

à des internautes bien trop naïfs

Comment se fier à une information numérique par nature vulnérable ? En recourant à un “tiers de confiance” neutre, pérenne et légitime.

*Un pirate informatique peut usurper
une identité – la vôtre peut-être –
intercepter des mails, voire modifier leur contenu
à votre insu ou à celui de votre interlocuteur*

Depuis toujours, la confiance ne se décrète pas, elle s’acquiert et, aujourd’hui, le problème auquel nous sommes de plus en plus confrontés tient dans le fait que, professionnellement et personnellement, nous échangeons, communiquons et commerçons de plus en plus de façon dématérialisée, c’est-à-dire dans un monde virtuel. Alors que dans le monde matériel bon nombre de mécanismes et de procédures nous permettent de pouvoir accorder notre confiance à un document, une information ou tout autre support physique, dans le monde virtuel nous ne pouvons que très rarement utiliser ces repères.

Problème : passer du monde réel au monde virtuel

Dans le monde réel, de nombreux critères objectifs et subjectifs nous permettent, par exemple, de nous assurer de l’identité de notre correspondant, de son lieu de travail, de son appartenance à une entreprise ou à une administration. Ces mêmes critères ne sont pas utilisables “en l’état” dans le cadre des échanges dématérialisés.

C’est ainsi qu’il est tout à fait possible, pour un pirate informatique, d’usurper une identité, la vôtre peut-être, d’intercepter des communications de type mail, voire de modifier le contenu d’un courrier électronique à votre insu ou celui de votre interlocuteur.

Actuellement, et ce sont les statistiques qui le montrent, dans le cadre des échanges sur Internet, nous accordons plus facilement notre confiance à une “image de marque”, à la réputation d’un produit, à une ligne de produits connue, à la réputation du vendeur ou à celle du concepteur.

Les nouvelles technologies de l’information et de la communication représentent un formidable potentiel d’amélioration, de simplification et de rationalisation des procédures d’échanges, tant pour le secteur privé que pour le secteur public. En un mot, un facteur essentiel de productivité.

Les usages qui peuvent en être faits sont multiformes et il serait regrettable, pour notre avenir et pour notre compétitivité, de s’en priver.

Il faut bien l’admettre, l’information dématérialisée porte en elle-même des notions totalement contradictoires. En effet, l’information numérique est par nature vulnérable car elle peut être détruite, amputée, falsifiée, plagiée, dupliquée et modifiée à l’infini. De surcroît il est difficile de distinguer, en matière de dématérialisation, entre ce qui relève de l’original et de la copie.

Solution : le “tiers de confiance”

Pour établir une relation de confiance entre acteurs qui ne se connaissent pas, le recours à des “tiers de confiance” a toujours été la solution privilégiée. Dès le Moyen Âge, les banquiers lombards se portaient garants des billets à ordre qu’ils émettaient et qui étaient négociables dans toute l’Europe. Ils étaient de véritables “tiers de confiance” dont l’intermédiation a permis les échanges de valeurs en tout point de l’Europe, même durant les nombreuses périodes troubles.

C’est en reprenant le principe séculaire du “tiers de confiance” appliqué aux échanges sur Internet que des solutions dématérialisées à l’usage des entreprises, des personnes publiques comme des particuliers ont pu se développer.

Aujourd’hui dans l’univers de la dématérialisation, comme hier dans le monde du papier, les trois éléments qui caractérisent un véritable “tiers de confiance” sont sa neutralité, sa pérennité et enfin sa légitimité.

Pour être neutre, le “tiers de confiance” doit avoir une fonction et un rôle sans aucun intérêt direct avec les clients et partenaires pour lesquels il est opérateur. Pour assurer la pérennité du service, il doit pouvoir conserver les preuves des échanges et savoir les restituer

à qui de droit lorsque cela est juridiquement utile, ce qui en terme de preuves peut aller jusqu’à plusieurs dizaines d’années. Enfin la légitimité d’un “tiers de confiance” est issue d’une reconnaissance publique sous diverses formes comme, par exemple, la conformité à des critères juridiques et techniques.

Ces impératifs comportent des exigences fortes et vous comprenez donc aisément qu’il n’est pas possible de se proclamer “tiers de confiance” du jour au lendemain.

C’est ainsi que dans le monde Internet, par exemple, le “tiers horodateur” est un “tiers de confiance” qui remplace l’ancien “cachet de la Poste faisant foi”. De même, le “tiers archiveur” joue le même rôle que les “minutes du notaire” dans le monde réel. C’est pour cette raison que l’émergence de “tiers de confiance” référents est au cœur du développement des échanges dématérialisés. C’est l’une des conditions nécessaires au développement de relations solides et fiables entre tous les acteurs.

La confiance est et restera le fondement éternel des échanges et ce quelles que soient les technologies en usage.

Voilà pourquoi, dans l’univers de la dématérialisation et d’Internet, il est indispensable

de trouver plusieurs intermédiaires “tiers de confiance”, indépendants de l’émetteur et du destinataire, qui assureront, à chaque étape, les contrôles et les services nécessaires pour établir et garantir la confiance afin de créer une véritable “chaîne de confiance” assurant globale-

Dans le monde Internet, le “tiers horodateur” remplace l’ancien “cachet de la Poste faisant foi” ; le “tiers archiveur” les “minutes du notaire” du monde réel

ment la sécurité et la confidentialité des échanges dématérialisés.

Bien sûr pour que la “chaîne de confiance” soit incontestable, chaque “tiers de confiance” se doit d’être neutre par rapport au service qu’il apporte et donc, de ce fait, avoir une fonction et un rôle sans aucun lien direct avec les échanges pour lesquels il est opérateur ainsi qu’avec les autres “tiers de confiance” de la “chaîne de confiance” globale qui va de l’émetteur au bénéficiaire, voire à l’archivage.

Illustration : la facture électronique

Un exemple assez simple de mise en œuvre d’une “chaîne de confiance” dans le monde virtuel est celui de la facture électronique. En effet, dans un premier temps, on utilise un “opérateur de dématérialisation” qui transforme la facture en données électroniques. Un “tiers de correspondance” assure le transport du document électronique vers le client. Un “tiers horodateur” enregistre les dates et heures de chacune des opérations. Enfin, un “tiers archiveur” va conserver dans le temps la facture dématérialisée ainsi que toutes les informations qui lui sont associées.

Bien sûr une “chaîne de confiance” peut être plus ou moins complexe selon les cas et les exigences de l’activité concernée et de la législation en vigueur.

Accorder sa confiance dans un monde dématérialisé nécessite de contrôler la présence de “tiers de confiance” clairement identifiés au sein d’une véritable “chaîne de confiance”. C’est à ce prix que chacun d’entre nous pourra bénéficier sur Internet d’un véritable environnement technique, juridique et fiscal à la fois fiable, pertinent et pérenne.

Gilles de Chezelles,

Gérant d’A&G Project Management (www.ag-pm.com) et cofondateur d’AeSigne (www.aesigne.eu)

&

Bernard Schaming,

Avocat au barreau de Paris et président cofondateur d’AeSigne (Association européenne de la sécurisation des échanges dématérialisés et de la signature électronique)