ASPECTS JURIDIQUES DE LA DÉMATÉRIALISATION DES ÉCHANGES DANS LE COMMERCE ÉLECTRONIQUE

Bertrand Warusfel

Maître de conférences à la faculté de droit de Paris V-René Descartes,
Avocat au barreau de Paris (cabinet FWPA)

Par la terminologie désormais courante de "commerce électronique", on veut souligner que ce type d'activité commerciale se caractérise par sa modalité technique : ce commerce est électronique parce qu'il utilise des moyens informatisés de traitement de l'information pour mettre en relation vendeurs et acheteurs et pour conclure l'opération commerciale. Mais il ne suffit pas de qualifier les moyens techniques mis en œuvre pour donner à ce nouveau type d'activités économiques sa spécificité, et donc justifier que des normes juridiques spéciales s'y appliquent. Encore faut-il établir que le recours aux outils électroniques modifie d'une certaine manière la nature du commerce ainsi pratiqué.

Quelles transformations profondes peuvent ainsi s'opérer dans la relation commerciale lorsque celle-ci s'établit au travers de systèmes numériques appartenant au domaine des "nouvelles technologies de l'information et de la communication" (N.T.I.C.) ? Deux caractéristiques semblent prédominer : *primo*, la relation se dématérialise (puisque la relation physique peut être remplacée par des échanges de messages numériques) et, *secundo*, elle s'effectue à distance (puisque de tels échanges peuvent aisément emprunter les réseaux de communication, eux-même numérisés). Certes rien de tout cela n'est vraiment nouveau dans son principe car le commerce à distance existe depuis fort longtemps, notamment pour ce qui concerne les échanges internationaux. Mais la mise en œuvre des moyens numériques en accroît fortement les effets : l'échange peut être à la fois distant et quasi-immédiat (puisque la vitesse de transmission de l'information est quasi-nulle sur les réseaux) tandis que le produit ou la prestation objet de l'échange peut, parfois, être également livré ou exécutée en ligne, et ce sans aucune limitation territoriale ou temporelle. Comme le dit justement le Professeur Jérôme Huet, les trois caractéristiques du commerce électronique sont donc bien : immatérialité, interactivité et internationalité [1]. Et la première crée les conditions techniques des deux autres.

On s'attachera donc ici principalement aux effet de la dématérialisation qu'induit la numérisation, car elle est susceptible d'agir tant sur l'objet de l'échange que sur les modalités de celui-ci. En se numérisant, le commerce accroît donc la valeur potentielle des différents actifs immatériels qui permettent ou favorisent les échanges **(1.)** tout en renforçant les besoins de sécurité et de confiance **(2.)**. Les effets juridiques de cette dématérialisation du commerce se font donc sentir tant dans le domaine du droit des biens et de la propriété intellectuelle que dans ceux des obligations ou de la preuve.

[1] Jerôme Huet, "La problématique juridique du commerce électronique", *Colloque Droit et Commerce*, Deauville, 2000, p. 2.

*Publié in **Les Petites Affiches**, 6 février 2004, n° 27, p. 17 et s.*

I. Un processus qui accroît la valeur potentielle des actifs immatériels

Le premier effet de la dématérialisation est sans doute d'accroître considérablement l'importance – et donc la valeur économique et juridique - des éléments immatériels dans les échanges économiques et sociaux. Ces éléments dématérialisés sont non seulement les "contenus" déjà protégés par la propriété intellectuelle et désormais facilement échangeables et commercialisables sous forme numérique (a), mais aussi toutes les données qui accompagnent ou découlent indirectement des échanges électroniques (b). Et la lutte économique pour le contrôle et l'appropriation de ces nouvelles richesses immatérielles se traduit par des tensions juridiques fortes (c).

A) Les contenus numérisés peuvent faire l'objet d'échanges accrus et à coût marginal

Si la propriété intellectuelle est indépendante des supports techniques utilisés pour reproduire et exploiter les objets qu'elle protège (créations relevant du droit d'auteur ou droits protégés par la propriété industrielle), ses effets et sa valeur économique peuvent être accrus ou diminués en fonction de l'évolution technologique. S'agissant des effets induit par la numérisation, ils sont indéniablement positifs même si la mise en réseau suscite par ailleurs un essor renouvelé de la contrefaçon [2].

Le premier effet de la numérisation des contenus est, en effet, par-delà leur diversité (textes, images, sons, …) de leur donner un substrat technique commun, à savoir des fichiers numériques susceptibles d'être traités par des logiciels, d'être archivés sur les mêmes supports de stockage (disques durs, CD-ROM, …) et transmis sur tous les réseaux de transfert de données.

Cette convergence technique ouvre ainsi la voie à la constitution d'un large marché du commerce électronique de ces contenus. Là où dans le passé les chaînes de production et de diffusion des contenus culturels différaient totalement suivant qu'il s'agissait de l'écrit (impression-librairie-bibliothèque, etc), du son, de l'image fixe (photographie "argentique", laboratoires de développement, etc.) ou animée (cinéma, radio, télévision), désormais de simples micro-ordinateurs (reliés aux réseaux de télécommunication deviennent les outils d'acquisition et d'échanges de tous ces contenus à la fois. Et le passage progressif vers les communications dites "large bande" (du type A.D.S.L., par exemple) va accélérer ce processus qui se traduire logiquement par un élargissement de la clientèle pouvant consommer de tels objets intellectuels.

Mais les effets de la numérisation ne sont pas seulement quantitatifs, ils sont également économiques et qualitatifs. Économiquement, il est largement démontré qu'elle réduit tout à la fois les coûts de reproduction (en permettant des copies à l'identique effectuées automatiquement sur des supports bon marché) et les coûts de distribution (puisque le stockage peut être effectué sur des supports peu encombrants ou la diffusion se faire

[2] Cf. B. Warusfel, "Internet : nouvelles problématiques face à la contrefaçon", in *L'entreprise face à la contrefaçon de droits de propriété intellectuelle*, Actes du colloque de l'IRPI, Litec, 2003, pp. 57-67.

directement en ligne) [3]. Il devient donc théoriquement plus facile à un créateur de trouver les moyens économiques de diffuser ses créations et de les exploiter commercialement en les proposant à des coûts faibles (propres du coût marginal), ce qui devrait encore accroître son public potentiel (voire, peut-être atteindre des niveaux susceptibles de dissuader économiquement les différentes formes de contrefaçon). Qualitativement, la numérisation des contenus permet aussi de permettre leur traitement ultérieur par des logiciels qui pourront apporter à leurs usagers des bénéfices supplémentaires (comme par exemple, la possibilité d'apporter des retouches à une image ou la recherche automatique de mots dans un texte, ou encore la possibilité technique de partager en ligne l'accès de l'objet numérique concerné – par exemple sur un Intranet d'entreprise).

Dès lors, si la numérisation et les facilités techniques qui y sont associées peuvent parfois fragiliser le commerce traditionnel des droits de propriété intellectuelle (c'est par exemple, le cas actuellement dans le domaine musical avec l'essor de la contrefaçon de musique en ligne, notamment par le biais de logiciels dits "peer-to-peer"), on peut estimer que la dématérialisation devrait à terme favoriser le développement d'un véritable commerce en ligne des contenus protégés. Ceux-ci une fois numérisés possèdent, en effet, la caractéristique de pouvoir être accessibles et téléchargeables en temps réel, alors que le commerce électronique des biens matériels restera toujours tributaire des contraintes logistiques et des délais de livraison physique.

D'ores et déjà, on voit apparaître sur le marché des modes de commercialisation innovants des contenus numériques, qu'il s'agisse – pour prendre des exemples extrêmes – de modèle reposant sur la gratuité et la rémunération indirecte, comme pour les sites Web incorporant des bandeaux publicitaires, ou la diffusion de logiciels *Open Source* (dont le développement est assuré par la communauté des utilisateurs ou la commercialisation de services associés [4]) ou, au contraire, de systèmes utilisant les technologiques numériques de sécurité (ce que l'on appelle actuellement les systèmes de "*Digital rights management*" [5]) pour assurer une rémunération à l'acte (de type "*pay per view*").

B) Les autres données valorisables dans le commerce électronique

Mais le commerce électronique ne se limite pas au seul commerce des créations numériques protégées par le droit de la propriété intellectuelle. La vente en ligne de produits matériels (nouvelle forme de la traditionnelle "vente par correspondance") tout comme la réservation ou la consommation de services (réservations, voyages, spectacles, annonces, …) constituent également des secteurs importants (et même aujourd'hui dominants) du commerce électronique. Cela ne veut pourtant pas dire que ces activités ne sont pas concernés par l'accroissement de la valeur des actifs immatériels.

---

[3] V.. notamment, C. Shapiro & H. R. Varian, *Économie de l'information – Guide stratégique de l'économie des réseaux*, De Boeck Université, Bruxelles, 1999 (pour la traduction en français), p. 95.

[4] Sur les aspects juridiques des licences Open Source, cf. M. Clément-Fontaine, *La licence publique générale GNU*, Mémoire DEA, Université de Montpellier 1, 1999.

[5] V.Cf. notamment le document de synthèse rédigé par la Commission des communautés européennes, *Digital Rights - Background, Systems, Assessment*, SEC (2002) 197, 14 février 2002.

*Publié in **Les Petites Affiches**, 6 février 2004, n° 27, p. 17 et s.*

En effet, toute activité d'échange électronique met en œuvre ou produit des données ou des objets numériques susceptibles de représenter une valeur marchande directe ou indirecte.

En amont de l'échange, un service de commerce en ligne s'appuie sur des "objets numériques" [6] tels que des logiciels, des bases de données, les éléments visuels et multimédia constituant les pages du site, ou encore les adresses et les noms de domaine. Tous ces éléments jouent un rôle essentiel pour permettre la mise en relation "virtuelle" entre le commerçant et les consommateurs. Leurs qualités et performances intrinsèques (sur le plan technique ou esthétique), leur notoriété (en particulier pour les signes distinctifs et les noms de domaine) constituent souvent des facteurs décisifs de la réussite ou de l'échec commercial de l'activité d'un site marchand. Leur valeur économique et patrimoniale est donc potentiellement grande, particulièrement en cas d'entrée en bourse ou de fusion-acquisitions.

Mais le commerce électronique peut produire lui-même, en aval, des informations numériques qui peuvent représenter en elle-même une valeur économique autonome. Les données de trafic (c'est-à-dire les statistiques de connexion des différents utilisateurs sur les réseaux) sont des données très utiles pour les opérateurs de réseaux et les fournisseurs d'accès (qui peuvent ainsi prévoir l'évolution des besoins et programmer leurs investissements). Les informations recueillies par les sites sur les besoins et les habitudes des internautes-consommateurs (avec leur consentement, ou grâce à des moyens techniques comme les "*cookies*") jouent un rôle majeur dans les politiques commerciales et le marketing des acteurs du commerce électronique. Et il en va de même pour toutes les données qui sont échangées en relation avec le paiement des prestations ou des achats en ligne (et, en particulier – car cela reste le mode de paiement le plus répandu sur l'Internet – les coordonnées de carte bancaire [7]).

L'importance de toutes ces données associées au commerce électronique (que certains dénomment parfois du terme technique de "métadonnées") est telle que leur exploitation peut également servir à d'autres objectifs licites ou illicites et qu'elle met en jeu d'autres problématiques, notamment en termes de protection de la vie privée [8] ou encore – comme nous le verrons dans la seconde partie – de sécurité et de répression pénale.

Qu'il s'agisse donc des contenus numériques du commerce électronique, de ses outils logiciels et multimédia ou de ces métadonnées que son activité engendre, on peut souscrire à l'appréciation générale que formulait en juin 2000 le Professeur Pierre Catala : *"Au*

---

[6] Ce terme d'"objet numérique" n'est pas fréquent en langue française et n'a pas de signification juridique précise, mais il est parfois utilisé dans la littérature technique et économique anglo-saxonne (v. par exemple, P. A. Lyons, "Access to Digital Objects : A Communications Law Strategy", *D-Lib Magazine*, October 1995).

[7] Le dernier rapport annuel de la CNIL relève que ses services *"ont été saisis au cours de l'année 2002 d'un nombre croissant de plaintes de la part de consommateurs ayant pour objet la conservation et l'utilisation de leur numéro de carte bancaire par les commerçants spécialisés dans la vente à distance"* et que *"le numéro de carte bancaire est en effet devenu un véritable « outil marketing » au service des commerçants qui l'utilisent pour la fourniture de services spécifiques et distincts du paiement du bien pour lequel le numéro de carte bancaire avait été communiqué par le consommateur"* (Commission Nationale de l'Informatique et des Libertés, *23ème rapport d'activité 2002*, La Documentation française, 2003, p. 94).

[8] V. à titre d'exemple, l'étude réalisée en avril 2000 par la CNIL, "E-commerce en France : évaluation de 100 sites français de commerce électronique".

*Publié in **Les Petites Affiches**, 6 février 2004, n° 27, p. 17 et s.*

commencement était le verbe, dit l'Évangile de Saint Jean, et le verbe dans un sens laïc c'est l'information, et l'ordinateur convertit l'information en données numériques. Ces données sont en expansion illimitée. Leur valeur réelle est déjà grande ; leur valeur virtuelle fait chavirer tous les esprits. On a connu l'or jaune métallique, l'or noir, puis l'or vert, et voila le e.gold." [9] Même après la crise économique qui a ravagé la "nouvelle économie" depuis deux ans (et peut-être encore plus depuis lors), le contrôle et l'appropriation de ces nouveaux actifs immatériels liés au commerce électronique revêt une importance stratégique pour les acteurs qui sont engagés dans ces activités. La conséquence en est des tensions nouvelles sur le terrain juridique, notamment s'agissant de l'adaptation du droit de la propriété intellectuelle au contexte numérique.

C) Des controverses juridiques autour de l'appropriation des biens immatériels

Il existe une certaine corrélation entre le déploiement des nouvelles technologies – et particulièrement celles de l'information et de la communication – et le renforcement des droits de propriété intellectuelle.

On peut citer plusieurs étapes significatives au cours des vingt dernières années : la reconnaissance législative de la protection des logiciels par le droit d'auteur (effectuée en France par la loi du 3 juillet 1985), l'admission progressive par la jurisprudence américaine puis européenne (avec la décision *Vicom* de l'Office européen des brevets en juillet 1986 [10]) de la validité de brevets portant sur des innovations logicielles, l'adoption des accords A.D.P.I.C. lors de la conférence de Marrakech en 1994, la création par la directive du 11 mars 1996 d'un droit *"sui generis"* sur certaines bases de données, ou encore la protection juridique accordée aux mesures techniques mises en œuvre par les titulaires de droit sur les œuvres numérisées (protection découlant des traités signés à l'Organisation mondiale de la propriété intellectuelle le 20 décembre 1996 et introduite en Europe par la directive du 22 mai 2001 sur le droit d'auteur dans la société de l'information [11]).

Mais si cet effort normatif soutenu montre qu'à l'évidence*, "la propriété intellectuelle a su faire valoir ses exigences dans l'univers numérique"* [12], cette extension de la protection juridique autour des différents objets du commerce électronique (les logiciels, les créations multimédias, les bases de données, les noms de domaine, les contenus en ligne) ne s'est pas engagée sans controverse et suscite actuellement des tensions contradictoires.

---

9 P. Catala, in *Le Droit de l'Informatique à l'aube du 3ème Millénaire*, Colloque IFCLA 2000, Paris 15-16 Juin 2000, p. 240.

10 OEB Ch. de recours technique du 15 juillet 1986, Affaire T 208/84, *Vicom*, JO OEB 1987/014. Pour une synthèse sur cette évolution et les différentes approches européennes et américaines, v. B. Warusfel, "La brevetabilité des inventions logicielles dans les jurisprudences européenne et américaine", Actes du colloque de l'AFDIT (Association française du droit de l'Informatique et de la Télécommunication) du 17 juin 2002 (à paraître aux Éditions des Parques).

11 V. S. Dusollier & A. Strowel, "La protection légale des systèmes techniques – Analyse de la directive 2001/29 sur le droit d'auteur dans une perspective comparative", *Propriétés intellectuelles*, n°1, octobre 2001, pp. 10-27 ; également, sur le même sujet, les exposés de A. Latreille et de Gilles Vercken, reproduits in *Propriétés intellectuelles*, n°2, janvier 2002, pp. 35-51 et 52-57.

12 B. Warusfel, *La propriété intellectuelle et l'Internet*, Flammarion, 2001, p. 109.

*Publié in **Les Petites Affiches**, 6 février 2004, n° 27, p. 17 et s.*

D'un côté, certains acteurs économiques et certains théoriciens considèrent qu'il serait temps d'adapter définitivement le droit des biens aux nouvelles réalités technologiques (notamment dans le domaine numérique) en reconnaissant de véritables droits privatifs sur les "biens informationnels", voire sur l'information elle-même.

Les professeurs Catala (déjà cité) ou Philippe Le Tourneau sont en France parmi ceux qui ont plaidé pour la reconnaissance de véritables droits réels sur l'information [13]. Et l'on a cru parfois que des évolutions législatives (comme le droit *sui generis* du producteur de base de données) ou jurisprudentielles (comme certaines jurisprudences civiles pour concurrence déloyale ou parasitisme ou – plus rares et plus anciennes – les quelques décisions pénales reconnaissant indirectement l'existence possible d'un *"vol d'information"*) pourraient leur donner raison. Mais, en réalité, ces tentatives n'ont pas altéré les bases traditionnelles et les limites de la propriété intellectuelle [14]. C'est d'ailleurs la raison pour laquelle le recours aux moyens techniques de prévention et de protection (tatouage, chiffrement, dispositifs anti-copie, etc.) apparaît aujourd'hui à certains acteurs de l'économie numérique comme une voie alternative et non-juridique pour accroître la protection des actifs immatériels et favoriser la rentabilité des investissements immatériels [15].

Mais, de l'autre côté, s'inquiétant de ces efforts pour renforcer les droits privatifs directs ou indirects sur l'immatériel, de nombreux observateurs ou chercheurs remettent en cause les fonctions même de la propriété intellectuelle et s'interrogent sur sa possible obsolescence dans la future "société de l'information". Les critiques et les interrogations sont souvent de nature économique comme le montre bien le récent rapport publié par le Conseil d'analyse économique [16]. Mais elles prennent aussi une tonalité plus philosophique ou politique lorsqu'il s'agit d'opposer les logiques patrimoniales classiques (supposées être celles de la propriété intellectuelle) à des approches censées mieux correspondre à la modernité des réseaux et des services numériques et fondées essentiellement sur le partage et la circulation de l'information [17]. Les polémiques suscitées depuis la publication en février 2002 d'une proposition de directive relative à la brevetabilité des inventions mises en œuvre par ordinateur ont bien illustré ce clivage.

---

13 V. notamment, Ph. Le Tourneau, "Folles idées sur les idées", Journée d'étude *L'idée - Approche juridique, fiscale et économique*, Université Toulouse 1, 1998, p. 9 ; P. Catala, "La "propriété" de l'information", reproduit in *Le droit à l'épreuve du numérique - Jus ex Machina*, Puf, 1998, p. 247.

14 V.f. B. Warusfel, "Entreprises innovantes et propriété intellectuelle : les limites de la protection juridique du patrimoine immatériel", in B. Laperche (dir.) *Les enjeux économiques de la propriété industrielle : brevets, innovation et concurrence mondiale*, L'Harmattan, 2001.

15 Le Professeur Y. Poullet remarque justement que *"ces protections rendent inutiles les régimes de protection juridique, elles assurent aux détenteurs de simples " biens " informationnels une protection dont l'efficacité et l'ampleur sont sans commune mesure avec celles accordées par le droit de propriété intellectuelle en exception au principe sacré de libre circulation des idées."* .

16 J. Tirole & alii, *Propriété intellectuelle*, Rapports pour le Conseil d'analyse économique, La Documentation française, 2003.

17 Pour un exemple de cette vision d'un univers numérique en décalage avec les règles classiques de la propriété intellectuelle, v. C. Vandendorpe, "Pour une bibliothèque virtuelle universelle", *Le Débat*, no 117, novembre 2001, p. 31-42.

*Publié in **Les Petites Affiches**, 6 février 2004, n° 27, p. 17 et s.*

Mais la dématérialisation des échanges ne produit pas seulement ses effets juridiques dans le champ du droit des biens et, plus particulièrement, de la propriété intellectuelle. La "virtualité" apparente qui résulte du recours à des intermédiaires numériques (ordinateurs et logiciels) induit un fort besoin de sécurité et de confiance dans les moyens techniques qui assurent les échanges. Et cette exigence nouvelle qu'impose la technologie a déjà poussé à une réforme du droit de la preuve.

II. Des échanges virtuels qui reposent sur la sécurité et la confiance

Plus les échanges numériques prennent une valeur économique forte et apparaissent comme support potentiel de droits, plus ils apparaissent fragiles aux dysfonctionnements ou aux malveillances. La préoccupation de sécurité est donc intimement liée à l'évolution du commerce électronique et à celle de ses problématiques juridiques. Et de ce point de vue également, le panorama est assez contrasté : si les fonctions à assurer sont bien identifiées (a.) et si les réponses techniques et organisationnelles existent (b.) la réforme du droit de la preuve récemment menée à bien (c.) ne suffira peut-être pas à imposer rapidement les évolutions nécessaires.

A) Les fonctions de sécurité, facteur de confiance

Dans les échanges électroniques à distance, la confiance nécessaire à la conclusion des actes de commerce passe par deux préalables qui relèvent du domaine de la sécurité des systèmes d'information.

Le premier préalable concernent les parties à l'échange (typiquement, l'internaute-consommateur, d'un côté, et le cyber-marchand représenté par son site de l'autre). Entre eux la confiance passe tout d'abord par une identification fiable de chacun. S'assurer du fait que l'on échange bien avec le bon interlocuteur et que chacun est bien ce qu'il prétend être, voici la première exigence de la communication en ligne. En termes techniques, cela correspond à la fonction d'"authentification" qui se définit notamment comme *"la vérification d'une identité déclarée"* [18]. Et du point de vue juridique cette authentification permet alors d'assurer "'imputablité" (c'est-à-dire la possibilité d'attribuer à une personne la responsabilité de l'acte effectué par voie électronique).

Dans les échanges en ligne, l'authentification la plus couramment mise en œuvre (même à l'insu de l'internaute) est celle du site marchand sur lequel se connecte l'internaute. Le très répandu protocole SSL [19] permet notamment à l'ordinateur de l'internaute de vérifier automatiquement avant tout échange sécurisé (par exemple, avant la transmission d'une commande ou d'un numéro de carte bancaire) si le serveur avec lequel il est en relation possède bien une attestation numérique (dénommée "certificat") confirmant son identité.

[18] Définition donnée par le Manuel d'évaluation de la sécurité des technologies de l'information (ITSEM) utilisé et diffusé par la Direction centrale des systèmes d'information (SGDN/DCSSI).

[19] Secure Sockets Layer.

Mais dans certaines applications plus professionnelles (par exemple, pour accéder à un Intranet ou à la partie privée d'un site réservé à des abonnés), l'authentification peut être réciproque et l'internaute doit également prouver par un moyen numérique (souvent également un certificat, plus rarement un dispositif physique tel qu'une clé ou une carte à mémoire) qu'il correspond bien à l'identité qu'il revendique.

Enfin, l'authentification peut porter également sur les droits qui sont reconnus à un individu ou à une entité sur un contenu numérique. Les différents moyens de "tatouage" numérique des contenus (recourant souvent à la technologie du "*watermarking*") permettent par exemple de connaître de manière fiable (c'est-à-dire difficilement altérable) l'identité de l'auteur de l'œuvre concernée [20] ou l'étendue des droits reconnus par celui-ci à l'utilisateur.

Le second préalable à la confiance concerne ensuite le contenu de l'échange. Il ne suffit pas de s'être assuré de l'identité de son interlocuteur et de ses droits à engager une transaction, encore faut-il se prémunir contre toute altération, accidentelle ou volontaire, de ce qui va être échangé avec lui (contenu de la commande, coordonnées bancaires ou postales, clauses du contrat, etc.). La fonction technique qui assure ce niveau de confiance se dénomme "intégrité" et se définit comme "la prévention d'une modification non autorisée de l'information".

Suivant la sensibilité et les enjeux économiques des services concernés, le contrôle de l'intégrité se limitera à celui des échanges électroniques (intégrité des données émises et reçues) ou pourra aussi porter sur la vérification de l'intégrité des logiciels eux-mêmes (intégrité des systèmes), ce qui peut être particulièrement utile à vérifier lorsque le service met en œuvre des logiciels de traitement sophistiqués (par exemple, un logiciel de cotation sur un site d'enchères ou de place de marché).

Et cette exigence d'intégrité se perpétue dans le temps puisqu'il est généralement indispensable de pouvoir en garantir la conservation à moyen ou long terme (notamment jusqu'aux délais de prescription légaux). Il ne suffit pas de recueillir à l'instant de l'échange la preuve de l'intégrité de celui-ci, encore faut-il pouvoir la stocker et pouvoir en assurer à nouveau la vérification plus tard (en cas de litige, par exemple). L'échange dématérialisé ne supprime pas, en effet, la fonction "scripturale" exercée par le marchand électronique qui doit, tel le marchand médiéval inscrire en ses registres la trace indiscutable de la transaction (trace qui, dans le cas d'échanges purement immatériels, sera bien souvent la seule preuve tangible du fait que l'échange a bien eu lieu).

B) Des réponses techniques et organisationnelles possibles

Pour offrir aux parties à un échange électronique marchand les garanties d'authentification et d'intégrité qui sont nécessaires à établir la confiance entre elles, des moyens techniques conformes aux standards actuels de l'industrie sont déjà disponibles sur le marché. Mais l'utilisation efficace de ces moyens va impliquer nécessairement la mise en place d'une organisation et de procédures rigoureuses au sein des entités proposant des services en ligne.

[20] S. Dusollier parle du "*droit moral comme fondement du watermarking."* (S. Dusollier, "Le droit d'auteur et son empreinte digitale", *Ubiquité*, n° 2, Mai 1999, p. 31-45).

En d'autres termes, la confiance relative que l'on peut avoir dans la technique ne va pas sans les nécessaires exigences que l'on doit imposer aux hommes et à l'organisation des entreprises.

S'agissant des moyens techniques – et sans entrer ici dans trop de détails [21] – on se contentera d'indiquer que l'état actuel des connaissances mathématiques et informatiques a permis la mise au point de *"moyens de cryptologie"* [22] qui sont capables notamment d'assurer de manière fiable les fonctions d'authentification et de contrôle de l'intégrité des échanges (certains d'entre eux peuvent, de plus, assurer la confidentialité des données par chiffrement).

Le processus cryptographique qui assure cette double fonction de sécurité est communément appelée "signature". Et parmi les différentes techniques de signature disponibles, les dispositifs reposant sur un mécanisme cryptographique asymétrique (c'est-à-dire mettant en œuvre deux clés complémentaires, l'une publique et l'autre privée, d'où le recours fréquent au sigle anglo-saxon PKI : *"Public Key Infrastructure"*) sont généralement considérés comme la solution actuellement la mieux adaptée aux besoins de sécurisation des échanges en ligne [23]. La majorité de l'offre industrielle en matière de signature électronique repose donc désormais sur ces solutions PKI [24].

Schématiquement, l'émetteur d'un message ou d'un document échangé en ligne dispose d'une clé privée (dont il conserve strictement la confidentialité) et qui lui sert à "signer" le fichier considéré (c'est-à-dire à réaliser une empreinte mathématique infalsifiable établie à partir du contenu du fichier et de la clé privée de l'émetteur). Inversement, le destinataire de ce fichier signé dispose de moyens techniques pour vérifier que ce fichier n'a pu être altéré depuis sa signature et que seul l'émetteur a pu en assurer l'envoi. Pour ce faire, le destinataire doit obtenir et utiliser la seconde partie publique du bi-clé de l'émetteur (puisque la caractéristique mathématique de ces systèmes est qu'une seule clé publique, liée mathématiquement à la clé privée utilisée à l'origine, peut permettre la vérification de la signature).

Ces processus mis en œuvre automatiquement par les logiciels utilisables en ligne (tels que navigateurs Web, logiciels de messagerie, …) nécessitent simplement que le destinataire obtienne au préalable la clé publique de l'émetteur et s'assure qu'elle appartient bien à celui-ci. C'est le rôle des "certificats" (déjà évoqués plus haut) d'assurer cette fonction d'accès et de certification de la clé publique. Le certificat est un document électronique qui indique à la fois l'identité du titulaire de la signature et la clé publique de celui-ci et à partir duquel le logiciel de vérification (généralement intégré dans l'outil servant aux échanges en ligne) effectuera les opérations permettant d'authentifier de garantir l'intégrité des échanges.

---

21 Pour une présentation plus technique de la problématique de la sécurité des réseaux, v. B. Delforge, "Preuve électronique et sécurité des échanges dans les systèmes informatiques", in *Le droit des preuves au défi de la modernité*, Cour de cassation/Université Paris V, colloque du 24 mars 2000, La Documentation française, 2000, pp. 43-58.

22 Au sens qu'en donne l'article 28 de la loi n° 90-1170 du 29 décembre 1990 modifiée.

23 Pour un point de vue juridique en ce sens, v. A. Bensoussan, "Signature électronique, sécurité et protection des données personnelles : la solution PKI" in Colloque IFCLA 2000, *op. cit.*, pp. 39-50.

24 Pour un état du marché (établi en fin 1999 pour le compte d'un rapport officiel français), cf. MTIC, *Rapport sur l'état des technologies à clés publiques et de la certification*, 1999.

*Publié in **Les Petites Affiches**, 6 février 2004, n° 27, p. 17 et s.*

Contrairement à ce que le grand public imagine parfois, un tel processus assure – lorsqu'il met en œuvre des outils cryptographiques récents et bien utilisés - une sécurité des échanges en ligne bien supérieure à celle que l'on connaît usuellement dans les échanges sur papier ou même dans les échanges téléphonique (centre d'appels, …). Il est en effet beaucoup plus coûteux et difficile d'arriver à falsifier des fichiers numériques signés par de tels moyens que de contrefaire une signature manuscrite, de modifier le contenu d'un courrier imprimé ou d'imiter la voix d'une personne. Les moyens techniques de signature électronique et toutes les technologies connexes (comme le watermarking des fichiers) devraient donc considérablement accroître à terme la sécurité et la fiabilité du commerce à distance.

Mais cette sécurité numérique repose largement sur la fiabilité et la rigueur qui doivent être apportées à l'organisation et aux procédures de mise en œuvre par chaque acteur économique, car comme le dit le Professeur Gautrais : *"Alors que la gestion de l'information papier est chose connue, la gestion de l'information électronique balbutie et demeure en réalité une bien faible priorité. Au même titre que la vente à distance exigea au début du vingtième siècle une structure relationnelle solide, une vitrine efficace de commerce électronique requiert un encadrement sécuritaire stable. (...) il n'y aura pas, demain davantage qu'aujourd'hui, de commerce électronique sérieux et durable sans la mise en place d'une véritable structure organisationnelle de sécurité."* [25].

Pour prendre le cas des systèmes P.K.I. déjà évoqués, on voit bien que toute la confiance dépend de l'imputation d'une clé publique à une personne spécifique, c'est-à-dire sur la fiabilité du certificat qui atteste de cette liaison. Il faut donc que ce certificat soit établi par une entité en laquelle le destinataire pourra avoir confiance d'un double point de vue : en ce qui concerne la pureté de ses intentions (pour éviter la malveillance et la fraude), mais aussi en ce qui concerne la fiabilité de ses processus internes (pour éviter l'erreur technique ou administrative).

Typiquement, un processus de certification électronique sur lequel s'appuie la sécurité d'échanges numériques implique la constitution d'une "autorité de certification" qui assume la responsabilité technique et juridique de l'émission des certificats et la mise en œuvre de procédures administratives et techniques couvrant les différentes phases et en particulier : enregistrement du titulaire du certificat (c'est-à-dire vérification de son identité et attribution à celui-ci d'un bi-clé qui lui soit propre), création et diffusion du certificat correspondant, tenue à jour de listes accessibles aux tiers identifiant les certificats qui ne sont plus valides (LCR : liste de certificats révoqués) et procédure de renouvellement ou de révocation des certificats (par exemple quand le titulaire quitte l'entreprise ou change de fonction). Et souvent pour des raisons de coût comme de neutralité, il est plus pertinent de recourir à une autorité de certification extérieure avec laquelle l'entité concernée (par exemple, le cybermarchand) contractera en vue de doter son personnel et ses clients des bi-clés et des certificats nécessaires pour sécuriser les échanges.

Toute cette organisation fonctionnelle et administrative dont la fiabilité garantit seule la sécurité finale des échanges est certainement aujourd'hui la principale et la plus lourde

[25] V. Gautrais, "*Les aspects relatifs à la sécurité*", in *Le guide juridique du commerçant électronique*, Université de Montréal, 2003, p. 75.

exigence à satisfaire pour une entité qui souhaite proposer à ses clients de réels moyens de sécurisation des échanges dématérialisés [26]. En revanche, le cadre juridique de l'emploi de ces moyens techniques de sécurité est désormais bien fixé en Europe et en France, même si il s'agit d'un dispositif législatif et réglementaire complexe et encore peu connu.

C) Un encadrement juridique adapté mais qui demeure complexe

Pour favoriser le développement du commerce électronique et plus largement celui de tous les *"services de la société de l'information"*, la directive communautaire 1999/93 du 13 décembre 1999 a défini *"un cadre communautaire pour les signatures électroniques"*. Sur cette base, la loi française du 13 mars 2000 a modifié le Code civil sur plusieurs aspects importants et complémentaires : la définition de la signature électronique et de ses effets juridiques et la réforme du droit de la preuve afin d'admettre la recevabilité des "écrits numériques".

Sans entrer dans le détail de ce texte et des dispositions réglementaires qui en sont issues [27], cette importante réforme repose sur quelques principes essentiels que l'on peut succinctement résumer comme suit :

1°) l'article 1316 du Code civil définit la preuve par écrit d'une manière suffisamment large [28] pour couvrir l'écrit *"sous forme électronique"*, qui peut donc désormais être *"admis en preuve au même titre que l'écrit sur support papier"* (art. 1316-1) ;

2°) les conditions posées pour cette admission d'un écrit sous forme électronique à titre de preuve prennent directement en compte les deux exigences de sécurité précédemment exposées (authentification et intégrité) puisqu'il faut *"que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité."* (art. 1316-1) ;

3°) le nouvel article 1316-4 du Code civil définit, par ailleurs, les fonctions d'une signature en indiquant qu'elle *"identifie celui qui l'appose"* et qu'elle *"manifeste le consentement des parties aux obligations qui découlent de cet acte"*. Cela permet donc à un dispositif électronique remplissant les fonctions d'authentification et d'intégrité de servir de signature à un document numérique et de contribuer ainsi à son admission en tant que preuve écrite. S'il est en effet possible d'assurer techniquement - outre l'authentification de l'émetteur du message - que le contenu de celui-ci n'a pu être altéré lors de sa transmission ou de son stockage, on peut alors imputer à l'émetteur les conséquences juridiques qui découlent de ce contenu auquel il ne pourra nier avoir consenti ;

---

[26] Le rapport de la MTIC indiquait déjà en 1999, que *"les freins au développement de la certification seront principalement la complexité de tels systèmes au niveau technique et organisationnel, le coût mais aussi le manque de compétences chez les intégrateurs et les clients."* (MTIC, *préc...*, p. 5)

[27] Principalement les décrets du 30 mars 2001 et du 18 avril 2002 ainsi que l'arrêté du 31 mai 2002 ; pour un commentaire détaillé de ces textes, cf.. B. Warusfel, *Signature et Certification électronique*, Éditions Joly (à paraître).

[28] *"suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission"*.

*Publié in **Les Petites Affiches**, 6 février 2004, n° 27, p. 17 et s.*

4°) pour lui reconnaître les mêmes effets probatoires qu'à une signature manuscrite, ce même article 1316-4 impose que la signature électronique *"consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache."*. Et cette fiabilité est présumée lorsque les différents éléments du système de signature employé (c'est-à-dire le procédé cryptographique, le logiciel qui le met en œuvre et les certificats qui permettent de vérifier les signatures) remplissent les conditions qui ont été posées par le décret du 30 mars 2001. Ces conditions concernent :

- d'une part, le niveau de sécurité du procédé cryptographique de signature et des moyens techniques (logiciel et éventuellement matériels associés – tels que carte à mémoire, par exemple) qui permettent de créer les signatures ;
- d'autre part, le niveau de fiabilité et de qualité des certificats et du processus de certification sur lesquels s'appuie le système de signature.

Pour reprendre le vocabulaire particulier de ces textes, la signature et ses moyens de création sont considérés comme *"sécurisés"* lorsqu'ils ont fait l'objet d'une décision de certification prise par le Premier ministre [29] selon une procédure décrite par le décret du 18 avril 2002 précité. De leur côté, les certificats utilisés sont considérés comme *"qualifiés"* lorsqu'ils contiennent un niveau d'information suffisamment important et qu'ils sont émis par une autorité de certification respectant certaines obligations de sécurité (conditions toutes fixées par le décret du 30 mars 2001) et qui peut être elle-même reconnue comme "qualifiée" à l'issue d'une procédure volontaire (du type de celles applicables en matière d'assurance qualité [30]).

On en retiendra donc trois conséquences :

- les exigences de sécurité propres au commerce électronique (principalement authenticité et intégrité) peuvent être assurées par des moyens électroniques de signature dont l'utilisation est admise et reconnue par le droit ;
- les enregistrements numériques résultant de la mise en œuvre de ces moyens de signature peuvent être juridiquement utilisés à titre de preuve [31] si les moyens techniques et l'organisation de la certification satisfont à certains critères de fiabilité ;
- ces effets juridiques ne seront pleinement atteints que lorsque l'on utilisera un dispositif de signature certifié par l'autorité publique et que l'on s'appuiera sur un prestataire de certification satisfaisant aux exigences de qualification posées par la réglementation.

Autrement dit, si la technologie existe et si le droit positif est déjà mis à jour pour la prendre en compte, il va falloir pourtant encore du temps et de la volonté aux opérateurs économiques de la société de l'information pour en tirer tous les bénéfices potentiels. C'est pourquoi plus de

29 V. l'article 3 du décret du 30 mars 2001 modifié par le décret du 18 avril 2002.

30 V. l'article 7 du décret du 30 mars 2001 modifié par le décret du 18 avril 2002, ainsi que l'arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.

31 Voire - dès le vote de la prochaine loi sur la confiance dans l'économie numérique - à titre de condition de validité des actes (cf. le projet de futur article 1108-1 du Code civil que ce texte devrait créer).

trois années après l'adoption de la loi du 13 mars 2000, la signature électronique n'est toujours pas réellement déployée en France et n'est quasiment pas utilisée encore dans le contexte du commerce électronique, alors même qu'elle apporterait techniquement et juridiquement une contribution décisive à la sécurité et à la confiance dont cette activité a besoin pour se développer [32].

Conclusion

Nouvelle forme du commerce à distance mais aussi service de la nouvelle société de l'information, le commerce électronique subit tous les effets économiques et juridiques de la dématérialisation des activités humaines induite par la technologie numérique.

Il est normal que ces effets soient particulièrement intenses sur deux terrains : celui de l'appropriation des choses qui s'échangent et celui de la sécurité des processus qui permettent ces échanges. Le "bon père de famille" du Code civil - qui est quelque peu l'étalon des comportements juridiques – aspire toujours à la sécurité juridique et cherche à jouir "paisiblement" de ses biens.

Force est de constater que sur ces deux fronts notre droit sait réagir à la stimulation. Qu'il s'agisse d'adapter les règles de propriété intellectuelle au phénomène de l'Internet ou de revoir le droit de la preuve pour accueillir l'écrit numérisé et la signature électronique, il n'aura pas fallu plus dix ans pour que nos tribunaux élaborent des jurisprudences appropriées et que nos textes fondamentaux soient réécrits. Le commerce électronique ne va donc pas se développer dans ce "vide juridique" que certains craignaient il y a quelques années.

Mais on doit admettre que si la dématérialisation ne déstabilise le droit, elle le relativise, en attendant peut-être demain de le précariser.

A chaque fois, en effet, c'est désormais la technologie qui conditionne l'application du droit. Les critères fixés par les nouveaux textes et dont découlent les conséquences juridiques sont le plus souvent techniques (le procédé de signature est-il *"fiable"* ? la mesure technique est-elle *"efficace"* ? La reproduction est-elle "transitoire ou accessoire" et constitue t'elle *"une partie intégrante et essentielle d'un procédé technique* [33]" ? …). Et leur appréciation sera de plus en plus l'affaire des experts et moins celle des juges.

Mieux encore, on peut imaginer que dans certains cas, la technique puisse être utilisée comme un moyen autonome et extra-juridique de protection sur les réseaux. C'est l'un des enjeux de la discussion autour des moyens de sécurité utilisés pour protéger les contenus en ligne (qui pourraient gérer les droits d'accès et non plus faire respecter les droits d'auteur). Mais cela pourrait être également le cas sur le terrain de la preuve si, plutôt que de se plier aux exigences tatillonnes de notre nouveau droit de la signature électronique, les acteurs du

32 Sur les réticences et les freins actuels au déploiement des moyens de signature électronique, cf. H. Morin "Pourquoi la signature électronique reste lettre morte", *Le Monde*, 23 Mai 2003.

33 Article 5-1 de la directive du 22 mai 2001 sur le droit dans la société de l'information.

marché mettaient en œuvre des standards de sécurité dont ils organisaient simplement la reconnaissance mutuelle par voie contractuelle.

Enfin, en voulant décrire précisément les conditions et les effets de la mise en œuvre de ces nouvelles technologies numériques, nos nouvelles normes juridiques s'exposent non seulement à la complexité et au jargon [34] mais aussi à une obsolescence toujours plus rapide. Comment en effet permettre que de nouvelles générations technologiques viennent créer demain des situations nouvelles et non prises en compte ? On voit bien sur le terrain des droits d'auteur, que la récente technologie *peer-to-peer* complique déjà l'application du droit. De même, on perçoit bien que la complexe législation bâtie autour de la signature électronique aura du mal à s'appliquer si de nouveaux modèles de sécurité s'émancipent de la logique des systèmes P.K.I. qui dominent actuellement le marché.

Faut-il pourtant avoir un regard pessimiste et désabusé sur ce droit de la technologie précaire et vulnérable ? Assurément non, car plus le risque est grand de voir la technique se réguler elle-même [35], plus il est nécessaire que le juriste cherche à comprendre les nouvelles technologies, à en appréhender les évolutions et à rétablir une norme juridique (même évolutive dans sa formulation et provisoire dans ses effets) qui assure la médiation entre les effets de la technique et les besoins des hommes. Le numérique transforme radicalement notre rapport à la propriété et à la sécurité, il faut donc reconstruire progressivement notre droit de l'immatériel.

Bertrand Warusfel

[34] Pour un point de vue très critique sur les excès en la matière, v.. A. Lucas, "La réception des nouvelles techniques dans la loi, l'exemple de la propriété intellectuelle", *Juriscom.net*, 27 janvier 2001.

[35] V. B. Warusfel, "Le droit des nouvelles technologies : entre technique et civilisation", *Revue des anciens élèves de Sciences-Po*, n° 127, juin 2002, pp. 52-59.

*Publié in **Les Petites Affiches**, 6 février 2004, n° 27, p. 17 et s.*