La multiplicité des normes encadrant le contrat électronique : l'influence de la technologie sur la production de normes

Éric LABBÉ

Le contrat électronique

Conférence organisée par le Programme international de cooperation scientifique (CRDP / CECOJI), Montréal, 19 décembre 2003

Introduction

Par ses vertus simplificatrices, le commerce électronique fait figure de progrès : il facilite l'accès à l'information commerciale, la vente de biens et services, leur paiement ainsi que bien d'autres fonctionnalités. Ces vertus ne signifient pas, cependant, que l'établissement des engrenages économiques, juridiques et techniques nécessaires au développement du commerce électronique soit évident. La simplification de la vie humaine par la technique pose souvent une multitude de conditions. L'utilisation usuelle de l'automobile en fournit une illustration convaincante : celle-ci requérait non seulement la réalisation technique d'un véhicule à moteur, mais aussi un réseau routier adapté, un code de la route, un mode approprié de distribution de l'essence et bien d'autres conditions qui dépendaient de la technique ou encore des besoins que cette innovation faisait naître au gré des différentes sociétés.

Le développement du commerce électronique n'est pas étranger à ce type d'exigences. La possibilité de conclure des contrats sur le support électronique a, par exemple, posé plusieurs interrogations concernant l'identification des parties, la manifestation de leur

consentement, la preuve de leur entente et la responsabilité des intermédiaires techniques. Il devenait nécessaire de définir les bases sur lesquelles reposeraient les nouveaux rapports contractuels.

En réponse, nous connaissons désormais une architecture technique et juridique des contrats électroniques dont l'objet consiste essentiellement à établir leur sécurité et à circonscrire leur valeur probatoire. En marge de cette architecture où s'entrecroisent normes techniques et juridiques, se trouve toutefois une pratique contractuelle qui correspond peu à ces exigences. Comment alors expliquer que l'architecture techno-juridique qui caractérise le contrat électronique ne trouve pas ses fondements dans la pratique contractuelle la plus répandue ? Ce décalage témoigne certainement du caractère prospectif de la construction techno-juridique du contrat électronique, mais pourrait également révéler l'influence prédominante de certaines technologies dans l'élaboration de cette architecture. C'est du moins l'hypothèse que nous envisagerons après avoir dressé le portrait de la multiplicité hétérogène et concurrentielle caractérisant actuellement les normes encadrant le contrat électronique.

A. Les normes techniques, contractuelles et législatives : portrait d'une multiplicité hétérogène et concurrentielle

La multiplicité des normes encadrant le contrat électronique est d'abord synonyme d'hétérogénéité : des normes techniques, contractuelles et législatives viennent définir les ententes réalisées par le biais de ce support technologique.

Les **normes techniques** ont principalement pour fonction d'assurer l'intégrité matérielle du contrat électronique, de manière à éviter son éventuelle altération, et de garantir l'identité des parties qui, souvent dans ce cas, contractent à distance. Une fonction de confidentialité peut être recherchée lorsque l'entente s'effectue sur un réseau ouvert comme Internet, plus facilement soumis au risque de l'interception.

Suivant la poursuite de ces différentes fonctions, les normes techniques consistent généralement à consacrer un dispositif particulier[1] (de signature et/ou d'intégrité, comme

[1] On peut envisager qu'une entreprise ou encore une institution étatique oblige ses partenaires à recourir à une technologie de signature particulière pour toute entente conclue ou communication passée avec elle sur

une clé privée PGP[2]), à établir un protocole de communication sécurisé (comme le protocole SSL[3]) ou encore à définir les caractéristiques d'un certificat numérique produit par un tiers pour attester de l'identité d'une partie et du lien qui l'unit à un procédé d'identification donné (la norme X.509[4] par exemple). Les règles qui régissent l'accès à un répertoire de certification, la validité des certificats ainsi que les procédures d'enregistrement et d'identification nécessaires à l'obtention d'un certificat viennent ensuite parfaire le processus technique de « sécurisation » du contrat électronique. Ces règles sont généralement déterminées par le certificateur et figurent en détail dans sa politique de certification[5].

Les normes techniques encadrant les contrats électroniques sont entre elles gouvernées par les principes d'interopérabilité et d'efficacité. Leur élaboration doit prendre en compte non seulement l'environnement technique dans lequel elles s'inscrivent, mais

---

le support électronique. Par exemple, une directive administrative du gouvernement du Québec révèle que les transactions électroniques et l'échange d'information sensible en milieu gouvernemental (phase intérimaire) ou avec l'appareil étatique québécois (seconde phase) seront effectuées grâce à l'utilisation de la cryptographie asymétrique, mettant ainsi en œuvre la décision de 1999 du Conseil du Trésor de doter le gouvernement du Québec d'une infrastructure à clés publiques gouvernementale (ICPG). En outre, ce document précise que les clés privées de chiffrement devront correspondre à des *Spécifications techniques pour l'infrastructure à clés publiques gouvernementale*, qui seront déterminées par le Conseil du Trésor en tant que gestionnaire des encadrements administratifs et technique (GEAT). CONSEIL DU TRÉSOR, *Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire*, mars 2004, en ligne : http://www.autoroute.gouv.qc.ca/publica/pdf/Directive_sur_les_services_de_certification.pdf.

[2] Créé par Phil Zimmermann, PGP est un logiciel de chiffrement qui utilise la cryptographie asymétrique et dont l'acronyme signifie *Pretty Good Privacy*. PGP est aujourd'hui considéré comme le standard *de facto* pour le cryptage des courriers électroniques.

[3] Le protocole SSL, pour *Secure Sockets Layers*, est un procédé de sécurisation des communications Internet qui repose sur un procédé de cryptographie asymétrique. Intégré dans les principaux logiciels de navigation et assurant principalement la confidentialité des communications, son utilisation est largement répandue en matière de transactions bancaires, de paiement électronique et d'accès personnalisés (courrier électronique sur interface Web, communications de données personnelles avec l'État (impôt sur le revenu, par exemple), etc.). En d'autres termes, SSL est aujourd'hui une norme technique de fait pratiquement incontournable.

[4] La norme X.509, depuis longtemps en usage, définit le contenu et la forme de certificats de clés publiques. Selon ce standard ISO, les certificats X.509 doivent être infalsifiables et sont en conséquence signés par un clé privée (normalement celle du certificateur) intégrant une fonction de hachage, ce qui permet ultérieurement de vérifier l'intégrité du certificat. En plus d'être une norme ISO et de faire l'objet d'une recommandation de l'Union internationale des télécommunications (UIT), X.509 est aujourd'hui une norme de fait très largement répandue, notamment en matière de certification de clefs publiques utilisées pour l'identification de sites Internet.

[5] Par exemple, l'entreprise américaine Entrust précise la plupart de ces considérations dans son *Énoncé de pratiques de certification pour serveurs Web SSL* de novembre 2003, en ligne : http://www.entrust.net/about/practices.cfm.

également les dispositifs et autres normes techniques susceptibles d'affecter leur fonctionnement et leur essor. Les mécanismes et normes techniques qui ne suivent pas l'état de la pratique et les standards actuels risquent au contraire la marginalisation et l'obsolescence[6]. Sur le support classique, un stylobille dont l'encre ne peut être posée que sur un papier particulier ou encore un papier qui n'accepte qu'un seul type d'encre pourraient par exemple être rapidement exclus. Il en va ainsi, sur le support électronique, des dispositifs de signature, des certificats, des répertoires et de la certification proprement dite. L'envergure de leur déploiement dépend largement des efforts de compatibilité accomplis par tous les acteurs offrant un service technique relatif à l'une ou l'autre de ces fonctions. L'architecture technique du contrat électronique est dans ce sens fortement transitive et normative.

La nature des normes techniques du contrat électronique est plurielle. Il peut s'agir de normes de fait, qui ont vu le jour grâce à un monopole économique (pensons à l'hégémonie Microsoft et à son système d'exploitation) ou à l'efficacité d'une technique particulière (cryptographie asymétrique par exemple), ou encore de normes issues d'un organisme de normalisation, regroupant par exemple des acteurs de l'industrie (l'ISO), des représentants nationaux intéressés (comme l'UIT) ou des spécialistes mandatés par l'État. La reprise de ces normes par le droit est fréquente et peut servir plusieurs objectifs : encourager l'interopérabilité[7], faciliter la preuve des contrats électroniques (notamment à l'aide d'une présomption de fiabilité[8]), déterminer la responsabilité des acteurs qui ne respectent pas certains standards techniques, etc.

---

[6] Nous pensons notamment, dans un domaine connexe au contrat électronique, à toutes les initiatives de paiement électronique qui ont été écartées pour avoir négligé le moyen de paiement qui était alors le plus répandu, et qui le demeure, c'est-à-dire les cartes bancaires et de crédit.

[7] Il s'agit d'ailleurs de l'un des principaux objectifs de la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1 : « *La présente loi a pour objet d'assurer* […] *la concertation en vue de l'harmonisation des systèmes, des normes et des standards techniques permettant la communication au moyen de documents technologiques et l'interopérabilité des supports et des technologies de l'information* » (article 1-5º). Particulièrement, cette mission devra être assurée, selon l'article 64-1º, par un comité multidisciplinaire créé par la loi.

[8] Nous pensons principalement à la présomption de fiabilité de l'article 1316-4 du *Code civil* français, tel qu'ajouté par l'article 4 de la *Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, J.O. Numéro 62 du 14 Mars 2000, page 3968. Pour bénéficier de cette présomption, les technologies de signatures électroniques devront avoir été évaluées et certifiées conformément au *Décret no 2001-272 du 30 mars 2001 pris pour l'application de*

Les **normes contractuelles** dont l'objet consiste à encadrer un contrat électronique, et non simplement à fixer les modalités de ses obligations principales, visent essentiellement à assurer une certaine sécurité juridique, rendue nécessaire par l'aspect technologique du contrat. La sécurité juridique comporte, sous cette normativité contractuelle, trois aspects principaux que sont : la formation du contrat électronique, sa force probante et la responsabilité relative à l'utilisation des dispositifs servant à conclure l'entente.

Les normes contractuelles relatives à la formation du contrat électronique visent à établir le mode technique d'expression de consentement des parties, de manière à éviter les aléas juridiques que le caractère technologique du contrat est susceptible de générer. Lorsqu'aucune relation durable n'existe entre les parties, comme c'est souvent le cas sur Internet, les modes techniques d'expression du consentement visés par le contrat consistent généralement en la transmission d'une confirmation électronique par l'une des parties, l'utilisation d'une ressource donnée ou encore le simple fait de cliquer sur un élément technique. Les clauses contractuelles suivantes illustrent ces pratiques :

- Transmission d'une confirmation : « *Il n'existera de contrat de vente entre vous et Amazon.fr qu'à compter de l'acceptation de votre commande par Amazon.fr. Cette acceptation sera réputée complète et sera réputée vous avoir été effectivement communiquée au moment de l'envoi par Amazon.fr d'un e-mail confirmant que votre produit vous a été expédié* »[9];
- Utilisation d'un site Web : « *Chaque fois que vous utilisez le site Web, vous signifiez que vous acceptez, sans limitation ou réserve, d'être lié par la présente convention* » (Future Shop)[10];
- Clic : « *Quand vous cliquez sur le bouton "Valider" après le processus de commande, vous déclarez accepter celle-ci ainsi que l'intégralité des présentes Conditions Générales de Vente pleinement et sans réserve* » (Surcouf)[11].

---

l'article 1316-4 du code civil et relatif à la signature électronique, J.O. Numéro 77 du 31 mars 2001, p. 5070 et au *Décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information*, J.O. Numéro 92 du 19 avril 2002, p. 6944.

[9] *Informations légales de Amazon.fr sur la formation du contrat de vente* : http://www.amazon.fr/exec/obidos/tg/browse/-/548526/171-4682667-4241041.

[10] *Convention relative à l'utilisation du site web de Future Shop*, novembre 2003 : http://www.futureshop.ca/informationcentre/fr /useagreement.asp?logon=&langid=FR&dept=0&WLBS=fsweb7.

[11] *Conditions générales de vente de Surcouf* : http://www.surcouf.com/institutionnel/cgv.asp.

Si ces modes techniques d'expression du consentement sont largement utilisés dans la pratique contractuelle, elles ne font pas toujours l'unanimité : le fait que plusieurs clauses ne soient pas portées à l'attention du destinataire et, plus généralement, l'absence d'un certain formalisme, pourraient entacher leur validité[12]. Cette observation est toutefois sans fondement lorsqu'une relation de longue durée est projetée et qu'un contrat-cadre circonscrit le mode de formation des contrats sous-jacents[13], suivant l'exemple d'un contrat EDI. Dans ce cas, l'importance de la relation amène généralement les parties à formaliser leur entente principale par une signature manuscrite.

Le désir de garantir la valeur probante du contrat électronique fait aussi l'objet de certaines dispositions contractuelles. Ce besoin trouve sa rationalité dans le souci d'éviter que le caractère technologique du contrat empêche ou rende difficile sa mise en preuve devant un tribunal et ne prévienne ainsi son exécution légitime. Les parties peuvent en ce sens convenir que l'imprimé de leurs communications électroniques transmises par un processus sécuritaire pré-déterminé a pour eux la qualité d'un écrit original sur support papier[14]. Si ce type de clause caractérise les contrats-cadres du type EDI, il figure rarement au sein d'ententes plus ponctuelles, dont la valeur est souvent moins importante. En outre, des dispositions d'ordre public risquent d'annuler ce type d'arrangement probatoire, notamment lorsque le législateur exige des formalités particulières (un document papier notamment) pour la conclusion de certains contrats[15].

---

[12] Sur cette question, voir Vincent GAUTRAIS, « La couleur du consentement électronique », (2003) 16, 1 *Les Cahiers de propriété intellectuelle* 61.

[13] Par exemple : « Le contrat sous-jacent est supposé être conclu lors de la réception de l'accusé de réception par l'expéditeur de la confirmation de l'ordre d'opération ». Clause tirée du contrat-type rédigé par Vincent GAUTRAIS et Karim BENYEKHLEF, *Contrat de communication électronique de longue durée entre commerçants utilisant un « réseau ouvert »*, dans Daniel POULIN, Éric LABBÉ, François JACQUOT et Jean-François BOURQUE, *Guide juridique du commerçant électronique*, Montréal, Thémis, 2003, à la page 359. La précédente version de ce contrat concernait, par ailleurs, l'échange de documents informatisés (EDI).

[14] Par exemple : « *La Partie A et la Partie B reconnaissent également la qualité d'écrit original aux documents électroniques imprimés, comme s'il s'agissait de documents sur support papier, dès lors qu'ils répondent à un processus de transfert sécuritaire* ». *Id.*

[15] À titre d'illustrations, le législateur québécois exige le support papier pour certains contrats de courtage immobilier ou contrats de consommation, notamment en matière de crédit ou de vente itinérante. Article 34 de la *Loi sur le courtage immobilier*, L.R.Q., chapitre C-73.1 et article 25 de la *Loi sur la protection du consommateur*, L.R.Q., chapitre P-40.1, tels que modifiés respectivement par les article 99 et 101 de la *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 7.

L'utilisation de procédés techniques d'expression du consentement, de signature électronique, de certification et, plus largement, d'outils techniques proprement dits, constitue une autre singularité que la pratique contractuelle a souhaité circonscrire. L'inefficacité ponctuelle des dispositifs techniques ainsi que les possibles bris de sécurité représentent non seulement un risque pour la sécurité des contrats électroniques, mais également un facteur pouvant engager la responsabilité des acteurs techniques. Ces derniers ont en conséquence préféré limiter ou exclure contractuellement leur responsabilité relative à l'utilisation des technologies dont ils sont les instigateurs : logiciels clients/serveurs pouvant recourir au protocole SSL[16], dispositifs de signature électronique[17], certificats numériques[18] et répertoires font tous l'objet d'une protection juridique contractuelle contre d'éventuelles défaillances.

Telles que figurées par la pratique, les normes contractuelles encadrant le contrat électronique constituent une normativité intransitive et personnalisable : si leur contenu est lié aux besoins spécifiques des différentes relations du commerce électronique, il dépend également du choix plus ou moins réfléchi des acteurs et de la liberté de négociation qui leur est effectivement laissée au sein de la relation contractuelle. Cette liberté peu d'ailleurs être circonscrite par l'ordre juridique applicable au contrat, ce qui

---

[16] La clause d' « Exclusion de responsabilité pour les dommages accessoires, indirects et certains autres types de dommages » de la licence du logiciel Internet Explorer en fournit une illustration : « *Dans toute la mesure permise par la réglementation applicable, Microsoft ou ses fournisseurs ne pourront en aucun cas être tenus responsables de tout dommage direct, spécial, accessoire, incident, punitif ou indirect de quelque nature que ce soit (notamment, les pertes de bénéfices, pertes d'informations confidentielles ou autres informations, interruptions d'activité, préjudices corporels, atteintes à la vie privée, manquement à toute obligation (y compris l'obligation de bonne foi et de diligence) pour des actes de négligence, et pour toute perte pécuniaire ou autre), résultant de, ou lié à l'utilisation ou à l'impossibilité d'utiliser le produit, à la fourniture ou au défaut de fourniture des services d'assistance* […] ». Nous soulignons. Tiré du C*ontrat de licence utilisateur final supplémentaire pour logiciel Microsoft (« CLUF supplémentaire »)*, Microsoft Corporation, pour le logiciel IE6 SERVICE PACK 1.

[17] La licence du logiciel PGP 8.0.3 contient une clause d'exclusion de responsabilité similaire à celle qui prévaut chez Microsoft (voir note 16). Il est précisé que le fabricant ne garantit aucunement que le logiciel PGP est insensible aux défaillances, qu'il ne comporte pas d'erreur ou qu'il n'est pas sujet à des interruptions ou à d'autres types d'échec. *PGP Corporation End User License Agreement*, en ligne : http://www.pgp.com/products/freeware.html.

[18] Par exemple, le certificateur américain Entrust n'offre pas de garantie relative à la non-répudiation d'un de ses certificats ou d'une transaction facilitée par leur utilisation. *The Entrust SSL Web Server Certification Practice Statement (CPS)*, art. 2.2.1.1, en ligne : www.entrust.net/cps.

signifie que la normativité contractuelle demeure néanmoins juridiquement transitive, puisqu'elle demeure sujette aux règles dites d'ordre public.

Les **normes législatives** relatives au contrat électronique visent essentiellement à offrir un cadre juridique uniforme concernant les signatures électroniques, la valeur probante des documents technologiques et la responsabilité des acteurs jouant un rôle dans l'architecture technique du contrat électronique[19]. S'agissant sensiblement des mêmes objectifs que ceux poursuivis par les normes contractuelles, il apparaît étonnant de constater que les normes législatives encadrant le contrat électronique ont peu de parenté avec ce qui constitue aujourd'hui la pratique contractuelle du commerce électronique sur Internet. Le contenu législatif actuel semble plutôt se faire l'écho d'une architecture technique qui, bien qu'existante et fonctionnelle, est rarement utilisée pour la conclusion de contrats électroniques. En effet, fondé sur de pointilleux critères de sécurité, dont la non répudiation[20] et l'inaltérabilité[21], le réseau de normes techniques dont nous avons discuté précédemment caractérise assez mal la finalité contractuelle. Entre autres, peu de personnes, dont les consommateurs, disposent d'un procédé de signature électronique :

---

[19] Au Québec, la *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 7, contient l'essentiel de ce cadre juridique uniforme. En France, les normes spécifiques au contrat électroniques résultent de la *Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, précitée, note 8, qui transpose la *Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques*, JO L 13/12 du 19 janvier 2000.

[20] En France par exemple, la présomption de fiabilité d'un procédé de signature électronique requiert des conditions techniques qui sous-entendent la non répudiation. D'une part, les procédés visés par cette présomption doivent « [g]*arantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique : a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ; b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ; c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers* ». D'autre part, ils ne doivent « […] *entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer* ». *Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique*, J.O. Numéro 77 du 31 mars 2001, p. 5070, art. 3-I.

[21] Au Québec par exemple, l'inaltérabilité fait l'objet du critère d'intégrité des documents technologiques, qui est la condition *sine qua non* de leur valeur juridique (*Loi concernant le cadre juridique des technologies de l'information*, précitée, note 7, art. 5). Ce critère d'intégrité est défini par l'article 6, qui précise notamment que « [l]*'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue* ». La loi précise également que : « [l]*e document dont le support ou la technologie ne permettent ni d'affirmer, ni de dénier que l'intégrité en est assurée peut, selon les circonstances, être admis à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve, comme prévu à l'article 2865 du Code civil* » (art. 5). La condition d'intégrité du document est ainsi dépendante de la preuve de son inaltérabilité.

les entreprises en ligne n'exigent aucune signature (pensons aux clauses sur le consentement) et seul un dispositif de paiement, habituellement une carte bancaire, permet une vérification très relative de l'identité de l'acheteur réel[22]. Quant à la certification, elle ne concerne jamais que l'identification du site Internet du vendeur. Le contrat ainsi formé n'est jamais signé électroniquement au sens des critères juridiques retenus et ses éléments de preuve, bien que présentables devant un tribunal[23], sont loin d'assurer le niveau d'intégrité envisagé par les législateurs en matière de contrat électronique : par exemple, la confirmation de la commande transmise par le vendeur (notamment par courrier électronique) peut aisément être modifiée. En d'autres termes, l'architecture technique généralement utilisée relève davantage de la confidentialité des informations transmises lors de la conclusion de l'entente (protocole SSL notamment) et non de l'inaltérabilité ou de la non répudiation des communications électroniques ayant servi à la formation du contrat.

L'inadéquation de la pratique contractuelle du commerce électronique sur Internet avec l'architecture technique et juridique du contrat électronique est plutôt déconcertante. Synonyme d'hétérogénéité, la multiplicité des normes encadrant le contrat électronique présente des allures de concurrence virtuellement incompatible avec les objectifs de confiance et de sécurité visés par l'œuvre législative en cette matière. Celle-ci apparaît dès lors comme un tout normatif prospectif, qui tend plus à encadrer la pratique d'un avenir plus ou moins proche qu'à circonscrire celle d'aujourd'hui, vraisemblablement considérée comme immature et transitoire. Conçue ainsi en marge de l'expérience actuelle du commerce électronique, l'œuvre législative qui régit le contrat électronique trouve forcément ses rationalités ailleurs, dans une réalité d'anticipation, qui laisse à l'esprit une part créatrice plus importante. Se pose dès lors la question de son origine :

---

[22] Notons cependant que certains mécanismes, comme *Address Verification Service* (AVS) ou *Verified by Visa* (VbV), permettent de diminuer les risques de fraudes. AVS est service optionnel offert aux commerçants et a pour utilité de comparer l'adresse du détenteur de la carte avec celle transmise par son utilisateur. Lorsqu'il n'y a pas de correspondance, le commerçant peut décider de ne pas autoriser la transaction. Plus récent, le service VbV nécessite que le titulaire de la carte associe un mot de passe confidentiel à son numéro de carte bancaire lorsqu'il effectue un achat sur Internet. Le commerçant participant à ce système évite dès lors la possibilité que le paiement soit répudié (voir le site dédié à ce système : https://usa.visa.com/personal/secure_with_visa/verified_by_visa.html).

[23] Possiblement en tant que commencement de preuve, selon l'article 5 de la *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 7.

quels sont les facteurs qui ont contribué à construire un cadre réglementaire dont le contenu doit davantage à la projection qu'à la réaction ?

B. Les normes techno-juridiques du contrat électronique : l'origine de l'œuvre prospective du législateur

Mélange étonnant d'objectifs simplificateurs, comme la sécurité[24] et la confiance[25], et de dispositions d'une grande technicité[26], le contenu du cadre réglementaire du contrat électronique est tiré d'au moins deux sources : la technique elle-même et les besoins des acteurs, tels que manifestés par eux ou supposés par les décideurs. Mais à quelle source doit-on la part du lion? La technique est-elle plus déterminante que les besoins formalisés par la loi ou ces derniers sont-ils, au contraire, les instigateurs des critères techniques établis par le législateur ? La réponse à cette interrogation dépend largement du postulat épistémologique à partir duquel on conçoit la relation entre la technique et l'Homme. S'agit-il du déterminisme technique, pour lequel la technique constitue une réalité autonome qui détermine les choix sociétaux[27], ou plutôt d'un déterminisme cartésien[28],

---

[24] La sécurité constitue le premier objectif de la *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 7, art. 1 : « *La présente loi a pour objet d'assurer : 1 º la sécurité juridique des communications effectuées par les personnes, les associations, les sociétés ou l'État au moyen de documents quels qu'en soient les supports* ».

[25] Lors de son allocution au moment de l'adoption de la *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 7, la Ministre Diane Lemieux a souligné maintes fois l'objectif de confiance poursuivi par le nouveau texte et a conclut que « [l]*a Loi concernant le cadre juridique des technologies de l'information qui a été adoptée par les parlementaires québécois contribuera à bâtir la confiance dans les technologies de l'information et les transactions électroniques. Or, l'établissement de la confiance est une condition essentielle pour que ces moyens deviennent un tremplin pour le développement économique du Québec et l'enrichissement collectif de ses citoyens et citoyennes* ». Discours du 21 juin 2001, en ligne : http://mcc.quebectel.qc.ca/sites/mcc/discours.nsf/0774a5e7a75d823485256b7300494df5/7bda97f2361f123585256b180059ece8!OpenDocument.

[26] Le glossaire réalisé par le Centre de Recherche en Droit Public (sous la direction de Pierre TRUDEL, Daniel POULIN et France ABRAN) pour faciliter la compréhension de la *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 7, témoigne sans aucun doute de cette technicité. En ligne : http://www.autoroute.gouv.qc.ca/loi_en_ligne/glossaire/index.html.

[27] La pensée de Jacques ELLUL, *Le système technicien*, Paris, Calmann-Levy, 1977 reflète bien la perspective du déterminisme technique. Pour ce philosophe et juriste, l'intervention humaine est secondaire et renvoie inéluctablement le technicien à un rôle instrumental, un outil au service d'une technique autonome, qui ne « dépend que d'elle-même » et qui « trace son propre chemin » (p. 137).

[28] « […] *il est possible de parvenir à des connaissances qui soient fort utiles à la vie, et qu'au lieu de cette philosophie spéculative qu'on enseigne dans les écoles, on en peut trouver une pratique, par laquelle, connaissant la force et les actions du feu, de l'eau, de l'air, des astres, des cieux et de tous les autres corps qui nous environnent, aussi distinctement que nous connaissons les divers métiers de nos artisans, nous les*

qui subordonne les choix techniques à la volonté humaine ? La répartition des rôles n'est pas évidente, mais l'on peut déjà envisager l'une et l'autre de ces pistes.

Sous le paradigme du **déterminisme technique** d'abord, le principe fondateur de la technique, l'efficacité, engage toute décision sur une voie essentiellement technicienne[29] : l'existence de procédés techniques très sécuritaires, comme certains dispositifs cryptographiques, définit les besoins de sécurité du commerce électronique. Le degré d'efficacité recherché par les décideurs est forcément, sous cet angle, le plus élevé qui existe : la non répudiation des signatures électroniques et l'inaltérabilité des documents technologiques deviennent entre autres les critères juridiques qui déterminent la valeur probante des contrats électroniques. C'est la figure du progrès technique, qui aboutit à une architecture technique et juridique d'une sécurité communément acceptée comme la plus avancée.

Cette perspective n'est pas étonnante pour qui considère la subjectivité comme un produit de l'environnement social : droit, technique, économie deviennent des constructions sociales systémiques qui déterminent l'esprit humain[30]. Le processus d'anticipation qui caractérise l'œuvre législative du contrat électronique n'échappe pas à cette « tragédie

---

pourrions employer en même façon à tous les usages auxquels ils sont propres, et ainsi nous rendre comme maîtres et possesseurs de la nature ». René DESCARTES, *Discours de la méthode*, VI[e] partie, 1637.

[29] Cette perspective technocratique, selon laquelle la société moderne est déterminée par une logique du progrès scientifique et technique, a notamment été développée par J. HABERMAS, *La Technique et la Science comme idéologie (1963)*, trad. J.-R. LADMIRAL, Paris, Éd. Denoël, 1973, p. 45- 46. Selon l'auteur, le processus de formation démocratique de la volonté politique serait guidé et contraint par une idéologie technoscientifique, de manière à ce que les décisions visant un besoin fonctionnel écartent toute alternative à la logique rationnelle de la technoscience.

[30] La pensée du sociologue allemand Niklas Luhmann est représentative de cette perspective épistémologique. Celle-ci serait dépendante de l'idée freudienne d'un psychisme replié sur lui-même, idée selon laquelle le sujet s'auto-observe et expérimente le monde sans aucune autre référence que celles de sa propre organisation. Sans accès direct à la réalité, le sujet ne peut alors se construire qu'avec des éléments auto-constitués auxquels il a accès : d'abord le langage et la communication et ensuite des constructions imaginaires comme l'idée d'individu ou de personne . En conséquence, la connaissance n'est plus posée là, comme une réalité extérieure : elle est un produit d'échange systémique. Si le sujet participe à l'auto-constitution des systèmes sociaux, ce n'est pas tant comme conscience souveraine qu'à titre de sujet limité par sa structure psychique à connaître le monde exclusivement par une médiation corporelle et, en conséquence, par l'intégration d'une connaissance socialement construite, c'est-à-dire auto-construite en raison justement de cette limite herméneutique de la connaissance. En d'autres mots, toute forme de conscience doit être référée à la réflexivité du social. Hugues RABAULT, « *L'apport épistémologique de la pensée de Niklas Luhmann : un crépuscule pour* l'Aufklärung ? », (1999) 42/43 *Droit et* Société 449.

culturelle »[31]. Lorsqu'il se projette dans le futur, l'esprit peut difficilement se départir de la réalité (technique) dont il est le témoin actif. Il peut tout au plus envisager le prolongement de ce qui existe[32]. Sous la pression du principe fondateur de la technique, la projection qui en découle se conforme au prolongement de ce qui constitue le meilleur de la technique : un haut niveau de sécurité qui pourrait toutefois, dans un avenir où la cryptographie serait facilement neutralisée, ne plus exister, rendant obsolètes des critères juridiques construits à partir d'une réalité dépassée. « L'imprévisibilité absolue de la technique »[33], telle que soulignée par Jacques Ellul, constitue en ce sens un argument qui favorise le caractère déterminant de la technique.

Sous le paradigme opposé, celui du **déterminisme cartésien**, la technique est autrement : confinée au rang de simple outil, elle devient le moyen par lequel les aspirations économiques, politiques et autres peuvent s'exprimer. La volonté, le temps et l'argent sont les seules limites au développement de techniques efficaces et appropriées. Le processus décisionnel est donc, en ce qui concerne la technique, plus inductif que déductif : en maître de la Nature, l'Homme identifie d'abord ses besoins selon un processus rationnel (réflexion, discussion, appréciation et décision) et fixe ensuite les objectifs que la technique doit poursuivre pour y répondre. Ainsi, les critères juridiques de non répudiation et d'inaltérabilité résultent exclusivement et logiquement de la « nécessaire » confiance en l'économie numérique et de son pendant juridique, le besoin de prévisibilité des normes.

L'une et l'autre de ces hypothèses exposent des réalités bien différentes. On ne peut avec exactitude identifier lequel des deux déterminismes apparaît ici le moins artificiel. Ce ne sont, après tout, que des simplifications paradigmatiques que la réalité, toujours plus

---

[31] Le concept de tragédie culturelle du philosophe Georg Simmel exprime l'idée selon laquelle les produits culturels, comme la technique, servent davantage leur propre développement que celui de l'Homme : « *Tel est le concept de toute culture, que l'esprit crée une entité objective autonome* [la technique par exemple]*, par où passe l'évolution du sujet, allant de soi à soi. Mais par-là même, cet élément intégrateur, marqueur de culture, est prédéterminé pour un développement spécifique, qui certes consomme bien toujours les énergies des sujets, et entraîne bien toujours des sujets dans sa propre orbite, mais sans pourtant les mener au sommet d'eux-mêmes* ». Georg SIMMEL, *La tragédie de la culture*, Paris, Édition Rivages, 1988, à la page 209.

[32] J. ELLUL, *Le bluff technologique*, Paris, Hachette, 1988, p. 118.

[33] *Id*.

complexe, dépasse. L'idée du déterminisme technique néglige, par exemple, le rôle des rationalités étrangères à la technique, comme le besoin de sécurité juridique, dont l'expression est certes plus ancienne que le commerce électronique[34]. Sans un tel souci de prévisibilité, les normes législatives encadrant le contrat électronique seraient probablement moins nombreuses et pointues, laissant largement aux tribunaux le soin de séparer, en cette matière, le vrai du faux électronique.

En retour, le déterminisme cartésien n'est guère plus valable. D'une part, le postulat selon lequel la technique sert fidèlement les aspirations humaines ne prend pas en compte le fait que la technique pose souvent ses propres conditions[35] : elle offre un ensemble de solutions opérables parmi lesquelles il faut choisir. Cette contrainte signifie que certains besoins, comme la sécurité, peuvent recevoir une expression technique différente (en-dessous ou en-dessus) de ce qui est désiré. D'autre part, l'instrumentalisation de la technique est une idée qui oublie trop souvent les particularismes des techniques choisies et les nouveaux besoins qu'ils sont susceptibles de faire naître. La non transparence des technologies du contrat électronique emporte, par exemple, l'élaboration de clauses contractuelles d'exclusion de responsabilité des acteurs techniques, clauses inexistantes en ce qui concerne les contrats sur support papier. Dans ce dernier cas, les défaillances du moyen de signature (stylobille, plume) ou du support papier, comme l'apparition de taches, l'insuffisance de l'encre ou la décomposition du papier, sont plutôt évidentes, transparentes. L'univers numérique du contrat électronique est moins cristallin, puisqu'il met en œuvre des processus abstraits dont le succès peut être apparent et trompeur. Un dysfonctionnement ou l'exploitation d'un bris de sécurité par un tiers peuvent en effet affecter l'un ou l'autre des éléments nécessaires à la formation ou à la conservation du contrat électronique (système d'exploitation, logiciel, dispositif de signature, certificat,

---

[34] Sur cette question , Jacques Chevallier remarque que l'ordre juridique, en tant que facteur de sécurité et de stabilité sociale, doit se présenter comme un ensemble cohérent, intégré et monolithique. Visant à répondre à ce besoin de prévisibilité, la communauté juridique tend vers un ensemble cohérent, rationnel et logique de normes juridiques, relevant d'une identité commune. J. CHEVALLIER, « L'ordre juridique », dans J. CHEVALLIER et Danièle LOCHAK (dir.), *Le droit en procès*, Paris, PUF, CURAPP, 1983, p. 7.

[35] Comme le note Gilbert HOTTOIS, *Le signe et la technique*, Paris, Éditions Aubier Montaigne, 1984, p. 73 et s., la technique ne relève pas de l'ordre du symbole, mais plutôt de l'ordre de ce qui est opératoire. En conséquence, la technique entretient avec l'Homme une relation particulière l'empêchant de matérialiser toutes ses aspirations symboliques.

répertoire, etc.) sans que les parties en soient informées. Afin de contrer les risques d'inefficacité technique, il devient donc nécessaire, pour les acteurs techniques, d'exclure ou de limiter leur responsabilité, ce qui n'est évidemment pas le cas, par exemple, pour les fabricants de papier ou de stylobilles.

À la lumière de ces critiques, l'origine de l'œuvre prospective du législateur prend la forme d'un co-déterminisme, par lequel interagissent la technique et les besoins des acteurs : des allers-retours, en quelque sorte, qui rendent l'un et l'autre de ces facteurs responsables d'un cadre normatif d'anticipation construit à l'aune d'une réalité présente. Ainsi, le recours à un nouveau support contractuel, le numérique, conduit à s'interroger sur la valeur juridique des signatures et des contrats effectués sur ce support. On constate notamment que ces contrats ne sont pas tous équivalents, en ce qui concerne les fonctions d'identification et d'intégrité, aux contrats sous seing privé conclus sur le papier. Cette différence crée une incertitude et amène les décideurs à désigner les contrats électroniques qui, devant un tribunal, recevront une valeur probante semblable à celle des contrats sur support papier. Or, parmi les solutions techniques dont ils peuvent s'inspirer pour établir les nouveaux critères, aucune n'est vraiment équivalente : les contrats réalisés par simples courriers électroniques sont, par exemple, plus falsifiables que les contrats papiers, mais les contrats papiers se révèlent plus falsifiables que les contrats signés avec une clef privée de chiffrement adéquatement certifiée. En conséquence, les critères retenus font écho aux solutions numériques les plus efficaces en matière de réseau ouvert : la cryptographie asymétrique et son infrastructure à clef publique. Suivant les caractéristiques de ces solutions, les décideurs adoptent des dispositions qui privilégient de hautes garanties en matière d'identification et d'intégrité : par exemple, la non répudiation de la signature et l'inaltérabilité du support. Ce nivellement par le haut rend donc le degré de sécurité technique exigé par le droit pour le contrat électronique sous seing privé plus élevé que celui applicable à son équivalent papier[36], lequel n'ayant d'ailleurs jamais été expressément formulé par les législateurs.

[36] Certains auteurs, dont Jean DEVÈZE, « Perseverare diabolicum : À propos de l'adaptation du droit de la preuve aux technologies de l'information par le Décret no 2002-1436 du 3 décembre 2002 », (mars 2003) *JCP Communication, Commerce électronique* 12, 13, suggèrent d'ailleurs que la présomption de fiabilité

La technologie n'est pas neutre, puisque la condition d'opérabilité qui la caractérise oriente les décideurs vers des solutions qui ne correspondent pas nécessairement à leurs attentes (comme en matière de sécurité juridique). À cet égard, il est intéressant d'imaginer ce qu'auraient été les critères retenus par les législateurs si les procédés cryptographiques que nous connaissons n'avaient pas encore été inventés. On peut dès lors envisager que la condition d'intégrité du support aurait été moins exigeante, que l'inaltérabilité qu'elle suppose aurait, par exemple, laissé place à une appréciation plus circonstancielle de la sécurité, donnant ainsi une importance plus grande aux usages du commerce électronique et à ses techniques les plus usitées, comme le courrier électronique. Dans cet ordre d'idées, les contrats effectués grâce à ce moyen de communication, ou son éventuelle version améliorée, auraient peut-être reçu une valeur probante semblable au contrat conclu sur support papier. La possibilité de contester un tel acte aurait d'ailleurs été moins problématique que celle d'un contrat électronique qui, entendu au sens des présentes normes législatives, doit idéalement être non répudiable et inaltérable[37].

Conclusion

La multiplicité des normes encadrant le contrat électronique se caractérise par une construction techno-juridique rarement au diapason de la réalité qu'elle entend régir. En effet, les conditions exigées par la loi trouvent leur expression dans un appareillage technique que la pratique contractuelle n'a pas encore adoptée. L'élévation de cet appareillage au rang de standard *de facto* du commerce électronique est d'ailleurs économiquement incertaine[38]. L'œuvre d'anticipation du législateur risque en ce sens de

---

de l'article 1316-4 du *Code civil* français est, compte tenu de l'efficacité des dispositifs techniques actuels, superfétatoire.

[37] On peut en effet croire que le recours à une technologie moins efficace (que la cryptographie asymétrique et son architecture à clef publique) procurerait une latitude probatoire plus grande, un débat moins tourné sur les aspects techniques et, en d'autres termes, une place plus grande aux témoignages des parties et aux circonstances qui ont fait naître le conflit. Au contraire, l'utilisation de dispositifs ultra-sécuritaires risque de minimiser certaines possibilités (le vol du dispositif de signature et du mot de passe confidentiel qui lui est associé) au profit d'une appréciation essentiellement technique du procédé de signature, de son efficacité reconnue.

[38] D'une part, cette standardisation sous-entend l'adoption d'une nouvelle infrastructure technique qui, du point de vue des commerçants, représente un investissement peu rentable et, d'autre part, elle n'apparaît possible que si les internautes disposent en retour de dispositifs de signatures électroniques fiables (ce qui est aujourd'hui rarement le cas et qui, à notre avis, ne saurait changer sans un effort approprié des

ne jamais recevoir l'application réconfortante souhaitée pour le commerce en ligne et d'être, au mieux, confinée à l'échange de communications électroniques avec l'État. Par ailleurs, rien n'indique que les critères juridiques formulés à la lumière des représentations actuelles de la technique recevront toujours une expression technique valable : la cryptographie de demain pourrait bien être autant sécuritaire que le courrier électronique d'aujourd'hui.

principaux intermédiaires du paiement électronique, les institutions émettrices de cartes bancaires ou de crédit).