

# La confiance se gagne avec le temps...

Jean-Séverin Lair (87),  
directeur technique, Certi Nomis

L'ÉCHANGE de courrier électronique, la consultation d'informations commerciales en ligne, le téléchargement de démonstration de jeux ou de logiciels professionnels sont autant d'applications qui se sont développées en quelques années grâce à l'Internet. Ces usages simples et largement diffusés ont cependant une caractéristique commune : ils ne nécessitent pas une confiance particulière de l'utilisateur, ils sont de nature informelle. Le commerce électronique a plus de mal à se développer, et l'achat complètement dématérialisé d'une voiture ou d'une maison ne semble pas encore envisageable.

## L'Internet : un nouveau monde ?

Fort de l'apparition d'Internet et de l'envolée de la nouvelle économie, certains ont prédit un changement radical de tous nos modes de vie. Cette révolution devait toucher notre façon d'acheter, notre façon de rencontrer nos congénères, et même notre façon de travailler, chacun pouvant rester chez soi...

Grisés par la technologie, ils en ont oublié une donnée substantielle du problème : l'utilisateur. Celui-ci a réussi à "survivre" avant de pouvoir accéder à Internet, et a déjà un passé et des habitudes.

L'être humain change moins facilement de comportement que les ordinateurs de système d'exploitation ! Il sait que, s'il se rend dans un magasin, il repartira avec le produit souhaité, ou pour un achat plus conséquent

avec un bon de commande en bonne et due forme qu'il pourra faire valoir. Qu'en est-il sur Internet ?

Ce que l'on nous a présenté comme une révolution des comportements n'était en fait que l'apparition d'un nouveau média de transmission de l'information. La simple existence de l'Internet ne suffit pas. Il faut donner à l'utilisateur le temps et les moyens de faire évoluer ses pratiques de manière progressive du monde physique vers le monde électronique dans un climat de confiance.

## L'Internet : méfiance ?

Outre la prudence naturelle de l'utilisateur, on évoque régulièrement les pirates sur Internet, ce qui ne fait rien pour le rassurer. Y a-t-il émergence d'une nouvelle criminalité allant de pair avec la nouvelle économie ?

Les pirates informatiques existent depuis que les ordinateurs se connectent entre eux par des réseaux, c'est-à-dire depuis plus de trente ans. Leur activité et leur compétence ont cependant bien changé. À l'origine l'attaquant devait connaître parfaitement l'ordinateur cible, les particularités de son système et ses protocoles de communication. En bref il devait être un spécialiste. Qui plus est, il lui fallait pouvoir atteindre l'ordinateur en se connectant physiquement sur son réseau. Maintenant avec un PC acheté à 1 000 € dans un supermarché, et un accès gratuit à Internet, un pirate peut attaquer la majeure partie des ordinateurs de la planète, et s'il n'est pas assez doué, il peut même aller se renseigner

sur des sites spécialisés. En réponse à cette évolution, la protection des systèmes d'information, nouvelle priorité des fournisseurs de services dématérialisés, apporte de réelles solutions.

Au-delà des raisons techniques de développement de la criminalité, la police doit améliorer son efficacité face à la délinquance informatique. Le rapport gain potentiel sur risque encouru dans le domaine de la cybercriminalité est parmi les plus élevés. Cela n'a pas échappé au crime organisé, qui a pris le relais des "gentils hackers bouton-neux". Les forces de l'ordre, conscientes du phénomène, redoublent d'effort.

L'Internet, fleuron du XXI<sup>e</sup> siècle, a d'abord ressemblé à une route moyen-âgeuse où le voyageur pouvait craindre de rencontrer un coupe-bourse derrière chaque arbre. Ce n'est plus le cas. La sécurité des systèmes d'information ne cesse d'être renforcée tant d'un point de vue technique que judiciaire.

## Le besoin de services de confiance

Sans être le bouleversement attendu, l'Internet peut permettre de développer ou de faire évoluer encore bien des services. Mais ceci passe nécessairement par la prise en compte du besoin naturel de confiance de l'utilisateur.

Ainsi le courrier électronique, qui est utilisé pour des échanges personnels, des prises de contact, la mise au point de rendez-vous, pourrait aussi être utilisé pour échanger des accords de confidentialité, des contrats... Mais on évite, en général, de l'utiliser quand on recherche une validité juridique.

Si la dématérialisation des circuits de commande se développe dans les grandes entreprises, une rematérialisation est encore souvent demandée pour en garder une trace probante.

Ne serait-il pas idéal de pouvoir traiter une commande entièrement en électronique, y compris l'envoi vers le fournisseur, qui en retour procéderait lui aussi à une facturation électronique ?

Dans un appel d'offres public, la soumission des offres avant l'heure fatidique sous forme électronique permettrait d'en alléger le traitement, d'éviter les photocopies, ainsi que les envois en urgence.

Pour ces trois exemples, et pour beaucoup d'autres, la technique est prête. Des solutions existent, et font l'objet d'offres commerciales.

Mais pour que ces services soient opérationnels et pleinement valides, on comprend bien la nécessité d'un cadre légal ou contractuel en plus de la technologie. On parle d'engagement, de contrat, et pour créer la confiance, il faut disposer de preuves d'une force juridique équivalente à celle des documents papiers.

## La pierre d'angle : la signature

Dans la plupart des démarches administratives et commerciales la signature est nécessaire. Le contribuable signe sa déclaration d'impôts, pour s'engager et peut être de ce fait redressé en cas de fausse déclaration. Le client signe sa commande d'une voiture pour exprimer son consentement à l'acte d'achat, et s'engage ainsi à payer à la réception. Dans beaucoup d'actes quotidiens la signature est la pierre d'angle de la confiance, elle garantit l'engagement du signataire, et elle a une grande portée en termes de droit.

Pour pouvoir faire des services de confiance dans le monde électronique, il faut une transposition de la signature tant dans son aspect pratique que dans ses implications juridiques. Techniquement envisageable depuis presque trente ans, la signature électronique est une réalité depuis seulement quelques années. En effet, elle nécessitait la mise en place d'infrastructures importantes <sup>(1)</sup> portées par

des professionnels, et le droit devait progressivement évoluer. Suivant de près la technique, le droit a fait sa place à la signature électronique dans la loi et les décrets sur la période 2000-2002.

Des applications concrètes permettent dès à présent de signer électroniquement sa déclaration de TVA auprès du Minéfi, des souscriptions d'assurance, des ordres de transfert de fonds... L'utilisation de l'Internet dans un contexte formel est désormais possible.

La signature joue certes un rôle central mais elle n'est pas la seule fonction nécessaire à l'établissement de la confiance dans le monde électronique. Tout doit être prévu pour parer ou résoudre les conflits. Par exemple si l'on veut pouvoir prouver qu'une information a été transmise en temps et en heure, il faudra obtenir une marque de temps électronique similaire au classique tampon de La Poste, une preuve d'horodatage. De même lors d'un litige autour du contenu d'un contrat signé il y a quelques années, il faudra retrouver l'exemplaire faisant foi au sein d'une archive électronique.

## Tiers de confiance

Toutes ces fonctions – signature, horodatage, archivage... – sont réalisées grâce à l'intervention de tiers, assurant les prestations techniques, et apportant aussi les garanties nécessaires à la naissance de la confiance. Ce sont les tiers de confiance.

Pour établir une relation de confiance entre acteurs qui ne se connaissent pas, le recours à des tiers a toujours été privilégié. Au Moyen Âge, les banquiers lombards se portaient garants des billets à ordre dans toute l'Europe. Dans le même ordre d'idées les notaires participent à la signature d'actes importants... L'intermédiation de tiers a permis les échanges de valeurs et la contractualisation même dans des temps troublés. Ce principe séculaire s'applique désormais à l'Internet pour créer un espace de confiance. Aujourd'hui comme hier les trois caractéristiques essentielles du tiers sont :

- sa neutralité, en l'occurrence son absence d'intérêt dans les échanges,
- sa pérennité, son service étant garanti

tant qu'il est utile, ce qui en termes de preuves peut signifier plusieurs dizaines d'années,

- et enfin sa légitimité, issue de la reconnaissance publique.

Il est aisément compréhensible que seuls des grands institutionnels peuvent avoir ces caractéristiques, et qu'il n'est pas possible de se proclamer tiers de confiance du jour au lendemain. Les institutions financières, La Poste, au même titre que la CDC, les ordres professionnels en sont de bons exemples. Tous sont déjà reconnus dans le monde physique depuis de longues années.

## La confiance : un chemin

La confiance ne se décrète pas, elle s'acquiert. Dans le monde des échanges physiques bon nombre de mécanismes et de procédures, appliqués chaque jour de manière anodine, permettent d'avoir confiance en nos actes. Retrouver cette confiance dans les échanges électroniques ne se résume pas à résoudre un problème technologique. Les solutions techniques sont nécessaires, mais la confiance est aussi une question de droit, de psychologie, voire de communication. Un changement de pratiques des utilisateurs ne s'opère pas du jour au lendemain, l'adoption progressive de la carte bancaire en est un bon exemple.

Le positionnement des institutionnels traditionnels de la confiance est indispensable au développement des services de confiance sur les réseaux. Tiers dans le monde physique, ils apportent dans le monde électronique leur caution et leur stabilité aux échanges, par nature fugaces, de l'Internet.

Toutes les conditions pour la généralisation d'un Internet de confiance sont aujourd'hui réunies.

Reste pour l'utilisateur, avec l'aide des professionnels du domaine, à découvrir progressivement tout ce qui lui est possible et qui pourra faciliter sa tâche au quotidien, en toute confiance... n

---

(1) Infrastructures à gestion de clés ou *Public Key Infrastructures* gérant les certificats électroniques, qui sont similaires à des cartes d'identité sur les réseaux et sont à la base de nombreux services de confiance (signature, horodatage...).