

Problèmes juridiques liés à la sécurité des transactions sur le réseau



Par Maître Michel Jaccard

Avocat à Genève et chargé de cours à l'Université de Fribourg,
jaccard@ttv.ch

Introduction

Une des applications les plus répandues du commerce électronique est certainement la conclusion et l'exécution de véritables transactions juridiquement contraignantes sur un réseau ouvert comme Internet.

De telles transactions peuvent se nouer entre entreprises (*business to business* ou B2B) ou entre entreprises et consommateurs (*business to consumers* ou B2C), pour tous les cas où l'une des parties (personne physique) achète des biens, consomme des marchandises ou utilise des services à des fins non professionnelles. Mais l'on trouve également un commerce électronique entre particuliers (*private to private* [P2P] ou *consumer to consumer* [C2C]), dont un des aspects les plus spectaculaires est sans doute l'essor des ventes aux enchères en ligne, auxquelles participent d'ailleurs parfois aussi des sociétés commerciales.

Dans cet article, nous nous concentrerons sur quelques caractéristiques juridiques du commerce B2C en milieu ouvert, qui offre la plus grande vulnérabilité au plan de la sécurité. En effet, le commerce B2B se déroule en général entre partenaires connus faisant des affaires ensemble sur le long terme plutôt qu'occasionnellement, la plupart du temps au sein d'un réseau fermé. Dès lors, les problèmes sécuritaires, techniques et commerciaux sont généralement traités préalablement dans des contrats-cadres négociés, parfois appelés *Conventions d'interchange*.

Les transactions B2C en milieu ouvert

Concrètement, les transactions B2C typiques qui se déroulent sur le réseau s'analysent au plan juridique comme l'achat/vente de marchandises ou la prestation de services de toutes sortes (téléchargement de logiciels ou accès à des bases de données en ligne par exemple).

De telles transactions sont-elles juridiquement valables? La véritable question est plutôt: pour quelles raisons les transactions en cause ne seraient-elles plus juridiquement valables, ou seraient valables à des conditions différentes, par hypothèse plus strictes, que celles qui s'appliqueraient à ces mêmes transactions si elles étaient conclues et/ou exécutées en dehors du réseau, de façon traditionnelle?

Schématiquement, le passage à Internet entraîne les caractéristiques suivantes :

1. Automatisation des manifestations de volonté, en ce sens que l'ordre de commande ou son acceptation peut être transmis automatiquement sans qu'une personne physique confirme à chaque fois manuellement la volonté d'être lié contractuellement en visualisant les commandes à l'écran. Cette première caractéristique ne remet pas en cause la validité des mécanismes juridiques de formation des contrats, dans la mesure où, selon des théories déjà éprouvées, le comportement, les actions et les omissions d'un système informatique sont en général imputables à celui ou celle qui en a le contrôle.
2. Dématérialisation du support d'expression des volontés, puisque le contenu de l'accord n'est pas couché sur papier, ni, *a fortiori*, signé à la main. Cependant, le droit suisse connaît de manière générale le principe de la liberté des formes (cf. art.11 et suivants du Code des obligations). Dès lors, sauf exceptions confinées à des domaines qui ne sont pas encore courants sur le réseau, comme les transactions immobilières, l'assurance ou le petit crédit en ligne par exemple, les transactions commerciales évoquées plus haut ne perdent pas leur validité du simple fait qu'elles ne seraient pas reproduites sur papier avant d'être conclues ou qu'une signature manuscrite ne soit pas apposée au bas de l'engagement. En revanche, et c'est là le point important, la preuve de telles transactions pourrait être problématique, en l'absence de support *physique* matérialisant l'accord de volontés et de signature manuscrite établissant l'identité des parties. Comment le droit suisse aborde-t-il ces questions?

Les véritables problèmes juridiques du commerce électronique: la preuve et la sécurité

Au plan civil, les règles de preuves devant les tribunaux varient de canton à canton, même si quelques principes sont unifiés au plan fédéral. Il en va ainsi de la libre appréciation des preuves. En vertu de ce principe, il n'existe pas de catégories privilégiées de preuve (témoignage plutôt que document écrit, original plutôt que copie par exemple). Ainsi, un papier original signé à la main n'aura pas, *a priori*, une valeur probante supérieure à celle du *print-out* d'un *log file* stocké sur disque optique. Il demeure bien entendu qu'un avantage de fait peut subsister en faveur de celui ou celle qui étaye ses affirmations par des moyens de preuve plus traditionnels que des données informatiques, auxquelles les tribunaux suisses ne sont pas encore (entièrement) familiarisés.

Le principe de la libre appréciation des preuves implique également que toute preuve doit obligatoirement emporter l'intime conviction du juge pour être retenue. Prétendre donc qu'une preuve informatique est admissible *a priori* devant les tribunaux suisses ne dispense en aucun cas celui ou celle qui cherche à s'en prévaloir de tout mettre en oeuvre pour que le juge soit effectivement convaincu de la véracité du contenu de la preuve en question.

Dans cette perspective, c'est bien entendu la fiabilité des systèmes de sauvegarde, le professionnalisme de l'organisation interne et la qualité des mesures de sécurité prises qui joueront un rôle décisif. Typiquement, c'est par une combinaison des différents modes de preuve qu'une allégation pourra être démontrée: en plus de la production des documents pertinents imprimés à partir d'une copie de sauvegarde sûre, il s'agira de faire en sorte que le responsable de la sécurité informatique de la société incriminée témoigne des mesures prises

dans le traitement de l'information, dont la fiabilité pourrait encore être corroborée par un expert neutre.

Des solutions sont donc possibles; leur coût risque pourtant d'être disproportionné par rapport à l'objet du litige. C'est pourquoi l'adoption récente en Suisse d'une réglementation en matière d'infrastructure à clé publique (*Public Key Infrastructure* ou PKI) revêt une importance particulière.

L'ordonnance du Conseil fédéral du 12 avril 2000 sur les services de certification électronique (OSCert)

Cette ordonnance, entrée en vigueur le 1^{er} mai 2000, est le premier texte réglementaire en Suisse qui traite de manière cohérente de l'introduction d'une PKI et de la possibilité de recourir à des systèmes de signature numérique pour, en particulier, faciliter la preuve des transactions informatiques.

Concrètement, la signature électronique d'un fichier (texte, son, image) résulte de l'utilisation d'une clé mathématique privée (connue du seul signataire) et d'un algorithme cryptographique, appliqué au texte original. Ainsi, la signature électronique constitue un ensemble de données numériques chiffrées, distinctes du message original. Le lien entre le texte et sa signature n'est plus physique, mais logique. A la clé privée de l'expéditeur correspond une clé cryptographique publique, connue du destinataire, que celui-ci va utiliser pour déchiffrer la signature électronique et comparer le résultat au message original. S'ils correspondent, c'est la garantie que le message a été signé électroniquement par le titulaire de la clé privée correspondante et qu'il n'a pas été modifié ni altéré pendant sa transmission, puisque seul le titulaire de la clé privée peut générer une signature électronique et qu'il est (quasiment) impossible de la reconstituer en connaissant uniquement la clé publique. La confidentialité de la transmission est par ailleurs assurée si l'expéditeur du message le chiffre avec la clé publique du destinataire avant de le signer électroniquement avec sa propre clé privée. L'ensemble du processus est bien évidemment automatisé, quasi transparent pour l'utilisateur et ne prend que quelques secondes.

Pour parfaire la sécurité du système, il importe encore qu'une autorité de certification tierce (parfois appelée cybernotaire) atteste vis-à-vis de tous et notamment du destinataire d'un message signé numériquement que le titulaire de la clé privée qui a signé le message est bien une personne déterminée plutôt qu'une autre. La première tâche de l'autorité de certification est donc la vérification de l'identité de la personne en cause, par une apparition physique à un guichet d'enregistrement et la présentation de documents de légitimation. Sur cette base, un certificat électronique (sorte de passeport pour le monde virtuel) est établi, contenant en particulier le nom du client et la clé publique qui l'identifie vis-à-vis des tiers. Pour garantir son authenticité, ce certificat est signé électroniquement par l'autorité de certification elle-même, avant d'être mis à disposition de tous dans un registre librement accessible sur le réseau. L'autorité de certification doit enfin, le cas échéant, s'engager à suspendre ou à révoquer immédiatement un certificat s'il s'avère que son titulaire le demande ou que la clé privée a été perdue.

Dans un tel système, authentification, intégrité et confidentialité sont garanties, ce qui est bien entendu propre à renforcer la confiance des utilisateurs sur le réseau et à faciliter la preuve des transactions qui s'y déroulent.

Alors que la directive communautaire sur la question, adoptée en décembre dernier, règle non seulement le fonctionnement d'une PKI mais consacre également l'équivalence entre la signature manuscrite et la signature électronique, l'Ordonnance du Conseil fédéral se contente de prévoir les conditions juridiques, techniques et financières auxquelles autorités de certification doivent satisfaire si elles entendent être soumises à l'Ordonnance. Bien que volontaire, le régime est cependant incitatif si l'on considère qu'une autorité de certification reconnue jouira certainement d'une légitimité supérieure et du «label de qualité» officiel.

Sans entrer dans les détails, les conditions posées par l'Ordonnance ont trait en particulier à la qualification du personnel et à la solidité financière qui doit être suffisante pour faire face à l'éventuelle responsabilité qui découlerait d'une certification erronée. La responsabilité d'une autorité de certification peut en effet être engagée tant vis-à-vis de son client, au nom duquel elle a établi un certificat électronique erroné, que vis-à-vis des destinataires des messages signés électroniquement. De façon à renforcer la prévisibilité, l'Ordonnance prévoit que l'autorité de certification sera responsable en cas de certification erronée, à moins de pouvoir démontrer qu'aucune faute ne lui est imputable. Cette réglementation spécifique du régime de responsabilité est très certainement un des aspects importants de l'Ordonnance et devrait renforcer la confiance des utilisateurs. Dans ce même souci, l'Ordonnance prévoit également la possibilité d'obtenir des autorités de surveillance des fournisseurs des services de certification une attestation de la conformité et de la validité du certificat électronique à un moment donné, ce qui devrait faciliter la preuve des transactions, notamment dans le cadre de poursuites judiciaires.

Conclusion

Dans le cadre du commerce électronique les problèmes juridiques liés à la sécurité informatique sur un réseau ouvert comme Internet ne concernent pas en premier lieu la validité des contrats qui pourraient s'y conclure puisqu'une signature manuscrite et un support papier ne sont que rarement exigés par la loi pour les transactions en cause. La preuve n'est pas non plus impossible, même si elle risque d'être coûteuse, pour autant qu'elle s'appuie sur un ensemble de mesures préventives efficaces.

Dès lors, la véritable problématique juridique liée à la sécurité des transactions en ligne consiste à faciliter la preuve de l'intégrité des communications et l'identification des partenaires commerciaux sur le réseau, ce qu'une infrastructure à clé publique permet.

Dans cette perspective, l'entrée en vigueur de l'Ordonnance du Conseil fédéral sur les services de certification électronique constitue sans conteste un premier pas important vers la sécurisation du commerce électronique en Suisse. En choisissant une réglementation compatible avec les textes internationaux déjà existants, la Suisse démontre en outre qu'elle entend fournir aux acteurs de la Nouvelle Economie un environnement juridique et réglementaire adéquat. Cependant, un texte légal consacrant l'équivalence véritable entre la signature électronique et la signature manuscrite doit encore être adopté, et un projet de loi dans ce sens est d'ores et déjà annoncé dans les prochains mois. Espérons que le législateur suisse continue à ce rythme.

Quelques références bibliographiques et sites Internet utiles

Matthew D. Ford, *Identity Authentication and «E-Commerce»*, 1998 (3) The Journal of Information, Law and Technology (<http://elj.warwick.ac.uk/jilt/98-3/ford.html>).

Michel Jaccard, *Les relations juridiques et les responsabilités dans une infrastructure à clé publique*, in: "Geschäftsplattform Internet: Rechtliche und praktische Aspekte - Digitale Identität und Vertragsschluss im Internet", ZIK Band 10, Zurich 2000 (<http://www.schulthess.com/buch.htm>).

Michel Jaccard, *La conclusion des contrats par ordinateur Aspects juridiques de l'Echange de Données Informatisées (EDI)*, Berne 1996 (<http://www.staempfli.com/verlag/default.htm>).

Office fédéral de la justice, *Signature électronique et droit privé (droit des contrats)*, Avis de droit du 24 novembre 1998, JAAC 63.46 (<http://www.vpb.admin.ch/franz/doc/63/63.46.html>).

Matthias Ramsauer, *Die Public Key Infrastructur in der Schweiz*, in: "Geschäftsplattform Internet: Rechtliche und praktische Aspekte - Digitale Identität und Vertragsschluss im Internet", ZIK Band 10, Zurich 2000 (<http://www.schulthess.com/buch.htm>).

<http://www.swisskey.com/> (autorité suisse de certification).

<http://www.bakom.ch/> (Office fédéral de la communication texte de l'Ordonnance sur les services de certification électronique)

<http://www.uncitral.org/> (projet de loi uniforme)

<http://www.ispo.cec.be/ecommerce/legal/digital.html/> (Union européenne)

<http://www.tavernier-tschanz.com> (présentations, références et documents dans le domaine du e-commerce et du droit de l'informatique).

5 septembre 2000