Commerce électronique

Ivan Faucheux, Cyril Sniadower

COMMERCE ELECTRONIQUE : DE LA SECURITE A LA CONFIANCE

IVAN FAUCHEUX & CYRIL SNIADOWER

30 juin 1999

On est plus souvent dupé par la défiance que par la confiance.

Cardinal de RETZ, *Maximes et réflexions*

Remerciements

Nous tenons à exprimer notre gratitude aux personnes qui nous ont aidés à la rédaction de ce texte.

Pour les renseignements et l'aide qu'ils nous ont fournis, nous remercions tout particulièrement Mmes CADOUX, LEGOURRIEREC, NARBONNE, MM. ARDITTI, BLANCHET, BOUJENAH, BOURNON, CAPRIOLI, CHASSIGNEUX, COINTE, DARDAYROL, DEBOUT, DEBOUZY, DECAVELE, DESSAPT, DUCHER, FAYARD, LEVY, LIEVEN, MEGLE, NGO, NORA, PLICHON, SALLIO, STERN et VILLOING.

Pour les suggestions qu'ils ont formulées tout au long de la conception de ce document, nous exprimons notre reconnaissance à Mme GAUTHIER ainsi qu'à l'ensemble des membres de la Commission des Mémoires.

Table des matières

Introduction

« Internet, c'est comme une lame de fond de 6 mètres de haut qui arrive, et nous sommes ici en train de pagayer dans nos kayaks. Elle a parcouru des milliers de kilomètres à travers l'Océan en grossissant sans cesse, et maintenant elle va nous soulever et nous laisser retomber. »[1]

Derrière Internet et l'abondante littérature qui en parle, il est souvent difficile de se faire une opinion sur la réalité du phénomène et ses conséquences éventuelles, notamment sur le commerce et les échanges. Il est tentant d'y voir un simple effet de mode, un engouement passager qui retombera avec le temps. Il est cependant sensé d'envisager que pour certains produits, notamment pour les produits dématérialisés, le commerce électronique changera de façon significative les circuits actuels de vente.

Les Français ont acquis une certaine habitude de l'usage de la télématique et des réseaux dans le commerce. Les services Minitel ont ainsi généré en 1996 près de 10 milliards de francs de chiffre d'affaires, soit deux fois plus que les estimations du chiffre d'affaires du commerce électronique aux Etats-Unis[2] cette même année. Ces chiffres surprenants ne doivent pas cacher l'ampleur du phénomène qui se prépare : le Minitel, qui était techniquement en pointe au début des années 80, est aujourd'hui complètement dépassé. Dès que le succès commercial d'Internet aura atteint un seuil critique, ses atouts technologiques entraîneront un développement qui n'en sera que plus rapide.

En 1998, l'institut d'études *Benchmark Group* a mené une enquête auprès de soixante sites français particulièrement actifs en matière de commerce électronique. Si les achats effectués en ligne représentent une part encore très modeste, celle-ci va néanmoins croissant. Ainsi aux Etats-Unis, les achats en ligne du grand public sont estimés à 2,6 milliards de dollars en 1997, soit deux fois plus que l'année précédente. Cette progression devrait se poursuivre au même rythme dans l'avenir. Côté commerce interentreprises, le commerce *Business to Business (B2B)* représentait déjà 7 milliards de dollars en 1997 et pourrait atteindre plus de 300 milliards de dollars en 2002[3]. Pour la France, les chiffres sont bien entendu plus modestes. Les estimations font état d'un chiffre d'affaires en 1997 de 50 millions de francs. Pour l'instant, les produits qui se vendent le plus sur Internet sont les produits de grande consommation (livres, voyages, cédéroms) et les produits électroniques (ordinateurs, logiciels). Les analystes estiment que le volume du commerce électronique sur Internet devrait dépasser celui du Minitel vers les années 2000 – 2001.

---

[1] *Fortune*, 8 juillet 1996, interview d'A. GROVE, PDG d'Intel.
[2] Les estimations vont de 500 millions de dollars à 5 milliards de dollars, mais le consensus s'est établi autour de 1 million de dollars.
[3] Source : Forester Research

Le potentiel de croissance du commerce électronique est immense. Pourtant, on pouvait lire dans *Les Enjeux* d'octobre 1996 : « Dans leur majorité, les « cyberpatrons » ne voient pas dans Internet le vecteur capable de bousculer leurs relations aux clients et aux fournisseurs, l'image de l'entreprise ou leur mode de management... Le « réseau des réseaux » a encore des allures de couteau suisse : un beau jouet qu'on aime montrer, si grisant avec tous ses gadgets... Mais qu'on utilise peu et dont on oublie qu'il peut blesser. »

Les initiatives se multiplient pour faire prendre conscience aux entrepreneurs et aux consommateurs de l'importance du commerce électronique. En mars 1997, à l'initiative de l'Union européenne, s'est tenu un colloque intitulé : « Le commerce électronique, facteur de croissance des PME ». Depuis son arrivée au pouvoir, le gouvernement JOSPIN n'a cessé d'afficher son intérêt pour les nouvelles technologies de l'information et tente, par diverses modifications de la législation, de promouvoir ce nouveau moyen de communication. Le gouvernement français n'est pas le seul à s'engager dans cette voie, de nombreuses initiatives voient également le jour dans les pays étrangers.

Commerce en ligne, galeries marchandes et boutiques virtuelles, vitrines attractives, forums de discussion, conclusions directes de contrats entre entreprises, ou entre professionnels et consommateurs ; nouveaux marchés, internationalisation des échanges, possibilité d'acheter en temps réel des produits du bout du monde, création d'entreprises entièrement virtuelles ; le commerce électronique ne laisse pas indifférent. C'est la révolution sur le réseau, avec une alternance d'enthousiasme et d'inquiétude. L'enthousiasme provient de cette sensation de liberté : chacun peut communiquer partout, avec n'importe qui et à n'importe quel moment. L'inquiétude résulte d'une sensation d'insécurité car les délinquants et les escrocs ne seront pas les derniers à s'intéresser à ce fabuleux système qui touche des millions de personnes, faisant autant de victimes potentielles.

A l'origine, ce mémoire s'intitulait « La sécurisation des transactions informatiques ». En en changeant le titre et en préférant l'appeler « Commerce électronique : de la sécurité à la confiance », nous ne comptons nullement nier la réalité des risques que nous venons d'évoquer brièvement ou les efforts que requiert leur résolution. En revanche, nous voulons par là affirmer que l'approche du commerce électronique[4] sous l'angle de la sécurité est une approche partielle. Nous pensons que l'essor du commerce électronique ne repose pas uniquement sur la sécurité technique ou juridique des échanges. Le commerce électronique, avant d'être électronique, est du commerce. Ses acteurs ne réclament pas la sécurité absolue, de la même façon que les acteurs du commerce traditionnel ne l'ont jamais réclamée. La piraterie, les bandits de grand chemin, la fraude, les chèques en bois ou les escrocs ont toujours fait partie du paysage commercial, ils n'ont jamais empêché le développement des échanges classiques.

[4] Nous nous intéresserons dans ce mémoire uniquement au commerce *Business to Consumer*, c'est-à-dire aux échanges entre des entreprises et des particuliers. Nous laisserons de côté le commerce *Business to Business*.

Par contre, il est beaucoup plus important que l'on parvienne à créer entre les différents acteurs des relations de confiance. Celles-ci sont indispensables à l'essor du commerce électronique.

Nous articulerons par conséquent notre étude en deux parties. Il s'agira tout d'abord de dresser la liste des problèmes de sécurité que peuvent rencontrer acheteurs et vendeurs sur Internet, et de voir quelles solutions techniques et juridiques il est possible de leur apporter à l'heure actuelle. Mais nous n'oublierons pas que ces solutions, censées apporter un niveau satisfaisant de sécurité entre partenaires, sont une condition nécessaire mais non suffisante au développement du commerce électronique. C'est pourquoi nous essaierons alors d'imaginer quel développement peut être raisonnablement envisagé, et quels moyens devront être mis en œuvre pour donner confiance aux usagers d'Internet et pour accroître le champ du commerce électronique.

La sécurité des transactions informatiques

Les sites marchands se développent et se multiplient sur Internet. Le plus célèbre d'entre eux, AMAZON, spécialisé dans la vente de livres et de CD, voit son chiffre d'affaires croître régulièrement. Il inspire ses concurrents : en France, la FNAC ou ALAPAGE construisent leur site sur le modèle de leur précurseur américain et se lancent à leur tour dans la lutte pour la vente informatique. A l'aide d'un moteur de recherche quelconque, il est désormais aisé de trouver une multitude de sites, plus ou moins connus, vendant les objets les plus divers : ordinateurs, cassettes vidéo, musique, logiciels, services bancaires, voyages... On peut quasiment tout trouver sur Internet. En outre, le consommateur ne se limite plus à l'offre disponible dans sa rue, son quartier ou sa ville ; toutes les propositions du monde entier lui sont désormais accessibles depuis son ordinateur.

Examinons un acte d'achat, tel que tout consommateur le pratique, tant de façon classique que sur les réseaux. Tout achat réfléchi commence par la recherche du produit (liste des commerçants, conditions de prix, de livraison, de règlement...). Puis viennent la comparaison des propositions et le choix de la proposition la plus appropriée. Ensuite la commande est rédigée, elle lie le consommateur au commerçant retenu, elle exprime la volonté des parties de réaliser la transaction. Il est alors temps que le client paie son fournisseur et qu'en contrepartie, le commerçant livre son client. Dans la plupart des cas du commerce classique, la livraison est immédiate et le client repart avec son produit ; c'est là un avantage indéniable du commerce traditionnel. Mais lorsque la livraison est différée, par exemple lors d'un achat par correspondance, le vendeur et le client savent qu'il existe un risque, qu'il y ait un écart entre ce que le client souhaitait et ce qui lui a été livré, ou que le client indélicat disparaisse sans payer.

Dans ce processus qui mène du désir de consommer à la consommation elle-même, toutes les étapes sont susceptibles d'être traitées de manière électronique, de façon plus ou moins simple selon les cas. Les phases de recherche et de comparaison ne semblent pas causer trop de difficultés. Les capacités multimédia des réseaux permettent au consommateur de choisir avec plus de facilité sur un catalogue électronique que sur un catalogue papier. Ce n'est pas le cas des phases de règlement et de livraison, qui posent de nombreux problèmes pratiques.

Les transactions acceptées entre ordinateurs créent un risque potentiel majeur : un ordinateur « client » peut, dans un intervalle de temps très court, effectuer une multitude de transactions. Si celles-ci sont frauduleuses, de nombreuses entreprises vendeuses seront affectées. Il est donc important de renforcer les mécanismes de protection ou de sécurisation des engagements du client, et notamment son paiement. Aujourd'hui, le paiement à distance est accepté en donnant un numéro de carte de crédit et sa date d'expiration. Il n'est pas évident que ce mécanisme soit suffisant d'une part pour garantir l'acheteur contre le vol de ses numéros de carte, d'autre part pour épargner au vendeur

l'utilisation abusive d'un numéro. Inversement, le consommateur veut avoir la garantie que le bien acheté lui sera effectivement livré dans le délai prévu et que l'article correspondra à ce qu'il a choisi. Il veut également être sûr que le numéro de carte bleue qu'il a transmis sur Internet ne pourra pas être intercepté et utilisé à des fins malhonnêtes.

Nous avons ainsi identifié les principaux problèmes de sécurité que posent les échanges sur Internet. La signature électronique du message doit être fiable, afin d'éviter qu' une personne ne puisse usurper l'identité d'une autre personne ou nier qu'elle est le signataire d'un message. La confidentialité doit garantir au consommateur que les opérations qu'il effectue sur le réseau ne pourront être recueillies et utilisées par des individus autres que le destinataire. Il s'agit bien sûr que les coordonnées bancaires du consommateur ne puissent être récoltées par des personnes mal intentionnées ; il faut aussi que la vie privée du consommateur ne puisse être violée et que les pages consultées, les objets achetés ou ses habitudes de consommation ne puissent être connus, répertoriés et exploités à son insu.

Le hasard des sciences fait qu'un même outil, la cryptologie, permet de remplir ces deux fonctions que sont la signature et la confidentialité. Il est alors tentant, à l'instar du Conseil d'Etat, de voir dans la cryptologie *la* solution à tous ces problèmes. « Sur Internet, la cryptologie est indispensable pour assurer la confidentialité des messages, mais également la sécurité des transactions et des moyens de signature électronique. (…) Les pouvoirs publics sont convaincus de la nécessité de libéraliser dans une large mesure la fourniture et l'utilisation de moyens de cryptologie afin de favoriser l'essor du commerce électronique. » La position ambiguë du gouvernement français à l'égard de la cryptologie, sur laquelle nous reviendrons, et le battage médiatique autour de la réglementation s'y rapportant, ont contribué à faire croire que la libéralisation de la cryptologie résoudrait toutes les difficultés. Il n'en est rien et il faudra abandonner cette vision quelque peu simpliste. La cryptologie n'est qu'un moyen, et ne peut à elle seule assurer la sécurité du consommateur ou du vendeur. De nombreux autres efforts doivent être réalisés.

Nous commencerons notre étude en présentant quelques rudiments de cryptologie, sans lesquels les débats ultérieurs sur la signature électronique, la confidentialité, mais aussi et surtout sur la sécurité de l'Etat risqueraient d'être mal compris. Nous présenterons ensuite les difficultés et les enjeux de la signature électronique. Puis nous enchaînerons sur les questions de confidentialité et de sécurité de l'Etat, qui ont été les points les plus sensibles dans l'élaboration des diverses réglementations. Enfin nous terminerons cette partie en montrant que de nombreux autres problèmes de sécurité se posent, qui ne peuvent être résolus par la seule cryptologie.

Quelques rudiments de cryptologie

> *On convint de suivre à l'avenir l'ancien alphabet* alla Monaca, *qui, afin de n'être pas deviné par des indiscrets, change le numéro ordinaire des lettres, et leur en donne d'arbitraires ; A, par exemple, porte le numéro 10 ; le B, le numéro 3...*
>
> STENDHAL, *La Chartreuse de Parme*

Différents procédés de cryptage

Le procédé cryptographique mentionné dans la phrase placée en exergue a certainement l'avantage de la simplicité, il n'en présente pas moins deux inconvénients rédhibitoires. Tout d'abord, il conserve la fréquence des lettres, ce qui rend la cryptanalyse du message fort aisée. Mais il pose un problème de fond bien plus grave : celui qui sait coder un message sait également le décoder, car les clefs de codage et de décodage sont identiques, ou tout au moins peuvent être facilement déduites l'une de l'autre. En conséquence, l'expéditeur et le destinataire doivent avoir trouvé un moyen sûr de s'échanger ces clefs. Or ce procédé sécurisé n'existe pas : s'il existait, on l'utiliserait aussi pour échanger les messages !

Dans ses commentaires sur la *Chartreuse*[5], H. MARTINEAU s'étonnait de la légèreté et de l'insouciance avec lesquelles les héros communiquaient, mais rappelait que STENDHAL « lui-même écrivait sous le chiffre à son ministre et lui donnait dans la même enveloppe la clef de ce chiffre ». Les procédés de cryptage se sont bien améliorés depuis cette époque !

Les méthodes les plus modernes utilisent la cryptologie à clef publique. Dans les systèmes cryptographiques à clef publique, il existe deux clefs, l'une permettant de déchiffrer ce que l'autre a chiffré, et réciproquement. Ces deux clefs sont en correspondance univoque, mais la connaissance de l'une des clefs ne permet pas de retrouver facilement l'autre clef. L'une des clefs est tenue secrète par son détenteur : c'est la clef privée. L'autre clef peut être connue de tous : c'est la clef publique. Pour envoyer un message crypté à quelqu'un, il suffit de le chiffrer avec la clef publique de cette personne. Seul le destinataire pourra déchiffrer le message avec sa clef secrète. A l'inverse, un message chiffré avec la clef secrète pourra être déchiffré avec la clef publique, donc virtuellement par tout le monde. Ainsi, en cryptant un message à l'aide de la clef publique, l'expéditeur en assure la confidentialité ; en le cryptant à l'aide de la clef privée, l'expéditeur signe son message. Les

[5] *La chartreuse de Parme*, ed. Classiques Garnier

procédés de cryptographie permettent donc d'assurer à la fois les fonctions de confidentialité et de signature électronique.

Il existe nécessairement une relation entre la clef publique et la clef privée, relation qui permet théoriquement de déterminer la seconde en connaissant la première. Toute la difficulté consiste donc à trouver des algorithmes tels que ce lien ne soit pas exploitable avec un temps de calcul raisonnable.

Les systèmes à clef publique résolvent le problème de distribution des clefs, puisque la clef servant à chiffrer n'a plus besoin d'être transmise secrètement. Il est même possible d'envoyer un message chiffré à un correspondant jamais contacté auparavant. Il suffit pour cela de récupérer sa clef publique sur un serveur spécialisé. Seul le propriétaire de la clef privée correspondante sera alors capable de déchiffrer le message.

Longueur de la clef

Pour décrypter un message sans en posséder la clef privée, il existe une méthode séduisante mais complexe : retrouver de façon logique la clef privée connaissant la clef publique. Les procédés de cryptage actuels[6] rendent pour l'instant impossible une telle opération. Il existe une autre méthode, bien moins élégante mais très efficace : essayer de manière exhaustive toutes les clefs de décryptage possibles, jusqu'à tomber par hasard sur la bonne clef. Cette méthode finit toujours par fonctionner, mais peut consommer énormément de temps.

La longueur de la clef donne une idée du temps qui sera nécessaire pour décoder le message en essayant toutes les clefs. La longueur de la clef se mesure en bits. Si la clef fait 40 bits, il existe 2^{40} clefs différentes. Celui qui veut décoder le message sans connaître la clef privée prend le risque de devoir essayer 2^{40} clefs avant de trouver la bonne clef. A l'heure actuelle, un Etat dispose de moyens lui permettant de casser en une seconde un message codé avec une clef de 40 bits, un particulier suffisamment équipé y perdrait une heure. Si la longueur de la clef est de 128 bits, il existe 2^{128} clefs différentes. Celui qui veut décoder le message sans connaître la clef privée prend alors le risque de devoir essayer de l'ordre de 10^{39} clefs ! Il semble qu'aujourd'hui encore ce soit une performance que même les Etats les plus puissants ne peuvent accomplir dans un laps de temps raisonnable.

La longueur de la clef est donc l'une des caractéristiques importantes du cryptage appliqué à un message. Plus la clef est longue, moins les correspondants prennent de risques : même si leur message est intercepté, il est peu probable que celui-ci puisse être décrypté. Les Etats qui autorisent des procédés de cryptage avec des clefs de longueur supérieure à

[6] Le procédé le plus connu est RSA, nommé à partir des initiales de ses inventeurs : RIVEST ; SHAMIR ; ADLEMAN

56 bits se placent dans l'incapacité aujourd'hui de décoder des messages cryptés avec de tels systèmes.

Il nous faut maintenant présenter comment la cryptologie contribue à assurer la sécurité des échanges commerciaux, celle du vendeur, en aidant à la signature électronique, celle de l'acheteur, en permettant la confidentialité des messages.

Signature électronique : vers une consécration juridique

La signature électronique peut être effectuée à l'aide de plusieurs technologies qui permettent de remplir les exigences de la signature manuscrite, à savoir l'identification du signataire et l'expression de sa volonté. Dans cette perspective, aux termes de l'article 7 de la loi type de la Commission des Nations Unies pour le droit commercial international (CNUDCI), « lorsque la loi exige la signature d'une personne, cette exigence est satisfaite (...) si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données ; et si la fiabilité de cette méthode est suffisante. »

Ainsi les Etats disposent dès aujourd'hui d'un texte, sans force obligatoire, qu'ils peuvent intégrer à leur système légal en vue de conférer à la signature électronique une validité juridique et une force probante.

Pour obtenir la méthode fiable envisagée, différentes technologies peuvent être utilisées : RSA, cryptographie à courbes elliptiques, cryptographie quantique, cartes à puce, dispositifs biométriques... Mais la technologie reposant sur la cryptographie à clef publique, que nous avons présentée plus haut, est parfaitement satisfaisante – pourvu, bien sûr, que la longueur de la clef soit suffisante.

A l'heure actuelle, c'est d'ailleurs ce système de signature numérique à clef publique qui a été retenu par tous les systèmes juridiques qui ont adopté des textes de loi : Utah, Allemagne... L'Italie a adopté une loi sur les documents dématérialisés et sur la signature électronique. Les contrats dématérialisés authentifiés par des signatures électroniques certifiées se voient reconnaître la force probante d'un écrit. L'Union européenne se penche avec intérêt sur ces sujets. Elle est d'ailleurs obligée, dans sa dernière proposition de directive, de prendre acte des divergences existantes et des indéniables besoins d'harmonisation des législations européennes.

Néanmoins, en France, la question n'est pas encore résolue. La consécration juridique de la signature électronique cause de nombreuses difficultés et implique une refonte substantielle de nos textes. Mais les problèmes sont également techniques et le développement d'autorités de certification, pour lesquelles il faudra prévoir un statut juridique, est à la fois indispensable et inéluctable.

Nécessité d'une réforme législative

La fonction d'une signature est triple. Elle affirme la volonté du signataire ; elle est un élément de preuve ; elle est un élément de formalisme. Dans ce dernier cas, la signature manuscrite reste requise et ne saurait être remplacée par une signature électronique. Par contre, la législation doit être adaptée pour que la signature électronique puisse satisfaire les deux premières fonctions.

En France, à l'heure actuelle, la preuve est libre, avec une exception particulièrement notable. En effet, l'article 1341 du Code civil dispose : « Il doit être passé acte devant notaires ou sous signatures privées de toutes choses excédant une somme ou une valeur fixée par décret (...) et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes... » La somme a été fixée à 5000 francs par un décret du 15 juillet 1980. Au vu de l'évolution des masses monétaires en circulation et des réalités économiques, une telle limite devrait évidemment être réévaluée. Il est néanmoins plus intéressant de constater qu'aujourd'hui, la loi elle-même rend les documents électroniques irrecevables comme mode de preuve, et ce à double titre : au-delà de 5000 francs, une preuve écrite doit être préconstituée ; quelle que soit la somme, l'écrit prime tous les autres moyens de preuve.

Toutefois, cet article n'est pas d'ordre public. En conséquence, les parties peuvent y renoncer. La jurisprudence est constante sur ce point. L'article 1341 s'impose au juge seulement lorsque les parties n'y ont pas explicitement ou tacitement renoncé. En particulier, les conventions de preuve sont parfaitement admises, comme le proclame le fameux arrêt *Crédicas*, relatif à la preuve d'un ordre de paiement donné par utilisation d'une carte magnétique et composition concomitante du code confidentiel. La Cour de cassation a en effet jugé en l'espèce que les parties peuvent, par contrat, accorder une valeur de preuve à un document dépourvu de signature manuscrite. Dans son rapport annuel de 1989, la Cour de cassation a confirmé ce point de vue, en estimant que « ce procédé moderne présente les mêmes garanties que la signature manuscrite, laquelle peut être imitée tandis que le code secret n'est connu que du seul titulaire de la carte. »

En l'absence de modification de l'article 1341, il est possible d'imaginer que le document électronique soit considéré comme un commencement de preuve par écrit, à l'instar d'une photocopie, même s'il céderait alors devant un écrit contraire. Il est possible d'imaginer également que l'article 1348 alinéa premier, relatif à l'impossibilité matérielle ou morale de se procurer une preuve littérale de l'acte juridique, soit modifié de telle façon que l'impossibilité matérielle de produire un écrit soit étendue au cas d'une transaction électronique.

D'autres difficultés existent. Le Code civil mentionne à plusieurs reprises l'obligation d'une signature. L'article 1322 sur les actes sous seing privé, l'article 1325 sur les contrats synallagmatiques ou l'article 1326 à propos des reconnaissances de dettes imposent ainsi le recours à l'écrit. Il est fort probable que la modification de ces articles soit prochaine, afin de conférer aux actes électroniques une validité équivalente à celle des actes écrits.

Le législateur français pourra d'ailleurs s'inspirer de son homologue québécois. En effet, le législateur du Québec a pris soin d'insérer dans le Code civil une définition de la signature. « La signature consiste dans l'apposition qu'une personne fait sur un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement. » En outre, dès 1993, le Québec a reconnu aux documents informatisés une valeur probante. Le législateur a toutefois fait attention à clairement distinguer les documents électroniques des autres écrits ; il a également énoncé la prééminence du document papier sur le document électronique.

Ce sont là des réflexions dont le législateur devrait rapidement s'inspirer. Il y sera de toute façon vraisemblablement contraint du fait du projet de directive européenne relative à la signature électronique. Celle-ci prévoit en effet d'octroyer à la signature électronique garantie par un certificat la même valeur probante qu'une signature manuscrite. Le tiers de certification apparaît alors comme un élément essentiel du système de signature électronique et semble voué à un avenir particulièrement enviable.

Le tiers de certification, un acteur primordial dans les transactions de demain

Conformément à la recommandation 509 de l'Union internationale des télécommunications (UIT), une autorité de certification est « une autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clef publique et leur certificat ». Les tiers de certification remplissent donc une fonction essentielle : formaliser et assurer le lien qui existe entre une personne physique ou morale et une paire de clefs asymétriques.

Pour vérifier l'identité du signataire d'un message, le destinataire doit récupérer sur un serveur spécialisé la clef publique de l'expéditeur du message. Le destinataire est alors sûr que seul le détenteur de la clef privée correspondante a pu signer le message. Malheureusement, il n'est pas garanti que le détenteur de cette clef privée soit effectivement la personne avec qui il souhaite communiquer. Il se peut que la clef publique ait été déposée frauduleusement par une autre personne, qui souhaite se faire passer pour l'expéditeur du message. Il s'agit par conséquent de prévenir cette usurpation d'identité. Le tiers de certification a pour mission – et cette mission est essentielle si l'on veut garantir la sécurité des transactions commerciales – d'assurer que la clef publique récupérée appartient effectivement à la bonne personne. D'une certaine manière, le tiers de certification joue donc vis-à-vis du commerçant le rôle d'une préfecture de police délivrant une carte d'identité, et vis-à-vis du consommateur le rôle d'un registre du commerce permettant d'identifier avec précision la société cocontractante.

L'importance de cette fonction amène à s'interroger sur le fonctionnement du tiers de certification, sur son régime juridique, et en particulier sur son statut.

Le rôle du tiers de certification est d'émettre des certificats. Le certificat est simplement un message électronique délivré par le tiers de certification qui a pour fonction d'établir un lien entre une personne physique ou morale dûment identifiée et une clef publique. Il sert donc à l'identification du titulaire de la clef privée correspondant à la clef publique mentionnée dans le certificat pour la signature.

En principe, le certificat contient une série d'informations qui sont relatives à l'utilisateur, le nom du tiers émetteur du certificat, la clef publique de l'utilisateur, un numéro de série, la date de délivrance et d'expiration. Les tiers de certification authentifient eux-mêmes les certificats en y apposant leur propre signature numérique.

Avec un tel certificat, un destinataire qui entend se fier à une signature numérique créée par la personne nommée dans le certificat peut utiliser la clef publique mentionnée dans le certificat afin de vérifier que l'émetteur a bel et bien utilisé la clef privée correspondante. Si la vérification est satisfaisante, le destinataire a la certitude que la signature numérique émane de la bonne personne.

L'importance évidente des tiers de certification dans les transactions commerciales amène à s'interroger sur leur responsabilité. Il faut que les utilisateurs soient attentifs au niveau de sécurité garanti par les autorités de certification. Il faut également être renseigné sur le sérieux technique et organisationnel du tiers de certification, en particulier sur la façon dont celui-ci gère le délicat problème de la suspension ou de l'annulation des certificats. Dans tous les cas, et nous y reviendrons plus tard, il ne faut pas oublier que le tiers de certification ne garantit que l'identité de l'interlocuteur et non son honnêteté.

Un autre point important est le statut de ce tiers de certification. Nous avons vu qu'il peut être considéré, dans une certaine mesure, comme un registre du commerce ou comme un organisme délivrant des pièces d'identité. Faut-il par conséquent qu'il soit public ? A l'inverse, on peut affirmer que les tiers de certification ne sont que de simples intermédiaires, que de simples intervenants dans un circuit purement commercial. Peut-on dans ce cas admettre que les tiers de certification soient de pures sociétés privées issues du marché ? La solution n'est pas évidente. Les organismes privés ont la faveur du projet de directive, qui admet même des organismes non agréés par les pouvoirs publics comme tiers de certification. C'est là une solution audacieuse. Si cette directive était adoptée, il faudrait donc espérer que le marché sache sélectionner des autorités de certification sérieuses, ou que les Etats puissent octroyer par leur agrément un avantage commercial suffisant à des sociétés auxquelles ils auraient imposé un cahier des charges exigeant.

Au terme de cette présentation de la signature électronique, la façon dont peut être assurée la sécurité du vendeur, qui cherche à connaître l'identité de son client, apparaît

plus clairement. Il nous faut maintenant exposer la manière dont peut être garantie la sécurité de l'acheteur, peu enclin à envoyer ses coordonnées bancaires sur le réseau.

Confidentialité : la fin d'un tabou ?

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Constitution des Etats-Unis d'Amérique, premier amendement

Il peut sembler étrange que dans une étude consacrée au commerce électronique, nous ayons placé en exergue le premier amendement de la Constitution américaine. Ce choix se justifie parfaitement. En effet, lorsque la confidentialité doit être assurée, lorsque le cryptage est utilisée à des fins de confidentialité, il ne faut pas oublier que la sécurité de l'Etat est en jeu.

Inventer de nouveaux algorithmes, créer des logiciels plus modernes afin de transmettre des références bancaires dans des conditions plus sûres sont des objectifs tout à fait nobles et indispensables au développement du commerce électronique. Malheureusement, ces mêmes logiciels, ces mêmes algorithmes peuvent être utilisés à des fins beaucoup moins avouables : échanges entre terroristes, grand banditisme, pédophilie… Ainsi les atteintes à la sécurité de l'Etat ou à l'ordre public peuvent être nombreuses grâce au cryptage.

L'Etat conserve la faculté d'intercepter tous les messages qui transitent sur Internet. C'est d'ailleurs ce que les Américains sont en mesure de faire à l'échelle mondiale grâce au réseau Echelon. Lorsque les services de sécurité intérieure interceptent des conversations téléphoniques, ils peuvent les traiter immédiatement, car celles-ci passent « en clair ». Mais un codage efficace peut rendre des messages sur Internet totalement indéchiffrables.

L'Etat, dans sa politique relative au cryptage, est donc confronté à un perpétuel dilemme : sécuriser les échanges ou assurer sa propre sécurité. La question est résolue de façon fort simple aux Etats-Unis. Toute restriction des moyens de cryptographie y serait vue comme une violation du premier amendement et serait donc inconstitutionnelle. La National Security Agency (NSA) est donc condamnée à une véritable fuite en avant, à une course scientifique, de façon à toujours être capable de casser des codes de plus en plus sophistiqués.

L'attitude de la France a été tout autre : longtemps restrictive, la France semble s'engager sur la voie de la libéralisation de la cryptologie, même si les conséquences de ce revirement ne semblent pas toutes bien évaluées.

La cryptologie, une ancienne arme de guerre

La cryptologie fait son entrée dans le droit français par un décret-loi du 18 avril 1939, fixant le régime des matériels de guerre, armes et munitions. Le décret 73-364 du 12 mars 1973, modifié par le décret 86-250 du 18 février 1986, classe en arme de deuxième catégorie « les moyens de cryptologie, matériels ou logiciels conçus soit pour transformer à l'aide de conventions secrètes des informations claires ou des signaux en informations ou signaux inintelligibles, soit pour réaliser l'opération inverse ».

Cette position sécuritaire est légèrement assouplie par la loi 90-1170 du 29 décembre 1990 portant réglementation des télécommunications. Son article 28 justifie les restrictions apportées à l'utilisation des moyens de cryptologie pour « préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat ». Les moyens de cryptologie utilisés à des fins de signature sont soumis à déclaration préalable, les moyens de cryptologie utilisés à des fins de confidentialité sont soumis à autorisation préalable du Premier ministre.

Vers la libéralisation

Cette législation, à l'époque la plus stricte du monde occidental, aussi peu libérale que celles de la Russie ou de Singapour, fut assouplie par la loi 96-659 du 26 juillet 1996, portant elle aussi réglementation des télécommunications. Toujours pour « préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat », mais en invoquant « la protection des informations et le développement des communications et des transactions sécurisées », cette loi libéralise complètement l'usage des moyens de cryptologie à des fins d'authentification. Par contre, elle soumet l'usage des moyens de cryptologie à des fins de confidentialité à un régime d'autorisation, sauf à recourir à des « organismes chargés de gérer pour le compte d'autrui les conventions secrètes de moyens ou prestations de cryptologie permettant d'assurer des fonctions de confidentialité », que nous appellerons par la suite « tiers de confiance ».

Le tiers de confiance, une innovation contestée

La loi du 26 juillet 1996 a fait l'objet de nombreuses critiques, qui nous semblent justifiées. Le régime des tiers de confiance est contraignant et peu efficace face à des entités criminelles. Les sanctions prévues sont très faibles. Enfin, l'Etat garde tant de moyens légaux d'obstruction que les objectifs de développement du commerce électronique annoncés dans la motivation de la loi paraissent difficiles à atteindre.

Le tiers de confiance se voit confier un rôle ambigu. Le tiers de confiance recueille les clefs privées de ses clients. Il possède donc les moyens de décrypter tous les messages reçus

par ceux-ci. Comment imaginer que Dassault accepte de confier à Matra, dont l'une des filiales a été agréée comme tiers de confiance, ses clefs secrètes qui permettraient à son concurrent, devenu malhonnête, de déchiffrer tous ses messages confidentiels (appels d'offre, spécifications techniques...) ? A plus forte raison, comment imaginer une société étrangère acceptant de remettre ses clefs à un organisme français agréé par l'Etat français, et susceptible de les remettre à tout moment au gouvernement français ?

Certes la loi n'impose pas le recours au tiers de confiance. Les utilisateurs de cryptologie peuvent demander au Service central de la sécurité des systèmes d'information (SCSSI) une autorisation préalable, dont les conditions d'attribution sont particulièrement sévères. Ils peuvent aussi, s'ils ne sont pas trop exigeants, utiliser des moyens de cryptologie dits « faibles » (c'est-à-dire dont la longueur de la clef était inférieure à 40 bits[7]). Ceux-ci sont difficilement cassables par un amateur, mais ne résistent qu'une seconde aux services de sécurité nationaux, et une heure à une organisation motivée et disposant d' un million de dollars.

En outre l'Etat peut exiger la mise en œuvre de la convention secrète afin de récupérer le message en clair. Bien sûr, des garde-fous sont prévus. Cette procédure s'effectue dans le cadre de la loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, et il est bien précisé que le tiers de confiance est tenu d'avertir le propriétaire de la clef lorsque le procureur de la République requiert la mise en œuvre de la convention. Mais ce texte comporte des lacunes : la loi 91-646 opère une distinction entre les écoutes judiciaires et les écoutes administratives ; quant au texte de 1996, il prévoit seulement le cas où le procureur demande la mise en œuvre de la convention, mais ne fait pas mention du cas où le juge d'instruction, ou l'administration, ou certains services spécialisés dans les questions de sécurité intérieure ou extérieure, demanderaient la remise de ces clefs. Comment croire que le tiers de confiance, qui est un organisme agréé par l'Etat et dépendant de lui pour pouvoir continuer à opérer, puisse résister aux légères pressions de celui à qui il doit tout ?

Enfin, les tiers de confiance ont une viabilité économique quasi nulle. La seule fonction économique intéressante pour des entreprises est la fonction de séquestre de clefs, si jamais ces dernières sont perdues, oubliées ou volées. Le tiers de confiance est alors en mesure de leur en fournir un double. Il est étonnant et regrettable que l'Etat fasse assumer par des acteurs privés une fonction purement régalienne.

De plus, la loi prévoit des sanctions particulièrement faibles à l'encontre des contrevenants, ce qui limite son efficacité. Les peines maximales infligées à ceux qui auraient « importé, exporté, ou utilisé des moyens de cryptologie en vue de faciliter la préparation ou la commission d'un crime ou d'un délit » sont de trois ans d'emprisonnement et de 500 000 francs d'amende. Celui qui se ferait passer pour un tiers de confiance sans avoir

[7] Un décret récent (17 mars 1999) relève le seuil à 128 bits. Nous examinerons les conséquences de ce décret dans un paragraphe ultérieur.

reçu l'agrément encourt deux ans d'emprisonnement et 300 000 francs d'amende. Il est facile d'imaginer la terreur que ces textes inspirent dans l'esprit de terroristes déterminés, qui risquent la prison à perpétuité pour les crimes qu'ils commettent. Nul doute que ce texte et les sanctions qu'il prévoit les incitent à déposer leurs clefs chez un tiers de confiance...

L'importation et la fourniture d'un moyen de cryptologie sans autorisation préalable sont punies de six mois d'emprisonnement et de 200 000 francs d'amende. Cette sanction est doublement irréaliste : il est tellement aisé de télécharger un logiciel théoriquement interdit, par exemple PGP (*Pretty Good Privacy*, de P. ZIMMERMAN), que cet article de loi permettrait certainement d'envoyer en prison la quasi-totalité des étudiants et chercheurs en informatique ; de plus, on imagine mal le gouvernement français déployer les moyens de surveillance nécessaires pour empêcher qu'un logiciel interdit ne franchisse les frontières de notre territoire...

En fin de compte la seule utilité de ce texte semble être la matérialisation du délit. Il est probable que la police et la justice soient incapables d'établir que des bandits communiquant par messages codés s'apprêtaient à commettre ou commettaient déjà tel ou tel crime. En effet, comment utiliser comme preuves des documents fortement codés et indéchiffrables ? Il faudra donc se contenter de faire tomber des criminels pour un délit matériellement constitué : l'absence de recours à un tiers de confiance.

Enfin il ne faut pas perdre de vue que la motivation de la loi était de permettre « la protection des informations et le développement des communications et des transactions sécurisées ». Cet objectif paraissait difficilement conciliable avec l'autre objectif de la loi, préserver la sécurité de l'Etat. Force est de constater qu'il n'a pas été atteint. Cet état de fait a amené le Premier ministre à annoncer la libéralisation de la cryptologie, lors de son discours du 19 janvier 1999. Cette déclaration n'a rien d'un coup de théâtre, elle était attendue et espérée par la plupart des acteurs depuis de nombreux mois. Dans cette déclaration, trois points essentiels peuvent être dégagés :

- le recours au tiers de confiance deviendra facultatif ;
- l'utilisation des moyens de cryptologie à des fins de confidentialité est libre pour des systèmes dont la clef est de longueur inférieure ou égale à 128 bits ;
- le propriétaire de la clef aura l'obligation, sous peine de sanctions pénales, de remettre aux autorités le message en clair.

A l'heure actuelle, seul le deuxième point a été traduit dans l'ordonnancement juridique grâce à un décret du 17 mars 1999. Les deux autres points relèvent du domaine législatif et devraient nécessiter davantage de temps pour être transcrits. Une révision de la loi de 1996 est peu probable. Cette loi, relative à la libéralisation des télécommunications, est très controversée ; le gouvernement ne devrait pas oser la retoucher.

Il ne faudrait toutefois pas croire que cette déclaration de Lionel JOSPIN constitue une réelle avancée : elle n'est que l'aveu d'une défaite. La position de la France était intenable, tant

au sein de l'Union européenne que dans le cadre des échanges commerciaux internationaux. Toutefois, un passage trop rapide à un régime libéral n'est pas souhaitable. En effet, de nombreuses interrogations demeurent quant à la sécurité de l'Etat et une évolution trop peu réfléchie et incontrôlée risque de faire le jeu des Américains. N'oublions pas qu'il y a une quinzaine d'années, les Américains avaient incité les Européens à interdire la protection des logiciels, ce qui leur avait ensuite permis de s'emparer du marché...

Le relèvement du seuil à 128 bits a surpris les observateurs, il faut le reconnaître, sur un point : ceux-ci pensaient que le seuil serait remonté seulement à 56 bits. Il semblerait, mais ce sont là des renseignements difficiles à obtenir, que les agences de sécurité américaines soient capables de déchiffrer des messages codés à 56 bits, alors que les services français en sont incapables. Avec un seuil à 128 bits, l'égalité est rétablie, les deux pays semblant tout autant incapables de casser les codes.

Ce revirement soudainement avant-gardiste changera-t-il quelque chose à la situation du commerce électronique ? Cela paraît peu probable. Pour l'instant, les connexions sur Internet et les échanges qui s'ensuivent se font principalement à l'aide de navigateurs américains, tels Explorer ou Netscape. Leurs fonctions de sécurité à l'export sont bridées à 56 bits, ainsi que l'exige la loi américaine[8]. La libéralisation annoncée ne devrait donc pas concerner immédiatement la masse des consommateurs français.

L'attention des médias, des politiques, des juristes, des professionnels ou des consommateurs s'est longtemps focalisée sur la question de la cryptologie, présentée comme la solution miracle pour les problèmes de confidentialité et de transmission sécurisée sur Internet. Nous nous en sommes fait l'écho, mais il ne faut surtout pas croire que la cryptologie soit la panacée. De nombreux autres « trous » de sécurité existent.

La sécurité technique, une question globale

L'usage de la cryptologie permet de prévenir les écoutes seulement après que le message a été crypté. Tant que l'algorithme de cryptage n'a pas été mis en œuvre, les interceptions exploitables restent possibles et les messages échangés sont vulnérables. Normalement, dans une communication sécurisée, aucun message n'est envoyé sur le réseau sans être codé. Mais il est tout à fait possible d'intercepter le message avant même qu'il ait été codé, et avant même qu'il ait quitté l'ordinateur de l'expéditeur.

Lorsque l'utilisateur tape un message sur son ordinateur, un fil électrique transmet les informations à l'unité centrale. Le courant électrique entraîne une modification du champ électromagnétique environnant. De la même façon, l'affichage à l'écran induit des variations encore plus importantes du champ électromagnétique. Celles-ci peuvent être

interceptées et le message peut ainsi être écouté avant que toute transformation ne lui ait été appliquée.

D'autres failles de sécurité peuvent être trouvées. Elles sont nombreuses ; nous n'en citerons que quelques-unes, de façon non exhaustive, et sans les détailler. Le microprocesseur de l'ordinateur est-il sûr ? Le scandale déclenché par la tentative de la firme Intel d'insérer un mouchard dans ses microprocesseurs prouve le bien-fondé de cette interrogation. N'a-t-il pas été piégé de façon à transmettre vers un site non identifié ce que l'utilisateur est en train d'écrire, et ce à son insu ? Le système d'exploitation est-il fiable ? Le code source de Windows 98 n'a jamais été révélé, les suppositions les plus folles sont donc susceptibles de naître. Qui sait s'il n'existe pas, dissimulé dans cet immense logiciel, un module permettant d'espionner l'utilisateur ? Un virus n'a-t-il pas investi l'ordinateur pour permettre à un pirate d'écouter celui-ci ? Le logiciel de cryptage est-il de bonne qualité ?

Nous amenons le lecteur à réfléchir à cet exemple surprenant et édifiant : chacun connaît le logiciel Word. Il s'agit certainement du plus célèbre de tous les traitements de texte. Le sérieux de Microsoft, qui le commercialise, n'est plus à prouver. Pourtant, les programmateurs de ce logiciel, quelque peu facétieux, y ont dissimulé, à l'insu de la très grande majorité des utilisateurs... un flipper[9] ! Il se peut fort bien que les programmateurs d'Explorer ou de Netscape aient inclus un module qui atténue la qualité du codage effectué ou qui, parallèlement au codage, envoie le message en clair vers un site que l'utilisateur ne connaîtrait pas. Ce ne sont là que quelques hypothèses, angoissantes et paranoïaques, mais plausibles.

La sécurité, un faux problème pour le consommateur ?

Grâce au développement de la carte à puce, la France est peu sensible à la fraude électronique. Son montant est évalué à 0,05 % du montant global des transactions. A titre de comparaison, aux Etats-Unis, où la carte à puce ne s'est pas implantée et où règnent encore les cartes à piste magnétique, le taux de fraude est évalué à 3,5 %. Pourtant, le commerce y est prospère ; le risque de fraude ne freine ni le consommateur ni le vendeur.

Faut-il en conclure que la sécurité est un faux problème et qu'elle n'intéresse personne ? Aux Etats-Unis, en cas de fraude, la banque rembourse le propriétaire de la carte bancaire.

---

[8] La loi américaine interdit l'exportation de moyens de cryptologie dont la longueur de la clef dépasse 56 bits.

[9] Pour le faire apparaître, effectuez les opérations suivantes :

- Ouvrir Word 97 ;
- Taper 'Blue' (avec la majuscule), sélectionner le mot, aller dans le menu 'Format / Police', mettre la police en gras et en bleu ;
- Déselectionner le mot, taper une espace puis sur la touche 'Enter' ;
- Aller dans le menu '? / A propos de Microsoft Word' ;
- Presser 'Ctrl+Shift' (touches de gauche du clavier) et en même temps cliquer sur l'icône en haut à gauche de la fenêtre que vous venez d'ouvrir. Normalement, le flipper se lance.

La banque fait office d'assurance : elle applique une franchise au remboursement ; elle vend sa carte bancaire à un prix élevé en guise de prime d'assurance ; elle prélève une commission importante à chaque utilisation de la carte. Toutefois, il est douteux qu'un tel schéma de fonctionnement puisse être transposé en France.

A l'heure actuelle, les banques françaises sont tenues de rembourser leurs clients qui contestent une transaction payée par carte bleue, lorsque seuls le numéro de carte bleue et sa date d'expiration – et non le code secret ou la signature manuscrite – ont été nécessaires pour effectuer le paiement. C'est le cas sur Internet, où le code secret n'est jamais exigé. Un développement massif du commerce électronique accompagné d'un essor massif de la fraude mettrait en péril le système actuel de tarification de la carte à puce, et donc sa viabilité. Il est donc évident que les banques sont intéressées au premier chef par le développement de la sécurité sur Internet.

Malheureusement, il n'est pas sûr que le consommateur y attache la même importance. Nous en voulons pour preuve ces ventes par téléphone, de type Téléachat, où le client donne en clair son numéro de carte bleue et sa date d'expiration à un employé qu'il ne connaît pas et qu'il n'a jamais vu. Des risques existent également pour les paiements classiques par carte bleue : il suffit de regarder le récépissé d'un paiement effectué chez un commerçant pour s'apercevoir que le numéro de carte bleue et sa date d'expiration y apparaissent entièrement et en clair.

Pourtant le téléachat s'est développé, et personne n'hésite à régler un commerçant par carte bleue. Ces deux exemples, combinés au cas des Etats-Unis, où la fraude est importante et le commerce florissant, nous amènent à penser que la sécurité n'est pas la condition primordiale pour le développement du commerce électronique.

Par contre, il est important et essentiel de faire naître chez l'utilisateur final un sentiment de confiance. A partir de ce moment-là seulement, le commerce électronique pourra espérer connaître les taux de croissance que d'aucuns lui prédisent actuellement.

La confiance, voie du succès

Le commerce a été de tout temps une question de confiance ; le développement des sociétés occidentales s'est fondé, comme l'a montré A. PEYREFITTE dans *La Société de Confiance*, sur ce facteur, indépendamment des conditions réelles d'efficacité des protections employées. Ainsi, la marque est aisément falsifiable, mais elle est un facteur indéniable de confiance.

Le caractère informatique du commerce électronique ne doit pas faire oublier qu'il s'agit là de commerce avant tout. Les aspects électroniques ne jouent qu'à la marge, même s'ils impliquent quelques adaptations. En conséquence, quels que soient les discours politiques ou les credos assenés, la condition essentielle du commerce électronique est le développement du sentiment de confiance chez les acheteurs potentiels.

Il faut tout d'abord réussir à définir le terme de confiance. Le dictionnaire Hachette en donne la définition suivante :

> *Confiance n. f.*
>
> 1. *Espérance ferme en une personne, une chose. Avoir confiance en qqn, en l'avenir. Homme de confiance, en qui l'on peut avoir confiance, dont on est sûr.*
>
> 2. *Assurance, hardiesse. Avoir confiance en soi.*
>
> 3. *Poser la question de confiance : demander à l'Assemblée nationale d'approuver sa politique par un vote, en parlant du gouvernement.*

La première définition évoque d'abord la confiance en un homme, et c'est bien là le début de la transaction. Certes, l'acheteur et le vendeur recherchent la conclusion du contrat ; mais ils espèrent souvent bien plus. L'acheteur peut attendre du bien acheté qu'il remplisse une demande ressentie comme essentielle, mais au-delà du bien, il peut aussi rechercher un lien social et humain.

Dans le premier cas, le bien importe plus que le reste et l'achat se fait de façon relativement rationnelle, au sens où le bien est l'objet du désir. Dans le second cas, le lien importe davantage et l'acte d'achat est un acte plus social qu'utile. On paie une consommation au bar pour avoir l'occasion de discuter et de créer un lien. De la même façon, on achète une baguette de pain en discutant avec la boulangère, les journaux en devisant sur les dernières nouvelles avec le marchand. Bien sûr, le bien acheté possède une valeur intrinsèque, mais en outre il donne l'occasion de s'insérer dans la société.

Les lieux d'achats non plus ne sont pas innocents. L'homme pressé n'ira que dans le magasin qui ne lui fait pas perdre de temps, le bavard fréquentera le magasin où il peut deviser à son gré. Et ce, indépendamment de la valeur du bien acheté ; la baguette de pain sera équivalente, le prix aussi.

Quelle pourrait être la valeur sociale d'un achat sur Internet ? Affirmer que l'achat est totalement dénué de tout sens social est une position difficilement défendable. Aujourd'hui, acheter sur Internet constitue une sorte de prouesse, dont la prime de risque est une certaine reconnaissance sociale : l'acheteur sur Internet appartient *de facto* à une certaine catégorie, il peut se rattacher à un groupe « moderne ». Aux yeux du monde, il peut se prétendre « branché ». Mais cette reconnaissance est par nature éphémère. Si le commerce électronique se développe de façon importante, l'acte d'achat sur Internet ne pourra plus se parer d'une telle signification.

Pour attirer la masse des clients, il faudra lui inspirer confiance. Lorsque certains spécialistes affirment que le commerce électronique abolit les frontières et permet l'essor des échanges mondiaux, ils semblent oublier que la confiance, difficile à bâtir dans un espace géographique restreint, est tout à fait illusoire à l'échelle du globe. Cette simple remarque doit nous amener à réfléchir aux limites raisonnables que l'on peut fixer au développement du commerce électronique. Il sera alors temps de présenter les structures et les intermédiaires indispensables au développement du cybercommerce.

Le commerce électronique sera-t-il vraiment mondial ?

Le commerce électronique aura un effet bénéfique sur l'économie mondiale et sur les échanges mondiaux seulement s'il permet à un public peu habitué au commerce international d'y accéder de façon simple et rassurante. Or la complexité des règles régissant les échanges internationaux risque de décourager les clients potentiels. Le moindre litige, déjà complexe à résoudre sur le territoire national, devient un véritable parcours du combattant dès lors que les parties ne sont pas de la même nationalité. En conséquence, le développement du commerce électronique ne se fera très vraisemblablement qu'à l'échelon local dans un premier temps.

Le commerce international, un univers complexe

Le commerce électronique a déjà un régime juridique. Le fait qu'il puisse être international ne pose pas *a priori* de problème car le commerce a toujours eu vocation à être international. Déjà dans l'Antiquité ou au Moyen Age s'était développé un commerce régi par des usages à caractère international. Aujourd'hui, des conventions existent qui régissent le commerce international. Le commerce électronique n'y échappe pas.

Nous ne tenterons pas de dresser un tableau exhaustif des conventions et traités qui peuvent s'appliquer au commerce international. C'est là une performance qui relève plutôt d'un cours de droit international privé. Nous voulons simplement ébaucher une esquisse de la complexité juridique du commerce international, qui risque de décourager le consommateur potentiel.

En effet, comment un consommateur normal pourra-t-il affronter sereinement et avec succès l'imbroglio suivant : Français en voyage au Royaume-Uni, il y appelle localement Compuserve auquel il s'est abonné en France, et accède au serveur Internet d'une société irlandaise ; le serveur est basé à Malte, mais son adresse se terminant par « .com » laisse supposer une implantation nord-américaine[10] ; le client paye avec un porte-monnaie virtuel Digicash, dont les deux banques associées sont finlandaise et américaine ; le fournisseur fait livrer par un transporteur espagnol le bien acheté par un grossiste néerlandais. Qui contacter en cas de problème ? Qui est responsable ? Qui répare le préjudice ?

L'un des premiers problèmes à résoudre est le conflit des lois. Le réseau étant international, le litige sera lui aussi international et il faudra choisir entre plusieurs lois. Il existe plusieurs conventions internationales qui peuvent intéresser le commerce électronique. La convention de La Haye, signée le 15 juin 1955 et ratifiée par la France le 6 août 1967, concerne la loi applicable à la vente d'objets mobiliers corporels. La vente est régie par la loi du pays qu'ont choisi les cocontractants, et à défaut par la loi du pays du vendeur. De la même façon la convention de Vienne signée le 11 avril 1980 et entrée en vigueur le 1er janvier 1988 concerne la vente internationale de marchandises. Elle est d'autant plus importante que les Etats-Unis y sont partie, ce qui n'était pas le cas pour la convention de La Haye. Elle reprend les dispositions de la convention de La Haye, même si son champ d'application est assez restreint : elle ne concerne pas les ventes de biens de consommation personnelle. De manière générale, la difficulté d'identifier la loi applicable est accrue sur Internet : comme nous l'avons vu dans l'exemple du paragraphe précédent, la localisation du contrat peut être impossible à déterminer. C'est pour cela qu'une sorte de loi internationale applicable au commerce électronique a été rédigée dans le cadre de la CNUDCI.

Le caractère international du commerce sur Internet oblige également à réfléchir à la question du juge compétent. L'exemple français suffit à illustrer la complexité de la situation. Les juridictions françaises peuvent être compétentes pour juger des litiges entre Français, entre Français et étrangers, et même entre étrangers. Le juge peut s'estimer compétent dès lors que l'une des parties est française, qu'elle soit défenderesse ou demanderesse. Enfin il faut noter l'article 48 du Nouveau code de procédure civile qui dispose que « toute clause qui, directement ou indirectement, déroge aux règles de compétence territoriale est réputée non écrite à moins qu'elle n'ait été convenue entre des personnes ayant toutes contracté en qualité de commerçant et qu'elle n'ait été spécifiée de

[10] Les adresses Internet reflètent l'organisme auquel a été demandée l'attribution d'une adresse. Elles n'ont aucun lien technique ou juridique avec le lieu d'implantation du serveur.

façon très apparente dans l'engagement de la partie à qui elle est opposée ». Si le contrat est soumis à la loi française, aucune clause attributive de juridiction ne peut donc être opposée à un consommateur.

Néanmoins, lorsque les deux parties résident dans un pays de l'Union européenne, le tribunal compétent est déterminé conformément à la convention de Bruxelles. Celle-ci, conclue le 27 septembre 1968, concerne la compétence judiciaire et l'exécution des décisions en matière civile et commerciale. Le principe de base est que le tribunal compétent est celui du domicile du défendeur. C'est l'application classique de l'adage *actio sequitur forum rei*. Quelques exceptions sont prévues, notamment en matière contractuelle : le demandeur a alors le choix entre la juridiction du domicile du défendeur et celle du lieu où l'obligation devait être exécutée.

Il existe d'autres difficultés, notamment l'exécution des décisions : une décision prise dans un pays pourra-t-elle s'appliquer à l'étranger ? Les règles permettant l'exécution des décisions existent mais de nombreux freins réduisent leur mise en œuvre. Souvent il faut obtenir l'*exequatur* de la décision étrangère, mais cet *exequatur* n'est jamais de droit. Dans le cadre de l'Union européenne, la convention de Bruxelles rend l'*exequatur* presque automatique ; l'efficacité des jugements est ainsi maximale. Mais c'est là une exception européenne et le problème de l'effectivité des jugements demeure sur le plan mondial.

L'utopie d'un commerce électronique international

La complexité de ce qui précède ne doit pas faire oublier qu'il ne s'agissait que d'un aperçu réducteur et simplificateur de la réalité. La vérité est bien pire. Le consommateur, peu habitué jusqu'à présent au commerce international, obtient grâce à Internet la possibilité d'être plongé dans une jungle inextricable. Les litiges potentiels sont nombreux, qu'ils portent sur le paiement, l'identité des cocontractants ou sur la livraison des biens. Il est fort probable que la foule des consommateurs potentiels sera échaudée après la survenue de quelques procès.

Pourtant des efforts sont faits. Nous avons déjà cité cette loi internationale sur le commerce électronique rédigée dans le cadre de la CNUDCI. Nous pouvons également mentionner le recours croissant à l'arbitrage. Une association américaine, l'American Arbitration Association propose en effet depuis le mois de mars 1996 le Virtual Magistrate, un juge virtuel. Ce magistrat est un bénévole qui n'est lié par aucun droit national. Toute la procédure se déroule par courrier électronique. Ce sont là des efforts notables mais insuffisants.

Mettons-nous en effet à la place de l'utilisateur d'Internet désirant effectuer un achat sur le réseau. Que redoute-t-il ? Que sa commande soit interceptée par les services de sécurité nationaux ? Pas vraiment, à moins peut-être que l'objet du contrat soit illicite ! Que son numéro de carte bleue soit recueilli par des pirates ? Non plus ! Par contre, il redoute

davantage que son interlocuteur soit un escroc ou que le bien qu'il a commandé ne lui arrive jamais. Pour preuve, le téléachat, le commerce sur minitel se sont développés alors même que les numéros de cartes bleues circulent en clair et sont facilement interceptables. Il y a bien eu quelques cas de fraude, mais ceux-ci n'ont jamais réduit la confiance des utilisateurs. La raison en est simple. Les services de téléachat ou de vente sur minitel sont nationaux. Chaque utilisateur connaît la société avec qui il traite. La SNCF, Dégriftour, la FNAC... sont des enseignes connues qui suscitent la confiance. Par contre il est fort peu probable que l'internaute français aille faire ses courses en confiance chez un revendeur américain dont il n'a jamais entendu parler.

Pour réussir à s'imposer sur Internet, le vendeur doit réussir à se faire connaître du consommateur et à acquérir une image de sérieux. Certaines marques nationales ont déjà acquis leur célébrité dans le commerce traditionnel ou dans la vente par correspondance classique. Il est fort probable que leur succès se confirmera également dans le cadre du commerce électronique. D'autres marques, étrangères, sont si connues qu'elles ne sont plus ressenties par le consommateur comme étant internationales. Coca-Cola ou Microsoft en sont de bons exemples. Il est évident que ces marques peuvent obtenir la confiance du consommateur français. Il est vrai que ces sociétés ont des filiales françaises. Mais ce n'est pas là le point essentiel. En effet la présence d'une antenne sur le sol français n'est pas la condition indispensable pour développer ce sentiment de confiance. Considérons la société AMAZON. C'est une société américaine, localisée uniquement aux Etats-Unis, mais qui est en train de devenir le standard mondial de la vente de livres et de disques sur Internet. Supposons qu'elle décide d'accroître ses ventes de disques en France. Il y a fort à parier qu'à condition qu'elle développe un site en français, qu'elle se fasse connaître en France par des moyens traditionnels[11] et que la presse écrite s'en fasse l'écho, elle acquerra une notoriété en France sans qu'elle ait besoin de s'y installer physiquement. Par contre, il est tout à fait impensable qu'une société étrangère conquière des clients français par sa seule présence sur Internet. La création d'un site web est un effort important mais insuffisant pour susciter la confiance des consommateurs. La politique de marque est essentielle. La nationalité, ou l'apparence de nationalité, ne peuvent être négligées. En étant français, ou en paraissant français, les vendeurs inspireront confiance aux consommateurs français et pourront espérer s'implanter sur le marché national.

Tel est le champ du commerce électronique que l'on peut imaginer aujourd'hui. Néanmoins son développement nécessite la mise en place de certaines structures indispensables pour bâtir la confiance.

---

[11] Par moyens traditionnels, nous entendons principalement la publicité à la télévision. La publicité sur Internet est encore marginale et n'est pas devenue un gage de qualité et de sérieux. La publicité à la télévision, le label « vu à la TV » sont au contraire de bons moyens de développer la confiance chez l'utilisateur. Il est d'ailleurs intéressant de noter que les sociétés de courtage en ligne ne se contentent plus de publicité sur Internet, mais commencent à acheter des espaces publicitaires à la télévision. C'est le cas de Cortal, de Banquedirecte, de Selftrade ou de Directfinance.

Les voies de la confiance

Nous avons montré que la sécurité de la transaction n'était pas le seul élément essentiel pour que le commerce électronique se développe. Il ne faudrait pas pour autant conclure hâtivement que toute sécurité est inutile et que les cocontractants y sont indifférents. Cela signifie simplement que le consommateur et le vendeur attendent le niveau de sécurité adapté à leur transaction. Ce niveau dépend évidemment du montant de la transaction et de la fréquence de ce type de transaction. Mais les exigences de l'acheteur et du commerçant sont bien plus vastes. De nombreux intermédiaires, de nombreux réseaux doivent se créer pour mettre en confiance le consommateur et le garantir de l'impression de manque de sérieux du commerce électronique propice à la fraude.

A la recherche du bon niveau de sécurité...

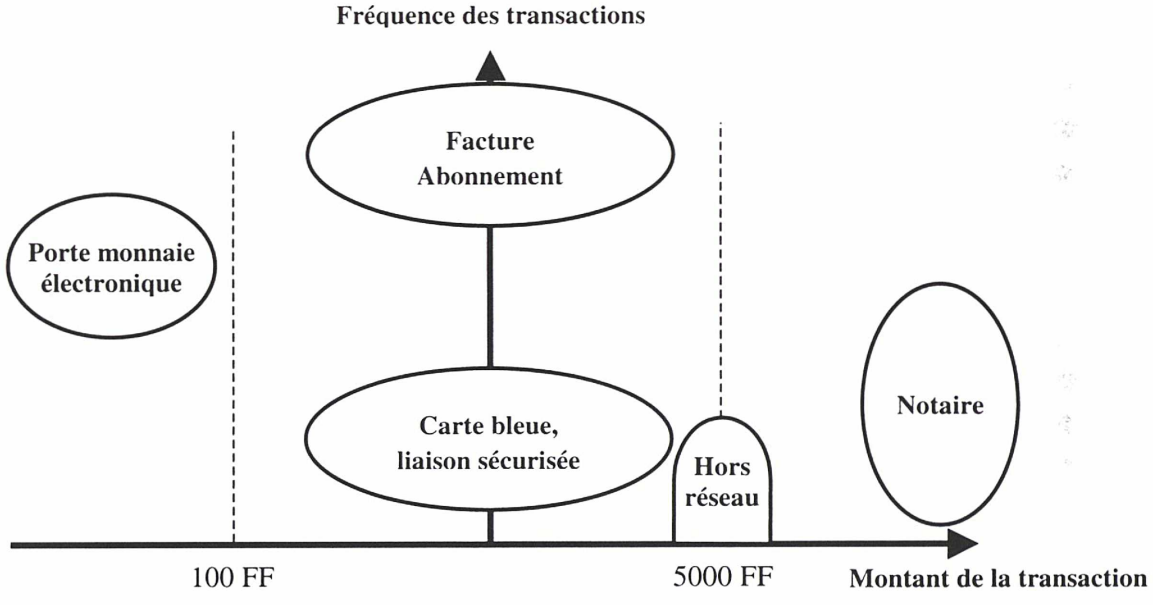
Le niveau de sécurité mis en place doit être adapté au type de transaction réalisé, de la même façon que la sécurité n'est pas uniforme pour les échanges classiques. On ne règle pas une baguette de pain comme on achète une maison ; de même, sur Internet, on ne paiera pas un livre à cent francs comme un ordinateur à dix mille francs.

Lorsque le montant des transactions effectuées est peu important, la méthode idéale de paiement est le porte-monnaie électronique. Le porte-monnaie électronique est alimenté à l'avance. Il est évident que son usage est limité à des sommes réduites. De la même façon que personne ne transporte des fonds importants dans un porte-monnaie classique, par peur du vol ou de la perte, personne n'approvisionnera son porte-monnaie électronique avec des sommes importantes. Le risque serait trop grand, en effet, que ce porte-monnaie électronique disparaisse, soit en raison d'une défaillance technique, soit en raison d'une fraude. Il est probable que le possesseur d'un porte-monnaie électronique n'y dépose pas plus de cent francs, une somme raisonnable qu'il a généralement dans son portefeuille et qu'il accepte de perdre. Dans ce cas, le niveau de sécurité est minimal. L'acheteur se protège en limitant la perte maximale qu'il peut réaliser.

A l'inverse les achats peu fréquents et d'un montant élevé doivent être entourés de toutes les précautions. Au-delà d'un montant de cinq mille francs, les transactions ne peuvent plus se réaliser entièrement sur réseau. Dans les situations les plus extrêmes, le passage devant le notaire est envisageable. Plus généralement, une facture sera envoyée au consommateur, et le paiement se fera par des moyens traditionnels, d'ordinaire par chèque. Il n'est pas évident que ce soit là encore du commerce électronique. En effet, le réseau Internet se voit cantonné à un rôle de catalogue géant et ses fonctionnalités sont très peu exploitées. Même si le seuil légal de 5000 francs est relevé, il est improbable que les comportements se modifient. Devant l'importance de la somme, les consommateurs risquent de ne pas avoir confiance dans Internet, et vont très certainement se rabattre sur des moyens de paiement classiques.

Enfin il existe des montants intermédiaires. En fonction de la fréquence des achats, la méthode de paiement devra être adaptée. Si les achats sont répétés, le consommateur hésitera à entrer systématiquement ses coordonnées bancaires et à les envoyer sur Internet, et ce pour deux raisons : c'est à chaque fois une perte de temps ; c'est aussi une multiplication inutile des risques. Le recours à un tiers est alors particulièrement profitable. Celui-ci aura pour rôle de comptabiliser les achats et d'envoyer au consommateur une facture périodique, qui pourra être réglée soit de manière classique, soit de manière informatique. Au contraire, si l'achat est rare, le recours au paiement par carte bleue à l'aide d'une liaison sécurisée paraît tout à fait satisfaisant.

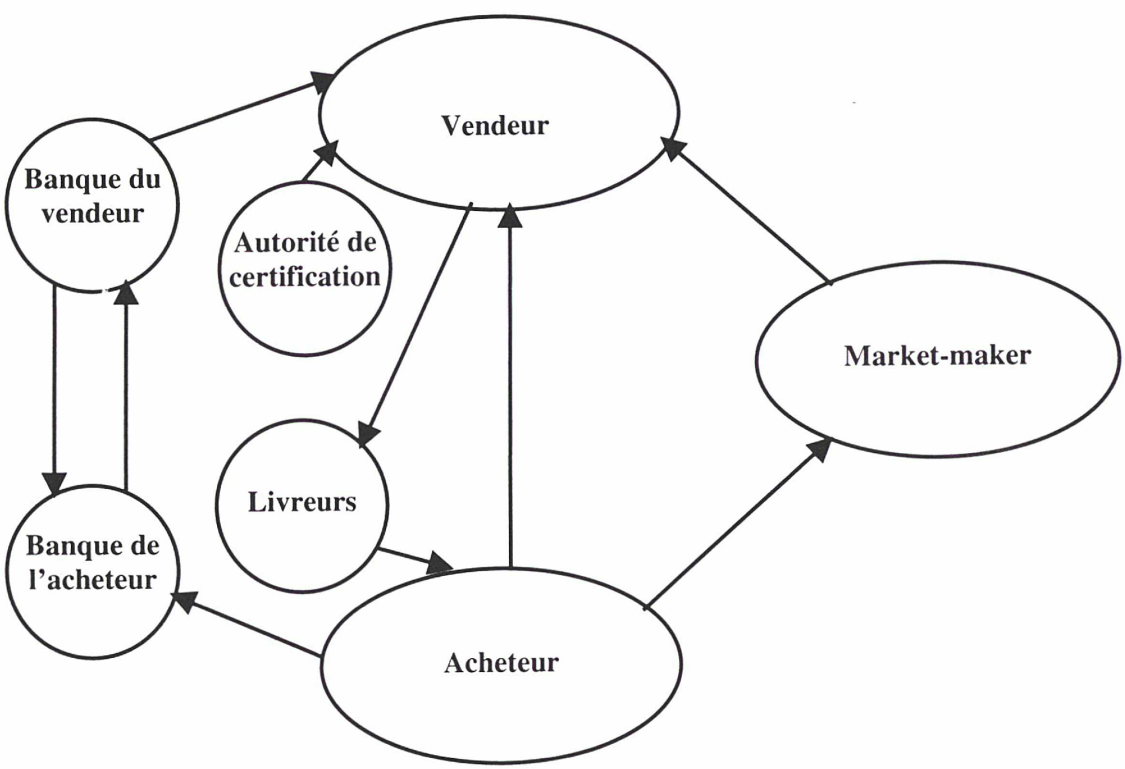
Ces différents cas de figure sont résumés sur le schéma suivant :



Toutefois, l'essor du commerce électronique requiert le développement de plusieurs intermédiaires, indispensables à l'instauration de la confiance chez les consommateurs.

Quel commerce électronique dans l'avenir ?

Le commerce électronique, tel que pratiqué aujourd'hui par les différents acteurs, est encore à l'état embryonnaire. Seules quelques grandes firmes arrivent à réaliser de substantiels chiffres d'affaires... et des pertes tout aussi substantielles. Elles sont souvent hors de tout schéma organisé de commerce. On ne se connecte et on n'achète sur ces sites que parce qu' on les connaît par ailleurs et que la relation de confiance a été bâtie de façon aléatoire (bouche-à-oreille, hasard, audace...). Le développement d'un commerce électronique valable ne peut se faire que dans le cadre de procédures de confiance structurées. Aujourd'hui, les projets d'intermédiaires dans les transactions électroniques futures, tels qu'ils se définissent eux-mêmes, permettent d'ébaucher à grands traits un schéma possible de la transaction commerciale électronique. Le schéma ci-dessous tente d'esquisser les relations indispensables entre les diverses parties prenantes du commerce électronique.



Lorsqu'un consommateur entre en contact direct avec un vendeur, il est fort probable qu'il le connaisse déjà. Peut-être est-il un client fidèle ; peut-être a-t-il connu ce site grâce à un ami déjà client ou grâce à la publicité. En tout cas la relation de confiance est déjà établie.

Lorsque le consommateur recherche un produit sur Internet, la situation est beaucoup plus complexe. Il nous semble que dans ce cas l'intervention de ce que nous avons décidé d'appeler un *market-maker* est indispensable. Par *market-makers*, nous entendons des intermédiaires connus qui indiqueraient au consommateur des sites dont ils garantiraient le sérieux et l'honnêteté. Cet intermédiaire, qui jouirait de la confiance des consommateurs grâce à sa taille ou à sa notoriété déjà acquise, permettrait ainsi à divers vendeurs, trop petits ou trop éloignés des consommateurs pour inspirer confiance *a priori*, d'être connus, d'être repérés des acheteurs et d'être pour ainsi dire cautionnés par un organisme garant de leur moralité.

Sans lui le consommateur n'aura pas confiance et interrompra vraisemblablement la transaction avant son terme. Il ne faut pas croire que les moteurs de recherche, à l'instar de www.voila.fr ou de www.yahoo.com, puissent être considérés comme des *market-makers* acceptables. Ces sites ne sont que des annuaires géants plus ou moins intelligents et plus ou moins bien programmés. Les sites qui y sont référencés sont de qualité fort variable. La procédure de référencement, très rapide, ne donne lieu à aucune enquête de la part des gérants des moteurs de recherche. Ils ne peuvent donc en aucune manière être ces intermédiaires capables de générer de la confiance dans les esprits des consommateurs.

Ce genre d'intermédiaires existe déjà aux Etats-Unis. Certains sites servent en effet d'intermédiaires entre acheteurs et vendeurs de voitures d'occasion. L'acheteur transmet au site le type de voiture qu'il cherche. Le site sélectionne alors une série de vendeurs qui pourraient satisfaire cette demande. La présence de ces vendeurs sur le site est censée être une preuve du sérieux de l'offre, voire de la qualité de la voiture.

De tels intermédiaires commencent à se développer en France. Récemment, le fournisseur d'accès AOL a proposé à quatre sociétés de courtage par Internet d'être référencées sur son site. Le ticket d'entrée, fixé à 250000 francs, crédibilise les sociétés qui font l'effort d'être présentes. AOL permet en échange à ses abonnés de connaître ces sociétés de courtage et leur assure implicitement que ces sociétés n'hébergent pas une armée d'escrocs.

Dans le même ordre d'idée, France Télécom a inauguré en mai 1998 le service Télécommerce. Ce site est une vitrine sur le monde pour le commerçant. Grandes entreprises et PME y ont la même visibilité, et ce pour un coût modeste. En outre, toutes les sociétés profitent de la promotion de leur enseigne sur les sites d'audience de France Télécom. A la fin 1998, le site de Télécommerce hébergeait une cinquantaine de boutiques.

Il est tentant de voir dans ces intermédiaires la préfiguration du commerce électronique de demain. Toutefois, une question au moins devra être résolue avant qu'il en soit ainsi, celle de la responsabilité du *market-maker*. En effet, si le consommateur est escroqué ou même simplement déçu par le vendeur, c'est en partie à cause du *market-maker*, en qui il a eu confiance et qui avait référencé ce site. Il est fort probable que le *market-maker* s'empressera de retirer de ses listes ce commerçant indélicat. Il n'en restera pas moins qu'un préjudice aura été subi. La responsabilité du *market-maker* ne peut pas se substituer *a priori* à celle du commerçant. Le vendeur pourrait alors être tenté de s'adonner à des attitudes peu professionnelles. Mais la responsabilité du *market-maker* ne doit pas non plus être écartée d'office car il faut qu'en cas de fraude le conseilleur soit – partiellement – le payeur. C'est là un équilibre difficile à trouver, mais indispensable au développement de ce type d'intermédiaires. Le consommateur ne peut en effet accepter qu'en cas de problème la société conseillère décline toute responsabilité.

D'autres intermédiaires sont nécessaires au sentiment de confiance. Parmi eux se trouve le livreur. Il est d'ailleurs significatif que depuis quelque temps la plupart des sites marchands mettent en avant la société de livraison avec laquelle ils sont en relation, voire laissent le client choisir le livreur qu'il préfère. Ces sociétés de livraison, qui sont connues, sont censées inspirer confiance au client. Elles sont également un gage de sérieux de la société commerciale.

Bien entendu, les autorités de certifications auront un rôle important à jouer dans le schéma de fonctionnement du commerce électronique de demain. Nous ne reviendrons pas sur ce point, que nous avons amplement développé précédemment. Nous rappelons seulement que ces autorités de certification garantissent uniquement que le site auquel est connecté le consommateur appartient à la bonne personne et que l'interlocuteur est effectivement celui qu'il prétend être. En aucune façon elles ne sont garantes de la moralité de l'interlocuteur. Elles remplissent donc une fonction complémentaire et différente de celle qu'exercent les *market-makers.*

Enfin, les banques seront amenées à jouer un rôle central dans le développement des échanges électroniques. En effet, le paiement direct de banque à banque peut protéger les commerçants contre les impayés. Dans le schéma actuel, l'acheteur transmet au vendeur à la fois sa commande et ses coordonnées bancaires. On peut imaginer qu'à l'avenir, l'acheteur transmette au vendeur seulement sa commande. Le vendeur lui donne alors le nom de la banque auprès de laquelle le paiement doit être effectué. L'acheteur demande alors à sa propre banque, en qui il a théoriquement confiance, d'effectuer le paiement. Une fois le règlement effectué, la banque du vendeur prévient le commerçant, qui peut donner l'ordre de livrer en toute sécurité[12].

[12] Le protocole SET, développé par VISA, assure le paiement et la confidentialité des achats. Il tarde néanmoins à s'imposer, car il n'est pas inclus de façon standard dans les navigateurs ou sur les ordinateurs.

Conclusion

Aujourd'hui, deux typologies d'acheteurs se dégagent : le butineur et le spécialiste. Le premier passe du temps sur un site et en profite pour regarder de nombreux articles, pour fouiner et pour feuilleter les pages du catalogue qui lui est proposé. Ce client est en règle générale très fidèle, et revient souvent sur les mêmes pages. Il se comporte en fait comme un consulteur de catalogue classique. Les sites qui ont de tels clients sont les sites de vente par correspondance, qui réservent des fonctions spéciales à leurs clients. Les acheteurs de ce type se connectent principalement le soir et le week-end, aux heures où la famille est réunie autour du micro-ordinateur.

Le deuxième type de client est ce qu'on pourrait appeler le spécialiste : il sait ce qu'il cherche, et veut essentiellement des renseignements d'ordre technique, financier... Cet acheteur est extrêmement volatil, il se peut qu'il aille en fin de compte acheter sur un autre site ou chez un vendeur traditionnel. Ce client consulte différents sites. En règle générale, il ne fait pas confiance. Il poursuit la procédure d'achat jusqu'au moment où il doit payer, puis se rétracte au dernier moment.

Face à ces deux sortes de clients, les sites réagissent de façon différente. La Redoute, par exemple, pour tirer partie de sa relation privilégiée avec le client qui se connecte, présente un site très convivial permettant de rentrer dans une relation personnalisée avec le magasin. Ce site propose en fait un choix assez limité d'articles, mais permet de butiner comme s'il s'agissait d'un catalogue classique. Le principe est exactement celui d'une liste de commande de VPC classique. Il y a alors un panier de commande avec récapitulatif.

Ce site fait fortement penser à un catalogue en ligne. Il n'y a pas d'information supplémentaire par rapport à un catalogue La Redoute. La véritable nouveauté, c'est le contact personnalisé avec un vendeur ou un employé de la Redoute. Le client de la Redoute qui se connecte sur le site a alors l'impression d'être un client privilégié de la VPC moderne, d'être écouté et pris en compte.

A l'autre bout du spectre se trouve un client plus insaisissable. Le spécialiste se connecte principalement au bureau, il se sert de son temps libre pour collecter des informations. Il est plus insaisissable, car son activité est par essence coupable, il doit faire vite pour éviter de se faire repérer. Une fois sur le site, il se faufile très rapidement vers l'article qui l'intéresse, télécharge les informations techniques gratuites, puis s'évapore ! Tel est le client[13] classique du site FNAC. Il peut y trouver des informations techniques téléchargeables. Ces fiches sont particulièrement bien remplies et concourent à faire comprendre au client que le vendeur est sérieux.

[13] Terme certainement inadéquat, puisque ce client n'achète pas !

Aujourd'hui, la proportion des ménages français qui ont accès à Internet autrement que par la connexion au bureau est de 4 %. La cible potentielle des sites marchands est donc une frange relativement minime de la population. La tranche de population aujourd'hui susceptible d'être touchée par le commerce électronique est une population qui a du pouvoir d'achat ; or aujourd'hui, la majeure partie des personnes qui se connectent sont des « moins de dix-huit ans », dont l'habilité à surfer sur le Net est évidente, mais dont la capacité d'achat reste très limitée. Cette tranche d'âge sera sans doute dans l'avenir une cible potentielle intéressante, car elle aura les capacités techniques et la capacité d'achat. Mais dans cette hypothèse, il ne faut pas attendre de décollage mirifique du commerce électronique avant quelques années.

L'autre partie de la population susceptible de pratiquer le commerce électronique est une frange de la population relativement particulière. En effet, c'est une population de haut niveau d'éducation dont le revenu est largement supérieur à la moyenne. Cette population semble plus pratiquer le commerce électronique comme un gadget, au sens où elle ne paraît pas encore lui reconnaître d'utilité intrinsèque.

Les employés de bureau, qui pourraient enfin fournir un gisement de clients potentiels sont enfin peu susceptibles de commercer depuis leur bureau de façon massive. En effet, si un tel phénomène se produisait, il y aurait fort à parier que les employeurs, aux raisons de rentabilité, ne voient pas d'un œil très favorable un tel engouement pour le commerce pratiqué sur le lieu de travail, aux horaires de travail ! Néanmoins, cette voie est aussi un facteur de développement, car l'importance prise au travail de l'*e-mail*, et la connexion journalière donnent souvent envie de s'équiper et de se connecter pour son propre compte. Il pourra à terme devenir un des usagers *internautes* qui peuplera le *cyberespace* et devenir un *cyberconsommateur*, mais le chemin de décision est souvent bien long.

Ces deux types d'utilisateurs d'Internet ont beau être extrêmement différents, ils possèdent néanmoins un point commun. Ni l'un ni l'autre ne voient dans la sécurité l'une de leurs préoccupations essentielles. Il ressort en effet des enquêtes menées par les gestionnaires de site que les attentes du consommateur sont tout autres. Connecté, le consommateur recherche tout d'abord de la simplicité. L'ergonomie du site est essentielle. Il y a fort à parier que nombre de consommateurs renonceront à acheter non parce qu'ils douteront de la sécurité de la transaction, mais parce qu'ils se seront lassés avant d'atteindre le point de paiement... D'autres attentes ont été identifiées, comme l'harmonisation des procédures entre les divers sites concurrents ou la multiplicité du choix. Mais jamais la sécurité n'apparaît comme une attente prioritaire du consommateur. C'est tout à fait compréhensible lorsqu'on se souvient que le consommateur traditionnel ne l'a jamais réclamée ; c'est encore plus compréhensible dans le cas du commerce électronique, car la complexité technique à mettre en œuvre pour assurer la sécurité des transactions est difficilement présentable au consommateur non initié. Celui-ci est bel et bien contraint de faire confiance à la technique.

Par conséquent, les professionnels auront certainement intérêt à présenter les questions de sécurité comme étant réglées. Ils devront aussi se souvenir que seule, la sécurité n'est pas un argument de vente. L'essentiel de leur effort sera de réussir à se faire connaître, à susciter de la confiance chez les consommateurs et à faire en sorte que cela se sache auprès des autres consommateurs potentiels. Le système du « satisfait ou remboursé », qui a contribué de façon importante au succès de la vente par correspondance classique, devra être transposé au commerce électronique. Les moyens de communication traditionnels, plus éprouvés et touchant un plus large public, devront être utilisés de façon beaucoup plus intensive qu'aujourd'hui. Enfin il semble évident que le marché est ouvert pour quelques intermédiaires, peu nombreux mais ressentis comme sûrs par le public, qui garantiront les transactions et amèneront les consommateurs et les vendeurs en confiance vers le commerce électronique de masse.

Annexe : quelques compléments sur la cryptologie

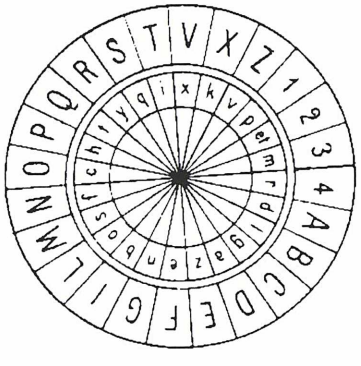
Petite histoire de la cryptologie

Genèse

Née en l'an 2000 av J.C. sur les bords du Nil, dans une ville appelée *Menet Khufu*, la cryptologie était à l'origine l'œuvre d'un scribe voulant rendre plus solennelle la pierre funéraire de son maître, et qui a sciemment altéré les hiéroglyphes qu'il utilisait. Cette méthode connut un certain engouement parmi les scribes, mais le manque de cohérence dans les altérations pratiquées ne suscita pas chez les lecteurs l'enthousiasme souhaité.

Sparte, au V^{e} siècle avant J.C., inventa le premier moyen de chiffrement militaire connu : *la scytale*. Il s'agissait d'un morceau de bois, autour duquel on enroulait en spires jointives un ruban de papyrus, cuir ou parchemin. Le texte était alors écrit en lignes droites successives parallèles à l'axe du morceau de bois. Le ruban, une fois déroulé, n'était alors lisible que par une personne possédant un morceau de bois de même géométrie. Un tel procédé est mentionné par des historiens grecs tels que THUCYDIDE ou PLUTARQUE.

CESAR fut le plus célèbre utilisateur de procédé cryptologique de guerre en envoyant à CICERON un texte où chaque lettre claire était remplacée par celle située trois rangs plus loin dans l'alphabet. L'Occident chrétien au Moyen Age ne pratique quasiment pas la cryptologie, et il n'y eut aucune recherche suivie en matière de cryptanalyse, sauf au Moyen-Orient, où l'intérêt pour la cryptologie se manifesta en l'an 855 avec le savant Abu Bakar ben Wahshiyya, auteur d'un traité de cryptologie traitant des premiers alphabets secrets connus.



Cadran chiffrant d'Alberti

En 1467, Leon Batista ALBERTI inventa la substitution polyalphabétique : deux disques concentriques et de diamètres différents font correspondre des lettres. En tournant le disque, on substitue de cette façon une lettre à une autre. En convenant avec le destinataire du cryptogramme d'une lettre repère, on peut par exemple à la fin de chaque groupe de quatre ou cinq mots, décider de changer la place de cette lettre repère en faisant tourner les disques, et indiquer quelle est la lettre correspondant à cette lettre repère en l'écrivant en clair au début de chaque groupe de mot correspondant à un changement des positions relatives des deux disques.

En 1518, le bénédictin Jean TRITHEME inventa lui aussi un système de substitution polyalphabétique ; il utilisait un tableau appelé *tabula recta :*

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Afin de procéder au cryptage du texte, l'abbé TRITHEME utilisait pour la première lettre le premier alphabet, pour la deuxième, le deuxième alphabet, et ainsi de suite. En 1563, Giovanni Batista BELASO invente la notion de *clef littérale de chiffrement*. Cette clef est une suite de caractères qui indique quelle substitution polyalphabétique utiliser à tour de rôle.

L'importance croissante que prit la cryptologie dans le domaine politique fit la fortune de cryptologues tels que Antoine ROSSIGNOL ; ses décryptements le rendirent suffisamment riche pour lui permettre de se construire un château à Juvisy. Au XVIII^{e} siècle, de nombreux cabinets noirs se développent à travers toute l'Europe, faisant les riches heures des ouvreurs de lettres. Mais au moment où ces cabinets, sous la pression démocratique et l'indignation des concitoyens, allaient disparaître en Angleterre au XIX^{e} siècle, une invention allait donner à la cryptologie un essor nouveau, et aux gouvernements de nouveaux vices en matière d'écoute de la vie privée : le télégramme.

Les Temps Modernes

Le bureau 40 fut le plus emblématique organisme de la première guerre mondiale en matière de chiffrement. Ce bureau, composé de plusieurs professionnels passionnés de cryptologie, déchiffra les messages destinés à la flotte allemande, et d'octobre 1914 à février 1919, plus de quinze mille télégrammes de l'armée allemande furent déchiffrés dans ce bureau. Le plus fameux des télégrammes qui passa dans les mains de ce bureau fut le télégramme ZIMMERMAN, qui précipita l'entrée dans la Première guerre mondiale des Etats-Unis.

Avec la Première guerre mondiale et l'essor que prit la communication parmi les armes de guerre, la cryptologie, sur la base de quelques succès (bombardement de Thielt, télégramme ZIMMERMAN...), prit au yeux des militaires une importance primordiale. Une des causes directes de cette montée en puissance fut l'augmentation considérable du volume des communications.

Une des histoires les plus connues de la Seconde guerre mondiale en matière de chiffrement fut l'épopée de la machine ENIGMA. En 1923, la *Chieffrenmaschinen Aktien Gesellschaft* montre au congrès postal de Berne la première version de la machine à coder ENIGMA. Les gouvernements sont intéressés et sont pratiquement les seuls à acheter ces machines. En 1934, la marine allemande l'utilise, suivie peu après par l'aviation en 1935.

La Grande-Bretagne, comme en 1914, réunit des savants à Bletchley sous la conduite de TURING, qui réussirent à briser le code, même lorsque les Allemands mettaient au point des versions plus avancées d'ENIGMA.

Après-guerre, le gouvernement américain mit sur pied une agence spécialisée dans l'écoute et la surveillance des messages, la NSA (*National Security Agency*), dont le rôle controversé dans l'affaire du réseau ECHELON et la volonté d'un écoute hégémonique en font, avec environ trente mille collaborateurs, le *Big Brother* de la planète.

Quelques systèmes simples

La première étape dans la réalisation d'un cryptogramme est la découpe du texte en éléments de « longueur » n, n fournissant la taille de l'unité de base. On établit alors une équivalence entre les éléments de texte et $\mathrm{Z}/n\mathrm{Z}$; par exemple, $n=26$ correspond au codage simple $\mathrm{A}\leftrightarrow 1\,[26], \mathrm{B}\leftrightarrow 2\,[26], ..., \mathrm{Z}\leftrightarrow 26\,[26]$. Mais prendre des puissances de 2 ($n=2^8$, $n=2^{16}$, $n=2^{32}$...) correspond au codage des systèmes d'exploitation les plus couramment employés. A partir de cette étape, le travail de codage s'opère dans l'espace $\mathrm{Z}/n\mathrm{Z}$. Si on se place dans l'exemple du langage de l'ordinateur regardé comme suite de 0 et de 1, chaque élément de cette suite étant appelé *bit*, on transforme chaque lettre en bloc de huit bits, soit 256 caractères possibles, selon une table de conversion standardisée.

Un texte X que l'on désire crypter est considéré comme une suite $x_1, ..., x_p$ de blocs élémentaires de « longueur » n ; l'ensemble des blocs élémentaires sera noté Ξ. Le système de cryptage est alors la donnée de (K, e, d), avec :

- K un ensemble fini de clefs de cryptage possibles ;
- $e : K\times\Xi\rightarrow\Xi$, la fonction de cryptage ;
- $d : K\times\Xi\rightarrow\Xi$, la fonction de décryptage.

La clef est un code convenu à l'avance entre les communicants et qui permet d'utiliser le même système tout en gardant le secret. La fonction e et la fonction d sont telles que pour tout k de K, on ait la relation suivante : $d(k, e(k, x)) = x$. En termes non mathématiques, il faut que la fonction de décryptage puisse décrypter ce que la fonction de cryptage a réalisé.

Le premier système cryptographique, celui de Jules CESAR, est un cryptage par décalage : $n=26$, et la fonction de cryptage et de décryptage sont les suivantes : $e(k, x) = x + k$; $d(k, y) = y - k$. Dans le cas historique, $k=3$. Par exemple, avec $k=11$, le texte clair suivant :

WEWILLMEETATMIDNIGHT

sera transformé dans $\mathrm{Z}/26\mathrm{Z}$ en :

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19

puis en ajoutant $11[26]$ deviendra :

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

soit finalement :

HPHTWWXPPELEXTOYTRSE

Un autre système est le codage par permutation. Dans ce cas, $n = 26$, et K est l'ensemble des permutations possibles de $\mathrm{Z}/26\mathrm{Z}$. On définit alors $e(p,x) = p(x)$ pour p permutation de $\mathrm{Z}/26\mathrm{Z}$, et $d(p,y) = p^{-1}(y)$.

Le système de codage dit affine est le système suivant : soit a inversible dans $\mathrm{Z}/26\mathrm{Z}$ et b un élément quelconque de $\mathrm{Z}/26\mathrm{Z}$; la clef est alors notée (a,b) et on définit le système par $e((a,b),x) = ax + b$. Comme a est un élément inversible, il existe alors a^{-1}, et la fonction de décryptage est : $d((a,b),y) = a^{-1}(y - b)$.

De façon plus générale, on définit le système de VIGENERE par la donnée d'une clef k dans $\mathrm{M}_m(\mathrm{Z}/26\mathrm{Z})$, l'ensemble des matrices inversibles de taille $m \times m$ dans $\mathrm{Z}/26\mathrm{Z}$; la fonction de cryptage est alors donnée pour une chaîne $x_1, ..., x_m$ par la fonction suivante : $e(k, x_1, ..., x_m) = (x_1, ..., x_m).k = (y_1, ..., y_m)$. Comme k est inversible, on définit la fonction de décryptage par $d(k, y_1, ..., y_m) = (y_1, ..., y_m).k^{-1}$.

L'ensemble de ces moyens de cryptage connus depuis longtemps possèdent un biais par lequel il est possible de repérer facilement la clef, ainsi que la longueur de celle-ci. Les occurrences des lettres dans les langues sont spéciales. Pour deux textes $x = x_1, ..., x_m$ et $y = y_1, ..., y_{m'}$, on définit l'indice de coïncidence par la probabilité qu'un élément quelconque de x soit égal à un élément quelconque de y. Si le premier texte est un texte en clair et le second un texte crypté par décalage, suivant l'indice de décalage k, on obtient les résultats suivants :

k	Indice de coïncidence
0	0.065
1	0.039
2	0.032
3	0.034
4	0.044
5	0.033
6	0.036
7	0.039
8	0.034
9	0.034
10	0.038
11	0.045
12	0.039
13	0.043

Le seul indice qui soit supérieur à $0{,}06$ correspond à $k=0$, c'est-à-dire à deux textes clairs. A partir d'une grande quantité de textes cryptés par de tels systèmes, ou à partir de textes clairs et de textes cryptés correspondants, des méthodes probabilistes utilisant ces occurrences de lettres permettent de retrouver rapidement la longueur de la clef, puis sa structure. Aujourd'hui, de tels procédés ne sont plus utilisés, car les procédés de cryptanalyse basés sur ces méthodes probabilistes permettent de casser très rapidement ces cryptages.

Data Encryption Standard (DES)

En mai 1973, le National Bureau of Standards lança un appel d'offre pour un système de cryptage. IBM offrit alors son standard (LUCIFER) qui fut adopté en 1975, et est devenu depuis l'un des standards mondiaux pour le cryptage.

Si on note B_l l'ensemble des chaînes de l bits ($B_l = \{(a_1,...,a_l), a_i \in \{0,1\}\}$), le système comporte deux permutations de clef, p_1 et p_2, une fonction $f : B_{32} \times B_{48} \to B_{32}$ et une permutation initiale notée p.

Le système DES utilise en entrée une clef de 56 bits notée k, qui est accompagné de 8 bits utilisés pour la détection d'erreurs dans le cryptage. On écrit $p_1(k) = C_0 D_0$, puis pour i allant de 1 à 16, on définit $C_i = S_i(C_{i-1})$ et $D_i = S_i(D_{i-1})$, avec S_i représentant la fonction de décalage (vers la gauche) de un cran pour $i = 1, 2, 9, 16$, et de deux crans sinon. On récupère alors seize sous-clefs $k_i = p_2(C_i D_i)$. On code alors par bouts de

soixante-quatre bits de la façon suivante : soit x le texte en clair, on écrit $x_0 = p(x) = L_0 R_0$. Pour i compris entre 1 et 16, on procède aux opérations suivantes : $L_i = R_{i-1}$ et $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$, où $\oplus$ représente le ou exclusif bit à bit. On obtient ainsi $L_{16} R_{16}$, et le texte crypté est alors $y = p^{-1}(L_{16} R_{16})$.

DES est un algorithme symétrique (même si cela ne saute pas aux yeux !) car la fonction de cryptage e et la fonction de décryptage d sont les mêmes, et aujourd'hui, les méthodes d'attaque sur cet algorithme sont des méthodes dites de cryptanalyse différentielle, introduites par BIHAM et SHAMIR. Elles utilisent les comparaisons ou exclusif bit à bit entre deux textes clairs et entre les deux textes cryptés correspondants.

Cryptologie à clef publique

La cryptologie à clef publique a trouvé la source de son développement dans la difficulté à pouvoir transmettre la clef de chiffrement k de façon sûre entre les parties voulant communiquer. L'idée est de donner une information connue de tous, appelée clef publique, permettant :

- de coder les messages, que seule une autre partie de la clef peut décoder, et ce dans un but de confidentialité ;
- de décoder les messages, que seule une autre partie de la clef peut coder, dans un but de signature,

avec la condition supplémentaire que la connaissance de la partie publique de la clef ne permette pas de retrouver facilement le reste de la clef.

Concrètement, il existe aujourd'hui différents systèmes de cryptage à clef publique ; on peut citer le système MCELIECE, ELGMMAL, CHOR-RIVEST ou celui des courbes elliptiques. Néanmoins, le plus répandu et le plus simple est le système dit RSA (de ses « inventeurs » RIVEST, SHAMIR et ADELMAN) , qui est aujourd'hui utilisé par le logiciel de cryptage le plus usuel : PGP.

Le système RSA est le suivant : soit p et q deux entiers premiers de grande taille et $n = p.q$. Soit a et b deux entiers tels que $a.b = 1\ [\varphi(v)]$ où $\varphi(v)$ est la fonction indicatrice d'Euler de n. On rappelle que $\varphi(v)$ est le nombre d'entiers inférieurs à n et premiers avec ce dernier. Dans le cas particulier où $n = p.q$, $\varphi(v) = (p-1).(q-1)$. On rappelle de même pour tout x dans $\mathbb{Z}/n\mathbb{Z}$, on a l'identité suivante : $x^{\varphi(v)} = 1\ [n]$. La partie publique de la clef est alors (b,n), la partie privée est (a,n), la clef est formellement définie par $k = (a,b,n,p,q)$. On définit alors la fonction de cryptage par $e(k,x) = x^b\ [n]$ et

la fonction de décryptage par $d(k,y) = y^a \ [n]$. On a bien $d(k,e(k,x)) = x \ [n]$ car $d(k,e(k,x)) = x^{ab}$ avec $a \,.\, b = 1 \ [\varphi(v)]$.

On utilise alors ce système de la façon suivante : l'envoyeur qui veut crypter un message utilise la clef publique de son correspondant, qui étant le seul à posséder la clef privée correspondante est le seul à pouvoir lire le message crypté. L'expéditeur qui veut signer son message utilise sa clef privée qui, étant connue de lui seul, authentifie que le message n'a pu émaner que de lui.

On peut remarquer qu'en fait, seule la connaissance de (n,a,b) est suffisante pour les utilisateurs, et si on veut retrouver rapidement a à partir de b, il n'y a aujourd'hui qu'une seule solution satisfaisante du point de vue de la faisabilité et de la rapidité : factoriser n en p et q, et donc retrouver $\varphi(v)$ rapidement. Or aujourd'hui, une telle factorisation est « impossible » car il n'existe pas d'algorithme suffisamment rapide dès que p et q sont suffisamment grands.

Prenons par exemple $p = 101$ et $q = 113$. Alors $n = 11413$ et $\varphi(v) = 11200 = 2^6.5^2.7$. Pour la clef privée b, tout nombre entre 0 et 11200 qui ne soit pas divisible par $2, 5$ ou 7 convient. Prenons $b = 3533$; on a $b^{-1} = 6597 \ [11200]$. La partie publique de la clef (qui est disponible pour tous) est alors $(3533,\ 11413)$, la partie privée est $(6597,\ 11413)$. Si l'on veut envoyer le message 9726 (correspondant à un texte du style OK) de façon sécurisée au possesseur du système ci-dessus, l'envoyeur utilise alors la clef publique de son correspondant et calcule $9726^{3533} \ [11413] = 5761$. Le correspondant recevant alors ce message utilise sa clef privée et calcule $5761^{6597} \ [11413] = 9726$.

Le principal défaut de RSA est dû au caractère particulièrement lent des calculs de modulo dans un système informatique. Aujourd'hui, la plupart des systèmes de cryptage utilisent un algorithme symétrique pour la transmission des données, et un algorithme de type RSA pour l'échange préalable des clefs de cryptage de l'algorithme symétrique.

Glossaire

Clef : code secret permettant d'encoder ou de décoder un message.

Commerce électronique : tous échanges commerciaux faisant appel, à plus ou moins grande échelle, au réseau Internet.

Cryptanalyse : art de retrouver les systèmes et les clefs de cryptage à partir des textes codés.

Cryptologie : toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens matériels ou logiciels conçus à cet effet.

Internaute : utilisateur d'Internet.

Internet : le plus important réseau informatique mondial.

Market-maker : intermédiaire commercial référençant des vendeurs et s'en portant garant dans une certaine mesure.

Moteur de recherche : service proposé aux internautes leur permettant de trouver les sites correspondant aux mots clefs qu'ils ont sélectionnés (sorte d'annuaire).

PGP : logiciel de cryptage asymétrique à clef publique capable d'assurer confidentialité et authenticité aux communications électroniques.

Produits dématérialisés : produits qui sont livrables directement par le réseau tels que les logiciels, la musique, les films…

RSA : système de cryptage asymétrique mis au point en 1977 par RIVEST, SHAMIR et ADLEMAN.

Signature : désigne les quelques lignes de texte que l'on ajoute à un message électronique pour en identifier l'auteur.

Tiers de confiance : intermédiaire se chargeant de la séquestre des clefs privées, et susceptible de les remettre aux autorités étatiques.

Tiers de certification : intermédiaire attestant l'identité du possesseur d'une clef publique.

Virus : logiciel capable de se dupliquer causant des dégâts aux ordinateurs infectés.

Bibliographie

Applied Cryptography, Bruce SCHNEIER, John Wiley & Sons

Au-delà du Marché : Quand le Lien Importe plus que le Bien, Bernard COVA, L'Harmattan

Créer et exploiter un commerce électronique, Michelle JEAN-BAPTISTE, Litec

Cryptography, Theory and practice, Douglas R. STINSON , CRC Press

Droit de l'Internet, Valérie SEDALLIAN, Net Press

Internet et le Droit, Olivier ITEANU, Eyrolles

Internet et les réseaux numériques, Conseil d'Etat, La documentation française

Internet, Que sais-je ?, Arnaud DUFOUR, PUF

La Science du Secret, Jacques STERN, O. Jacob

La Société de Confiance, A. PEYREFITTE, O. Jacob

Le commerce électronique, aspects juridiques, dir. Alain BENSOUSSAN, Hermès