à la fraude et à la vie privée. Les risques stratégiques surviendront à la suite du choix de politiques et d'actes de procédure par l'autorité de certification en vue de contrôler la procédure de vérification.

2.2 Gestion des certificats

Lorsque le certificat est délivré, l'autorité de certification peut agir comme un dépositaire. Le risque supporté par l'autorité de certification apparaît sous l'aspect d'un risque transactionnel, stratégique et de réputation. En particulier, les politiques et les actes de procédure entourant la création et la gestion d'un service d'aide aux usagers soulèvent tous les risques décrits ci-dessus. Concernant la configuration d'un logiciel, l'OCC croit que « [b]ecause a bank providing [certification authority] service ultimately may wish to maintain the customer relationship, the practical decision may be to provide customer service either internally or to contract with a firm with appropriate expertise[85] ». Néanmoins, les risques les plus importants sont liés à l'usage non autorisé. Si une autorité de certification se sert de politiques et d'actes de procédure non adaptés, ou n'agit pas dans un délai raisonnable, les risques décrits plus haut sont susceptibles d'apparaître. Le cas échéant, l'autorité de certification peut révoquer ou suspendre le certificat. La révocation survient lorsque le signataire a compromis son autorité de sa capacité de signer, et la suspension est utilisée lorsque la détermination du statut du certificat est nébuleuse. Une erreur ou un délai dans la révocation ou la suspension pourrait soulever des risques transactionnels et de réputation[86].

À l'égard de la gestion des risques, il convient de noter la stratégie organisationnelle de l'ACP, qui concerne l'obligation pour les membres d'atténuer les risques en restreignant la définition de l'usage possible d'un

83. *Id.*, p. 8.
84. *Id.*, p. 8 et 9.
85. *Id.*, p. 10.
86. *Id.*, p. 11.

certificat[87]. Plus précisément, les certificats ne sont délivrés qu'aux membres de l'ACP, ce qui permet d'autant de diminuer les risques[88].

2.3 Responsabilité des autorités de certification

De quelle manière convient-il de réglementer la responsabilité des autorités de certification quant à leur devoir de vérification des signatures électroniques ? Nonobstant la discrétion de la jurisprudence à l'égard de cette question, quelques tentatives ont été mises en avant par les organisations internationales et intérieures, de même que par les législateurs. Nous présentons ci-dessous les points de vue international (2.3.1.1) et européen (2.3.1.2) en premier lieu, vu leur influence sur les législations nord-américaines (2.3.2.1 et 2.3.2.2).

2.3.1 Réglementation internationale et européenne

2.3.1.1 Commission des Nations Unies pour le droit commercial international (CNUDCI)

La CNUDCI se penche depuis quelques années sur l'élaboration de règles uniformes pour la réglementation des signatures électroniques[89], lesquelles sont destinées à compléter la *Loi type de la CNUDCI sur le*

87. Cela peut se faire, par exemple, en limitant le nombre de certificats pouvant être délivrés — et re-délivrés — de même qu'en accordant une longue durée de vie aux certificats : Business Strategy, précitée, note 71, p. 24.

88. *Ibid.*

89. CNUDCI, GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE, *Projet de guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur les signatures électroniques*, Vienne, 25 juin–13 juillet 2001, A/CN.9/493 (ci-après cité : « Projet de guide »), [En ligne], [http ://www.uncitral.org/fr-index.htm] ; CNUDCI, « Projet de Loi type de la CNUDCI sur les signatures électronique », dans *Rapport du Groupe de travail sur le commerce électronique sur les travaux de sa trente-septième session*, Vienne, 18-29 septembre 2000, A/CN.9/483, Annexe, [En ligne], [http ://www.uncitral.org/fr-index.htm] (ci-après cité : « Projet de règles uniformes »). L'idée de réglementer les signatures électroniques et les autorités de certification est apparue en 1996 lorsque la CNUDCI a approché le Groupe de travail sur le commerce électronique à ce sujet : CNUDCI, « Rapport de la Commission des Nations Unies sur le droit commercial international sur les travaux de sa vingt-et-unième session », dans *Annuaire de la Commission des Nations Unies sur le droit commercial international*, t. XXVII, 1996, New York, 28 mai–14 juin 1996, A/51/17, nº 17. L'ensemble des documents préparatoires est disponible dans le site Internet de la CNUDCI : CNUDCI, *Documents préparatoires sur les signatures électroniques*, [En ligne], [http ://www.uncitral.org/fr-index.htm].

commerce électronique[90] en tant qu'instrument juridique distinct[91]. L'article premier de la *Loi type de la CNUDCI sur les signatures électroniques*[92] détermine l'étendue des règles, en mentionnant qu'elle « s'applique lorsque des signatures électroniques sont utilisées dans le contexte d'activités commerciales. Elle ne se substitue à aucune règle de droit visant à protéger le consommateur[93]. » Ainsi, ce projet n'exclut aucunement la protection des consommateurs[94], mais il reconnaît que les législations qui ont pour objet la protection des consommateurs peuvent avoir préséance sur la loi type[95]. Les articles 8, 9 et 11 de la *Loi type sur les signatures électroniques* traitent des normes de conduite du signataire, du prestataire de services de certification — autorité de certification — et de la partie se fiant à la signature ou au certificat[96].

L'article 8 (1) de la *Loi type sur les signatures électroniques* impose au signataire des normes de conduites analogues à celles des autres projets de réglementation des signatures électroniques[97]. En l'occurrence, le signataire doit : 1) prendre des mesures raisonnables pour empêcher les usages non autorisés ; 2) s'il estime que le certificat est compromis, aviser toute personne se fiant aux données dudit certificat ; 3) prendre toute disposition

90. CNUDCI, « *Loi type de la CNUDCI sur le commerce électronique*, A/51/17 », dans CNUDCI, *Annuaire de la Commission des Nations Unies sur le droit commercial international*, t. XXVII, 1996, *op. cit.*, note 89 Annexe I, p. 247 (ci-après citée : « Loi type sur le commerce électronique »).
91. Projet de guide, précité, note 89, nº 65, p. 29.
92. CNUDCI, « *Loi type de la CNUDCI sur les signatures électroniques* », dans Projet de guide, précité, note 89, Annexe (ci-après citée : « *Loi type sur les signatures électroniques* »).
93. Le champ d'application s'aligne avec la *Loi type sur le commerce électronique*. La CNUDCI ajoute que le terme « commerciales » s'interprète au sens large et comprend notamment les investissements, le financement et les opérations bancaires : Projet de guide, précité, note 89, nº 87, p. 37.
94. Tel est le cas pour d'autres modèles de loi de la CNUDCI : CNUDCI, « Loi type de la CNUDCI sur les virements internationaux », dans *Annuaire de la Commission des Nations Unies sur le droit commercial international*, t. XXIII, 1992, New York, 14 mai–22 juin 1992, A/CN.9/346, Annexe II, p. 437 (ci-après citée : « Loi type sur les virements internationaux »), et la *Loi type sur le commerce électronique*, précitée, note 90.
95. Projet de guide, précité, note 89, nº 91, p. 38.
96. Le concept de « prestataire de services de certification » fait référence à « une personne qui émet des certificats et peut fournir d'autres services liés aux signatures électroniques » : art. 2 de la *Loi type sur les signatures électroniques*, précitée, note 92.
97. C'est le cas notamment des projets européens, canadiens et américains présentés dans les sections suivantes.

afin de s'assurer de l'exactitude de la signature. Le signataire sera responsable en cas de manquement à ces exigences[98].

Une partie se fiant à la signature ou au certificat doit assumer une responsabilité si elle omet de prendre des dispositions raisonnables pour vérifier la fiabilité d'une signature électronique, ou pour vérifier la validité d'un certificat ou encore si celui-ci est suspendu ou révoqué[99]. Malgré la charge apparemment considérable que l'article 11 impose à cette partie, rappelons que les rédacteurs de cette loi type ont suggéré que cette dernière n'a pas pour objet de porter préjudice aux consommateurs[100].

En vertu de l'article 9 de la *Loi type sur les signatures électroniques*, le prestataire de services de certification doit notamment : 1) respecter ses déclarations concernant ses politiques et ses pratiques[101] ; 2) prendre des dispositions raisonnables pour assurer que les déclarations essentielles faites au sujet du certificat — durant tout son cycle de vie — ou figurant dans le certificat sont exactes et complètes ; 3) fournir à toute partie qui se fie au certificat des « moyens raisonnablement accessibles » de déterminer : l'identité de l'autorité de certification ; que le signataire désigné dans le certificat avait, lors de la délivrance de ce certificat, le contrôle des données relatives afférentes à la création de la signature ; que ces données étaient valides et non compromises, à ce moment-là ou antérieurement ; la méthode utilisée afin d'identifier le signataire, les restrictions prévues dans le certificat ou quant à l'étendue de la responsabilité stipulée par le prestataire de services de certification, et la possibilité de révocation en temps utile ; 4) utiliser des systèmes, des procédures et des ressources humaines fiables pour la prestation de services. Bref, les devoirs du prestataire de services de certification se résument à l'obligation d'agir de bonne foi, d'exercer une diligence raisonnable, de permettre l'accessibilité à toute partie qui se fie au certificat et de permettre au détenteur de la signature d'utiliser un système sécuritaire.

Le paragraphe 2 de l'article 9 établit le corollaire qu'un prestataire de services de certification sera tenu responsable en cas de tout manquement aux exigences mentionnées plus haut. Les commentaires du Groupe de tra-

---

98. *Loi type sur les signatures électroniques*, précitée, note 92, art. 8 (2). Le Groupe de travail sur le commerce électronique pose le principe de la responsabilité du signataire en cas de manquement, mais il laisse le soin aux législations nationales d'en réglementer les conséquences juridiques : Projet de guide, précité, note 89, n° 141, p. 55.
99. *Loi type sur les signatures électroniques*, précitée, note 92, art. 11.
100. *Supra*, notes 92-95, ainsi que le texte correspondant.
101. Cette première obligation représente la règle fondamentale : Projet de guide, précité, note 89, n° 142, p. 56.

vail sur le commerce électronique énoncent clairement que les législations nationales conservent toute la latitude requise afin d'établir le niveau de responsabilité d'une autorité de certification[102], mais il suggère certaines balises afin de délimiter le cadre de cette responsabilité, telles que le coût d'obtention du certificat, la nature de l'information, l'existence et l'ampleur de toute restriction qui limitent les fins d'utilisation du certificat, l'existence d'une limite de l'étendue de la responsabilité du prestataire de services de certification ainsi que toute conduite fautive de la partie qui se fie à la signature[103].

Dans l'éventualité où une autorité de certification agit en tant que mandataire d'une banque, il nous semble que les exigences décrites ci-dessus seront respectées. En fait, l'obligation d'agir de bonne foi et d'exercer une diligence raisonnable représentent des devoirs de droit civil, de common law et statutaires qu'une banque doit respecter[104].

2.3.1.2 Union européenne

En mai 1998, la Commission européenne a présenté une proposition de directive afin d'instaurer un cadre commun pour les signatures électroniques[105], laquelle a été arrêtée par le Parlement européen et le Conseil de

---

102. *Id.*, n° 145, p. 57.
103. *Id.*, n° 146, p. 57.
104. *Infra*, section 2.3.3.
105. CE, *Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques*, [1998] J.O. C. 325/5, adoptée par la Commission en mai 1998 (ci-après citée : « Proposition 325/5 »). Subséquemment, cette proposition a engendré des avis de deux comités en décembre 1998 et en janvier 1999 : COMITÉ ÉCONOMIQUE ET SOCIAL, *Avis du comité économique et social sur la « Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques »*, [1999] J.O. C. 40/29, et COMITÉ DES RÉGIONS, *Avis du Comité des régions sur la « Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques »*, [1999] J.O. C. 93/33. À la suite de ces avis, le Parlement européen a adopté cette proposition en première lecture et suggéré quelques modifications : CE, *Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (COM(98)0297 — C4-0376/98 — 98/0191 (COD))*, [1999] J.O. C. 104/49 (ci-après citée : « Proposition 104/49 »). Voir de plus : COMMISSION JURIDIQUE ET DES DROITS DES CITOYENS, *Rapport sur la proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (COM(98)0297 — C4-0376/98 — 98/0191 (COD))*, Doc. A4-0507/98, 16 décembre 1998 (rapporteur : Mr. Wolfgang Ullmann) (ci-après cité : « Rapport Ullmann n° 2 »). En juin 1999, le Conseil a adopté une position commune : CE, *Position commune (CE) No 28/1999 arrêtée par le Conseil le 28 juin 1999 en vue de l'adoption de la directive 1999/.../CE du Parlement européen et du Conseil du ... sur un cadre communautaire pour les signatures électroniques*, [1999] J.O. C. 243/33. Ensuite, le Parlement

l'Union européenne en décembre 1999[106]. Cette directive a pour objet d'établir un environnement juridique fiable entourant l'utilisation des signatures électroniques et leur reconnaissance juridique en vue de renforcer la confiance des usagers dans les signatures électroniques[107]. Plus précisément, la directive permettra d'encadrer le développement des activités des prestataires de service de certification sur des réseaux ouverts, ce qui pourrait inciter les entreprises à concevoir de nouvelles occasions pour le commerce électronique[108]. Enfin, la *Proposition 325/5* prévoyait explicitement l'importance d'harmoniser les règles des autorités de certification, car « des différences dans le champ d'application et le contenu de ces réglementations risquent de susciter des incertitudes juridiques », ce qui pourrait porter préjudice au « commerce transfrontalier et [entraver] le bon fonctionnement du marché intérieur »[109] ; le Parlement et le Conseil ne reprennent pas en détail cette philosophie, mais ils la sous-entendent dans le préambule[110].

---

européen et le Conseil ont proposé d'autres amendements en deuxième lecture : CE, *Résolution législative du Parlement européen sur la position commune du Conseil en vue de l'adoption de la directive du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques (7634/1/1999 — C5-0026/1999 — 1998/0191(COD))*, Doc. A5-0034/1999, 27 octobre 1999 ; voir de plus : COMMISSION JURIDIQUE ET DU MARCHÉ INTÉRIEUR, *Recommandation pour la deuxième lecture sur la position commune du Conseil en vue de l'adoption de la directive du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques (7634/1/1999 — C5-0026/1999 — 1998/0191(COD))*, Doc. A5-0034/1999, 27 octobre 1999 (rapporteur : M. Kurt Lechner). Finalement, la Commission européenne a produit un avis sur la seconde directive du Parlement européen et du Conseil, et elle a soumis une proposition de directive : COMMISSION DES COMMUNAUTÉS EUROPÉENNES, *Avis de la Commission conformément à l'article 251, paragraphe 2, alinéa c) du traité CE, sur les amendements proposés par le Parlement européen à la position commune du Conseil concernant la proposition de directive du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques, portant modification à la proposition de la Commission conformément à l'article 250, paragraphe 2 du traité CE*, COM/99/0626 Final — COD 99/0191, 26 novembre 1999.

106. CE, *Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques*, [2000] J.O. L. 13/12 (ci-après citée : « Directive 1999/93/CE »).
107. *Id.*, préambule, par. 4 ; art. 1.
108. *Id.*, préambule, par. 4.
109. Proposition 325/5, précitée, note 105, préambule, par. 5, 7, et 11.
110. Notamment, voir les paragraphes 5 et 20 du préambule de la Proposition 325/5, précitée, note 105. Toutefois, le paragraphe 17 affirme que l'harmonisation ne doit pas porter « atteinte aux obligations d'ordre formel instituées par le droit national pour la conclusion de contrats ni aux règles déterminant le lieu où un contrat est conclu ».

La Directive 1999/93/CE suggère deux définitions de la signature électronique, soit la simple signature électronique et la « signature électronique avancée[111] ». La première est décrite comme « une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification », tandis que la seconde représente une signature électronique qui respecte des critères précis : « être liée uniquement au signataire[,] permettre d'identifier le signataire[,] être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et [...] être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable[112] ».

L'article 6 de la directive traite de la responsabilité de l'autorité de certification, appelée « prestataire de service de certification[113] ». Il est important de lire l'article 6 avec les Annexes I à IV, lesquelles abordent respectivement les exigences concernant les certificats qualifiés (Annexe I), les exigences au sujet des prestataires de services de certification délivrant des certificats qualifiés (Annexe II), les exigences quant aux dispositifs sécurisés de création de signature électronique (Annexe III) et les recommandations pour assurer la vérification sécurisée de la signature (Annexe IV). En particulier, soulignons que l'Annexe II exige que les prestataires de service de certification vérifient l'identité de la personne à qui le certificat est délivré, emploient du personnel compétent, utilisent des systèmes et des produits fiables, prévoient des mesures contre la fraude, gardent l'information pour une durée suffisante en vue de respecter la prescription juridique et fournissent de l'information précontractuelle.

L'article 6 (1) mentionne que le prestataire de service de certification peut être tenu responsable envers une personne physique ou morale qui se fie à l'information contenue dans le certificat qualifié, à l'identité du signataire et à l'utilisation de données « de manière complémentaire », à moins que le prestataire de service de certification ne démontre « qu'il n'a commis aucune négligence » ; cela représente une démarcation significative par

111. Directive 1999/93/CE, précitée, note 106, art. 1 (1) et (2). Toutefois, la Directive 325/5, précitée, note 105, précédant la Directive 1999/93/CE, ne l'avait point retenue. Sur cette question, il est intéressant de noter que la Proposition 104/49 a modifié cette définition pour englober l'éventail des signatures électroniques et ne pas se limiter aux signatures digitales, permettant ainsi une neutralité du moyen de communication nécessaire pour les développements futurs, et suivant l'orientation de la CNUDCI et de l'OCDE : Proposition 104/49, précitée, note 105, p. 20.

112. Voir l'analogie avec la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, *infra*, note 128.

113. Directive 1999/93/CE, précitée, note 106.

rapport à la Proposition 325/5[114], laquelle prévoyait « un certain compromis entre une responsabilité stricte et une responsabilité par négligence[115] ». L'article 6 (2) mentionne que le prestataire de service de certification est responsable pour un préjudice causé à une personne, physique ou morale, s'il a omis d'enregistrer la révocation du certificat, à moins de prouver « qu'il n'a commis aucune négligence ». Les paragraphes 3 et 4 permettent à un prestataire de service de certification de limiter sa responsabilité par une indication d'une limite d'utilisation du certificat et la valeur de la transaction, pour autant que « ces limites soient discernables par des tiers ».

Ainsi, l'article 6 de la Directive 1999/93/CE[116] est plus exigeant que la *Loi type sur les signatures électroniques*[117] par rapport aux responsabilités des prestataires de service de certification. Cette approche converge vers notre postulat de base, selon lequel une autorité de certification pouvant agir sous les auspices d'une banque, il devient nécessaire de renforcer sa responsabilité.

2.3.2 Réglementation intérieure

2.3.2.1 Canada

Au Canada, la situation des signatures électroniques est embryonnaire par rapport aux projets de la CNUDCI et de l'Union européenne. Au niveau national, la *Loi uniforme sur le commerce électronique*[118], préparée par la Conférence pour l'harmonisation des lois au Canada (Conférence), a pour objet l'implantation des principes fondamentaux de la *Loi type sur le commerce électronique* au Canada[119]. La *Loi uniforme sur le commerce électronique* se divise en trois parties : 1) fourniture et conservation de l'information, qui présentent des règles de base analogues à celles de la *Loi type sur le commerce électronique* ; 2) communication de documents électroniques ; et 3) transport de marchandises. Malheureusement, la *Loi uniforme sur le commerce électronique* est principalement orientée vers les documents électroniques aux dépens du développement d'un cadre juridique cohérent gouvernant les signatures électroniques, sous réserve de quelques aspects, telle la définition de la signature.

---

114. *Id.*
115. Rapport Ullmann nº 2, précité, note 105, p. 26.
116. Directive 1999/93/CE, précitée, note 106.
117. *Id.*
118. CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA, *Loi uniforme sur le commerce électronique*, [En ligne], août 1999, Ottawa, [http ://www.ulcc.ca/fr/us].
119. *Id.*, p. 2.

L'article premier de la *Loi uniforme sur le commerce électronique* définit une signature électronique comme une « information sous forme électronique qu'une personne met ou associe à un document et qu'elle a créée ou adoptée avec l'intention de signer le document ». Cette définition doit être lue en parallèle avec le paragraphe 2 de l'article 10, qui n'exige pas que la signature soit fiable, mais prévoit qu'une telle condition puisse être requise par l'autorité compétente. La Conférence reconnaît que l'intention de signer doit primer la nécessité que la signature électronique ressemble à la signature manuscrite[120]. Ce point de vue s'achemine vers l'article 2827 du *Code civil du Québec*, lequel définit la signature comme « l'apposition qu'une personne fait sur un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement[121] ». Plus précisément, la Conférence ajoute que cette définition signifie qu'une « signature électronique est simplement une signature sous forme électronique » et que la signature électronique n'est pas nécessairement associée à un document électronique, comme cela se produit avec les documents sur supports traditionnels ; en d'autres termes, la *Loi uniforme sur le commerce électronique* prévoit qu'une signature électronique et un document électronique sont deux éléments distincts[122]. Bien que nous soyons d'accord avec cette définition, nous ne partageons pas l'orientation de la Conférence au sujet de la non-imposition de la condition de fiabilité de la signature ainsi que du fardeau de la preuve de la signature électronique.

D'abord, la Conférence signale qu'une exigence de la fiabilité de la signature « nuirait au principe de la Loi uniforme qui cherche la neutralité quant au moyen de communication », ce qui va à l'encontre du point de vue de la CNUDCI, et ce, de l'aveu même de la Conférence[123] ! Il convient de rappeler que l'exigence de la fiabilité de la signature électronique est présente non seulement dans la *Loi type sur les signatures électroniques*[124], mais aussi à l'article 2837 C.c.Q., de même qu'implicitement dans la Directive 1999/93/CE[125].

---

120. Comme le reconnaissent les rédacteurs, il est possible qu'une signature numérisée ressemble à une signature manuscrite : *id.*, p. 4.
121. Les commentaires sous-jacents à l'article premier de la *Loi uniforme sur le commerce électronique* indiquent que cette définition se réfère à « l'intention de signer » un document et « ne donne pas un sens juridique différent à la signature dans le milieu électronique » : *id.*, p. 3.
122. *Id.*, p. 3.
123. *Id.*, p. 10.
124. *Loi type sur les signatures électroniques*, précitée, note 92, art. 6 (1).
125. Directive 1999/93/CE, précitée, art. 1 (2), 5 (1).

D'autre part, la Conférence prévoit que celui qui entend se prévaloir d'un document accompagné d'une signature électronique a le fardeau de prouver qu'une telle signature répond aux exigences de l'article 10. En pratique, une telle attitude ne favorise pas l'utilisation des signatures électroniques, non plus que l'éclosion du commerce électronique, puisque cette preuve peut être difficile à obtenir dans bien des cas. Par exemple, la jurisprudence impose un tel fardeau — presque insurmontable — aux titulaires de cartes de débit qui allèguent s'être fait retirer des fonds de leur compte à la suite du vol de leur carte de débit[126]. D'ailleurs, l'article 2838 C.c.Q., qui énonce une présomption en faveur de celui qui tente de se prévaloir d'un document informatisé présentant des garanties suffisamment sérieuses pour s'y fier lorsqu'elle est effectuée de manière systématique, plaide à l'encontre de l'approche de la Conférence.

Malheureusement, la *Loi uniforme sur le commerce électronique*[127] n'aborde pas certaines conséquences de l'utilisation des signatures électroniques, telle la responsabilité. Au surplus, cette loi ne prend pas en considération le rôle de l'autorité de certification. À ce jour, il n'existe aucun signe d'une loi fédérale régissant les autorités de certification, en dépit de la nouvelle *Loi sur la protection des renseignements personnels et les documents électroniques*[128].

---

126. Voir notamment : *Caisse populaire de Bathurst Ltée* c. *Couture*, (1997) 185 N.B.R. (2d) 386 (C.A.) ; *Royal Bank of Canada* c. *Devarenne*, (1998) 205 N.B.R. (2d) 250 (B.R. (1re inst.)) ; *Royal Bank of Canada* c. *Egan*, [1996] B.C.J. nº 2706 (B.C.Prov. Ct. (p.cr.)) ; *Gaudreault* c. *Caisse Populaire Desjardins de St-Rédempteur*, B.E. 98E-1271 (C.Q. (p.cr.)) ; *Laberge* c. *Caisse populaire Desjardins de Cowansville*, [1999] R.L. 503 (C.Q.). Toutefois, le *Code de pratique canadien de services de cartes de débit* (ci-après cité : « Code de pratique »), préparé par le Groupe de travail sur le transfert électronique de fonds de l'Association des banquiers canadiens (ABC), n'impose pas explicitement un tel fardeau au titulaire, mais il le tient responsable des retraits non autorisés ; le Code de pratique est entériné par l'ABC, l'ACP, l'Association des compagnies de fiducie du Canada, la Centrale des caisses de crédit du Canada, la Confédération des caisses populaires et d'économie Desjardins du Québec, le Conseil canadien du commerce de détail, la Fédération canadienne de l'entreprise indépendante ainsi que l'Association des consommateurs du Canada, et il a obtenu l'appui des organismes et ministères suivants : Industrie Canada, le ministère des Finances et le Bureau du surintendant des institutions financières. Au sujet du Code de pratique, voir : ABC, *Code de pratique canadien de services de cartes de débit*, Toronto, mai 1992, modifié en 1996, [En ligne], [http ://www.cba.ca/fr/Publications/DebitCode/debitcode.htm].

127. *Loi uniforme sur le commerce électronique*, précitée, note 118.

128. *Loi sur la protection des renseignements personnels et les documents électroniques*, précitée, note 112. L'article 31 de cette loi propose deux types de signatures électroniques : d'abord, la simple signature électronique, définie comme une « [s]ignature constituée d'une ou de plusieurs lettres, ou d'un ou de plusieurs caractères, nombres ou autres

Bien que la plupart des juridictions provinciales canadiennes reconnaissent le concept de la signature électronique[129], la question de la responsabilité des autorités de certification n'est discutée en profondeur que dans la *Loi concernant le cadre juridique des technologies de l'information*[130]. Cette loi québécoise traite précisément du concept de l'équivalence fonctionnelle des documents électroniques et de leur reconnaissance pour en assurer la sécurité lors de la transmission ; de plus, elle a pour objet l'harmonisation des systèmes techniques et des standards de communication utilisés pour les documents électroniques ; finalement, elle gouverne les activités des autorités de certification[131].

Selon l'article 47 de la *Loi sur les technologies de l'information*[132], un certificat « peut servir à établir un ou plusieurs faits dont la confirmation de l'identité d'une personne, [...] de l'exactitude d'un identifiant d'un document ou d'un autre objet, de l'existence de certains attributs d'une personne, d'un document ou d'un autre objet ou encore du lien entre eux et un dispositif d'identification ou de localisation tangible ou logique ». De plus, un « certificat d'attribut peut, à l'égard d'une personne, servir à établir notamment sa fonction, sa qualité, ses droits, pouvoirs ou privilèges au sein d'une personne morale, d'une association, d'une société, de l'État ou dans le cadre d'un emploi. Il peut, à l'égard d'une association, d'une société ou

---

symboles sous forme numérique incorporée, jointe ou associée à un document électronique » ; ensuite, la signature électronique sécurisée, définie comme « [s]ignature électronique qui résulte de l'application de toute technologie ou de tout procédé prévu par règlement pris en vertu du paragraphe 48 (1) ». Cette disposition se réfère au droit du gouverneur en conseil, sur une recommandation du Conseil du Trésor, de prévoir les types de technologies qui satisfassent à la définition de la signature électronique sécurisée utilisée ; pour ce faire, l'article 48 (2) suggère quelques éléments : *a*) la signature électronique résultant de l'utilisation de la technologie ou du procédé est propre à l'usager ; *b*) l'utilisation de la technologie ou du procédé pour l'incorporation, l'adjonction ou l'association de la signature électronique de l'utilisateur au document électronique se fait sous la seule responsabilité de ce dernier ; *c*) la technologie ou le procédé permet d'identifier l'usager ; *d*) la signature électronique peut être liée au document électronique de façon à permettre de vérifier si le document a été modifié depuis que la signature électronique a été incorporée, jointe ou associée au document.

129. Outre le Québec, voir notamment : Alberta : *Electronic Transactions Act*, Projet de loi 21 (1re lecture le 28 mai 2001), 1re session, 25e législature, art., 1(c), 16, 22, 25, 26 ; Colombie-Britannique : *Electronic Transactions Act, 2000*, S.B.C. 2001, c. 10, art. 1, 11 ; Ontario : *Loi de 2000 sur le commerce électronique*, L.O. 2000, c. 17, art. 1(1), 11, 17, 24-26, 32 ; *Loi sur les sociétés par actions*, L.R.O. 1990, c. B-16, art. 1, 109.

130. *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, c. 32 (ci-après citée : « *Loi sur les technologies de l'information* »).

131. *Id.*, art. 47-62.

132. *Supra*, note 130.

d'un emplacement où l'État effectue ou reçoit une communication, établir leur localisation[133]. » Le certificat doit inclure un minimum de renseignements, tels que le nom distinctif du prestataire de services, son énoncé de politique, y compris ses pratiques au sujet des garanties du certificat délivré, la version du certificat et son numéro de série, le début et la fin de la période de validité du certificat, s'il s'agit d'un certificat qui confirme l'identité d'une personne, son nom distinctif, et « s'il s'agit d'un certificat d'attribut, la désignation de l'attribut dont le certificat confirme l'existence et l'identification de la personne[134]. » La loi prévoit également la possibilité de créer un répertoire, lequel serait destiné à identifier une personne ou un objet, ou même à établir une connexion entre les deux[135]. Le répertoire n'aurait pas à publier les raisons justifiant une suspension ou un refus de délivrance d'un certificat[136] ; soulignons que cette disposition ne devrait pas s'appliquer aveuglément dans tous les cas, mais devrait plutôt tenir compte de certaines situations, par exemple la fraude ou pour des fins d'ordre public.

L'article 51 définit le rôle des services de certification, soit la vérification de l'identité des émetteurs et la délivrance de certificats. Pour toute délivrance ou renouvellement du certificat, le prestataire de services de certification doit fournir un énoncé de politique spécifiant en détail la précision de l'information, son utilité, la manière d'obtenir de l'information, sa politique de confidentialité et les personnes à qui l'information est transmise[137]. Cet énoncé de politique doit de plus être accessible au public[138]. L'article 54 (1) mentionne que les certificats délivrés par un prestataire de services de certification selon d'« autres normes que celles applicables au Québec peuvent être considérés équivalents aux certificats délivrés par un prestataire de services de certification accrédité[139]. » Outre l'énoncé de politique, d'autres éléments doivent être pris en considération, tels qu'une preuve de la création de l'identité du requérant, ainsi que des garanties d'intégrité, d'accessibilité et de sécurité du répertoire et du certificat délivré ou renouvelé par le fournisseur[140].

La *Loi sur les technologies de l'information*[141] présente également certaines dispositions sur la responsabilité d'une autorité de certification,

---

133. *Id.*, art. 47, al. 2.
134. *Id.*, art. 48, al. 2 (6).
135. *Id.*, art. 50, al. 1.
136. *Id.*, art. 50 *in fine*.
137. *Id.*, art. 47, al. 2 (2) et art. 52, al. 1.
138. *Id.*, art. 52, al. 2.
139. *Id.*, art. 54, al. 1 : l'équivalence doit être constatée par un organisme gouvernemental.
140. *Id.*, art. 55.
141. *Supra*, note 130.

de même que sur la responsabilité du détenteur de la clé. Dans le premier cas, le prestataire de services de certification doit garantir l'intégrité du certificat, incluant la modification, la suspension, l'annulation et l'archivage, et doit confirmer le lien entre le dispositif d'identification et le signataire[142]. En d'autres termes, le prestataire de services « doit présenter des *garanties d'impartialité* par rapport à la personne ou l'objet visé par la certification, *même s'il n'est pas un tiers à leur égard* » [l'italique est de nous]. Cela représente une obligation cruciale en rapport avec notre prémisse, car, selon cette dernière, l'autorité de certification agit en tant que mandataire d'une banque et non à titre de partie indépendante. Bien qu'en apparence une banque qui offre des services d'autorité de certification à ses clients ne soit pas un tiers, et donc ne semble pas présenter *prima facie* des garanties d'impartialité, il convient de rappeler que la structure hiérarchique présentée précédemment permet de combler cette lacune[143].

Dans le second cas, l'article 56 *in fine* contient une disposition ayant pour objet de s'assurer que le prestataire de services vérifie l'information transmise lorsqu'il produit « un document présenté comme un certificat confirmant l'identité d'une personne ou l'exactitude d'un identifiant d'un objet, alors qu'aucune vérification n'est faite par le prestataire de services ou pour lui ou que l'insuffisance de la vérification effectuée équivaut à une absence de vérification ». De plus, le prestataire de services de certification doit préserver la confidentialité des secrets commerciaux[144].

Le détenteur d'une clé doit contrôler la confidentialité de son usage ; toute utilisation de la clé est présumée provenir du détenteur[145]. Cette présomption est susceptible de protéger l'autorité de certification, la banque, et indirectement la personne se fiant à l'information en cas de fraude commise par le signataire ou un tiers. Toutefois, en cas de perte ou de vol de la clé, si le détenteur a des motifs raisonnables de croire que la confidentialité de la clé privée est compromise, il doit aviser le prestataire de services de certification dans les meilleurs délais[146]. Finalement, il a une obligation de diligence analogue à celle qui repose sur les prestataires de services de certification et de répertoire[147].

Les prestataires de services de certification et de répertoire ainsi que les détenteurs d'une clé publique « ne sont tenus qu'à des obligations de

142. *Id.*, art 56, al. 1 (3).
143. *Supra*, section 1.4.
144. *Id.*, art. 57.
145. *Loi sur les technologies de l'information*, note 130, art. 57, al. 2.
146. *Id.*, art. 58.
147. *Id.*, art. 60.

moyens[148] », et nul ne peut refuser d'assumer sa part de responsabilité résultant de « l'inexactitude ou de l'invalidité du certificat, ou d'un renseignement contenu au répertoire », selon l'article 61 (2). Toutefois, puisque la *Loi sur les technologies de l'information*[149] n'est pas d'ordre public, il est possible pour le prestataire de services de certification et le signataire de déroger conventionnellement aux articles 56 et 57[150].

2.3.2.2 États-Unis

L'American Bar Association (ABA) a présenté un projet de lignes directrices destiné à gouverner les signatures électroniques, appelée *Digital Signature Guidelines*[151]. Les ABA Guidelines ont pour objet d'établir une relation juridique entre les autorités de certification, les signataires ainsi que les personnes se fiant à une signature et à un certificat[152]. Bien qu'elles n'aient pas été produites dans le but d'être adoptées formellement par un texte législatif, ces lignes directrices doivent être perçues comme un point de départ pour l'harmonisation des principes juridiques et peuvent être utilisées en tant que « common basis for more precise rules in various legal systems[153] ». Contrairement à la *Loi uniforme sur le commerce électronique*[154], les ABA Guidelines sont essentiellement orientées vers les signatures digitales et non vers les signatures électroniques[155].

Les ABA Guidelines déterminent les devoirs des autorités de certification, de l'émetteur et du destinataire. Concernant le signataire, l'article

148. *Id.*, art. 61.

149. *Supra*, note 130.

150. Il n'existe aucune indication dans la loi à savoir que celle-ci est d'ordre public.

151. SECTION OF SCIENCE AND TECHNOLOGY, ELECTRONIC COMMERCE DIVISION, INFORMATION SECURITY COMMITTEE (ABA), *Digital Signature Guidelines*, [En ligne], 1996, Chicago, [http ://www.abanet.org/scitech/ec/isc/dsg-toc.html] (ci-après citées : « ABA Guidelines »).

152. *Id.*, p. 22.

153. *Id.*, p. 22 et 23.

154. *Loi uniforme sur le commerce électronique*, précitée, note 118.

155. ABA Guidelines, précitées, note 151, p. 21. Les signatures digitales ont trait à la cryptographie asymétrique ; les signatures électroniques proviennent de technologies plus variées. Voir de plus : E.D. KANIA, « The ABA's Digital Signature Guidelines : An Imperfect Solution to Digital Signatures on the Internet », (1999) 7 *Comm Law Conspectus* 297, 301. Les ABA Guidelines définissent une signature digitale comme suit : A transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine

(1) whether the transformation was created using the private key that corresponds to the signer's public key, and

(2) whether the initial message has been altered since the transformation was made.

4.1 des ABA Guidelines prévoit qu'il doit utiliser un système fiable pour produire les clés[156]. Également, comme cela se fait pour les autres dispositions législatives, le signataire doit fournir une information précise à l'autorité de certification, lui notifier en cas de découverte d'une erreur[157], éviter de compromettre la clé privée[158] et, le cas échéant, avertir l'autorité de certification de suspendre ou de révoquer la clé[159].

Les devoirs de l'autorité de certification sont énumérés dans la partie 3 des ABA Guidelines. Selon ces dernières, l'autorité de certification doit utiliser un système fiable, ce qui représente une condition *sine qua non*[160]. De plus, elle doit notamment : divulguer l'information au signataire dans un délai commercialement raisonnable[161] ; enregistrer et conserver l'information pour une période de temps suffisante en vue de respecter la prescription légale qui s'applique à la délivrance, à la suspension ou à la révocation du certificat[162] ; permettre à n'importe qui de vérifier la signature[163] ; confirmer que les informations respectent les exigences des lignes directrices, c'est-à-dire que la clé privée du signataire correspond à la clé publique du détenteur de celle-ci et qu'elles constituent une paire de clés fonctionnelle[164] ; s'abstenir de publier un certificat si elle sait qu'il n'a pas été délivré ou que le signataire ne l'a pas accepté[165] ; suspendre ou révoquer un certificat sur demande du signataire ou d'un de ses mandataires[166] ; suspendre ou révoquer un certificat sans le consentement du signataire, si elle découvre qu'un fait matériel est faux ou si un tel fait, qui est nécessaire

156. Une paire de clés se réfère aux clés privée et publique, définies respectivement aux articles 1.24 et 1.25 des ABA Guidelines, précitées, note 151. Le Commentaire n° 4.1.1, sous-jacent à l'article 4.1, spécifie qu'un système fiable doit suivre les exigences d'un système cryptographique à clé publique — défini à l'article 1.3 — afin de générer la paire de clés.
157. ABA Guidelines, précitées, note 151, art. 4.2.
158. *Id.*, art. 4.3.
159. *Id.*, art. 4.4.
160. *Id.*, art. 3.1. Le Commentaire n° 3.1.1 renvoie au Commentaire n° 1.35.3 : « [c]omputer security is a matter of degree rather than an absolute », et le niveau le plus sécuritaire n'est pas nécessairement souhaitable ; ainsi, il devient nécessaire de considérer les éléments suivants pour évaluer un système raisonnablement sécuritaire : « whether more secure or reliable systems and practices are available and feasible », et « [i]f such systems and practices are feasible and available, the cost of providing a higher level of assurance balanced against the seriousness of the risk incurred by foregoing the higher level of assurance ».
161. *Id.*, art. 3.2.
162. *Id.*, art. 3.5.
163. *Id.*, art. 3.6.
164. *Id.*, art. 3.7.
165. *Id.*, art. 3.8.
166. *Id.*, art. 3.9 et 3.10.

à la délivrance et qui n'a pas été obtenu en accord avec le système fiable du signataire, est compromis[167] ; notifier promptement la situation au signataire lorsqu'une suspension ou une révocation survient[168]. Enfin, la terminaison des relations d'affaires de la part de l'autorité de certification doit survenir « in a manner that will cause minimal disruption to the subscribers of valid certificates and to relying parties[169] ».

Si une autorité de certification respecte les exigences des ABA Guidelines, particulièrement concernant les devoirs décrits ci-dessus, elle ne sera pas tenue responsable pour les pertes subies par le signataire, l'autorité de certification ou toute autre personne. Si la perte résulte du certificat, d'une signature digitale ou d'une information représentée dans un certificat ou un répertoire, l'autorité de certification ne sera pas tenue responsable[170]. Cette disposition doit être lue parallèlement avec l'article 2.2, lequel permet une dérogation conventionnelle entre l'autorité de certification et le signataire, bien que cette dérogation ne lie pas les tiers[171].

Finalement, le seul devoir d'une partie qui se fie au certificat est de s'assurer que la signature digitale est raisonnable dans les circonstances ; si tel n'est pas le cas, ce destinataire supporte le risque d'une signature digitale invalide[172]. L'élément important est de déterminer la signification du terme « raisonnable ». Selon l'article 5.4, la « reasonableness of reliance » doit être évaluée en fonction des quatre facteurs suivants : 1) les faits connus d'une partie qui se fie au certificat ou les faits pour lesquels elle a reçu une notification ; 2) la valeur ou l'importance du message signé de manière digitale, s'il est connu ; 3) l'état des transactions (*course of dealing*) entre la partie qui se fie au certificat et le signataire ; et 4) les usages du commerce, dont ceux qui sont liés à l'utilisation d'un système fiable[173].

En plus des ABA Guidelines, plusieurs États américains ont adopté des législations au sujet des signatures électroniques[174]. À cet égard, soulignons que la première et la plus importante loi américaine sur le sujet,

---

167. *Id.*, art. 3.11.
168. *Id.*, art. 3.11 *in fine* et 3.12.
169. *Id.*, art. 3.13.
170. *Id.*, art. 3.14.
171. *Id.*, Commentaire n° 2.2.1.
172. *Id.*, art. 5.3 (2).
173. Pour plus de détails, voir : ABA Guidelines, précitées, note 151, Commentaires n^{os} 5.4.1-5.4.5.
174. Voir par exemple : Californie : *California Digital Signature Act*, Cal. Civ. Code Ann. § 1633.2 (West 2001) et *California Signature Regulations*, Cal. Code Reg. § 22000 (West 1998) ; Floride : *Electronic Signature Act of 1996*, Fla. Stat. § 668.001 (West 2000) ; New York : *Electronic Signatures and Records Act*, NY State Tech § 101 (McKinney, 2001) ;

l'*Utah Digital Signature Act*[175], puise ses racines dans les ABA Guidelines. Cette loi est destinée à admettre les signatures digitales et les documents électroniques. Sa caractéristique majeure est qu'elle ne permet qu'une seule méthode de sécurité : la cryptographie asymétrique[176]. Cette loi contient en outre plusieurs dispositions gouvernant les devoirs, les obligations et la responsabilité des autorités de certification. De plus, ajoutons que, contrairement à la *Loi type sur les signatures électroniques*[177], à la Directive 1999/93/CE[178] ou aux ABA Guidelines[179], l'*Utah Digital Signature Act* spécifie en détail la manière dont une autorité de certification doit procéder pour obtenir une licence[180].

La partie 3 de l'*Utah Digital Signature Act* traite des devoirs du signataire et des autorités de certification. Comme le prévoient les ABA Guidelines[181], le signataire doit exercer un soin raisonnable lorsqu'il agit comme dépositaire de la clé privée, et ce, afin de prévenir toute divulgation

---

Virginie : *Uniform Computer Information Transactions Act*, Va. Code Ann. § 59.1-501.1 (West 2001). Voir également : M.J. OSTY et M.J. PULCANIO, « The Liability of Certification Authorities to Relying Third Parties », (1999) 17 *J. Marshall J. Computer & Info. L.* 961, 971-974. De plus, notons que le comité de rédaction du *Uniform Commercial Code* (UCC) travaille depuis 1995 à l'élaboration de l'Article 2B, destiné à réglementer les transactions informatisées. La philosophie du nouvel Article 2B tourne autour du concept de licence dans les transactions d'information et de biens intangibles, innovant ainsi par rapport à l'Article 2 gouvernant la vente de biens et services. Une autre innovation a trait au concept de signature, maintenant remplacé par celui d'authentification (art. 2B-202(3)), terme plus général qui comprend toutes autres formes techniques de manifestation, tels les enregistrements vocaux : AMERICAN LAW INSTITUTE et NATIONAL CONFERENCE OF COMMISSIONNERS ON UNIFORM STATE LAWS, *Uniform Commercial Code Article 2B : Software Contracts and Licenses of Information — With Notes*, [En ligne], août 1998, Chicago (Illinois), [http ://www.law.uh.edu/ucc2b/080198/080198.html]. Pour l'historique de l'élaboration de l'article 2B, voir : UNIVERSITY OF HOUSTON LAW CENTER, *Uniform Commercial Code Article 2B Revision Draft Download Site*, [En ligne], 1998, Houston (Texas), [http ://www.law.uh.edu/ucc2b].

175. Utah Code Ann. §§ 46-3-101 — 46-3-504 (1953) (ci-après cité : « *Utah Digital Signature Act* »).
176. *Supra*, note 2.
177. *Loi type sur les signatures électroniques*, précitée, note 92.
178. Directive 1999/93/CE, précitée, note 106.
179. ABA Guidelines, précitées, note 151.
180. *Utah Digital Signature Act*, précitée, note 175, §§ 46-3-201 — 46-3-204. Soulignons notamment que l'autorité de certification « may not conduct its business in a manner that creates an unreasonable risk of loss to subscribers of the certification authority, to persons relying on certificates issued by the certification authority, or to a repository » : § 46-3-204 (1). Cette loi définit un répertoire comme « a system for storing and retrieving certificates and other information relevant to digital signatures » : § 46-3-103 (29).
181. *Supra*, notes 160-169, ainsi que le texte correspondant.

de celle-ci[182], de certifier l'exactitude de l'information contenue dans le certificat et détenir la bonne clé qui correspond à la clé publique[183].

En général, les devoirs de l'autorité de certification ressemblent à ceux qui sont contenus dans les ABA Guidelines[184], bien qu'ils soient plus précis. D'abord, l'autorité de certification doit utiliser un système fiable pour la délivrance, la suspension ou la révocation d'un certificat, ainsi que pour la création d'une clé privée[185], et elle doit divulguer « any material certification practice statement[186] ». Au sujet de la délivrance des certificats, si le signataire accepte le certificat délivré, l'autorité de certification doit publier une copie d'un certificat dans le répertoire[187]. L'article 46-3-303 (1) mentionne que, par l'entremise de la délivrance d'un certificat, l'autorité de certification garantit au signataire que le certificat est exact et satisfaisant, et l'article 46-3-303 (3) ajoute que cette dernière certifie à tous ceux qui se fient raisonnablement à l'information contenue dans le certificat que celle-ci est exacte, que le certificat a été accepté par le signataire et que l'autorité de certification respecte les lois existantes. La publication du certificat permet de rassurer les personnes se fiant au certificat, à savoir que ce dernier a été délivré au signataire par une autorité de certification[188].

Dans certaines circonstances, l'autorité de certification peut révoquer un certificat. Elle peut le faire s'il n'a pas été délivré tel que cela était requis[189], à la demande du signataire [190] ou si le signataire décède ou encore que l'entreprise est dissoute[191]. Aussi, l'autorité de certification peut révoquer le certificat si la Division of Corporations and Commercial Code de

182. *Utah Digital Signature Act*, précitée, note 175, § 46-3-305 (1).
183. *Id.*, § 46-3-304 (1). La partie 4 des ABA Guidelines détaille plus amplement les devoirs du signataire, présentés en un endroit séparé pour plus de commodité.
184. ABA Guidelines, précitées, note 151.
185. *Utah Digital Signature Act*, précitée, note 175, § 46-3-301 (1). Pour une comparaison avec les ABA Guidelines, voir les articles 3.1 et 3.2. Un système fiable est défini au paragraphe 46-3-103 (38) comme « computer hardware and software which : (a) are reasonably secure from intrusion and misuse ; (b) provide a reasonable level of availability, reliability, and correct operation ; and (c) are reasonably suited to performing their intended functions ». Ainsi formulée, cette définition est analogue à celle de l'article 1.35 des ABA Guidelines. À titre de comparaison, voir le concept de « commercially reasonable method of providing security » avec celui qui est prévu dans la réglementation entourant les transferts électroniques de fonds : UCC, précité, note 174, articles 4A-202 (b) et (c) ; *Loi type sur les virements internationaux*, précitée, note 94, art. 5.
186. *Utah Digital Signature Act*, précitée, note 175, § 46-3-301 (2).
187. *Id.*, § 46-3-302 (2) (a).
188. *Id.*, § 46-3-303 (4).
189. *Id.*, § 46-3-302 (4) (a) (i).
190. *Id.*, § 46-3-307 (1) (a)
191. *Id.*, § 46-3-307 (3).

l'Utah Department of Commerce (Division) l'ordonne. Cela pourrait se produire dans le cas d'une déllivrance substantiellement non conforme, tenant pour acquis que « the noncompliance poses a significant risk to persons reasonably relying on the certificate[192] ». Finalement, l'autorité de certification peut révoquer le certificat si sa fiabilité est mise en doute, que le signataire consente ou non à la révocation[193].

En d'autres occasions, le certificat doit être suspendu à la demande d'un signataire ou, si la Division l'ordonne, à la suite du non-respect important d'une obligation menant à un risque significatif[194]. Toutefois, l'autorité de certification peut décider de suspendre le certificat afin de mener une enquête en vue de confirmer ou non les raisons de la révocation[195]. Quant à la Division, elle peut, à sa discrétion[196], suspendre un certificat : sur demande de la part d'un signataire si l'autorité de certification n'est pas disponible[197] ; pour obtenir des preuves au sujet de toute information[198] ; et s'il est délivré sans être conforme ou à la suite d'un non-respect important d'une obligation menant à un risque significatif[199].

2.3.3 Responsabilité bancaire

Selon la première prémisse énoncée plus haut, l'état actuel du droit autorise les banques à exploiter des entités offrant des services d'authentification de niveau subalterne[200] ; la seconde prémisse affirme qu'il est souhaitable que les chambres de compensation et les associations bancaires professionnelles agissent à titre d'autorités de certification de niveau supérieur[201]. Cette structure accorde ainsi une certaine sécurité aux parties — le signataire et la personne se fiant à la signature — utilisant les services de certification des banques. Ce sentiment de sécurité est renforcé par les nouveaux cadres juridiques qui gouvernent les activités des autorités de certification. Toutefois, en cas d'une erreur de la part d'une autorité de certification, une des parties faisant affaire avec cette dernière (mandataire) possède-t-elle un recours contre la banque (mandante) ? Qu'en est-il de la possibilité d'un recours contre une autorité de certification supérieure ?

---

192. *Id.*, § 46-3-306 (2) (b) (i) et § 46-3-302 (5) (a).
193. *Id.*, § 46-3-307 (4).
194. *Id.*, § 46-3-306 (1) (a).
195. *Id.*, § 46-3-302 (4) (a) (ii).
196. *Id.*, § 46-3-306 (2) (b) (ii).
197. *Id.*, § 46-3-306 (2) (a).
198. *Id.*, § 46-3-306 (2) (b) (i).
199. *Id.*, § 46-3-302 (5) (a).
200. *Supra*, section 1.3.1.
201. *Supra*, sections 1.3.2 et 1.4.

En droit des sociétés par actions, il est reconnu qu'une société mère ne peut être tenue responsable pour les actes de sa filiale, sous réserve que ceux-ci aient servi à masquer une fraude, un abus de droit ou une contravention à l'ordre public[202]. Inversement, en droit bancaire, une banque est responsable pour les actes de sa succursale, entre autres pour les erreurs de ses dirigeants[203]. Le cas échéant, faut-il conclure qu'une erreur de la part de l'autorité de certification engendre automatiquement la responsabilité de la banque ?

Nous avons énoncé plus haut que, dans le présent contexte, une banque qui exploite une autorité de certification agit selon une relation de mandat[204]. De cette manière, l'article 2160 C.c.Q. prévoit que sa responsabilité sera retenue soit lorsque l'autorité de certification agit dans les limites de son mandat, soit lorsque la banque ratifie les actes de sa mandataire qui excèdent son mandat.

Bien que le rôle d'une autorité de certification diffère de celui d'une succursale bancaire vouée à l'acceptation de dépôts et au prêt d'argent, il importe de noter que, en vertu du projet de loi C-8[205] (modifiant la *Loi sur les banques*)[206], une société mère pourra non seulement détenir un contrôle *de facto* sur une autorité de certification, mais également un contrôle *de jure*[207]. À nos yeux, la théorie du mandat doit donc céder la place aux usages bancaires, malgré que l'effet concret demeure le même, c'est-à-dire que la banque sera responsable lors d'une erreur commise par une autorité de certification agissant sous sa tutelle.

Il ressort de ce premier développement qu'une partie ayant un lien de droit avec l'autorité de certification de niveau inférieur conserve un droit

---

202. Au Québec : art. 317 C.c.Q. Cette disposition codifie le droit existant en la matière : QUÉBEC, *Commentaires du ministre de la Justice. Le Code civil du Québec : un mouvement de société*, t. 2, Sainte-Foy, Les Publications du Québec, 1993, p. 213. Au sujet de cette disposition, voir : M. MARTEL et P. MARTEL, *La compagnie au Québec*, t. I, Montréal, Wilson & Lafleur, 1999, p. 1-62–1-74 ; S. ROUSSEAU, « Immunité des actionnaires et levée du voile corporatif : perspectives de l'analyse économique du droit », (1999) 78 *Can. B. Rev.* 1. En common law : *1005633 Ontario Inc.* c. *Winchester Arms Ltd.*, [2000] O.J. (Quicklaw) nº 2404, par. 89 et 90 (S.C.) ; *Rafiki Properties Ltd.* c. *Integrated Housing Development Ltd.*, [1999] B.C.J. (Quicklaw) nº 243, par. 11 et 17 (B.C. S.C.) ; *Constitution Insurance Co. of Canada et al.* c. *Kosmopoulos et al.*, [1987] 1 R.C.S. 2, (1987) 34 D.L.R.(4th) 208 ; *Canada Life Assurance Co.* c. *Canadian Imperial Bank of Commerce* (1974), 3 O.R. (2nd) 70, 84 et 85, 44 D.L.R. (3rd) 486 (C.A.), demande d'appel à la Cour suprême du Canada refusée : [1974] R.C.S. viii.

203. N. L'HEUREUX et É. FORTIN, *op. cit.*, note 58, nº 1.150, p. 254-256.

204. *Supra*, section 1.3.1.

205. Projet de loi C-8, précité, note 44.

206. *Loi sur les banques*, précitée, note 43.

207. *Supra*, notes 43-46, ainsi que le texte correspondant.

d'action envers la banque — société mère et mandante. L'intensité de l'obligation de la banque à cet égard repose principalement sur l'obligation d'agir avec prudence et diligence, de même qu'avec loyauté[208]. Dans le premier cas, considérons, par analogie, le cas d'une banque qui n'exécute pas les ordres de son client, par exemple lors de transferts de fonds : celle-ci est responsable envers son client pour ne pas avoir agi avec la diligence nécessaire en de telles circonstances, c'est-à-dire d'avoir failli à son obligation de prudence et de diligence[209]. D'ailleurs, les banques sont déjà familiarisées avec les systèmes de sécurité utilisés à des fins précises, notamment pour les cartes de débit[210] ; une banque qui ne respecterait pas cette obligation engendrerait sa responsabilité[211]. Dans le second cas, la raison d'être de l'obligation de loyauté repose sur un « [contrat] [fondé] sur la confiance[212] », ce critère étant le but essentiel recherché — la sécurité — par les parties qui utilisent les services d'une autorité de certification.

Au regard des services de certification de niveau supérieur, offerts par une chambre de compensation ou une association bancaire, quelle est l'intensité de la responsabilité de la banque ?

Dans l'éventualité où la chambre de compensation ne respecte pas ses propres règles, il va de soi qu'elle sera tenue responsable[213]. Le cas échéant,

---

208. Voir généralement : N. L'HEUREUX et É. FORTIN, *op. cit.*, note 58, nos 1.141-1.168, p. 243-282.
209. *Id.*, no 1.147, p. 250 et 251.
210. Le réseau interbancaire Interac garantie une haute sécurité pour ces types de paiements. Voir le portail d'Interac : [http ://www.interac.ca]. La sécurité technique des cartes de débit, assurée par un numéro d'identification personnel (NIP), permet de limiter substantiellement les erreurs et les fraudes ; en fait, les recours judiciaires ont trait généralement à des vols de cartes, et sont habituellement rejetés pour cause de négligence de la part du titulaire, ce dernier ayant soit conservé son NIP sur un morceau de papier, soit utilisé un numéro facile à retenir : *supra*, note 126, ainsi que le texte correspondant.
211. Dans la très célèbre décision *Evra Corp.* c. *Swiss Bank Co.*, 673 F.2d 951 (7th Cir. 1982), une banque a été tenue responsable pour les dommages directs causés par le manque de papier dans son télécopieur, ce qui l'a empêché de recevoir un ordre de paiement. Voir également : *supra*, note 185, ainsi que le texte correspondant. Comme le mentionne à juste titre un auteur, « the banks who design, operate, and supervise the system are in the best position to make the optimal decision about the efficient level of precautions at which the marginal cost of any improvement exceeds the marginal gain in reduced losses » : L. THÉVENOZ, *Error and Fraud in Wholesale Funds Transfers : U.C.C. Article 4A and the UNCITRAL Harmonization Process*, Zürich, Schulthess Polygraphisher Verlag, 1990, p. 50.
212. N. L'HEUREUX et É. FORTIN, *op. cit.*, note 58, no 1.164, p. 271.
213. *Stanley Works of Canada Ltd.* c. *Banque Canadienne Nationale et Banque Royale*, [1982] R.L. 433, (1982) 20 B.L.R. 282 (C.A.) (ci-après avec renvois à la R.L.) ; *Process Piping Specialities Inc.* c. *La Banque Canadienne Nationale du Canada*, [1986] R.J.Q. 2429 (C.S.).

un client pourrait-il invoquer la responsabilité de la banque envers lui ? Cette question nécessite de qualifier la relation entre la banque et la chambre de compensation. Les règles des chambres de compensation prévoient que les relations entre les banques et ces dernières sont contractuelles et non fondées sur une relation de mandat, car les banques sont considérées comme des membres d'une chambre de compensation[214]. D'ailleurs, la jurisprudence et la doctrine opinent que les règles formulées par les réseaux interbancaires font partie implicite du contrat bancaire conclu entre le client et la banque. À cet égard, dans la décision *Stanley Works of Canada Ltd.* c. *Banque Canadienne Nationale et Banque Royale*[215], la Cour d'appel a jugé qu'une banque tirée est responsable envers le tireur d'un chèque si elle ne respecte pas les règles de la chambre de compensation, car elle doit protéger les intérêts de son client[216]. Celui-ci peut donc se fier à la négligence de la chambre de compensation (mandataire) pour tenir la banque (mandante) responsable envers lui-même. De cette manière, les banques ne peuvent éluder leurs responsabilités envers leurs clients.

2.3.4 Stipulation de non-responsabilité

En droit québécois, les articles 1470 et suivants permettent à une personne d'être exonérée de sa responsabilité. Ce concept, interprété de

---

214. *British Eagle International Airlines Ltd.* c. *Compagnie Air France*, [1975] 2 All E.R. 390, 405, [1975] 1 W.L.R. 758 (H.L.) ; R. CRANSTON, *Principles of Banking Law*, Oxford, Clarendon Press, 1997, p. 310. Par exemple, l'article 20.1(b) de l'*Operating Circular n° 4*, précité, note 59, établit clairement qu'une « Reserve Bank does not act as the agent or subagent of another bank or person ». Depuis le 2 janvier 1998, toutes les tentacules de la Réserve fédérale ont adopté une réglementation similaire : FEDERAL RESERVE SYSTEM, *Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire*, 62 F.R. 48166-01, 48169 (1997), [1997] WL 565684 (F.R.). Les autres règles de chambres de compensation se réfèrent à la relation entre elles-mêmes et les participants — ou les membres — comme étant d'ordre contractuel, par exemple : l'article 5 de la *Loi sur la compensation et le règlement des paiements*, L.C. 1996, c. 6, art. 162 ; ACH Rules, précitées, note 51, art. 1.1.

215. *Stanley Works of Canada Ltd.* c. *Banque Canadienne Nationale et Banque Royale*, précité, note 213.

216. *Id.*, 438 : plus précisément, la banque tirée avait débité le compte de son client après le délai de 48 heures — maintenant 24 heures — dont elle disposait pour ce faire et, en conséquence, le chèque a été retourné pour fonds insuffisants, ce qui a créé un préjudice au client. Ce dernier a allégué avec succès que la banque avait été négligente en n'agissant pas dans le délai requis. La Cour a ajouté que la banque ne pouvait se libérer de ce devoir et devait protéger les intérêts de son client. Voir en doctrine : B. CRAWFORD, *op. cit.*, note 74, n° 3203(a), p. 746 ; N. L'HEUREUX et É. FORTIN, *op. cit.*, note 58, n° 1.22, p. 63 et 64 ; J. CHOQUETTE, « Chronique de législation et de jurisprudence », (1982) 60 *R. du B. can.* 746.

manière restrictive il va sans dire[217], s'applique en droit bancaire, que ce soit pour les transactions commerciales ou de consommation[218]. Par exemple, dans la décision *Banque de Nouvelle-Écosse* c. *Angelica-Whitewear Ltd.*, la Cour suprême du Canada a approuvé le point de vue de la Cour d'appel à savoir qu'une clause d'exonération de responsabilité contenue dans une entente entre la banque et son client « ne relèverait pas la [b]anque de l'obligation d'honorer la traite si elle avait connaissance de la fraude de la bénéficiaire du crédit[219] ».

Dans la décision *Les Entreprises Wyknott International Inc.* c. *Banca Commerciale Italiana of Canada*[220], la Cour du Québec a également déclaré qu'une banque ne pouvait limiter sa responsabilité dans le cas d'une fraude d'une traite régie par les *Règles uniformes pour l'encaissement de papier commercial*[221]. En l'espèce, la Cour a jugé que la Banca Commerciale n'avait pas agi avec prudence et diligence et qu'elle avait commis une négligence grossière puisqu'elle ne s'était pas informée si la traite avait été délivrée à temps.

---

217. Au Québec : *Meany* c. *Caisse populaire Ste-Geneviève de Pierrefonds*, [1991] R.R.A. 813 (C.Q.) ; art. 1474, C.c.Q. La common law prévoit qu'une personne ne peut limiter ni exclure sa responsabilité pour dommage matériel lorsqu'elle a agi de manière intentionnelle ou a commis une négligence grossière : *Stanek* c. *National Bank of Detroit*, 430 N.W.2d 819, 821 (Mich. Ct. App. 1988) ; R. HERSBERGEN, « The Bank Customer Relationship under the Louisiana Commercial Law », (1975) 36 *Louisiana L.R.* 29, 48 ; F.H. MILLER et A. HARRELL, *The Law of Modern Payment Systems and Notes*, Oklahoma City, University of Oklahoma University Press, 1985, p. 264.

218. Voir, par exemple, au Québec : *Loi sur la protection du consommateur*, L.R.Q., c. P-40.1, art. 10 ; *Lévesque* c. *Concept santé Nautilus*, [1996] R.R.A. 733 (C.S.) ; *Gosselin* c. *Services de voyages Yves Bordeleau Inc.*, [1990] R.J.Q. 1454 (C.Q.) ; N. L'HEUREUX, *Droit de la consommation*, Cowansville, Éditions Yvon Blais, 2000, n° 42, p. 54-56. En Ontario : *Loi sur la protection du consommateur*, L.R.O. 1990, c. C.31, art. 33.

219. *Banque de Nouvelle-Écosse* c. *Angelica-Whitewear Ltd.*, [1987] 1 R.C.S. 59, 108 et 109, (1987) 36 D.L.R. (4th) 161. Voir de plus : *Morguard Trust Co.* c. *Royal Bank of Canada*, (1988) 60 Alta. L.R. (2nd) 99, 121, [1988] 5 W.W.R. 415 (Q.B.), confirmé par (1989) 71 Alta. L.R. (2nd) 85, 104 A.R. 22 (C.A.). Sur la question de la fraude, voir également les décisions antérieures à l'affaire *Angelica-Whitewear : Stewart Estate* c. *Royal Bank*, [1930] R.C.S. 544, 549, [1930] 4 D.L.R. 694 ; *Levasseur* c. *Banque de Montréal*, [1978] C.S. 1157, 1159.

220. *Les Entreprises Wyknott International Inc.* c. *Banca Commerciale Italiana of Canada*, [1998] R.R.A. 922, REJB 1998-05958 (C.Q.) (ci-après avec renvois au REJB).

221. CCI, *Règles uniformes pour l'encaissement de papier commercial*, Paris, CCI, 1967, Publication CCI, n° 254. Dans cette histoire, Les Entreprises Wyknott International Inc. étaient bénéficiaires d'une traite bancaire d'environ 20 000 $ tirée sur la Banca Populare Commercio y Industria — une banque italienne de Milan. La traite a été déposée par Wyknott à la Banca Commerciale Italiana of Canada, laquelle a ajoutée l'inscription « *endorsement guarantee* ». Ces types de dépôt étaient crédités de manière inhabituelle

Dans une autre décision, *Les fenêtres St-Jean Inc.* c. *Banque Nationale du Canada*[222], Les fenêtres St-Jean Inc. — l'appelante — entretenait une relation d'affaires avec Les industries Unik ltée depuis quelques années. Inquiète de la stabilité financière d'Unik, elle avait demandé une vérification du crédit auprès de la Banque Nationale du Canada. Celle-ci avait formulé un avis favorable, alors que les faits démontraient manifestement qu'Unik était en sérieuse difficulté financière. En dépit d'une clause de non-responsabilité, le juge Baudouin a déclaré que la banque avait agi de manière trop négligente pour être admise à invoquer cette dernière[223].

Il semble que les tribunaux de common law soient plus stricts à l'égard de tels échappatoires juridiques. La Cour du Banc de la Reine de l'Alberta a été aux prises récemment avec une histoire de vérification de crédit, semblable à la situation précédente[224]. À la suite d'une demande de l'appelante, par l'entremise de la Banque de Hong Kong, l'intimée avait transmis des informations au sujet de l'entreprise Woodland Construction Inc., et non Woodland Construction (1994) Inc. En dépit de la similarité des faits, la Cour a écarté l'arrêt *Les fenêtres St-Jean Inc.* sur la base d'un *obiter dictum* du juge Baudouin[225], pour s'appuyer plutôt sur la décision *Hedley*

---

au compte de Wyknott dans un délai de trois à cinq semaines. Après avoir reçu un état de compte bancaire, Wyknott a remarqué que le montant n'avait nullement été crédité. La traite avait été transmise par la Banca Commerciale à la Banca Populare par le truchement d'un courrier enregistré. Des recherches postérieures effectuées par cette dernière ont permis de découvrir que la traite avait été dérobée à la suite de la transmission par la Banca Commerciale et avait été présentée au paiement à la Commercial Bank of Greece à Athènes. Celle-ci n'a jamais reçu un contrordre de paiement et la preuve a démontré que la Banca Commerciale n'avait jamais vérifié si la traite avait été délivrée par la Banca Populare : *id.*, par. 24.

222. *Les fenêtres St-Jean Inc.* c. *Banque Nationale du Canada*, [1990] R.J.Q. 632, (1990) 69 D.L.R. (4th) 384 (C.A.) (traduite en anglais dans les D.L.R. ; ci-après citée : « *Les fenêtres St-Jean Inc.* » avec renvois au R.J.Q.).

223. *Id.*, 637. Voir de plus : *Zidle* c. *Banque de Commerce Canadienne Impériale*, [1983] 1 R.C.S. 654, 655 ; *Banque de Montréal* c. *Manuvie, Compagnie d'assurance-vie Manufacturers*, [1994] R.R.A. 8, 14 (C.A.) ; *Mc Vety* c. *Banque Toronto-Dominion*, [1986] R.R.A. 447, J.E. 86-741 (C.P.) ; *Les Entreprises Wyknott International Inc.* c. *Banca Commerciale Italiana of Canada*, précité, note 220.

224. *Totem Building Supplies Ltd.* c. *Toronto-Dominion Bank*, (1999) 248 A.R. 241 (B.R. (1re inst.)).

225. *Les fenêtres St-Jean Inc.*, précité, note 222, 635 : « Ce précédent de common law canadienne trace des règles analogues, mais non pas nécessairement identiques, à celles qu'il convient d'appliquer à une instance mue au Québec. On doit donc lui reconnaître une incontestable autorité morale. Il ne me paraît pas opportun cependant, pour décider de la responsabilité, de substituer à l'analyse civiliste classique de la responsabilité civile le schéma proposé par la Cour pour déterminer l'existence du « *tort of negligence* » en common law résultant d'une « *negligent misrepresentation* » ».

Byrne & Co. Ltd. c. *Heller & Partners Ltd.*[226] afin de rejeter la réclamation[227].

En fait, l'approche de la common law à l'égard des clauses d'exonération de responsabilité est moins conviviale que celle qui a été adoptée par le droit québécois. En général, bien que ces clauses défient la liberté contractuelle, Fridman rappelle que leur légitimité repose sur trois conditions[228] : d'abord, la partie recherchant la protection doit informer le cocontractant des modalités de cette clause[229] ; ensuite, il y a lieu de considérer l'éventualité qu'une personne ne respecte pas le contrat ; finalement, il est important de déterminer si la portée d'une telle clause englobe l'événement à l'origine du non-respect du contrat. Il semble que ce dernier point diffère plus de la perspective civiliste que les deux premiers. Toujours selon Fridman, l'aspect critique est la violation fondamentale (*fundamental breach*) du contrat. Il existe une telle violation lorsqu'une partie néglige d'exécuter une obligation élémentaire (*primary obligation*), causant ainsi un préjudice à « the other party of substantially the whole benefit which it was the intention of the parties that the other party should obtain from the contract[230] ». Puisque, contrairement au droit québécois, la violation du devoir de prudence et de diligence n'invalide pas une clause exonératoire de responsabilité, comme cela a été exprimé dans l'affaire *Totem Building Supplies Ltd.* c. *Toronto-Dominion Bank*[231], la contravention à un tel devoir ne doit pas être associée aveuglément à une violation fondamentale du contrat.

Un rapide tour d'horizon des sites bancaires virtuels dénote que les banques n'ont point tendance à épouser une approche sympathique à l'égard de leur clientèle, qu'il s'agisse d'entreprises commerciales ou de consommateurs : les exonérations de responsabilité sont rédigées en termes

---

226. *Hedley Byrne & Co. Ltd.* c. *Heller & Partners Ltd.*, [1964] A.C. 465, [1963] 3 W.L.R. 101 (H.L.) (ci-après cité avec renvois aux A.C.). En l'espèce, la Chambre des lords a jugé que, bien qu'une banque se voit imposer un devoir de prudence et de diligence dans l'évaluation de la stabilité financière d'une entreprise, ce devoir n'existait pas vu une clause de non-responsabilité rédigée par la banque : *id.*, 477. Voir de plus : *Commercial Banking Company of Sidney Limited* c. *R. H. Brown & Company*, (1972) 126 C.L.R. 337, 344 et 345 (Austr. H.L.).
227. *Totem Building Supplies Ltd.* c. *Toronto-Dominion Bank*, précité, note 224, 244 et 245.
228. G.H.L. FRIDMAN, *The Law of Contracts in Canada*, Toronto, Carswell, 1999, p. 610.
229. Voir de plus : *Tilden Rent-a-Car Co.* c. *Clendenning*, (1978) 83 D.L.R. (3rd) 400, 18 O.R. (2nd) 601 (C.A.).
230. *Photo Production Ltd.* c. *Securicor Transport Ltd.*, [1980] A.C. 827, 849 [1980] 1 All. E.R. 556 (H.L.).
231. *Totem Building Supplies Ltd.* c. *Toronto-Dominion Bank*, précité, note 224.

vagues et de manière très large[232]. Faut-il conclure qu'une autorité de certification, agissant sous les auspices d'une banque, pourrait décliner sa responsabilité de la sorte ? À nos yeux, il importe de tenir compte des obligations de prudence, de diligence et de loyauté — imposées de manière implicite au contrat bancaire en droit civil québécois —, jumelées à l'état du droit énoncé plus haut au sujet des clauses d'exonération de responsabilité, en vue d'encadrer l'évolution du droit en ce domaine.

2.4 Dommages-intérêts

Les cadres juridiques gouvernant la responsabilité et l'octroi de dommages-intérêts de la part d'une autorité de certification, du signataire et d'une personne qui se fie au certificat diffèrent substantiellement entre eux. Par exemple, les dommages-intérêts indirects ne peuvent être accordés que dans un seul cas, la majorité ne permettant que des dommages-intérêts directs. Les sections suivantes discutent de cette question.

2.4.1 Dommages-intérêts directs

Contrairement aux versions précédentes[233], la *Loi type sur les signatures électroniques*, adoptée en 2001, ne prévoit pas le type de dommages-intérêts qui peuvent être réclamés, laissant aux législations nationales le soin d'en déterminer les balises[234]. À l'instar de la CNUDCI, la Directive 1999/93/CE[235], de même que les versions antérieures de cette directive[236], ne fournissent aucun détail sur le type de dommages-intérêts dont l'autorité de certification peut être tenue responsable, à l'exception d'un plafond équivalant à la valeur de la transaction[237]. La *Loi uniforme sur le commerce électronique* est également silencieuse sur les dommages-intérêts.

---

232. Par exemple, le site de la Banque Nationale du Canada prévoit qu'elle-même, « ses filiales et ses sociétés affiliées dégagent leur responsabilité de tous dommages que vous pourriez subir découlant de l'échange de renseignements avec elles » : BANQUE NATIONALE DU CANADA, *Avis important à tous les utilisateurs du site Internet de la Banque Nationale du Canada*, [En ligne], 1998, Montréal, [http ://www.bnc.ca/index.html]. À la Banque de Montréal, la clause de non-responsabilité est similaire. « La Banque de Montréal, et ses filiales et sociétés affiliées, ne sont pas responsables de quelque manière que ce soit, des dommages directs, indirects, spéciaux ou consécutifs, ou pour quelque raison que ce soit, découlant de l'utilisation du présent site Web » : BANQUE DE MONTRÉAL, *Avis importants à tous les utilisateurs de ce site web*, [En ligne], 2000, Montréal, [http :// www.bmo.com/francais/legal/index.html].
233. Par exemple : Projet de règles uniformes, précité, note 89.
234. *Loi type sur les signatures électroniques*, précitée, note 92.
235. Directive 1999/93/CE, précitée, note 106.
236. *Supra*, note 105.
237. Art. 6 (4), al. 2.

Aux États-Unis, alors que les ABA Guidelines[238] demeurent discrètes sur la question des dommages-intérêts, l'*Utah Digital Signature Act* prévoit que le signataire doit indemniser l'autorité de certification pour toute perte ou tout dommage qui découle soit de la délivrance ou de la publication d'un faux certificat, soit du défaut de divulguer un fait matériel, peu importe qu'il survienne intentionnellement ou négligemment[239]. L'autorité de certification n'est aucunement responsable si la perte est liée à une fausse signature digitale, à condition que le signataire se soit conformé aux exigences requises[240]. De plus, le montant des dommages est plafonné, à l'image de la Directive 1999/93/CE[241]. Dans tous ces cas, l'autorité de certification sera responsable si elle a renoncé à l'application de l'article 46-6-309 (2). De même, elle n'est responsable que pour les dommages-intérêts directs et compensatoires[242].

À l'inverse de l'*Utah Digital Signature Act*[243], la *Loi sur les technologies de l'information*[244] est laconique quant à l'octroi de dommages-intérêts. Comme nous l'avons souligné plus haut, l'article 62 de cette loi ne prévoit pour le prestataire de services de certification, le titulaire visé par le certificat et la personne qui se fie au certificat que l'obligation de réparer un préjudice découlant de « l'inexactitude ou de l'invalidité du certificat ou d'un renseignement contenu au répertoire », et ajoute que cette obligation est conjointe dans certains cas[245].

---

238. ABA Guidelines, précitées, note 151.
239. *Utah Digital Signature Act*, précitée, note 175, §§ 46-3-304 (4) (a) et (b).
240. *Id.*, § 46-3-309 (2) (a).
241. *Id.*, § 46-3-309 (2) (b). La limite est le montant prévu dans le certificat, la loi ne déterminant aucune somme précise. Les dommages peuvent résulter d'une erreur ou d'un faux certificat à la suite de la non-conformité par l'autorité de certification ou d'une omission de publier un certificat valide, par exemple ; ils peuvent prendre la forme de dommages-intérêts compensatoires — perte de profits —, punitifs, et pour trouble et inconvénients.
242. *Utah Digital Signature Act*, précitée, note 175, § 46-3-309 (2) (c).
243. *Ibid.*
244. *Loi sur les technologies de l'information*, précitée, note 130.
245. Notamment, lorsque plus d'une de ces personnes — le prestataire de services de certification, le titulaire visé par le certificat et la personne qui se fie au certificat — est responsable, l'obligation est conjointe ; si leur part de responsabilité ne peut être déterminée, l'obligation est répartie en parts égales. Également, « en l'absence de faute de la part de toutes ces personnes, elles assument la réparation du préjudice conjointement et à parts égales ».

2.4.2 Dommages-intérêts indirects

Comme nous l'avons mentionné à la section 2.4.1, la *Loi type sur les signatures électroniques*[246], les ABA Guidelines[247] et la *Loi uniforme sur le commerce électronique*[248] ne traitent pas de la question des dommages-intérêts. Seule l'*Utah Digital Signature Act* prévoit explicitement l'exclusion des dommages-intérêts indirects — dommages punitifs ou exemplaires, pertes potentiellement subies ou gains potentiellement privés, ainsi que troubles et inconvénients — du champ de responsabilité de l'autorité de certification[249]. Nous croyons que les dommages-intérêts indirects devraient

---

246. *Loi type sur les signatures électroniques*, précitée, note 92. Toutefois, il est intéressant de noter qu'une version antérieure de la CNUDCI permettait d'attribuer des dommages-intérêts indirects. Le Projet de règles uniformes, précité, note 89, était considéré comme très libéral en la matière. Au regard de l'autorité de certification, la variante X de l'article 10 (5), moulée sur l'article 74 de la *Convention des Nations Unies sur le contrat de vente internationale de marchandises*, U.N. Doc. A/CONF.97/18, Vienne, 11 avril 1980, dans *Annuaire de la Commission des Nations Unies sur le droit commercial international*, t. XI, 1980, Annexe I-B, p. 161 (ci-après cité : « CIVM »), prévoyait une règle de prévisibilité du préjudice, ce qui inclut les dommages indirects. À ce sujet, voir notamment : *Handelsgericht des Kantons Zürich*, HG950347 (5 février 1997), sommaire publié dans le Recueil de Jurisprudence concernant les Textes de la CNUDCI (ci-après cité : « CLOUT »), cause n° 214, [En ligne], 2000, Vienne (Autriche), [http ://www.uncitral.org/fr-index.htm], et en allemand dans : [1998] 1 *Schweizerische Zeitschrift für Internationales und Europäisches Recht* 75 ; *Delchi Carrier, SpA* c. *Rotorex Corporation*, [1994] WL (Westlaw) 495787, 5 (N.D.N.Y.) ; K.H. NEUMAYER et C. MING, *Convention de Vienne sur les contrats de vente internationale de marchandises : commentaire*, Lausanne, CEDIDAC, 1993, 486 ; V. HEUZÉ, *La vente internationale de marchandises : droit uniforme*, Paris, GLN Joly, 1992, n° 486, p. 329 ; J.S. SUTTON, « Measuring Damages under the United Nations Convention on the International Sale of Goods », (1989) 50 *Ohio St. L.J.* 737, 743 et 744. Comme le souligne Sutton, le commentaire officiel de l'article 70 (art. 74, CIVM) du *Projet de convention sur la formation des contrats relatifs à la vente internationale d'objets mobiliers corporels*, U.N. Doc. A/CONF.97/5 (1979), mentionne que la règle concerne « the injured party in the same economic position he would have been in if the contract had been performed » : *id.*, 743 ; E.A. FARNSWORTH, « Damages and Specific Relief », (1979) 27 *Am. J. Comp. L.* 247, 249. Finalement, le fardeau repose sur les épaules du requérant, ce qui risque de devenir une entreprise ardue : V. HEUZÉ, *op. cit.*, n° 486, p. 329 ; *Handelsgericht des Kantons Zürich*, précitée, *Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry*, Sentence arbitrale n° 155/1994 du 16 mars 1995, sommaire publié dans CLOUT, précitée, cause n° 140, [En ligne], [http ://www.uncitral.org/fr-index.htm] ; *Schiedsgericht der Handelskammer Hamburg* (21 mars 1996), sommaire publié dans CLOUT, cause n° 166, [En ligne], [http ://www.uncitral.org/fr-index.htm], et en allemand : [1996] N.J.W. 3229.

247. ABA Guidelines, précitées, note 151.

248. *Loi uniforme sur le commerce électronique*, précitée, note 118.

249. *Utah Digital Signature Act*, précitée, note 175, § 46-3-309 (2) (c).

être accordés seulement s'ils sont stipulés au contrat, comme le prévoit par exemple l'article 4A-305 (c) du UCC, et ce, contrairement à la règle établie par la décision britannique *Hadley* c. *Baxendale*[250].

Conclusion

Depuis quelques années, les banques peuvent offrir des services d'autorités de certification, considérés comme un prolongement du concept d'opération bancaire. De telles initiatives favorisent, certes, l'épanouissement du commerce électronique. Cet engouement implique cependant quelques répercussions importantes.

Il est souhaitable d'établir une hiérarchie pyramidale d'autorités de certification, le niveau inférieur étant régi par un niveau supérieur, ce dernier étant à son tour gouverné par une autorité de certification principale. Une telle hiérarchie est, à nos yeux, nécessaire pour créer un état d'esprit sécuritaire chez le signataire et la personne se fiant à la signature. Toutefois, ce sentiment de sécurité doit être accompagné d'un cadre juridique reflétant une protection accrue tant des usagers que de l'autorité de certification. D'ailleurs, le Commentaire n° 3.14.1 des ABA Guidelines[251] précise que « [t]he role of a certification authority is developing, and few will enter this uncharted area of business without first having the basic rules established with sufficient clarity to enable an evaluation of the legal risks of the new business ».

Les récents développements juridiques en matière de signatures électroniques accordent une telle garantie. Par exemple, il convient de noter que, lors de la délivrance d'un certificat, le prestataire de services de certification doit utiliser un système fiable, fournir des garanties d'intégrité du certificat, s'assurer de la confidentialité des clés, de même que fournir l'accès au répertoire, à défaut de devoir répondre des conséquences de ses actes à l'égard des usagers.

---

250. *Hadley* c. *Baxendale*, (1854), 9 Ex. 341, 156 E.R. 145, 151. Au milieu du XIX^e siècle, cet arrêt de principe a admis la règle de prévisibilité des dommages-intérêts, à condition d'équivaloir à ce que les parties auraient prévu au moment de la conclusion du contrat. Au surplus, la Cour a ajouté que « in the great multitude of cases of millers sending off broken shafts to third persons by a carrier under ordinary circumstances, such consequences (the stoppage of the mill and resulting loss of profits) would not, in all probability, have occurred ; and these special circumstances were never communicated by the plaintiffs to the defendants ».

251. ABA Guidelines, précitées, note 151.

Malgré l'émergence d'un environnement juridique destiné à protéger les acteurs pivotant autour de la certification électronique, les banques sont susceptibles de se dérober de leurs responsabilités à travers les méandres juridiques. Il importe donc, d'une part, que les banques répondent des actes d'une autorité de certification agissant sous leur tutelle, et d'autre part, de circonscrire la portée des clauses exonératoires de responsabilité. De cette manière, la confiance des usagers envers le réseau Internet sur le plan bancaire — et le commerce électronique en général — sera rehaussée.