**David Crochemore**[1]

# LES ENJEUX DE CONFIANCE ET DE SÉCURITÉ DANS L'UTILISATION DES TIC

Dans les mondes virtuels comme dans le monde réel, nous avons tous des besoins. Respirer, manger et boire sont nos besoins essentiels dans le monde réel. Abraham Maslow avait placé ces besoins physiologiques au niveau inférieur d'une pyramide hiérarchisant les besoins de l'être humain. Par analogie, on peut associer, dans la « société de l'information », ces besoins physiologiques aux besoins fondamentaux de l'*homo communicans* : accès à l'information, équipement, connexion et débit. On notera ici que ces besoins de premier niveau ne sont satisfaits que pour un faible nombre d'individus dans le monde, et que l'immaturité du développement de la société de l'information est donc soulignée par les multiples fossés numériques, entre le Nord et le Sud, le milieu urbain et le milieu rural, les jeunes et les anciens, les hommes et les femmes, etc...

Pour Maslow, les besoins de deuxième niveau sont liés à la protection, à la **sécurité** et à la **confiance** dans notre environnement. Le Sommet Mondial pour la Société de l'Information (SMSI) a pris en compte ces besoins de sécurité dans les documents publiés en décembre 2003 à Genève. Les paragraphes correspondant dans la Déclaration de Principe et dans le Plan d'Actions s'intitulent tous les deux *Etablir la confiance et la sécurité dans l'utilisation des TIC*.[1] D'après le texte de la Déclaration de Principe : « Renforcer le climat de confiance par des mesures garantissant notamment la sécurité de l'information et la sécurité des réseaux, l'authentification ainsi que la protection de la vie privée et du consommateur est un préalable au développement de la société de l'information et à l'établissement de la confiance parmi les utilisateurs des TIC ».

C'est la peur de l'inconnu qui induit souvent le manque de confiance. Dans la société de l'information, non seulement parmi les utilisateurs, mais également parmi les décideurs et les financeurs, il provient plus précisément de cette sensation de mal comprendre et de ne rien maîtriser vraiment. On connaît généralement peu ce que des individus mal intentionnés pourraient,

[1] David Crochemore est membre du Comité directeur du *Forum of Incident Response and Security Teams* – FIRST. (http://www.first.org)

sauraient ou voudraient faire subir à nos systèmes d'information, mais on sait encore moins ce qu'il leur serait techniquement possible ou impossible de faire. Cette double méconnaissance des *risques* pesant sur notre infrastructure de communication, et de *l'infrastructure* elle-même et de ses vulnérabilités, entraîne un triple manque de confiance : manque de confiance en les autres, manque de confiance en l'environnement technologique et manque de confiance en soi.

On sait que confiance et sécurité ne sont pas synonymes, et que la confiance se construit plutôt sur le *sentiment* qu'on a d'être en sécurité. Le premier vrai défi qui devra être relevé dans les années à venir, si l'on veut favoriser la confiance dans la société de l'information, est donc la clarification des menaces et la prise de conscience des risques réels encourus. Cela passe par la destruction des idées fausses autour de ces questions et la déconstruction d'une certaine mythologie qui s'est bâtie depuis une vingtaine d'année, depuis le film *War Games*[2] jusqu'à la couverture médiatique de certaines affaires récentes.

Parallèlement à cette meilleure compréhension des risques, il est nécessaire que l'*homo communicans* s'adapte mieux à son environnement de communication, et que cet environnement s'adapte mieux à l'être humain. Cela fait l'objet de deux autres défis. Pour se sentir plus confiant dans la société de l'information, il devra y retrouver des repères simples et compréhensibles qui lui permettent de s'orienter dans cette société. Ces repères sont non seulement temporels mais aussi topographiques. Ils devront être les plus proches possibles de ceux qu'il possède dans le monde réel. L'atténuation des différences n'implique pas un processus dans un seul sens : le monde réel commence lui aussi déjà à s'adapter à la globalité et à la vitesse des réseaux de communication. Il faudra donc que ce processus d'adaptation se poursuive, et que l'être humain *réel* possède des repères solides dans la société de l'information pour qu'il augmente le niveau de confiance qu'il peut y placer.

Ces trois premiers défis devront donc être relevés : clarification des risques, alignement des échelles de temps du monde réel et du monde virtuel, et rapprochement des géographies du monde réel et des mondes virtuels. Il restera un quatrième défi, probablement plus long et plus difficile : la maîtrise de l'identité numérique, qui soit à la fois acceptable et acceptée par tous, efficace mais qui ne porte pas atteinte à la vie privée de l'*homo communicans*.

## La clarification des risques et la fin de la mythologie

Lorsqu'on parle de sécurité dans la société de l'information aujourd'hui, on place dans ce thème un grand nombre de risques et de phénomènes différents : les virus informatiques, les défigurations de sites web, le vol d'information numérique, les vers Internet, l'usurpation d'identité, les saturations volontaires de trafic, les courriers électroniques non sollicités, etc... Ces phénomènes correspondraient, dans le monde réel par exemple, aux accidents de voiture, aux cambriolages, aux épidémies de grippe, aux

vols à la tire, aux graffitis sur des affiches ou des vitrines, aux escroqueries, aux incendies volontaires et à la publicité intempestive dans les boites aux lettres. Dans cette analogie, on voit bien que les sources des menaces sont différentes, les victimes potentielles sont différentes, les risques encourus sont différents, les moyens de se protéger sont différents, et les attitudes à adopter en cas de problème sont différentes. Ce qui est clairement visible et identifié pour la seconde liste ne l'est pas encore pour la première. On peut ajouter à cette confusion, l'amalgame qui permet d'associer médiatiquement aux délits entièrement intégrés dans la société de l'information, la simple utilisation de moyens informatiques pour des délits beaucoup plus classiques. C'est ainsi que l'on a pu qualifier de « pirate informatique » un adolescent qui avait fabriqué de la fausse monnaie avec une imprimante en couleur, ou que l'on confond souvent un moyen technique (les réseaux *peer-to-peer*[3]) avec le contenu illégal qu'il permet d'échanger, tel que de la musique protégée par le droit d'auteur, des films à peine sortis en salle ou des fichiers de pornographie enfantine.

Malgré les efforts pédagogiques importants entrepris depuis plusieurs années, en France et ailleurs, la sécurité des systèmes d'information reste encore considérée comme une nébuleuse incompréhensible par le grand public, l'affaire de spécialistes techniques et de leurs outils ; c'est un peu comme si l'on pensait que la sécurité routière devait être prise entièrement en charge par les constructeurs automobiles et les garagistes. Pourtant, de la même manière qu'un conducteur vigilant et respectueux du code de la route diminue fortement son risque d'accident, le respect par l'*homo communicans* de règles simples de comportement dans la société de l'information réduira considérablement le risque de subir un incident de sécurité. Il existe au moins deux raisons à cette difficulté de faire passer le message que la sécurité est l'affaire de tous : constructeurs, opérateurs, entreprises et utilisateurs. Primo, certains raccourcis publicitaires mensongers vantent encore les réseaux qui se protégeraient seuls et les solutions qui garantiraient sans effort une sécurité à 100%. Secundo, il s'est développé depuis une vingtaine d'années toute une mythologie autour du personnage du pirate informatique, tour à tour montré comme un petit génie, une menace impossible à contrer, voire un être doté de pouvoirs quasi surnaturels.

Il est donc très difficile pour le néophyte de connaître et de comprendre, au milieu d'un brouillard médiatico-cinématographique, les vrais risques et les moyens de se protéger contre eux. Il faudra donc, en continuant les efforts de formation et d'information, essayer de faire disparaître cette mythologie et faire admettre que la sécurité dans la société de l'information, comme dans la vie réelle, repose sur des comportements humains, simples mais constants. Mieux vaut une vigilance constante qu'une paranoïa intermittente ! La méconnaissance des menaces, dont il était question plus haut, entraîne un manque de confiance dans les autres membres de la société de l'information. La clarification des risques devra lever cette inconnue et permettre ainsi le développement de la confiance.

**Le rapprochement des échelles de temps *protection*/*détection*/*réaction***

Cependant, nous n'avions pas évoqué uniquement la méconnaissance des menaces pesant sur l'infrastructure, mais la méconnaissance de l'infrastructure elle-même. On vient de le voir, aucun système de protection n'est efficace à 100%. Beaucoup d'experts s'accordent à dire qu'il ne faut pas chercher à exprimer le niveau de sécurité en taux de protection (quel serait le sens d'une protection à 95% ?), mais plutôt en *temps* de protection. Comme dans le cas d'un coffre-fort, quel serait le temps que mettrait un individu mal intentionné ordinaire pour porter atteinte à un système d'information donné ? En combien de temps peut-il voler des informations, modifier des données, ou rendre le système d'information inaccessible ? Plus le temps de protection est long, mieux le système est protégé. Cependant, comme dans le cas du coffre-fort, si un voleur a le loisir d'essayer toutes les combinaisons possibles du coffre sans être inquiété, même si ce temps est long, il finira par réussir. On peut donc affirmer qu'un système d'information est bien protégé lorsque son temps de protection est supérieur au temps qu'il faut pour détecter une attaque et réagir pour la contrer.

Aujourd'hui, le temps de protection de beaucoup de systèmes est assez court, car la protection n'a pas été pensée de manière globale dès le départ, mais seulement comme l'addition hétérogène et désordonnée d'un ensemble de briques techniques de protection. Chacune de ces briques peut être solide, mais l'ensemble est troué et fragilisé par le manque de cohérence. Là encore, dans les systèmes d'information de très nombreuses organisations, ce sont les effets de mode et la publicité qui décident des investissements en sécurité : « Il nous faut un pare-feu ! » - « Avec notre antivirus, vous n'aurez plus de problème de sécurité ! », ou encore « Il parait que la biométrie, ça marche ». Seule une minorité des entreprises affirme avoir défini une politique globale de sécurité des systèmes d'information[4], et pourtant, c'est le seul moyen d'augmenter *réellement* le temps de protection, en prenant en compte les aspects organisa-tionnels, techniques et humains de tous les éléments élémentaires du système d'information et de leurs interactions. L'échelle de temps caractéristique de la protection représente l'échelle de temps typique des réseaux de communication, car elle ne dépend que du système d'information et des menaces extérieures. Allonger ce temps de protection revient donc à rapprocher l'échelle de temps de la société de l'information, qui s'exprime en millisecondes et en secondes, avec celle du monde réel, où l'on parle plus facilement d'heures ou de jours.

Dans le même élan, réduire les temps de détection et les temps de réaction - qui sont des activités essentiellement humaines - revient à diminuer l'échelle de temps typique dans le monde réel, et donc la rapprocher de l'échelle de temps dans la société de l'information. Aujourd'hui, le temps de détection d'un incident peut être parfois très long, en particulier parce que la complexité des systèmes rend difficile cette détection. L'amélioration croissante de la compréhension des systèmes et l'utilisation de plus en plus répandue d'outils d'aide à la détection d'intrusion devraient contribuer dans un futur proche à la réduction du temps moyen de détection des incidents de sécurité dans la société de

l'information. Mais, le temps de réaction, dans beaucoup de cas est aujourd'hui infini, aucune structure experte n'étant en place pour l'analyse et l'apport de la réponse adéquate à une attaque. Il faut donc chercher à rapprocher les échelles de temps *protection*/*détection*/*réaction*, en réduisant significativement les délais de réaction. C'est le rôle des CERTs (*Computer Emergency Response Teams*), qui existent depuis 1988 et du FIRST (*Forum of Incident Response and Security Teams*), qui regroupe les CERTs et les aide à améliorer leur expertise. Le FIRST diminue également le temps de réaction global en mettant les équipes en réseau et en accélérant les flux d'échanges d'informations. C'est en favorisant le développement de ces équipes de sécurité en lesquels les utilisateurs des outils de communication peuvent avoir confiance en cas de coup dur, qu'on élèvera le niveau global de confiance qu'ils ont dans la société de l'information.

**Réduire l'inadéquation entre topologies des réseaux et géographie du monde réel**

Cependant, accélérer le flux d'information et rapprocher les échelles de temps entre le monde réel et le monde virtuel ne suffit pas toujours, car les topologies physiques des réseaux de communication sont également complètement différentes de la géographie du monde réel. Les services d'urgence chargés de sécurité et de secours dans le monde réel (polices, pompiers, SAMU...) sont organisés selon des schémas géographiques, locaux, régionaux ou nationaux, adaptés aux réalités topographiques. Si l'on prend en compte la topologie des réseaux, ce découpage géographique n'est ni adéquat ni opportun. Quelle serait en effet la raison d'organiser localement au sens géographique (dans une ville) les équipes de sécurité pour tous les utilisateurs des réseaux de communication de cette ville ? En effet, deux voisins pris au hasard dans le monde réel n'ont qu'une probabilité infime d'être également voisins dans la société de l'information, c'est-à-dire d'utiliser les mêmes réseaux, les mêmes services, et d'être en communication l'un avec l'autre par ces moyens. La notion de *proximité* dans la société de l'information doit donc être analysée et traitée avec plus de soin. En tout cas, sans prise en compte de la proximité, même virtuelle, la confiance aura beaucoup de mal à se développer.

On pourrait par ailleurs croire qu'Internet n'est qu'un seul grand réseau sur lequel on pourrait calquer les frontières politiques existantes. En réalité, il existe de multiples découpages, suivant qu'on observe le réseau comme interconnexion de réseaux d'opérateurs et de fournisseurs d'accès, ou qu'on étudie la multitude des services et applications qui forment autant de sous-réseaux distincts avec leur propre topologie. Il n'existe donc pas une seule topographie de la société de l'information, mais une multitude de communautés, à des niveaux et de natures très différents. Ces communautés peuvent regrouper les clients d'un fournisseur d'accès donné, des utilisateurs d'une messagerie instantanée, les abonnés d'une liste de diffusion ou d'un forum de discussion, les employés d'une même entreprise, les utilisateurs d'un même système d'exploitation, les membres d'une même administration publique ou les abonnés à un service interactif.

Dans ce cas, créer des organismes chargés de veiller à la sécurité de ces multiples sous-réseaux est un défi très difficile à relever. La tentation de structurer ces réseaux pour les faire entrer dans un cadre géographique traditionnel sera vouée à un échec au moins partiel. Par exemple, tous les mécanismes de filtrage de sites de la *toile* pour un ensemble territorial donné ont toujours été contournés très facilement. De plus, la confiance dans les organismes chargés de sécurité et de secours dans le monde réel provient en grande partie du fait que le découpage apparaît naturel et adapté, et là encore, la proximité joue un rôle essentiel. A contrario, l'auto-régulation au sein de ces réseaux virtuels pourrait régler certains problèmes légers, mais montre rapidement ses limites pour les incidents plus importants.

Il est donc nécessaire de trouver des solutions originales qui puissent s'adapter aux différents réseaux virtuels tout en respectant les contraintes topographiques du monde réel. Ce n'est qu'en parvenant à un tel équilibre qu'on pourra fournir à *l'homo communicans* un environnement dans lequel il pourra avoir confiance. Pour être propice au développement naturel de la confiance, l'environnement de l'être humain dans la société de l'information devra donc se rapprocher de celui du monde réel dans ses repères spatiaux et temporels. Après la méconnaissance des autres, ce sera celle de l'environnement qui se dissipera en partie. Il restera alors un enjeu pour la confiance dans la société de l'information : la gestion de l'identité numérique.

**Améliorer les processus d'authentification, sans atteinte à la vie privée**

Qui dit « société de l'information » dit « authentification », à la fois des informations et de leurs auteurs, mais aussi pour l'accès aux informations. Formellement, l'authentification a pour but de vérifier l'ensemble des droits dont une entité se réclame, ces droits étant généralement attachés à une identité. On parle donc souvent d'une phase d'identification-authentification, comme de la séquence où l'entité (humaine ou machine) décline son identité (identification) puis en apporte la preuve (authentification). Dans le passé, l'identification-authentification numérique se limitait à quelques identifiants et mots de passe. Aujourd'hui, nous devons retenir de nombreux codes de cartes de crédit, mots de passe, digicodes, codes porteur[5]... Demain, on nous annonce des moyens révolutionnaires d'authentification qui s'appuient sur la biométrie, les cartes à puces, les étiquettes intelligentes, les infrastructures de clés publiques, et d'autres technologies, encore en développement.

Malheureusement, il existe souvent dans les solutions commerciales proposées pour permettre la *sécurisation* des systèmes d'information, une confusion entre ces concepts d'identification et d'authentification. Comme le rappelait par exemple Philippe Wolf[6], responsable du centre de formation à la DCSSI[7], « *l'utilisation de la biométrie comme moyen d'authentification dans le cadre d'une politique de sécurisation d'un système d'information*

*est à déconseiller*. » Il avance deux raisons principales : d'abord qu'une donnée biométrique est une donnée publique (une empreinte digitale peut être récupérée), qu'elle peut donc être recopiée et utilisée facilement ; ensuite qu'elle ne peut pas être modifiée ou révoquée. On ne peut pas changer de doigt comme on doit changer de mot de passe tous les deux ou trois mois. La biométrie serait donc un exemple d'amélioration de l'identification, mais pas du tout un moyen d'authentification.

Au-delà même de cette confusion entre identification et authentification, il est très important de comprendre le rôle de l'être humain dans ces processus. Même s'il s'agit d'identité *numérique*, les conventions permettant l'authentification d'un individu dans la société de l'information sont les mêmes que pour l'identité dans le monde réel. Elles reposent sur : ce que l'on sait : un secret partagé, tel qu'un mot de passe ou un code porteur ; ce que l'on possède : un objet défini, tel qu'une carte à puce ou une clé ; ce que l'on sait faire : un savoir-faire, tel qu'une signature manuscrite ; ce que l'on est : une caractéristique physique, telle qu'une empreinte biométrique.

Il est important de se souvenir que la combinaison de plusieurs de ces méthodes renforce le processus d'authentification, mais que la tendance actuelle à utiliser de moins en moins la première méthode (*ce que l'on sait*) au profit des autres, permet sans doute de limiter les risques d'oubli, mais peut se révéler une tendance dangereuse. En effet, c'est *ce que l'on sait* qui caractérise le mieux l'être humain. *Ce que l'on possède* peut être volé, *ce que l'on sait faire* peut être imité, *ce que l'on est* peut être usurpé, mais *ce que l'on sait* peut plus difficilement être deviné. L'amélioration de la technique des processus d'authentification ne doit donc pas se faire au prix d'une augmentation de la vulnérabilité aux attaques du processus lui-même, en oubliant que c'est un être humain qu'on cherche à caractériser, même de façon numérique.

Le fait le plus paradoxal dans la gestion de l'identité numérique est donc que pour obtenir une bonne authentification à des fins de sécurité, pour augmenter la confiance, on doit demander à l'*homo communicans* de fournir une authentification forte de sa personne, mais que s'il doit s'identifier à chacun de ses gestes dans la société de l'information, l'utilisateur se sentira suivi, traqué, et l'ombre de Big Brother empêchera le développement réel de la confiance. En fait, garantir la sécurité tout en respectant la vie privée et les droits de l'Homme n'est pas une problématique nouvelle de la société de l'information, mais elle est assurément exacerbée par toutes les possibilités technologiques nouvelles.

*

Les quatre défis qui doivent être relevés pour que les utilisateurs des réseaux de communication accroissent pour des raisons reconnues la confiance qu'ils placent dans la société de l'information paraissent donc simples à formuler : clarifier les risques encourus dans la société de l'information pour mieux y faire face, rapprocher les repères temporels des

réseaux de communication et ceux du monde réel, rapprocher les repères géographiques des mondes virtuels et ceux du monde réel, et enfin améliorer la prise en compte de l'identité numérique sans entrave à la vie privée.

On peut remarquer qu'aucun de ces défis ne pourra être relevé uniquement par des moyens technologiques, au contraire. Il est temps de reconnaître que pour garantir la sécurité au sein de la société de l'information, la technologie ne reste qu'un outil neutre au service des êtres humains. Grâce à la formation, à l'information, à la sensibilisation, les utilisateurs peuvent apprendre des comportements qui leur permettront de mieux réduire la plupart des risques de sécurité et leurs conséquences.

Le développement de la société de l'information repose sur la confiance que les citoyens de l'information veulent bien y placer. Cette confiance repose elle-même sur le sentiment de sécurité qu'ils ressentent. Elle ne se décrète pas. Elle se développe lentement et se nourrit de l'accroissement de la compréhension globale et réelle des enjeux de la sécurité dans la société de l'information. Améliorer la compréhension est une activité humaine, adapter la société de l'information à l'être humain ne doit pas être envisagé sous un aspect technique, et l'évolution de la gestion de l'identité numérique ne doit pas être analysée sur des critères purement technologiques. Derrière chaque *homo communicans* se cache un être humain, et la confiance qui est une notion humaine ne peut se développer qu'au sein de cet être humain.

**Notes :**

[1] Ces textes peuvent être téléchargés à : http://www.itu.int/wsis/documents/

[2] *War Games* : film américain de 1984 dans lequel un jeune passionné d'informatique, voulant pirater des jeux vidéo, se branche sur un ordinateur secret de l'armée américaine. Croyant être aux commandes d'un jeu virtuel, le garçon déclenche sans le savoir le compte à rebours d'une troisième guerre mondiale.

[3] Réseaux d'échange direct de fichiers entre internautes

[4] 36% seulement selon la dernière étude publiée par le CLUSIF : https://www.clusif.asso.fr/fr/production/sinistralite/docs/etude2002.pdf

[5] Code porteur (en français) pour PIN code (en anglais)

[6] *De l'authentification biométrique*, dans le numéro 46 (octobre 2003) de la revue *Sécurité Informatique* du CNRS. L'article est disponible sur le site web : http://www.cnrs.fr/Infosecu/Revue.html

[7] DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information.