

ÉCHANGES VIRTUELS : UNE QUESTION DE CONFIANCE

Commerce électronique, transactions à distance, trading : dans des domaines où la technique et le droit ne peuvent, à eux seuls, garantir la sécurité des échanges, la confiance devient une question centrale pour leur développement. Mais comment celle-ci peut-elle se construire dans un système d'échanges « *virtuels* » ? Qui en sont les nouveaux acteurs ? Quels en sont le statut et la crédibilité ? En s'appuyant sur des expériences de milieux diversifiés, peut-on dessiner une « *architecture de confiance* » favorable au développement de ces échanges ?

DÉBAT (*) ANIMÉ PAR **Gérard MOATTI**, SOCIÉTAL, AVEC LA PARTICIPATION DE : **Isabelle FALQUE-PIERROTIN**, CONSEILLÈRE D'ÉTAT, PRÉSIDENTE DU FORUM DES DROITS SUR L'INTERNET ; **Pierre-Noël GIRAUD**, DIRECTEUR DU CÉRNA, **Thierry DAUBIGNARD**, DIRECTEUR-ADJOINT DE GASELYS ; **Matthieu BERGOT**, CONSULTANT, ANCIEN DIRECTEUR MARKETING ET DÉVELOPPEMENT DE CERTPLUS. DÉBAT MIS EN FORME PAR **Jean-Paul SCHAEER**.

Le développement des échanges virtuels suppose la confiance dans le respect des engagements, qu'il s'agisse d'échanges entre un nombre limité d'opérateurs – comme dans les transactions sur les marchés financiers ou sur ceux des matières premières – ou que ces échanges impliquent une population importante – comme dans le e-commerce. La lenteur de ce développement est-elle liée à l'insuffisance des outils requis pour garantir la sécurité des échanges ? Le manque de confiance a-t-il d'autres causes ?

(*) *Rendez-vous des Annales des Mines*, séance du 30 mai 2002, organisé par le Club des Annales des Mines.

Quelles sont les raisons du retard de la France par rapport à d'autres nations et quels moyens sont-ils mis en œuvre pour y remédier ? (1)

LES QUESTIONS DE SÉCURITÉ SONT-ELLES PRIMORDIALES ? (2)

En matière de commerce électronique, le raffinement des dispositifs de sécurité technique, juridique

(1) Introduction de la conférence par Jacques MAIRE, président du Club des Annales des Mines, et Gérard MOATTI, *Sociétal*.

(2) Introduction par Ivan FAUCHEUX et Cyril SNIADOWER, ingénieurs des Mines et auteurs d'un mémoire intitulé *La sécurité du commerce électronique*, École des Mines de Paris, 1998.

ou de protection de la vie privée ne constitue pas une motivation suffisante pour inciter le consommateur à utiliser l'internet pour ses achats. L'étude que nous avons menée montre par contre que, quels que soient les niveaux de sécurité, le degré de confiance des utilisateurs joue un rôle essentiel lors de ces transactions.

Le défaut de sécurité lié au piratage du numéro de Carte Bleue ou du numéro de compte bancaire n'est, en fait, pas plus important sur l'internet qu'il ne l'est sur le minitel, lors de transactions par téléphone ou du fait de l'impression d'un récépissé d'achat : la médiatisation de l'affaire Klappisch – du nom de l'auteur d'une carte

bancaire passe-partout – n'a pas modifié les comportements du public, qui semble accepter les aléas liés à ce mode de paiement. Le risque de contrefaçon de signature n'est donc guère différent sur l'internet de ce qu'il est avec la signature sur papier.

Dans les transactions classiques, les échanges de faible montant (moins de mille euros) sont garantis par la banque – pour les achats par carte de crédit – ou par l'existence d'un abonnement ; les échanges de montant moyen (mille à cent mille euros) font l'objet de documents

d'un achat ; l'acheteur confiant et décidé va droit au but.

La confiance se construit donc avec le temps et il ne faut pas s'étonner que ce soit long, par rapport au temps nécessaire pour mettre en place des garanties de sécurité.

Le défaut de sécurité lié au piratage du numéro de carte bleue ou du numéro de compte bancaire n'est, en fait, pas plus important sur l'internet qu'il ne l'est sur le minitel, lors de transactions par téléphone ou du fait de l'impression d'un récépissé d'achat.

Le manque de confidentialité ne semble émouvoir personne, le développement de la cryptographie de 48 bits à 128 bits (ou même 256 bits) ayant à peine été remarqué par le grand public. Cette argumentation technique compte essentiellement pour les professionnels fournisseurs de produits et de services, comme les banques. Qu'il s'agisse de commerce électronique ou d'échanges traditionnels, le problème du respect des engagements et des voies de recours en matière de commerce international se pose donc dans les mêmes termes et l'existence d'un tiers de confiance y joue un rôle primordial.

signés – la commande, la facture – et, pour les échanges importants (plus de cent mille euros), le recours solennel à un tiers – le notaire – apporte la garantie de bonne fin.

Le tiers de confiance électronique peut être la banque (pour le portemonnaie électronique, par exemple), le livreur (comme La Poste), l'autorité de certification (qui concerne surtout le vendeur), ou le « *teneur de marché* » (celui qui connaît à la fois les vendeurs et les acheteurs).

Sur l'internet aussi, la confiance se construit : l'acheteur indécis se promène sur les sites, revient au site qui semble répondre à son besoin, s'acclimate jusqu'à décider

LE REGARD DE L'ÉCONOMISTE (3).

La chronique d'un voyageur génois du XV^e siècle rapporte le mécanisme d'échange entre des nomades du Niger et des sédentaires du Mali, sur les bords du fleuve Niger, dans un fort climat de méfiance : les nomades déposent de petits tas de sel sur la rive et se retirent ; les sédentaires prélèvent le sel qui, selon eux, équivaut

(3) par Pierre-Noël GIRAUD, directeur du CERNA, auteur de : *Le Commerce des promesses – Petit traité sur la finance moderne*, Paris, Éditions du Seuil, 2001.

aux petits tas d'or qu'ils déposent en échange, et se retirent ; les transactions se poursuivent jusqu'à ce que les quantités, objet du troc, apparaissent satisfaisantes aux uns et aux autres. La confiance se construit ainsi dans le temps, sans même que les opérateurs se rencontrent.

Georges Akerlof – couronné par le Prix Nobel d'économie pour ses travaux sur l'asymétrie d'information – utilise l'exemple du « *Market for lemons* » (le marché des voitures d'occasion) : si un vendeur propose trois véhicules d'un même modèle, apparemment remis en état mais en réalité très différents (l'un presque neuf, l'autre normalement utilisé, le dernier faisant courir des risques à l'acquéreur), l'acheteur informé du prix moyen du marché (l'Argus) hésitera, conscient de ce que le vendeur motivé par la recherche du profit lui proposera de préférence le véhicule en moins bon état. La transaction n'aura alors pas lieu.

L'asymétrie d'information sur la qualité d'un produit freine les transactions.

L'économiste distingue trois niveaux de connaissance de la qualité des produits :

- les produits standards, de qualité constante et communément admise ;
- les produits dont la valeur n'apparaît qu'à l'usage ;
- les produits dont la valeur n'est jamais prouvée (par exemple les produits verts).

Dans tous les cas, la confiance s'élabore par la répétition des transactions, à condition que la réputation du vendeur constitue pour lui un actif crucial et que sa défaillance fasse l'objet de publicité. Ces conditions sont réunies, même en l'absence de tiers de confiance, sur un marché où opèrent un petit nombre de vendeurs et d'acheteurs (marché des *swaps*

financiers, par exemple). Elles ne le sont pas sur les marchés du grand public, qui requièrent un certificateur (le contrôle technique, pour les voitures ; le guide gastronomique, pour les restaurants ; l'agence de notation, pour les produits financiers) ou lorsque la fluidité du marché repose sur l'existence d'intermédiaires (comme c'est le cas pour les produits dérivés).

Restent les questions auxquelles l'économiste est renvoyé à mesure qu'il approfondit le sujet : comment fonder la confiance dans le certificateur et dans l'intermédiaire, sachant que les certificateurs sont concurrents entre eux et qu'ils peuvent chacun faire de la publicité sur les dérapages des autres ? Quel est le rôle de l'État ? Celui-ci peut-il être le garant de l'objectivité requise ?

LA MAÎTRISE DES RISQUES DANS LE COMMERCE ÉLECTRONIQUE DE L'ÉNERGIE (4).

Joint-venture entre Gaz de France et la Société Générale, Gazelys a été créée pour réaliser des opérations de *trading* sur le gaz et l'électricité, rendues possibles par l'ouverture des marchés depuis deux ans.

Comme sur le marché du pétrole depuis dix ans, les relations s'organisent entre acheteurs et vendeurs, des services de compensation se mettent en place et des transactions à terme se développent, afin d'assurer la fluidité des échanges, de réduire les risques de contrepartie et d'insolvabilité. Et on peut imaginer une convergence, à l'avenir, entre les marchés du gaz, de l'électricité, du pétrole et du charbon.

Les risques sont de nature diverse

(4) par Thierry DAUBIGNARD, directeur adjoint de GASELYS.

et leur maîtrise appelle des réponses différentes :

- le risque juridique est maîtrisé au moyen de contrats-cadres entre les opérateurs ;
- le risque opérationnel (mauvaise compréhension d'un ordre, défaut de saisie...) est traité par la mise en œuvre de procédures strictes ;
- le risque de marché (lié à des variations brutales du prix) est contrôlé par une limitation des positions acheteur ou vendeur (les plafonds d'engagement autorisés) en fonction de la santé financière des contreparties ;
- le risque de blanchiment d'argent est limité par la vérification de l'origine des fonds, c'est-à-dire par la connaissance des acteurs.

Les *risk-managers*, indépendants des opérationnels, sont chargés, au sein de chaque organisation, de donner les autorisations, de fixer les limites des positions et de vérifier le respect des procédures.

Les plates-formes électroniques sont organisées par les pouvoirs publics (les bourses), des opérateurs privés (Enron...) ou des courtiers (ICE – International Commercial Exchange –, détenu par des banques, des producteurs et des traders).

Dans l'exemple d'ICE, les actionnaires garantissent la liquidité du marché, les relations sont automatisées et informatisées, mais le risque de contrepartie n'est pas supprimé ; ainsi, ICE a racheté la Bourse de Londres pour se doter d'une chambre de compensation. Mais le risque systémique demeure (l'effondrement en cascade des acteurs) et il serait sans doute utile d'harmoniser les réglementations qui diffèrent aujourd'hui entre les opérateurs industriels (dont le poids est déterminé par les actifs) et les opérateurs financiers (limités dans leurs engagements par les ratios prudentiels).

QUELS OUTILS DE SÉCURITÉ INFORMATIQUE POUR UN MONDE INFORMATIQUE SÉCURISÉ ? (5)

Le monde de l'internet est dominé par la défiance, du fait de la puissance de l'outil, des possibilités de piratage, de falsification des messages, de répudiation des engagements, d'intrusion dans la vie privée.

Mais la confiance repose sur des outils, une communauté des utilisateurs et un contrôle par des tiers. Les fonctions élémentaires de confiance sont alors :

- l'identité (l'authentification du nom des acteurs) ;
- l'intégrité (la conservation du contenu du document) ;
- la validité dans le temps (la date certaine et la durée) ;
- la protection du secret (le chiffrement).

Ces fonctions sont assurées par la signature électronique qui permet à la fois l'horodatage et l'archivage du document. Ce certificat, associé au document, est un fichier de 2 ko qui inclut une clé publique (garantisant les quatre fonctions de confiance) et la signature de l'autorité tierce. Une infrastructure à clé publique est un système d'organisation du domaine d'utilisation des certificats.

On distingue trois types d'acteurs dans le monde numérique :

- les utilisateurs (administrations, banques, prestataires de services de transport et de télécommunications, places de marchés, industries...);
- les tiers de certification, d'horodatage, d'archivage ;

(5) par Mathieu BERGOT, consultant, ancien directeur Marketing et Développement de CERTPLUS.

– les autorités de contrôle.

Un industriel comme Airbus a ainsi mis en place une infrastructure à clé publique pour la diffusion des manuels de maintenance de ses avions. Dans ce cadre, les compagnies de transport aérien et de maintenance sont responsables de la mise en œuvre des consignes à compter de la réception des

Le monde de l'internet est dominé par la défiance, du fait de la puissance de l'outil, des possibilités de piratage, de falsification des messages, de répudiation des engagements, d'intrusion dans la vie privée. (Stede Bonnet (? – 1718), ancien major de l'armée anglaise devenu pirate, devant le drapeau des boucaniers).

manuels et Airbus exerce les fonctions de l'autorité de certification dans ce domaine particulier.

Dans le cadre des États, c'est la législation qui définit l'infrastructure. Ainsi, en Europe, une série de directives communautaires et leurs textes d'application nationaux ont organisé en quelques années les modalités d'exercice des fonctions de confiance, de telle façon qu'aujourd'hui, la signature électronique a la même valeur que la signature sur papier.

CAUSES ET REMÈDES DU FAIBLE DÉVELOPPEMENT DU COMMERCE ÉLECTRONIQUE EN FRANCE (6).

Malgré les textes législatifs et les outils relatifs à la signature ou à la cryptographie, les transactions électroniques se développent lentement :

si la sécurité technique et juridique résulte du cadre fixé par l'État et des moyens mis en œuvre, la confiance, elle, résulte des comportements. Dès lors, comment créer la confiance ?

La réglementation ne permet pas d'imposer la confiance, elle ne répond pas à toutes les questions (quelle est la responsabilité des intermédiaires ? le statut juridique des liens hypertextes ?), elle est mal adaptée au commerce électronique, elle s'adapte trop lentement aux pratiques, elle n'est pas mondiale, elle s'applique mal à des cas de figures très diversifiés.

Depuis 1996, l'autorégulation a permis – surtout aux États-Unis – des avancées significatives avec la définition de labels (sur le respect de la vie privée, des procédures comptables...) ou la publication de codes de conduite (spécifiques à certaines professions) ; mais elle rencontre des limites inhérentes à son caractère professionnel (qui est chargé de contrôler l'impartialité des agences de notation ? celle des déontologues ?)

La corégulation, initiée en France par le Conseil d'État en 1998, concrétise un effort pour surmonter les tentations d'édicter des règles

(6) par Isabelle FALQUE-PIERROTIN, conseillère d'État, présidente du Forum des Droits sur l'internet.

unilatérales, publiques ou privées, pour piloter l'interaction entre les parties intéressées, construire la « civilité de l'internet », la coexistence pacifique.

Le Forum de l'internet a été créé pour répondre à trois enjeux :

- organiser la concertation entre acteurs publics et privés (industrie, associations, consommateurs, administrations...) sur des sujets comme le télétravail, les élections par voie électronique, ou d'autres ;
- informer et sensibiliser le grand public pour donner à chaque individu les outils qui lui permettent de maîtriser les risques qu'il prend et jouer pleinement son rôle d'arbitre ;
- faciliter l'ouverture internationale pour rapprocher les pratiques et susciter la mise en œuvre de règles communes.

DEBAT (7)

Question (Q) *Qui sont les clients du commerce électronique, peut-on les caractériser ?*

Réponse (R) Il n'existe pas d'enquête publique sur ce sujet ; il existe des enquêtes internes à chaque site, évidemment, mais elles distinguent surtout les « butineurs », qui cherchent de l'information, des « spécialistes », qui l'achètent.

Les *cookies*, placés dans l'ordinateur de l'internaute, constituent une source d'information considérable et la question des limites à l'utilisation de ces informations n'est pas tranchée : les États-Unis et l'Europe s'affrontent sur ce sujet. Un pacte a bien été signé, qui engage les entreprises nord-américaines à protéger la vie privée, mais rien n'en garantit le respect.

Q. *N'a-t-on pas tendance à sous-estimer le rôle de la sécurité comme fondement de la confiance ? La lutte*

contre les pirates, dont on connaît les ravages, la maîtrise des outils (signature, cryptographie) par la collectivité nationale quand on évoque la puissance des réseaux américains, tout cela n'est sans doute pas suffisant, mais c'est absolument nécessaire.

R. Il est vrai que la confiance repose sur la croyance en la sécurité, donc sur la qualité et la réputation des opérateurs de certification dans la collectivité.

Q. *Sachant que la réputation est – et doit être – un capital crucial, comment sanctionne-t-on un acteur défaillant ?*

R. Dans les opérations de trading, les échanges sont enregistrés et l'acteur qui ne respecte pas ses engagements est éliminé, que la transaction ait eu lieu par téléphone ou par l'internet. Cela se produit, mais rarement. S'agissant des transactions sur le vin de Bordeaux, par exemple, c'est aux professionnels qui ont défini un code de bonne conduite qu'il revient d'exclure le vendeur indélicat, et cela arrive parfois. Les fédérations professionnelles communiquent très bien entre pays dans de tels cas.

Q. *Ne faut-il pas faire de la publicité en cas de manquement d'un acteur sur l'internet ?*

R. Deux réponses à cette question : - la régulation et la corégulation se développent en effet à la suite de scandales : la publicité sur les fraudes et les sanctions prises permet donc de développer la confiance, car l'inquiétude vient surtout de ce que l'on ignore ;

- il faut donner la priorité au contrôle interne pour éviter et sanctionner les manquements.

Q. *Les experts de la sécurité n'ont-ils pas tendance à postuler, à tort, que la confiance repose sur eux ? À mon sens, la sécurité n'a qu'un lien ténu avec la confiance : la sécurité concerne le vendeur et les demandes de sécurité accrues ne sont que des facteurs de coûts supplémentaires ; la confiance est le seul souci du client et elle repose sur*

la puissance de la marque, celle des grands opérateurs reconnus, celle de la banque qui s'engage à rembourser les achats effectués avec votre carte.

R. Le débat reste ouvert, en effet.

Q. *La France a-t-elle mis en place des indicateurs relatifs à la confiance du grand public ? Comment être sûrs que la France met en œuvre les moyens nécessaires pour instaurer cette « civilisation de l'internet » ?*

R. Le Forum de l'internet oriente son action pour atteindre ces objectifs :

- auprès du grand public : il s'agit alors de fournir des informations fiables sur le cadre juridique et sur les risques, de répondre aux questions des internautes, de leur donner des recettes pratiques pour gérer leur identité, de gérer les cookies ;
- dans le cadre de la coopération avec le Ministère de l'Éducation Nationale : il faut, dans ce cas, faciliter l'éducation à l'internet et aux problèmes de sécurité ;
- dans les groupes de travail : il s'agit de traiter, avec tous les acteurs, les sujets en toute transparence, de clarifier les enjeux et les débats, d'élaborer un consensus. Pour connaître les efforts accomplis et à venir, il suffit de consulter le site www.forum-internet.org

CONCLUSION (8)

Deux points de vue s'opposent manifestement : l'un qui laisse aux fournisseurs de services le soin d'assurer la sécurité et de défendre leur marque ; l'autre qui souligne la responsabilité des pouvoirs publics et du citoyen dans l'avènement d'une civilisation de l'internet.

Communiquer sur ces sujets est aujourd'hui une nécessité impérieuse et la presse doit jouer un rôle majeur en matière d'éducation du public et d'information sur les fraudes.

(8) par Gérard MOATTI.

(7) Animé par Gérard MOATTI, qui a consacré un dossier de la revue *Sociétal* à l'internet...