



# La sécurisation des sites de banque : exiger l'excellence

*La nature internationale du réseau internet et le caractère sensible des informations en circulation, imposent aux banques un souci constant de la sécurité.*



CATHERINE MARTY

Attachée juridique

Fédération bancaire européenne\*

**L**es services et produits financiers, d'ores et déjà largement dématérialisés dans nos économies, se prêtent aisément à une offre sur internet démultipliée et très accessible. Sur le réseau, les banques directes, les sociétés non financières ainsi que les banques traditionnelles cohabitent désormais pour pratiquer ce qu'il est devenu commun d'appeler «l'internet banking». Un tel phénomène s'accompagne de certains écueils et problématiques, notamment en matière de sécurité et de protection des données à caractère personnel qui circulent sur le web.

Car, par nature, les sites de banque véhiculent des informations financières sensibles même en dehors de tout acte de vente. Aussi les institutions bancaires se doivent-elles de proposer à leurs clients un niveau de confidentialité identique à celui dont ils peuvent bénéficier en usant de moyens de communication et d'échange plus conventionnels.

## DES EFFORTS À POURSUIVRE

En 1998, les principales banques allemandes (Deutsche Bank, Commerzbank, BfG Bank) ont donné l'exemple en se regroupant afin de créer un standard de sécurité commun sous la dénomination de Homebanking Computer Interface. L'objectif poursuivi était de susciter un climat de confiance vis-à-vis de la clientèle en lui proposant un cadre de transactions sécurisé et donc à terme de la fidéliser. Depuis, si d'autres initiatives ont fleuri au gré des innovations technologiques, elles n'ont pu créer un environnement sécurisé totalement satisfaisant.

Une étude réalisée en France par la société Projetweb<sup>1</sup> entre janvier et mars 2001 sur 104 sites de banque<sup>2</sup> doit nous interpeller à plusieurs titres. Entre autres, il apparaît que deux sites sur 104, n'offrent en réalité aucune sécurisation des données des internautes. Aussi peuvent être interceptés en clair les numéros de cartes bancaires qui ne sont aucunement protégés. Le niveau de cryptographie est également, pour 74 % des sites visités, inférieur à 128 bits<sup>3</sup>.

Un effort est donc de mise. Le capital de confiance dont les institutions financières bénéficient auprès du grand public ne peut être entamé et, plutôt qu'en user en terme d'alibi, il devrait stimuler une exigence de sécurité encore plus grande. Cela est vrai pour tout prestataire de services en ligne : on ne peut exiger du consommateur d'initier des habitudes de consommation nouvelles sans lui assurer en retour que celles-ci lui seront non seulement bénéfiques mais que sa prise de risques sera la mieux contenue possible. Il importe aussi que l'information sur le cryptage en particulier et les questions de sécurisation en général soit accessible au consommateur/client et

**«Il importe que l'information sur le cryptage et les questions de sécurisation soit accessible aux consommateurs de la manière la plus immédiate possible.»**

\* [www.fbe.be](http://www.fbe.be). Cette contribution n'engage que l'auteur.

<sup>1</sup> Société de services internet de seconde génération : <http://www.projetweb.com/>

<sup>2</sup> Sites de banque présentant une partie de type «accès aux comptes» ou «accès clients» ou encore «accès membres». Site de bourse permettant de passer des ordres de bourse, à l'exclusion des sites permettant uniquement de consulter les cours de bourse.

<sup>3</sup> Taille maximale de clé d'accès libre et qui assure un niveau de protection optimum.

## Opérations financières à distance : l'importance de l'identification

➤ L'ouverture d'un compte à distance illustre l'évolution des rapports entre la banque et son client et met en lumière l'intérêt des procédures d'identification techniquement innovantes. Les contraintes liées à l'ouverture traditionnelle d'un compte sont bien connues : nécessité d'une présence physique, écrit original signé, limitation territoriale. Est bien connue aussi l'obligation à la charge de l'institution financière de connaître son client. Son devoir de prudence la conduit à vérifier aussi bien la réalité du domicile du client que l'identité du postulant. Aussi le défaut ou l'insuffisance de ces contrôles engage-t-il la responsabilité de l'institution elle-même. Cette obligation de vigilance est légitime à plusieurs titres : la lutte contre le blanchiment de capitaux, la protection du consommateur (obligation d'information) comme la nécessaire garantie de la confidentialité des transactions (respect du secret bancaire). Dans la plupart des pays membres de l'Union, il n'existe pas de

dispositions réglementaires particulières pour l'identification du client en cas d'opérations à distance. Des solutions alternatives ont été mises en place tels la certification d'identité par une autorité qualifiée (notaire, ambassade...), l'envoi de documents par courrier recommandé, le contrôle par appel téléphonique ou auprès de l'employeur, ou encore à partir de listes électorales. En toute hypothèse, le maître mot doit demeurer la flexibilité. L'objectif d'identification adéquate est maintenu, les moyens d'y parvenir doivent être aussi souples que possible et découler du libre choix des institutions financières elles-mêmes<sup>1</sup>. A ce titre, la reconnaissance légale de la signature électronique et du rôle des autorités de certification<sup>2</sup> peut répondre aux exigences spécifiques qui sont celles du secteur bancaire en matière d'identification des personnes.

Le déploiement à plus grande échelle d'outils technologiques au service de la signature électronique demeure donc primordial. Pourtant, à l'analyse des dispositions de la directive, quelques remarques s'imposent.

### LES APPORTS DE LA DIRECTIVE

Tout d'abord, celle-ci ne s'intéresse qu'aux aspects probatoires et non aux questions relatives à la validité des contrats. C'est-à-dire que les Etats membres restent libres de maintenir les exigences formelles relatives à la conclusion des contrats tout en reconnaissant que lorsqu'un écrit est exigé, cette exigence peut être satisfaite par la signature électronique. Concernant le marché des services de certification, ce dernier n'en est aussi qu'à ses débuts et son fonctionnement demeure onéreux et complexe. Enfin, la réglementation communautaire gère la problématique de la preuve, pas la crainte

à laquelle le consommateur internaute lambda succombe lorsqu'il commerce sur internet ! Le travail de sensibilisation et de mise en confiance est la tâche des professionnels engagés dans les activités en ligne. Le consommateur a besoin de raisons convaincantes pour intégrer les réflexes d'un internaute. Il est enfin très remarquable qu'à l'heure d'internet, la signature, bien éminemment personnelle, en transitant par un tiers, semble ne plus appartenir tout à fait à son détenteur originel. Autre signe singulier de changement d'époque...

<sup>1</sup> Cf. la position commune du Conseil du 30 novembre 2000 en vue de la révision de la directive sur le blanchiment de capitaux de 1991 (91/308/CE). L'annexe à la proposition relative à l'identification à distance des opérations financières a été supprimée. Des dispositions plus générales et moins contraignantes ont été incorporées dans le corps du texte.

<sup>2</sup> Telle qu'opérée par la directive 1999/93/CE du 13 décembre 1999 sur la signature électronique qui en fixe le cadre légal communautaire.

ce de manière la plus immédiate possible. Ce qui n'est manifestement pas le cas, en effet 70 sites sur les 104 testés ne semblent donner accès à aucune information en la matière. Or, l'importance de la transparence de et dans l'information est primordiale. Nos attentes, à titre individuel, en termes de protection de la vie privée, sont de plus en plus grandes et monopolisent plus que jamais l'attention et l'intérêt des consommateurs. Le secteur bancaire ne peut donc

faire l'économie d'y consacrer l'énergie et les moyens nécessaires.

A cette fin, les sites de banque devraient avoir systématiquement recours à des techniques de sécurisation probantes qui sont maintenant très bien connues. Sur la forme, l'architecture des sites devrait être à la fois simple et lisible et capable de créer au bénéfice du consommateur un sentiment de sécurité et d'efficacité qui conforte sa démarche d'internaute. ●