Présente :

La protection du secret des courriers électroniques en Belgique :

Aspects techniques [1]

Travail réalisé dans le cadre du cours de
Criminalité liée aux nouvelles technologies
Université de Liège
Faculté de droit
Ecole Liégeoise de Criminologie Jean Constant

Frédéric COLANTONIO

D.E.S. en criminologie
Orientation Criminalité des organisations

Année académique 2001-2002

Date de mise en ligne :1décembre 2002

[1] Ce travail s'inscrit dans le cadre d'une triple contribution sur la même thématique : la protection du secret des courriers électroniques en Belgique. Le présent texte reprend la contribution de l'auteur, portant sur les aspects techniques du sujet.

“Internet, c'est d'abord une image, celle d'un réseau ouvert sur lequel les hommes communiquent sans frontières et s'échangent librement des informations” [2] .

[2] WARUSFEL B., *La propriété intellectuelle et l'Internet*, Évreux, Flammarion, 2001, p.9.

Texte à jour au 31 juillet 2002

Table des matières

Introduction

"Il est devenu un lieu commun de prétendre qu'en ce début de millénaire, l'avènement des technologies de l'information et des télécommunications a remodelé le paysage économique et social en lui conférant une coloration digitale, à la faveur de ce que d'aucuns qualifient de seconde révolution industrielle ou de révolution informatique" [3] .

Il est vrai que l'internet représente aujourd'hui un média tout à fait singulier qui a bouleversé la relation des individus au temps et à l'espace, ouvrant la voie à une nouvelle dimension que d'aucuns qualifient de "glocale". Le terme est employé pour désigner la vie en réseau, caractérisée par un rapprochement virtuel spatial et temporel dont il résulte une *"forte polarisation aux deux extrêmes : le local et le global"* [4] .

Dans ce contexte, affirmer encore que le développement de l'internet, comme moyen de communication tout d'abord, comme source d'information ensuite, constitue une révolution s'avère en effet pratiquement suranné. Après une période d'exaltation, l'heure est à présent à la structuration des développements foisonnants issus des premiers balbutiements. C'est ainsi que, parmi les considérations pragmatiques qui alimentent les réflexions actuelles sur le réseau, la sécurité a progressivement pris une place toute particulière.

Parce que *"l'information est devenue infinie"* [5] et infiniment disponible, l'internet offre un accès illimité à la mémoire du monde, annulant la courbe d'oubli de l'esprit humain. L'adage selon lequel "les paroles s'envolent, les écrits restent" prend par ailleurs tout son sens à l'heure de l'informatique en réseau. Une certaine vigilance s'impose donc quant à la préservation de certaines informations.

En outre, l'utilisation à des fins militaires, politiques ou économiques de certains renseignements privilégiés, obtenus licitement ou non, ne saurait être sous-estimée plus longtemps. Qu'il s'agisse de réseaux d'espionnage (tel Echelon [6]) ou des procédés de veille technologique [7] , l'information en tout genre fait aujourd'hui l'objet de toutes les convoitises, et les mesures de sécurité visant à protéger les données sont de plus en plus conséquentes.

D'un autre point de vue, le développement du commerce électronique et des

---

[3] MEUNIER C., La loi du 28 novembre 2000 relative à la criminalité informatique, *in* Actualités du droit des technologies de l'information et de la communication, C*UP*, février 2001, vol.45, p.41.

[4] FINKIELKRAUT A., SORIANO P., *Internet - L'inquiétante extase*, Turin, Mille&Une Nuits, 2001,p.63.

[5] SALVAGGIO S., Interview – Anthropologie de la société digitale, *Inside Internet*, n°47, novembre 2001, p.66.

[6] http://www.echelonwatch.org/. Pour plus d'informations, voy. notamment MARTIN D., MARTIN F.-P., *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, PUF, 2001, pp.51 et s.

[7] Voy. notamment VAN POUCKE F., Marketing – La veille : tout savoir sur vos marchés, *Inside Internet*, n°48, décembre 2001, pp.58-60.

transactions en ligne a contraint à la sécurisation des procédés de conclusion des contrats. L'importance des courriers électroniques (ou e-mails) en la matière, tant dans les relations B2B (*business-to-business*) que B2C (*business-to-consumer*), a imposé la sécurité des transactions afin que la prospérité de l'e-commerce ne soit pas compromise par la frilosité des consommateurs, due à un manque de confiance ou d'assurance dans les procédés actuels [8] .

Le respect de la vie privée constitue également une thématique particulièrement délicate à mettre en oeuvre sur l'internet. La stricte protection des données est ici dépassée par la problématique plus large de l'envoi et de la réception de courriers non sollicités. Dans ce cadre, des notions telles que la confidentialité, définie comme *"la préservation du secret du contenu de messages ou d'autres données"* [9] , l'authentification, *"technologie qui permet de garantir l'authenticité de la source d'une transmission électronique"* [10] , ou encore l'intégrité des transmissions de données informationnelles ont pris une dimension cruciale à l'heure de la vie en réseau.

L'écho médiatique entretient pour sa part un certain sentiment d'insécurité dans le chef des utilisateurs. Il est vrai que les actes de piratage perpétrés en ligne – et découverts! – sont inquiétants [11] , de même que la prolifération des attaques par virus [12] , phénomène que certains auteurs, comme P. Grabosky, dénomment *"vandalisme électronique"* [13] .

L'attention accordée à la sécurité sur l'internet par un nombre croissant d'entreprises, mais aussi de plus en plus souvent par les particuliers, témoigne de l'enjeu, que l'on pourrait libeller de la sorte, en empruntant le propos d'A. Finkielkraut et P. Soriano : *"Internet, c'est le danger que court la liberté quand on peut garder trace de tout, mais c'est aussi le danger qu'on fait courir aux autres et à soi-même quand on jouit d'une liberté sans limites"* [14] .

Dans le vaste contexte de la Société de l'information, la protection du secret des e-mails se positionne comme un débat fondamental de l'internet. A cet égard, les aspects techniques pertinents à analyser pour assurer l'échange sécurisé de courriers électroniques relèvent de deux niveaux de protection.

---

[8] Voy. entre autres EDLUND M., Learn Marketing – e-Marketing - L'e-consumer et sa vie privée, *Inside Internet*, n°32, mai 2000, pp.91-93.

[9] SZAFRAN E., La cryptographie sur Internet : aspects techniques et réglementaires, *Auteurs & Media*, Larcier, 1998 (2), p.120.

[10] VERBIEST Th., WÉRY É., *Le droit de l'internet et de la société de l'information – Droit européen, belge et français*, Bruxelles, DeBoeck & Larcier, p.609 (glossaire).

[11] Voy. sur le sujet A.N., Management Strategies – Actes de piratage : la menace interne, *Network & Telecom*, n°11, June 2000, p.24 ; A.N., Management Strategies – Le piratage ? Un jeu d'enfant…, *Network & Telecom*, n°11, June 2000, p.22 ; A.N., Management Strategies – Les pirates du Web se déchaînent, *Network & Telecom*, n°9, April 2000, pp.16-17 ; A.N., Technology – A la recherche du maillon le plus faible - Journal d'un pirate, *Network & Telecom*, n°8, March 2000, pp.74-76.

[12] Voy. MARTIN D., MARTIN F.-P., *op.cit.*, pp.27 et s. ; VERBIEST Th., WÉRY É., *op.cit.*, pp.173 et s.

[13] GRABOSKY P., Computer crime in a borderless world, *Annales Internationales de Criminologie*, 2000, vol.38 – 1/2, pp.67-92.

[14] FINKIELKRAUT A., SORIANO P., *op.cit.*, p.39.

• D'une part, il convient de sécuriser chaque réseau local sur lequel des e-mails sont échangés en interne (réseau intranet d'une entreprise, par exemple) mais aussi envoyés vers d'autres réseaux locaux, empruntant ainsi la voie de l'internet (par l'intermédiaire d'une connexion extranet). Dans la vaste “tuyauterie” [15] du Net, par laquelle transitent les informations en ligne, les réseaux locaux représentent en quelque sorte la plomberie de l'une des nombreuses habitations du village global internet.

• D'autre part, il convient d'assurer au sein même de l'architecture de la messagerie électronique, la confidentialité, l'authentification et l'intégrité des données informationnelles échangées. Faute d'une expertise exhaustive sur cette large thématique, la présente contribution se concentrera principalement sur quelques aspects ciblés de la problématique liés directement à la protection du secret des courriers électroniques.

Après avoir brièvement exposé le schéma de fonctionnement d'un serveur mail, les technologies autorisant la confidentialité des messages et l'authentification de l'expéditeur seront passées en revue. La problématique de la réception de messages non sollicités sera ensuite examinée, au titre de dérive d'utilisation des courriers électroniques. Pour conclure, les techniques de marketing direct sur l'internet (e-marketing) seront abordées, en tant qu'illustration de la difficile conciliation entre propagation du commerce électronique et respect de la vie privée.

[15] Voy. pour la métaphore MARIANO G., Peer-to-peer : Audiogalaxy accepte de filtrer ses tuyaux, *ZDNet.fr* (http://www.zdnet.fr/), *actualités internet*, 18 juin 2002.

Aspects techniques

A.- Identification de l'utilisateur sur le réseau

§ 1.- Aperçu du fonctionnement d'un serveur mail [16] et identification de l'utilisateur

L'e-mail, courrier électronique ou courriel désigne la *"méthode permettant d'échanger des messages écrits entre différents postes d'un réseau informatique"* [17] . Pour ce faire, le réseau doit être configuré pour l'envoi et la réception de courriers électroniques.

Un serveur de courrier électronique, basé sur un réseau local TCP/IP (*"protocoles qui administrent la manière dont ordinateurs et réseaux gèrent le flux d'informations sur l'internet"* [18] [19]), repose une architecture bipolaire : le poste client et le serveur.

Alors que le poste client désigne un des ordinateurs du réseau (le poste de travail d'un utilisateur, par exemple), le serveur est un ordinateur qui met à la disposition du réseau et des postes clients des ressources (exemple : des bases de données) et services (exemple : l'accès à l'internet) qu'il contrôle.

Il est important de souligner que, selon cette architecture, le procédé d'échange ne suppose pas l'existence d'une communication directe entre les deux interlocuteurs, comme c'est le cas avec la téléphonie, qui impose la présence simultanée des correspondants. Le système des serveurs mail repose plutôt sur la notion de "station-relais" et de "poste restante".

En réalité, ces relais sont, pour l'essentiel, effectués par les serveurs de courrier électronique (ou *mailhost*). Ceux-ci ont une double mission. D'une part, ils assurent l'expédition des messages envoyés par l'utilisateur à ses correspondants. D'autre part, ils reçoivent les messages destinés à l'utilisateur et les conservent jusqu'à ce que celui-ci les réceptionne [20] .

---

[16] Cette partie s'inspire de LIPS B., *Internet en Belgique – Le guide*, Bruxelles, Best of Editions, 1996, pp.85-106 ainsi que de GILLES L., Learn Protocol – La messagerie électronique - Monter un serveur mail, *Inside Internet*, n°27, novembre 1999, pp.97-99.

[17] VERBIEST Th., WÉRY É., *op.cit.*, p.611 (glossaire).

[18] *Ibidem*, p.614 (glossaire).

[19] Voy. pour plus de détails sur le TCP/IP notamment BARRET E., Pratique : planète techno - Le coin de l'expert – La pile TCP-IP, *SVM Mac*, VNU Publications France, n°135, janvier 2002, pp.122-124.

[20] C'est d'ailleurs la raison pour laquelle les adresses électroniques (exemple : frederic.colantonio@student.ulg.ac.be) sont composées de deux parties identifiables, séparées le @ : la première partie identifie l'utilisateur (frederic.colantonio), la seconde le serveur mail (student.ulg.ac.be).

Ces opérations ne sauraient être réalisées correctement sans le recours à des protocoles particuliers de transport, d'acheminement et d'échange d'informations en ligne. On distingue deux types de protocoles employés pour l'envoi et la réception de courrier électronique sur l'internet : SMTP et POP3 [21] .

a. SMTP

Le protocole SMTP (Simple Mail Transfert Procotol) régule l'expédition et l'acheminement des e-mails sortants, c'est-à-dire des messages qui sont envoyés, au départ du poste client, vers le serveur de courrier électronique. Celui-ci n'est qu'une station-relais dans la mesure où les courriers ne font qu'y transiter jusqu'à leur arrivée dans la boîte aux lettres du destinataire, située sur le serveur de courrier dont il dépend. Une fois les messages en transit postés, c'est au tour du protocole POP3 d'entrer en action.

b. POP3

Le protocole POP3 (Post Office Protocol version 3) gère la “poste restante”, c'est-à-dire qu'il prend en charge le stockage et le rapatriement des e-mails. Il assure ainsi le relevé des messages en attente dans la boîte aux lettres de l'utilisateur lorsque celui-ci se connecte à son serveur de courrier (qui peut éventuellement être le même que celui de l'expéditeur du message). Afin de préserver la confidentialité des courriers électroniques, le rapatriement des messages est conditionné à l'identification préalable de l'utilisateur par mot de passe.

Sur base de ces normes, chaque utilisateur se voit attribuer un compte de messagerie, défini comme *“un nom lui permettant de se connecter au serveur en mode POP3 afin d'y récupérer les messages”* [22] . Plusieurs adresses électroniques peuvent être associées à un même compte. Une telle configuration suffit pour fonctionner en réseau interne (intranet).

Pour s'ouvrir au monde extérieur (extranet), une messagerie électronique doit franchir une étape supplémentaire : souscrire, auprès d'un Fournisseur d'Accès à l'Internet (FAI, ou ISP pour Internet Service Provider), à une formule de connexion. Celle-ci proposera fréquemment un ou plusieurs comptes POP3 qui seront hébergés sur le serveur du fournisseur d'accès.

---

[21] Il faut signaler que le protocole POP3 est en passe d'être dépassé par le protocole IMAP (surtout dans les grosses structures à l'heure actuelle), selon lequel les messages n'ont pas besoin d'être rapatriés sur le poste client pour être consultés.

[22] GILLES L., Learn Protocol – La messagerie électronique - Monter un serveur mail, *op.cit.*, p.97.

§ 2.- Usurpation d'identité et vol de mot de passe

Que la connexion soit permanente ou non, une fois en ligne (en réseau), l'utilisateur est reconnu par l'intermédiaire de l'adresse IP (Internet Protocol - *"protocole d'acheminement d'informations sur l'internet"* [23]) de l'ordinateur à partir duquel la connexion est établie. En outre, au préalable, l'utilisateur aura du s'identifier sur son poste de travail (généralement au moyen d'un identifiant ou *userID* et d'un mot de passe ou *password*, procédé que l'on appelle encore *logon*).

L'identification de l'utilisateur (*logon*) par l'introduction d'un mot de passe (*login*) ne garantit pas que la personne physique obtenant l'accès à l'ordinateur (et, par voie de conséquences, potentiellement, au réseau) soit réellement la personne identifiée ; l'introduction d'un mot de passe valide peut être effectuée par une autre personne que le titulaire légitime dudit mot de passe.

Il apparaît bien, à l'heure actuelle, que la fiabilité d'un mot de passe soit sujette à caution et que ce moyen de protection s'avère pour le moins perméable [24] . Schématiquement, trois méthodes génériques sont utilisées pour s'accaparer un mot de passe : *social engineering*, *cracking* et *sniffing* [25] .

a. Social engineering

Le *social engineering*, rarement utilisé dans son acception française "ingénierie sociale", repose sur les faiblesses humaines plus que techniques. En effet, ce procédé a pour objectif de faire révéler aux utilisateurs leur mot de passe (de façon volontaire, voire spontanée) ou toute information de nature à compromettre la sécurité du système informatique.

L'illustration la plus classique consiste, pour la personne malintentionnée, à se faire passer pour un technicien. Dans cette hypothèse, le pirate (ou *hacker*) signale qu'il a besoin du mot de passe de l'utilisateur pour effectuer des travaux de maintenance ou d'administration du système informatique.

Les déclinaisons les plus évoluées de *social engineering* reposent sur la découverte, par le pirate, du mot de passe d'un utilisateur au départ d'informations personnelles de celui-ci : prénoms des enfants, date de naissance, plaque d'immatriculation…

---

[23] VERBIEST Th., WÉRY É., *op.cit.*, p.612 (glossaire).

[24] SIX N., Trop de mots de passe inefficaces sur les réseaux, *JDNet Solutions* (http://solutions.journaldunet.com/), actualité *Sécurité*, 24 mai 2002.

[25] Le développement de ces trois points fait référence à l'article : GILLES L., Learn Security – Le réseau en toute sécurité - 1ère partie : les types d'attaques et les faiblesses de l'Internet, *Inside Internet*, n°25, septembre 1999, pp.100-102 (p.100 plus spécialement).

b. Cracking

La technique du *cracking* se base sur le principe des essais-erreurs : un dictionnaire de noms communs et de noms propres est utilisé pour tenter de forcer l'accès au système. Des logiciels capables de tester des centaines, voire des milliers de mots à la seconde, ont été développés progressivement par la communauté des *hackers*.

Ces programmes, spécialisés pour “cracker” les mots de passe, contiennent de plus en plus de mots et offrent des possibilités sans cesse plus performantes, comme la prise en compte de variations sur les mots (minuscules ou majuscules au sein du mot, écriture à l'envers, ajout de chiffres à la fin d'un mot…).

c. Sniffing

Le *sniffing* est la troisième méthode permettant de s'approprier des informations. A la différence du *social engineering* ou du *cracking*, le *sniffing* recourt à la transmission de données en ligne pour intercepter les informations échangées entre deux ordinateurs connectés. Dans certaines hypothèses, l'identité des machines visées a une importance intrinsèque (recherche d'une information bien spécifique propre à un utilisateur particulier, comme un mot de passe, par exemple) alors que, dans d'autres cas, peu importe les ordinateurs connectés, pourvu que les données interceptées présentent un intérêt pour la personne malintentionnée (vol de numéro de carte de crédit, par exemple).

Certains logiciels spécialisés analysent les paquets d'information transmis et cherchent à reconstituer l'information émise. Ce procédé demande énormément de temps puisqu'il faut traiter les données en transit et identifier les informations pertinentes pour reconstituer le contenu des paquets qui pourraient contenir du matériel utilisable (mots de passe, numéro de carte de crédit…). Par ailleurs, les données transmises (le contenu des paquets) ne doivent pas être cryptées.

L'utilisation d'un mot de passe s'avère donc nécessaire pour identifier un utilisateur ; elle constitue par ailleurs un premier rempart de sécurité, puisqu'avant d'accéder au courrier, il est nécessaire d'accéder au réseau interne et aux données de l'utilisateur, lesquelles sont le plus souvent stockées sur le disque dur de l'ordinateur connecté au réseau.

Néanmoins, malgré toutes les précautions qui peuvent être prises pour choisir un mot de passe relativement sophistiqué et difficile à usurper [26] , on constate l'insuffisance de cette seule technique pour assurer l'identité de l'utilisateur et garantir la sécurité des échanges.

[26] Voy. notamment SIX N., De l'art de choisir le bon mot de passe, *JDNet Solutions* (http://solutions.journaldunet.com/), actualité *Sécurité*, 27 mai 2002.

Pour répondre à ces faiblesses en général et mieux protéger le secret des courriers électroniques en particulier, des solutions cryptologiques ont vu le jour et tendent aujourd'hui à se généraliser.

B.- Confidentialité des courriers électroniques et authentification de l'expéditeur : les techniques de la cryptologie

§ 1.- Cryptologie, cryptographie et crypto-analyse : balises terminologiques [27]

a. Cryptologie

Relèvent de la cryptologie l'ensemble des techniques visant à rendre un message inintelligible afin d'en préserver la confidentialité et l'authenticité, ainsi que les méthodes permettant le processus inverse de reconstitution du message.

Étymologiquement, le terme signifie “mot caché” et désigne historiquement la science des communications secrètes employée par les États pour protéger les communications militaires et diplomatiques [28] . Les applications de la cryptologie sont la cryptographie et la crypto-analyse.

b. Cryptographie

La cryptographie, décrite comme *“l'art de rendre les informations illisibles aux personnes non habilitées”* [29] , repose sur la technique du chiffrement (ou encryption),

opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale [30] .

c. Crypto-analyse

Par opposition à la cryptographie, la crypto-analyse tend au déchiffrement (ou décryption) du message qui a fait l'objet d'une mesure cryptographique.

---

[27] Voy. sur ces aspects : SZAFRAN E., *op.cit.*, p.121 ; VERBIEST Th., WÉRY É., *op.cit.*, p.610 (glossaire).
[28] Voy. SZAFRAN E., *ibidem*, p.121.
[29] A.N., Enterprise Applications – L'art du camouflage - Cryptographie et filigranes numériques, *Network & Telecom*, n°5, November 1999, p.51.
[30] Voy. VERBIEST Th., WÉRY É., *op.cit.*, p.610 (glossaire).

§ 2.- Cryptographie symétrique et asymétrique

Les technologies contemporaines de cryptage sont réparties en deux familles *"qui transforment chacune un groupe de symboles lisible en un deuxième assortiment de symboles illisible par le biais d'un processus mathématique complexe contrôlé par un numéro appelé une clé"* [31] .

Schématiquement, on peut dire que chaque tranche de données est passée dans un algorithme mathématique afin d'obtenir une version codée du message. Le message original est donc entièrement présent, mais sous une forme différente, qui lui est spécifique ; il s'agit en quelque sorte d'une traduction fidèle dans un langage incompréhensible sans une clé d'interprétation. La valeur ainsi obtenue est alors cryptée (on dit fréquemment que la valeur est "signée") dans la clé de l'utilisateur [32] .

Outre l'assurance de la confidentialité des messages, les méthodes relevant de la cryptographie jouent un rôle important d'authentification puisque l'emploi de clés secrètes ou de clés publiques autorise l'auteur du message à apposer à celui-ci une signature numérique.

a. Cryptographie symétrique à clé secrète

Les produits cryptographiques symétriques reposent généralement sur le *Data Encryption Standard* (DES) [33] . *"Il s'agit d'un système cryptographique à clé unique (dit aussi "à clé secrète") utilisant un algorithme qui, comme le suggère son nom, chiffre et déchiffre un message à l'aide d'une seule clé"* [34] . D'où la notion de symétrie.

"La faiblesse de la cryptographie symétrique réside dans le transfert sécurisé de la clé et dans le maintien du caractère secret de celle-ci, étant donné que deux personnes souhaitant communiquer de façon sécurisée doivent posséder chacune une copie de la même clé" [35] . La clé secrète peut donc s'avérer utile dans les réseaux internes.

Toutefois, les risques d'interception et de détournement de la clé dans un

---

[31] SZAFRAN E., *op.cit.*, p.121.

[32] BRADNER S., Enterprise Applications – "Certifiablement" vôtre, *Network & Telecom*, n°5, November 1999, p.43.

[33] A terme, le DES, qui existe depuis une vingtaine d'années et commence à présenter des faiblesses technologiques au niveau des performances, devrait être remplacé par des produits désignés comme *Advanced Encryption Standard* (AES), dont une illustration est fournie par les produits basés sur la technologie Rijndael (voy. A.N., Enterprise Applications – La saga du cryptage est loin de se terminer - L'algorithme Rijndael doit être accepté et passer des tests d'interopérabilité avant d'être implémenté, *Network & Telecom*, n°17, February 2001, p.54).

[34] VERBIEST Th., WÉRY É., *op.cit.*, pp.360-361.

[35] SZAFRAN E., *op.cit.*, p.121.

environnement ouvert à l'internet en font un outil dont on ne peut garantir complètement la fiabilité, tant en ce qui concerne la confidentialité que l'authentification. Non pas que la technologie proposée soit défaillante ; en l'état, elle est tout simplement insuffisamment développée. La cryptographie asymétrique remédie à ces problèmes.

b. Cryptographie asymétrique à clé publique

Ce système est dit asymétrique car, à la différence du procédé à clé secrète, *"l'utilisateur final possède un logiciel de cryptage et deux clés : une clé publique pour la distribution à d'autres utilisateurs et une clé privée, qui est gardée et protégée par le propriétaire"* [36] .

C'est le logiciel de cryptage (dont le plus connu est le programme PGP, pour *Pretty Good Privacy* [37]) qui génère, en même temps, les deux clés. La clé privée doit être maintenue secrète alors que la clé publique, qui *"représente une fonction irréversible de la clé privée"* [38] , a vocation à être librement distribuée.

Le déchiffrement s'effectue à l'aide des deux clés, qui jouent un rôle complémentaire : un message encrypté avec une clé privée particulière ne peut être décodé qu'avec la clé publique correspondante. *"Chaque utilisateur peut donc générer sa propre paire de clés et publier sa clé publique afin qu'elle puisse être utilisée par les personnes communiquant avec lui, tandis que l'autre clé sera maintenue secrète"* [39] .

Un des avantages majeurs de la cryptographie asymétrique résulte de l'amélioration de la sécurité des échanges de données, puisque seule la clé publique est distribuée. En outre, un tel procédé cryptographique permet à l'expéditeur d'apposer au fichier envoyé une signature numérique fiable, définie comme *"un court ensemble de données en rapport mathématique avec les données formant le contenu du document, assurant au destinataire que les données sont authentiques"* [40] . Pour réaliser tout cela, une architecture bien spécifique doit être mise en place.

---

[36] A.N., Technology – L'ABC de la PKI, *Network & Telecom*, n°9, April 2000, p.66.

[37] Voy. sur le fonctionnement du programme PGP notamment A.N., Pratique, comment faire – Chiffrez blindé avec PGP (Pretty Good Privacy), *SVM Mac*, VNU Publications France, n°121, octobre 2000, pp.144-145.

[38] VERBIEST Th., WÉRY É., *op.cit.*, p.361.

[39] SZAFRAN E., *op.cit.*, p.121.

[40] *Ibidem*, p.122.

§ 3.- *Public Key Infrastructure* (PKI) et Prestataires de Services de Certification (PSC)

L'infrastructure à clé publique et les prestataires de services de certification sont les deux services qui permettent d'assurer la bonne gestion des clés publiques et de garantir l'identité de l'expéditeur d'un message. Il arrive qu'une infrastructure à clé publique agisse également comme autorité de certification, mais ça n'est pas toujours le cas. Quoi qu'il en soit, par souci de clarté, l'exposé dissociera le fonctionnement de ces deux mécanismes.

a. La PKI

L'infrastructure à clé publique (ou PKI pour *public key infrastructure* [41]) a pour vocation d'administrer les clés et réguler leur usage. En effet, la PKI permet *"(…) la création, la distribution, le suivi et la révocation des clés, et ce de manière centralisée"* [42] . Pour ce faire, la PKI intervient comme autorité d'enregistrement des clefs.

L'étape essentielle consiste en l'authentification de l'utilisateur. Celui-ci doit, avant d'avoir le droit d'accès au réseau, être identifié. Si le système *logon* est une méthode très courante d'authentification, la technique la plus fiable consiste à recourir aux certificats numériques, *"espèces d'attestations électroniques établissant le lien entre une personne et sa clé publique"* [43] . C'est ici que le prestataire de services de certification entre en scène et prend le relais de la PKI.

b. Le PSC

Le problème des clés publiques est qu'il n'y a *"aucune garantie que la clé publique provienne effectivement de l'utilisateur auquel elle est supposée appartenir, n'importe qui ayant la possibilité de la publier sous le nom de l'utilisateur"* [44] . C'est pour remédier à ce travers que le PSC intervient.

Le Prestataire de Service de Certification (PSC), encore appelé autorité de certification (AC), prend le relais de la PKI pour délivrer un certificat numérique. Après avoir contrôlé l'identité de l'utilisateur, la PKI envoie une requête au PSC lui demandant de générer un certificat numérique contenant *"des informations d'identification spécifiques sur un utilisateur telles que son nom, sa clé publique et une signature numérique unique, qui relie l'utilisateur au certificat"* [45] .

---

[41] L'abréviation française ICP (pour infrastructure à clé publique) est rarement utilisée (voy. A.N., Technology – ICP : intérêt accru pour les entreprises, *Network & Telecom*, n°21, June 2001, p.66).

[42] A.N., Technology – L'ABC de la PKI, *op.cit.*, p.66.

[43] VERBIEST Th., WÉRY É., *op.cit.*, p.364.

[44] SZAFRAN E., *op.cit.*, p.123.

[45] A.N., Technology – L'ABC de la PKI, *op.cit.*, p.66.

Une fois émis, le certificat, opérant à la manière d'une signature numérique, est stocké dans un répertoire central et une copie est envoyée à l'utilisateur quand celui-ci en fait la demande. Le PSC est ainsi en mesure de garantir au récipiendaire que l'expéditeur d'un message en est bien l'auteur. La confidentialité du message est par ailleurs améliorée, puisque seules les personnes disposant de la clé publique de l'expéditeur pourront le déchiffrer.

C.- Réception de courriers non-sollicités : la problématique du spam ou pollupostage

§ 1.- *Spamming* - L'action

Problématique qui illustre parfaitement l'enjeu du respect de la confidentialité des courriers électroniques et du respect de la vie privée en ligne, le *spamming* désigne *"l'envoi massif – et parfois répété – de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc"* [46] .

Selon certains, cette pratique se révèle aussi basique que *"(…) glisser des brochures dans les boîtes aux lettres ou sous les essuie-glaces de véhicules en stationnement"* [47] .

§ 2.- *Spam* - Le message posté ou envoyé

a. Notions

Dénommé également *junk e-mail* ou *bulk e-mail*, pollupostage ou polluriel [48] (voire pourriel [49]), le spam est le message envoyé par la technique du *spamming*. Il est à noter que les déclinaisons les plus récentes de pollupostage tendent à dépasser le simple courrier électronique pour s'attaquer à toutes les formes de

---

[46] ALVERGNAT C. (rapport présenté par), Le publipostage électronique et la protection des données personnelles, *CNIL*, 1999 (http://www.cru.fr/droit-deonto/droit/spam/cnilpublpost.pdf) p.1.

[47] GAUTHRONET S., DROUARD E., Unsolicited Commercial Communications and Data Protection, *Commission of the European Communities (Internal Market DG – Contract n° ETD/99/B5-3000/E/96)*, 2001 (http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamtudyen.pdf), p.14.

[48] Voy. la définition du spam proposée par L'encyclopédie du Journal du Net (*JDNet Solutions*), à l'adresse : http://encyclopedie.journaldunet.com/ (verbo spam).

[49] PEETERS K., Spam : que le pollueur paie !, *Internet Addict* (http://www.internetaddict.be), *e-Business*, 24 juin 2002.

messages écrits [50] .

b. Typologie de contenu

Plusieurs catégories de messages spam peuvent être isolées en fonction du contenu proposé. Trois orientations peuvent être dégagées, en conservant à l'esprit que la motivation de l'expéditeur (le *spammer*) est toujours, *in fine*, commerciale.

• Le *spam commercial au sens strict* se caractérise par des propositions de gain d'argent facile (du type : *"get rich quicker"* ou *"make money at home"*) ou des promotions commerciales alléchantes (*"computer bargains : low prizes"* ou *"DVD at $ 1,99 each"*).

• Le *spam commercial au sens large* englobe toutes les autres offres, notamment les informations plus générales à caractère publicitaire (exemple : *"visit our website"* ou *"you liked [nom d'un site visité par l'internaute] ? You're going to love our website !"*).

• Le *spam à caractère pornographique* se présente généralement à l'utilisateur comme l'opportunité unique d'un accès illimité pour une période déterminée à un contenu explicitement licencieux (exemple : *"porn — 3 days-trial"*). Il peut également être question d'une annonce publicitaire à caractère pornographique (du type : *"sex for free"*). L'on rejoint ici la catégorie précédente, à ceci près que, selon certains, l'offre change ici potentiellement de nature : la sollicitation ne fait plus appel à des motivations exclusivement commerciales, mais se muerait en *"agression morale"* [51] . Ce qui semble établi, c'est que ce type d'offre en appelle moins à des opportunités commerciales – qu'elles soient avérées ou non – qu'à certains penchants peu glorieux de l'espèce humaine.

c. Typologie technique

Indépendamment du contenu proposé, il est possible de distinguer deux grandes catégories de spam, selon le vecteur de transmission et de diffusion des informations [52] .

• Le *spam Usenet* est historiquement la première forme de pollupostage

[50] DUMOUT E., L'affaire des SMS roses devant la justice, *ZDNet.fr* (http://www.zdnet.fr/), *actualités internet*, 10 juillet 2002 ; SOSNOWIEZ N., La vague des SMS rose profite d'une belle pagaille juridique, *ZDNet.fr* (http://www.zdnet.fr/), *actualités Business*, 18 juin 2002 ; RAPHAEL L., Ras-le-bol des e-mails publicitaires !, *La Libre Belgique* (http://www.lalibre.be), 24 juin 2002 ; SACRE J.-F., Compromis pour le marketing en ligne, *La Vie du net - Le Soir en ligne* (http://www.laviedunet.be/), 22 juin 2002.

[51] HUYNH T., L'explosion du spam met en péril l'e-mail marketing, *Le Journal du Net* (http://www.journaldunet.com/), *actualité Marketing*, 04 juillet 2002.

[52] Voy. sur cette distinction notamment HAZEN MUELLER S., What is spam ?, *Promote Responsible Net Commerce : Fight Spam!*, Fight spam on the Internet : http://spam.abuse.net/overview/whatisspam.shtml

identifiée sur le Net. Elle serait née en avril 1994 de l'esprit de deux avocats de l'Arizona qui ont proposé, par l'intermédiaire d'un message posté sur quelques 6 000 *newsgroups Usenet*, leurs services pour faciliter les postulants à l'acquisition de la *green card* américaine [53] . Le spam Usenet consiste donc à envoyer un même message à plusieurs groupes de discussion, auxquels sont inscrits et participent des dizaines, des centaines ou des milliers d'internautes.

• Le *spam e-mail*, quant à lui, prend pour cible non pas des groupes de discussion mais directement des utilisateurs individuels. Ceux-ci reçoivent un courrier électronique commercial ou publicitaire qui leur est personnellement adressé, sans pour autant l'avoir sollicité, c'est-à-dire sans que l'utilisateur ait consenti à donner son adresse électronique à cet effet.

Pour parvenir à leur fin, les *spammers* peuvent acheter des bases de données d'adresses e-mails [54] (un million de noms peuvent être achetés pour quelques dizaines d'euros [55]). Dans ce cas, il se peut que l'acquisition de la base de données soit tout à fait licite. Ce qui ne l'est pas, c'est l'utilisation qui est faite des adresses achetées. Cependant, technique plus fréquente – et moins coûteuse ? – que l'achat d'adresses, il semble que les *spammers* recourent à des outils logiciels appelés *spamware* [56] .

• Le premier type de logiciels permet la collecte d'adresses e-mail sur l'internet, l'adresse électronique étant alors *"capturée dans les espaces publics de l'internet (espaces de discussion, listes de diffusion, annuaires diffusés sur des sites web, etc.) sans que les personnes concernées ou le responsable du site diffusant les données n'en aient connaissance"* [57] .

• La seconde catégorie de logiciels, pour sa part, gère l'envoi massif et automatisé de courrier électronique sans devoir recourir à un serveur mail spécifique ou à un fournisseur d'accès particulier. Pour y parvenir, le programme transforme l'ordinateur du *spammer* en un serveur mail autonome en soi.

§ 3.- Dangers d'une telle pratique

Les sites de lutte contre le spam, qui se sont développés en nombre mais de manière foisonnante et sans réelle volonté d'unicité, mettent empiriquement en lumière les dangers et conséquences néfastes du *spamming* [58] .

---

[53] GAUTHRONET S., DROUARD E., *op.cit.*, pp.14-15.

[54] Voy. sur le sujet notamment BERANGER A.-L., Bases d'adresses e-mail : comment s'y retrouver ?, *Le Journal du Net* (http://www.journaldunet.com/), *Actualité Marketing*, 27 juin 2002.

[55] BLACK J. (traduit par CHAVANNE M.), L'arsenal discret des pollueurs de mail, *Le Monde* (http://www.lemonde.fr), édition du 27 juin 2002.

[56] GAUTHRONET S., DROUARD E., *op.cit.*, pp.31 et s.

[57] ALVERGNAT C., *op.cit.*, p.20.

[58] Voy. entre autres CASPAM – *le collectif anti-spam* (http://caspam.org/), Anti-Spam ! (http://members.hostedscripts.com/antispam.html), Break the chain – *stop junk e-mail and misinformation*

De façon lapidaire, le site du collectif français anti-spam (CASPAM) résume la problématique du spam en ces termes : *"il fait perdre de la bande passante à tout le monde ! Il nous fait perdre du temps quand nous traitons nos emails ! Les spammeurs ne respectent pas la Netiquette ! Les spammeurs ne respectent pas notre vie privée ! Ils volent nos adresses sur nos sites web ! Ils gagnent de l'argent par la revente de nos emails ! Cela coûte plus cher au spammé qu'au spammeur ! La plupart du temps l'objet du spam est une arnaque ! Il pollue notre espace privé et tout l'internet ! Et surtout : il est illégal et hors la loi en France !!!"* [59] .

Le site "Fight spam on the Internet" expose, toujours de manière empirique mais plus posément, les risques liés au *spamming* en six points, qui englobent le constat du CASPAM et des autres sites qui expriment leur aversion pour le pollupostage [60] . Ces six points, traduits et adaptés assez librement, sont repris ci-dessous.

a. "The free ride"

Le spam e-mail est un procédé unique dans la mesure où le récipiendaire supporte une charge financière bien plus importante que celle que prend en charge l'expéditeur. A titre d'exemple, AOL (l'un des ténors américains parmi les fournisseurs d'accès), a déclaré recevoir quelque 1,8 million de pollupostage par jour avant de prendre des mesures pour endiguer ce phénomène ; mesures qui coûteraient au provider américain jusqu'à 15 % du total des redevances mensuelles payées par ses utilisateurs [61] .

Compte tenu de ce qu'il ne faut à l'utilisateur moyen qu'une dizaine de secondes pour identifier et refuser ce type de message, cette seule activité d'effacement et de refus de spam représente tout de même, pour AOL seulement, un coût équivalent à environ 5 000 heures de temps de connexion par jour. A l'inverse, il suffit pour le *spammer* de disposer d'un accès à l'internet. Aucun autre investissement publicitaire ne coûte aussi peu à un annonceur et tant au destinataire.

b. Le problème des "océans du spam"

La plupart des pollupostages contiennent une mention du type : *"merci d'envoyer un message intitulé 'désabonnement' si vous souhaitez ne plus faire*

(http://www.breakthechain.org/), CAUCE – The Coalition Against Unsolicited Commercial Email (http://www.cauce.org/), SpamCop (http://spamcop.net/). A ne pas confondre avec le site de l'industrie alimentaire Hormel, qui produit de la viande en boîte de marque… SPAM (http://www.spam.com) !

[59] Voy. la page d'accueil du CASPAM – *le collectif anti-spam* (http://caspam.org/).

[60] Voy. LEVINE J., Why is spam bad ?, *Promote Responsible Net Commerce : Fight Spam!*, Fight spam on the Internet : http://spam.abuse.net/overview/spambad.shtml

[61] GAUDIN S., GASPAR S., Management Strategies – Lutte contre le spam, *Network & Telecom*, n°25, November 2001, p.12.

partie de la lite de diffusion". Sans même considérer le fait d'avoir à requérir une résiliation pour un service pour lequel aucune souscription n'avait eu lieu, il apparaît que cette opération devient matériellement impossible si le volume du trafic est important et s'accroît.

Pour l'heure, le nombre de spam demeure limité. Mais si seulement un dixième des membres de la communauté internet décide de pratiquer le *spamming* à raison d'une moyenne de 100 000 messages par jour (un nombre facile à atteindre avec une formule de connexion classique et les logiciels *spamware* appropriés), alors chaque utilisateur recevrait 1 000 pollupostages par jour. Est-il concevable de demander aux internautes d'envoyer un millier de messages de résiliation par jour ?

En outre, si le pollupostage augmente, les boîtes de réception seront encombrées à un point tel que les avantages du courrier électronique, dont les principaux sont la facilité et la commodité, disparaîtront.

c. Le vol de ressources

Un nombre grandissant de polluposteurs expédient la plupart de leurs courriers par des réseaux intermédiaires innocents, afin d'éviter les dispositifs mis en place par certains systèmes pour contrer le *spamming* direct. Les systèmes intermédiaires et les disques réseaux sont submergés de messages non sollicités, les administrateurs réseau sont débordés par les messages spam non délivrables et font l'objet de plaintes et récriminations de la part des utilisateurs qui concluent, par une heuristique, que puisque les intermédiaires transmettent les messages, ils doivent être de mèche avec les *spammers*.

Le *"hit and run"* est une autre technique à laquelle recourent beaucoup de *spammers*. Ceux-ci souscrivent à une formule de connexion d'essai (offre temporaire de quelques jours) auprès d'un fournisseur d'accès, postent des dizaines de milliers de messages, puis abandonnent leur compte en laissant le soin au fournisseur d'accès peu regardant de réparer les dégâts (à moins que celui-ci ait préalablement décelé l'activité et désactivé le compte). La plupart des *spammers* ont réalisé cette opération des dizaines de fois, contraignant les fournisseurs d'accès à employer des équipes pour épurer les systèmes et surveiller les offres d'essai, afin d'éviter les abus.

d. "It's all garbage " — Intox, fausses rumeurs et désinformation

Les pollupostages promeuvent fréquemment des produits, articles ou services inexistants, inutiles et partiellement ou totalement illicites [62] . Toutes ces

[62] Comme nous l'avons vu (voy. *supra*, § 2.- Spam - Le message posté ou envoyé) , il est question de *spamware*, de cures prétendument miraculeuses, de matériel informatique à prix cassé, de vagues plans d'enrichissement personnel rapide, d'accès instantané et illimité à des sites pornographiques exclusifs, et

offres sont trop médiocres pour faire l'objet de publicité régulière pour laquelle il faudrait par ailleurs investir des sommes d'argent en tant qu'annonceur.

En outre, vu le faible coût des techniques de pollupostage, il n'est nullement besoin de cibler les destinataires puisque, pour un même prix très bas, il est possible d'atteindre un nombre infiniment plus important de personnes, accroissant également le taux de perturbation pour les autres utilisateurs.

e. "They're all crooks" – Tromperie

Invariablement, les logiciels *spamware* s'accompagnent d'un éventail de noms de personnes prétendument d'accord de recevoir ce genre de publicité, mais ces listes sont en réalité constituées de victimes non consentantes glanées au hasard au départ de *newsgroups* ou de *mailing lists*. Les logiciels de spam allèguent aussi fréquemment le fait que les *spammers* utilisent le système d'un fournisseur d'accès de manière suffisamment discrète pour masquer l'activité.

Les *spammers* clament qu'ils enlèveront les noms des utilisateurs à la demande, ce qui n'est pratiquement jamais le cas. En effet, les internautes rapportent fréquemment qu'après avoir envoyé une demande de résiliation *via* un nouveau compte utilisateur, ils reçoivent alors souvent du spam à cette nouvelle adresse [63] . Pour le *spammer*, ce mécanisme permet ainsi de confirmer la validité de l'adresse utilisée.

En outre, les polluposteurs recourent généralement à de fausses adresses de retour afin de ne pas avoir à supporter les frais de réponses des internautes mécontents qui auraient reçu leurs messages.

f. L'illicéité potentielle

Certains types de pollupostage sont explicitement reconnus comme illégaux sur certains serveurs. Cette pratique peut ainsi, dans certains cas, entraîner des poursuites judiciaires.

---

toutes les formes dérivées de ces illustrations.

[63] Il est intéressant de noter que cette récrimination, récurrente parmi la communauté anti-spam, ne semble pas faire l'unanimité. Voy. GLASNER J., No subscription for spam relief, *Wired News* (http://www.wired.com/), 05 avril 2002 : *"in a recent experiment carried out by the U.S. Federal Trade Commission, researchers found that replying to spammers may not be as dangerous as previously thought"*…

§ 4.- Lutte contre le spam

Outre l'oeuvre législative en chantier [64] , des moyens techniques se sont développés pour lutter contre le pollupostage. Ceux-ci vont des mesures de défense, par le filtrage des courriers, à la riposte des milices anti-spam pour enrayer la mécanique des *spamware* employés par les polluposteurs.

a. Filtrage des courriers [65]

Plusieurs logiciels, basés serveur, ont vu le jour pour empêcher les courriers électroniques indésirables d'arriver dans les boîtes aux lettres des utilisateurs. *"Ces produits interceptent les messages au contenu douteux et les effacent ou permettent à l'administrateur de déterminer ce qu'ils doivent en faire"* [66] . Deux méthodes sont utilisées pour filtrer le courrier : la vérification et l'autorisation.

- La *vérification* permet de s'assurer que les adresses utilisées sont valides. Ainsi serait refusée une adresse du type Make.Money.Fast parce qu'elle ne renverrait pas à une réponse valide du serveur de noms de domaine (DNS, pour Domain Name Server/System).

- L'*autorisation* permet à l'administrateur de choisir s'il souhaite ou non que les utilisateurs reçoivent le courrier d'un utilisateur ou d'un domaine particulier. Il se peut que l'entreprise SpamCorp.com soit une firme valide, mais que l'administrateur préfère que les messages de cette société n'atteignent pas les utilisateurs. Même si la réponse du DNS est valide, il est possible de ne pas accepter le courrier.

De façon individuelle, mais sans que la solution soit basée serveur, les utilisateurs qui emploient des logiciels de gestion de courriers électroniques (comme Eudora, Mail, Outlook Express, Powermail…) peuvent appliquer des règles personnelles de filtrage pour envoyer à la corbeille, dès leur arrivée dans la boîte de réception de messages, certains courriers non désirés (exemple : tous les courriers comprenant le mot "sex" dans l'intitulé ou tous les messages auquel est joint un document contenant l'extension ".jpg").

b. Haro sur les spammers

Les sites de lutte anti-spam franchissent généralement une étape supplémentaire et proposent des solutions offensives pour enrayer cette pratique.

---

[64] RAPHAEL L., Ras-le-bol des e-mails publicitaires !, *op.cit.* ; WEARDEN G., THOREL J., Spam et cookies : le Parlement européen arrondit les angles, *ZDNet.fr* (http://www.zdnet.fr/), *actualités internet*, 03 juin 2002. Voy. également le site Spam Laws (http://www.spamlaws.com/).

[65] Voy. A.N., Buyers' Guide – Halte au "pollupostage" ! - Trois logiciels basés serveur empêchent les e-mails indésirables d'accaparer le temps des utilisateurs, *Network & Telecom*, n°9, April 2000, pp.82-85.

[66] *Ibidem*, p.82.

Ainsi, des *"milices antipollupostage"* [67] ont développé des listes noires répertoriant les personnes et sociétés soupçonnées de *spamming* [68] . Le polluposteur présumé voit alors son trafic de courrier électronique et IP bloqué pendant une durée déterminée.

Sans entrer dans les polémiques autour de la licéité ou du non respect de la présomption d'innocence lié à ces pratiques [69] , on peut signaler que, si les grands fournisseurs d'accès peuvent déployer un arsenal de surveillance et de défense propres, il semble que les petits et moyens providers recourent plus souvent à ces listes noires [70] .

Une autre contre-mesure offensive offerte pour lutter contre le spam est fournie par la page "Anti-Spam!" [71] , qui propose une liste d'une centaine de fausses adresses générées automatiquement à chaque chargement de la page. L'objectif est de compliquer la tâche des polluposteurs : lorsqu'un *spamware* inspecte une page Web à la recherche d'adresses électroniques, le logiciel explore aussi généralement les liens vers d'autres pages. Si parmi ceux-ci figure l'adresse de la page "Anti-Spam!", le *spamware* récoltera alors au moins une centaine de fausses adresses e-mail auxquelles le pollupostage sera envoyé.

Même si nous avons expliqué que les spammers se prémunissent généralement contre les courriers en retour, les initiateurs de la page "Anti-Spam!" postulent que, puisque les adresses utilisées sont non valides, le *spammer* recevra autant de messages d'erreur lui signifiant l'impossibilité de délivrer le message, alourdissant ainsi sa tâche et ralentissant ses activités. Dans tous les cas, l'efficacité du spam sera diminuée.

Tout récemment (depuis la mi-juillet 2002), en France, la CNIL (*Commission Nationale de l'Informatique et des Libertés*) a mis à disposition une adresse électronique à l'attention des particuliers victimes du spam : spam@cnil.fr. Les internautes sont invités à y transmettre tous les courriers électroniques commerciaux non sollicités qu'ils reçoivent. La CNIL analysera ces messages, déterminera s'il s'agit ou non de pollupostage et prendra les mesures adéquates si nécessaire [72] .

---

[67] GAUDIN S., GASPAR S., Management Strategies – Lutte contre le spam, *op.cit.*, p.12.

[68] Voy. notamment la liste RBL (Realtime Blackhole List) du MAPS – Mail Abuse Prevention System (http://www.mail-abuse.com).

[69] Il est également question des conséquences économiques liées à une telle paralysie des échanges, et donc des transactions en ligne.

[70] GAUDIN S., GASPAR S., Management Strategies – Lutte contre le spam, *op.cit.*, p.14.

[71] Anti-Spam ! (http://members.hostedscripts.com/antispam.html)

[72] DESAUTEZ L., Spam : la CNIL passe à l'action, *Le Journal du Net* (http://www.journaldunet.com/), *actualité Le Net*, 11 juillet 2002.

D.- E-marketing : du spam à l'opt-in

§ 1.- Aperçu de la problématique

Si l'on suit le raisonnement de J.-M. Cheffert, l'asymétrie d'information contribuerait à la lenteur du développement de l'e-commerce, dont l'avènement tarde par rapport aux prévisions initiales [73] . La méfiance des clients résulterait de leur méconnaissance de la fiabilité du vendeur, alors que celui-ci, lui, la connaît. De là naît l'asymétrie.

Pour se départir de cette ignorance des clients, on peut comprendre, dans le chef des vendeurs, l'intérêt offert par la publicité commerciale en ligne. Les avantages sont patents : maximisation de la visibilité de l'activité, minimisation des efforts à fournir pour annoncer, rapidité de la démarche, preuve du sérieux de la firme…

L'une des déclinaisons de la publicité en ligne, à côté des bannières ou des fenêtres de type *popup* (une icône publicitaire ou un message commercial s'affiche, dans une nouvelle fenêtre, au chargement d'une page web), réside dans l'utilisation du courrier électronique à des fins d'annonce. Seulement voilà : à ce rythme-là, l'e-mail marketing prend furieusement des allures de pollupostage !

§ 2.- *"Opt-in"* et *"opt-out"*

Le recours croissant au marketing direct par courrier électronique (croissance qui se poursuit selon les prévisions [74]) imposait la levée de la méprise entre l'e-mail marketing et le spam, tant dans la pratique que du point de vue juridique [75] . Sont ainsi apparus les concepts d'*opt-in* et *opt-out*.

a. Opt-out

La technique de l'*opt-out* repose sur le principe selon lequel *"les entreprises peuvent envoyer des propositions commerciales par voie électronique sans*

---

[73] CHEFFERT J.-M., Le commerce électronique : autorégulation et asymétrie d'information, *Revue Ubiquité – Droit des technologies de l'information*, Bruxelles, Larcier, n°12, 2002, pp.31-52.

[74] Aux États-Unis, les dépenses en e-mail marketing devraient augmenter de 17% au cours de l'année 2003 Voy. STIENAERS M., Augmentation des budgets de l'e-mail marketing, *Internet Addict* (http://www.internetaddict.be), *Marketing*, 03 juillet 2002.
En Belgique, au début 2001, 39 % des sociétés recouraient à l'e-mail marketing, et il est prévu qu'à la mi-2002, ce chiffre soit porté à 70 %. Voy. GEUENS J., L'e-mail marketing continue son essor en Belgique, *Internet Addict* (http://www.internetaddict.be), *Marketing*, 06 mai 2002.

[75] Notons au passage que la croissance de l'e-mail marketing ne fait qu'accompagner l'essor du courrier électronique en général, désigné comme la *"killer application"* de l'internet. Voy. PEETERS K., E-mail : l'application killer, *Internet Addict* (http://www.internetaddict.be), *Marketing*, 23 avril 2002.

demander l'avis du consommateur, à charge pour celui-ci, si nécessaire, de demander à l'expéditeur de ne plus lui en envoyer" [76] . Les entreprises qui reçoivent un tel message sont tenues de respecter la volonté du consommateur. En la matière, il semblerait que les firmes commerciales fassent montre de plus de scrupules que les polluposteurs. Cependant, cette forme d'*opt-out* n'est pas pleinement satisfaisante, puisqu'au minimum un message non sollicité arrive au destinataire.

Une autre déclinaison de l'*opt-out* consiste à apposer, dans un formulaire ou une page web, *"une phrase du type "j'accepte que mes données personnelles soient utilisées à des fins de marketing direct" suivie d'une case "oui" cochée par défaut, laissant le choix au consommateur d'opter pour le "non" s'il le souhaite, d'où la dénomination opt out"* [77] .

b. Opt-in

L'alternative à l'*opt-out* réside dans la pratique inverse, appelée *opt-in*, ou *permission marketing* [78] . La solution repose sur la sélection positive : aucun message à caractère commercial n'est envoyé au consommateur sans son consentement préalable. A moins que le client n'ait explicitement autorisé une entreprise à l'informer de ses produits, celle-ci ne pourra pas lui envoyer de messages à caractère commercial.

L'accord du consommateur est donc requis *a priori*, mais surtout de façon indubitable et volontaire, ce qui n'est pas toujours le cas avec l'*opt-out*, la majorité des consommateurs adoptant généralement un comportement passif (et laissant ainsi par exemple cochée la case qui autorise l'envoi de messages commerciaux). En requérant ainsi l'accord préalable à l'envoi de messages, les courriers électroniques commerciaux reposant sur le principe de l'*opt-in* se distinguent du pollupostage.

§ 3.- Double *opt-in* et soft *opt-in*

L'idée de l'*opt-in* a ouvert de nouveaux horizons pour le marketing et la publicité en ligne. Il était donc attendu que, d'une part, le principe se développe et, d'autre part, fasse l'objet d'une attention juridique toute particulière, respectant ainsi l'importante mouvance contemporaine de réglementation et de régulation de la Société de l'information [79] .

---

[76] SACRE J.-F., Compromis pour le marketing en ligne, *op.cit.*

[77] FOLON J., Focus – De l'opt out à l'opt in : risque ou opportunité pour le permission marketing ?, *Inside Internet*, n°44, juillet 2001, p.32.

[78] GAUTHRONET S., DROUARD E., *op.cit.*, p.23 notamment ; FOLON J., *ibidem*, p.32.

[79] Voy. sur les notions de réglementation et de régulation du réseau (ainsi que l'application à l'internet de concepts comme l'autorégulation et la co-régulation) VERBIEST Th., WÉRY É., *op.cit.*, pp.517 et s. (*Titre 6 - La régulation de la société de l'information*).

a. Double opt-in

La dichotomie *opt-in*/*opt-out* semble déjà pratiquement dépassée, au profit du double *opt-in*. Ce modèle préconise non seulement le consentement actif du consommateur qui marque clairement son accord de recevoir des e-mails commerciaux (*opt-in* n°1), mais requiert également la confirmation de cet accord (double *opt-in*). Cette confirmation est sollicitée dans le premier courrier envoyé par l'expéditeur commercial.

Ainsi, *"lorsqu'un utilisateur (…) choisit une liste de messages et entre son adresse sur un site, ce site devrait envoyer un message à l'adresse en disant que si le destinataire désire s'abonner à la liste, il doit répondre pour activer le compte. L'expéditeur doit alors attendre une ou deux semaines pour avoir une réponse et s'il la reçoit, le compte est activé"* [80] .

L'utilité de la pratique du double *opt-in* est à tout le moins… double !

- Ce procédé offre la possibilité de traiter avec les utilisateurs qui entrent une mauvaise adresse. En effet, *"ce n'est pas une surprise de recevoir des messages adressés par erreur à quelqu'un d'autre"* [81] . La confirmation requise avant l'activation du compte permet donc d'éviter des récriminations ultérieures ou des accusations de *spamming*. A charge pour l'expéditeur de ne plus envoyer d'e-mails et pour le consommateur qui s'est trompé dans l'utilisation de son adresse d'effectuer à nouveau l'opération avec soin.

- En outre, ce modèle se révèle plus rentable : *"s'il y a moins de clients, les fichiers contiennent des informations plus nombreuses par client et ceux-ci acceptent de recevoir des communications commerciales qu'ils utiliseront"* [82] . En effet, il n'est plus question d'intrusion d'un opérateur vers un client, mais de l'instauration, par l'intermédiaire d'une relation de confiance fondée sur la fréquence des correspondances, d'une relation d'échange. Il en résulte, dans le chef du consommateur, une plus grande communication d'informations personnelles, puisque les offres sont plus ciblées vers ses centres d'intérêt, mieux adaptées à ses besoins… bref, personnalisées [83] .

b. Soft opt-in

La directive européenne sur *"le traitement des données personnelles et la protection de la vie privée dans le secteur des communications électroniques"*,

---

[80] GIBBS M., Management Strategies – Double Opt-in exécuté dans les règles, *Network & Telecom*, n°19, April 2001, p.20.
[81] *Ibidem*.
[82] FOLON J., *op.cit.*, p.32.
[83] GAUTHRONET S., DROUARD E., *op.cit.*, p.23.

adoptée le 30 mai 2002, encadre la diffusion d'e-mails commerciaux [84] . L'*opt-in* y est décrit comme le modèle de l'accord préalable et l'*opt-out* celui du droit de rectification (le consommateur peut à tout moment rectifier les informations ou s'opposer au message). Le choix entre ces deux procédés est, quant à lui, laissé à l'appréciation de chaque législation nationale.

En Belgique, l'option prise, baptisée “soft *opt-in*”, relève du compris entre les deux modèles [85] . En réalité, le consentement préalable de l'*opt-in* est maintenu, à deux exceptions près : lorsqu'il existe déjà une relation contractuelle entre l'annonceur et le consommateur d'une part, quand une entreprise s'adresse à une personne morale de l'autre. Dans ces deux hypothèses, l'expéditeur ne se voit pas contraint de requérir le consentement *a priori* du destinataire, lequel peut à tout moment, retirer l'accord implicite donné initialement.

[84] WEARDEN G., THOREL J., Spam et cookies : le Parlement européen arrondit les angles, *op.cit.*
[85] RAPHAEL L., Ras-le-bol des e-mails publicitaires !, *op.cit.*

Conclusion

Quel que soit le nom qu'on lui attribue ou les intentions qu'on lui prête, l'internet n'est encore à l'heure actuelle qu'un vaste champ d'exploration. Vivier technologique confrontant le droit à une réalité difficilement contrôlable dont la jeunesse fougueuse et la mutation permanente ne facilitent ni l'apprivoisement ni le domptage, ce creuset bouillonnant d'idées n'en demeure pas moins un espace qui doit être balisé pour offrir à ses visiteurs, réguliers ou occasionnels, une certaine sécurité.

Cette indispensable assurance de sécurité, qu'elle prenne les traits d'une protection technique ou d'une reconnaissance juridique – idéalement, les deux –, se fait jour peu à peu et trouve sa place sur le Net. Les solutions techniques de sécurisation se propagent, parfois maladroitement. A tout le moins ont-elle le mérite d'exister : mots de passe, cryptage des données, clés privées et clés publiques, autorités de certification sont autant d'évolutions technologiques cherchant à garantir une certaine validité sur le réseau.

La vie réelle dispose de codes de fonctionnement et de garde-fous physiques, techniques et moraux. Il en va de même pour l'internet, dont le développement des aspects techniques visant au respect du secret des communications, ne constitue que l'expression contemporaine d'un garant des libertés fondamentales dans la Société de l'information.

La tentation de contrôle du réseau se révèle toutefois grande, et la marge entre le respect de la vie privée et le nécessaire contrôle social n'est pas toujours évidente à discerner. Les risques de dérive existent entre une Société de l'information anarchique où régnerait le paradigme de l'*individualité négative* [86] et un univers, digne des romans de science-fiction, où le moindre mouvement, la plus petite incartade, l'écart le plus minime serait vu, consigné et susceptible d'être utilisé à des fins de pression, surveillance, éviction ou licenciement.

C'est pourquoi le nécessaire développement des systèmes techniques de protection en ligne – et des textes de lois qui régissent l'ensemble – devra toujours être prudent, réfléchi et mûri avant d'être appliqué, en recherche constante du respect de l'indispensable *"balance des intérêts"* [87] entre tous les acteurs de la vie en réseau.

---

[86] CASTEL R., *Les métamorphoses de la question sociale – Une chronique du salariat*, Gallimard, 1995, p.44.

[87] SIRINELLI P., *"Exceptions et limites aux droit d'auteur et droits voisins"*, Atelier sur la mise en oeuvre du Traité de l'O.M.P.I. sur le droit d'auteur et du Traité de l'O.M.P.I. sur les interprétations et exécutions et les phonogrammes, 1999 (http://www.wipo.int/fre/meetings/1999/wct_wppt/pdf/imp99_1.pdf), p.13.

C'est là que réside le véritable paradoxe de l'informatique en réseau : dans un univers binaire où les intermédiaires aux pôles dichotomiques de réponse ne sont pas tolérés, l'internet se présente par essence comme une zone de négociation permanente entre les extrêmes. La rationalité technologique rigoureusement cartésienne s'oppose à la réalité humaine de navigation et vivotement constants en quête d'une homéostasie en devenir perpétuel.

Mais si l'on se résout à dépasser cette opposition apparemment inconciliable, on peut entrevoir alors les bases d'un modèle social où l'antagonisme fait place à la complémentarité. Dans une configuration postmoderne des échanges sociaux, économiques et autres, il semble bien que ce modèle de complémentarité doive prévaloir, puisqu'il n'est plus possible de faire machine arrière. Et à compter que cela soit encore envisageable, le souhaiterait-on vraiment ?

Bibliographie

A.– Ouvrages

- Collectif, par les rédacteurs des Éditions Life-Time, *Initiation à l'informatique – Le monde des ordinateurs*, Amsterdam, Life-Time, 1986.

- CASTEL R., *Les métamorphoses de la question sociale – Une chronique du salariat*, Collection Folio / Essais, Gallimard, 1995.

- DE CLOSETS F., LUSSATO B., *L'imposture informatique – Vive l'ordinateur simple et bon marché!*, Paris, Fayard, Le Livre de poche, 2000.

- FINKIELKRAUT A., SORIANO P., *Internet - L'inquiétante extase*, Turin, Mille&Une Nuits, 2001.

- LALOUX D., *Les virus informatiques*, Collection Marabout Service, Alleur, Marabout, 1989, 188 p.

- LIPS B., *Internet en Belgique – Le guide*, Bruxelles, Best of Editions, 1996.

- LOVINFOSSE J.P., *Le piratage informatique*, Collection Marabout Service, Alleur, Marabout, 1991, 223 p.

- MARTIN D., MARTIN F.-P., *Cybercrime : menaces, vulnérabilités et ripostes*, Collection Criminalité Internationale, Paris, Presses Universitaires de France (PUF), 2001.

- PANSIER F.-J., JEZ E., *La criminalité sur internet*, Collection encyclopédique Que sais-je ?, n° 3546, Paris, Presses Universitaires de France (PUF), 2001.

- PARKER D. B., *Fighting computer crime – A new framework for protecting information*, New York, John Wiley & Sons Inc..

- SALVAGGIO S., BAUWENS M. (sous la direction de), *Anthropologie de la société digitale*, Tome 1, 2001 (également disponible en téléchargement via l'adresse : http://www.salvaggio.net/RecPubl.html).

- STEPHENSON P., *Investing computer-related crime*, London, CRC Press, 2000.

- THIRAN Y., *Sexe, mensonges et Internet – Réseau et transparence*, Collection

Quartier Libre, Bruxelles, Labor, 2000.

- THOMAS D., LOADER B.D. (eds), *Cybercrime – Law enforcement, security and surveillance in the information age*, London & New York, Routeledge, 2000.

- VERBIEST Th., WÉRY É., *Le droit de l'internet et de la société de l'information – Droit européen, belge et français*, Collection Création - Information - Communication, Bruxelles, DeBoeck & Larcier, 2001.

- WARUSFEL B., *La propriété intellectuelle et l'Internet*, Collection Dominos, n° 225, Évreux, Flammarion, 2001.

B.– Articles, études et recherches

- A.N., Buyers' Guide – Des mises à jour Sendmail renforcent la sécurité des e-mails - Les agents Secure Switch permettent aux utilisateurs de crypter des livraisons de messages sur le serveur, *Network & Telecom*, Best of publishing, n°10, May 2000, p.92.

- A.N., Buyers' Guide – Etude : les clés de chiffrage en danger sur les serveurs, *Network & Telecom*, Best of publishing, n°7, February 2000, p.93.

- A.N., Buyers' Guide – Halte au “pollupostage” ! - Trois logiciels basés serveur empêchent les e-mails indésirables d'accaparer le temps des utilisateurs, *Network & Telecom*, Best of publishing, n°9, April 2000, pp.82-85.

- A.N., Enterprise Applications – L'art du camouflage - Cryptographie et filigranes numériques, *Network & Telecom*, Best of publishing, n°5, November 1999, pp.51-55.

- A.N., Enterprise Applications – La saga du cryptage est loin de se terminer - L'algorithme Rijndael doit être accepté et passer des tests d'interopérabilité avant d'être implémenté, *Network & Telecom*, Best of publishing, n°17, February 2001, p.54.

- A.N., Enterprise Applications – Mise en garde contre l'externalisation de la détection d'intrusion, *Network & Telecom*, Best of publishing, n°19, April 2001, pp.51-53.

- A.N., Infrastructure – Présentation de produits basés sur le standard émergeant de la protection de la vie privée, *Network & Telecom*, Best of publishing, n°12, September 2000, pp.24-25.

- A.N., Learn Mail – Gestion sécurisée et efficiente d'e-mails, *Inside Internet*,

Best of publishing, n°30, mars 2000, pp.105-107.

- A.N., Management Strategies – Actes de piratage : la menace interne, *Network & Telecom*, Best of publishing, n°11, June 2000, p.24.

- A.N., Pratique, comment faire – Chiffrez blindé avec PGP (Pretty Good Privacy), *SVM Mac*, VNU Publications France, n°121, octobre 2000, pp.144-145.

- A.N., Technology – A la recherche du maillon le plus faible - Journal d'un pirate, *Network & Telecom*, Best of publishing, n°8, March 2000, pp.74-76.

- A.N., Technology – ICP : intérêt accru pour les entreprises, *Network & Telecom*, Best of publishing, n°21, June 2001, p.66.

- A.N., Technology – L'ABC de la PKI, *Network & Telecom*, Best of publishing, n°9, April 2000, pp.66-67.

- A.N., Technology – La sécurité de bout en bout avec SSL, *Network & Telecom*, Best of publishing, n°12, September 2000, p.74.

- A.N., Technology – Le défi de la sécurité des e-mails, *Network & Telecom*, Best of publishing, n°11, June 2000, p.80.

- A.N., Technology – Passage sûr - Les récépissés numériques garantissent l'exécution de toute transaction confirmée, *Network & Telecom*, Best of publishing, n°10, May 2000, pp.72-74.

- A.N., Technology – SecureMe de Novell - Protection de sites intranet et de commerce électronique, *Network & Telecom*, Best of publishing, n°11, June 2000, p.104.

- A.N., Technology – Sécurité : la caverne d'Ali baba des sites, *Network & Telecom*, Best of publishing, n°17, February 2001, pp.64-66.

- A.N., Technology – Voyage en toute sécurité - Les fournisseurs de services de sécurité d'e-mails protègent vos messages sensibles des oreilles électroniques indiscrètes, *Network & Telecom*, Best of publishing, n°15, November 2000, pp.68-70.

- ALVERGNAT C. (rapport présenté par), Le publipostage électronique et la protection des données personnelles, *Commission Nationale de l'Informatique et des Libertés (CNIL)*, 1999 :
http://www.cru.fr/droit-deonto/droit/spam/cnilpublpost.pdf

- BARRET E., Pratique : planète techno - Le coin de l'expert – La pile TCP-IP, *SVM Mac*, VNU Publications France, n°135, janvier 2002, pp.122-124.

- BERANGER A.-L., Bases d'adresses e-mail : comment s'y retrouver ?, *Le Journal du Net* (http://www.journaldunet.com/), *Actualité Marketing*, 27 juin 2002.

- BERANGER A.-L., Dossier : e-mail marketing, *Le Journal du Net* (http://www.journaldunet.com/), juin 2002.

- BLACK J. (traduit par CHAVANNE M.), L'arsenal discret des pollueurs de mail, *Le Monde* (http://www.lemonde.fr), édition du 27 juin 2002.

- BRADNER S., Enterprise Applications – “Certifiablement” vôtre, *Network & Telecom*, Best of publishing, n°5, November 1999, p.43.

- CAULTON D., Microsoft response to the Windows Media Player 8 Privacy Advistory, 2002 : http://www.computerbytesman.com/privacy/wmp8response.htm

- CHEFFERT J.-M., Le commerce électronique : autorégulation et asymétrie d'information, *Revue Ubiquité – Droit des technologies de l'information*, Bruxelles, Larcier, n°12, 2002, pp.31-52.

- DESAUTEZ L., Spam : la CNIL passe à l'action, *Le Journal du Net* (http://www.journaldunet.com/), *actualité Le Net*, 11 juillet 2002.

- DUMOUT E., L'affaire des SMS roses devant la justice, *ZDNet.fr* (http://www.zdnet.fr/), *actualités internet*, 10 juillet 2002.

- EDLUND M., Learn Marketing – e-Marketing - L'e-consumer et sa vie privée, *Inside Internet*, Best of publishing, n°32, mai 2000, pp.91-93.

- FOLON J., Focus – De l'opt out à l'opt in : risque ou opportunité pour le permission marketing ?, *Inside Internet*, Best of publishing, n°44, juillet 2001, p.32.

- FOLON J., Society Law – La vie privée existe-t-elle encore sur Internet ?, *Inside Internet*, Best of publishing, n°36, octobre 2000, pp.90-92.

- GANY D., KETTANY S., Dossier E-mail – E-mail marketing : enfin le démarrage ?, *Inside Internet*, Best of publishing, n°45, septembre 2001, pp.44-53.

- GANY D., Market CRM – Marketing - Marketing Direct sur internet : enfin en Belgique!, *Inside Internet*, Best of publishing, n°36, octobre 2000, pp.54-56.

- GAUDIN S., GASPAR S., Management Strategies – Lutte contre le spam, *Network & Telecom*, Best of publishing, n°25, November 2001, pp.12-30.

- GAUTHRONET S., DROUARD E., Unsolicited Commercial Communications

and Data Protection, *Commission of the European Communities (Internal Market DG – Contract n° ETD/99/B5-3000/E/96)*, 2001. Disponible en téléchargement à l'adresse : http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf

- GEUENS J., L'e-mail marketing continue son essor en Belgique, *Internet Addict* (http://www.internetaddict.be), *Marketing*, 06 mai 2002.

- GIBBS M., Enterprise Applications – Identification gratuite, *Network & Telecom*, Best of publishing, n°3, September 1999, p.36.

- GIBBS M., Management Strategies – Double Opt-in exécuté dans les règles, *Network & Telecom*, Best of publishing, n°19, April 2001, p.20.

- GILLES L., Learn Protocol – La messagerie électronique - Monter un serveur mail, *Inside Internet*, Best of publishing, n°27, novembre 1999, pp.97-99.

- GILLES L., Learn Security – Le réseau en toute sécurité - 1ère partie : les types d'attaques et les faiblesses de l'Internet, *Inside Internet*, Best of publishing, n°25, septembre 1999, pp.100-102.

- GILLES L., Learn Security – Le réseau en toute sécurité - 2ème partie : les solutions passives, *Inside Internet*, Best of publishing, n°26, octobre 1999, pp.98-101.

- GILLES L., Learn Security – Le réseau en toute sécurité - 3ème partie : les solutions actives, *Inside Internet*, Best of publishing, n°27, novembre 1999, pp.100-103.

- GLASNER J., No subscription for spam relief, *Wired News* (http://www.wired.com/), 05 avril 2002.

- GRABOSKY P., Computer crime in a borderless world, *Annales Internationales de Criminologie*, 2000, vol.38 – 1/2, pp.67-92.

- HARDY J.-M., E-gov – PostBox : communications sécurisées avec l'administration, *Inside Internet*, Best of publishing, n°49, février 2002, pp.68-70.

- HAZEN MUELLER S., Frequently asked questions about spam ?, *Promote Responsible Net Commerce : Fight Spam!*, Fight spam on the Internet : http://spam.abuse.net/faq

- HAZEN MUELLER S., What is spam ?, *Promote Responsible Net Commerce : Fight Spam!*, Fight spam on the Internet : http://spam.abuse.net/overview/whatisspam.shtml

- HUYNH T., L'explosion du spam met en péril l'e-mail marketing, *Le Journal du Net* (http://www.journaldunet.com/), *actualité Marketing*, 04 juillet 2002.

- KOBIELUS J., Enterprise Applications – E-mail autodestructeur : pragmatique ou paranoïaque ?, *Network & Telecom*, Best of publishing, n°7, February 2000, pp.18-19.

- LEVINE J., Spammers do more than spam, *Promote Responsible Net Commerce : Fight Spam!*, Fight spam on the Internet : http://spam.abuse.net/scams/

- LEVINE J., Why is spam bad ?, *Promote Responsible Net Commerce : Fight Spam!*, Fight spam on the Internet : http://spam.abuse.net/overview/spambad.shtml

- LOUVEAUX S., DE TERWAGNE C., Protection des données à caractère personnel : application en Belgique de la directive européenne, *in* Actualités du droit des technologies de l'information et de la communication, *Commission Université-Palais, Formation permanente CUP*, février 2001, vol.45, pp.5-34.

- MARIANO G., Peer-to-peer : Audiogalaxy accepte de filtrer ses tuyaux, *ZDNet.fr* (http://www.zdnet.fr/), *actualités internet*, 18 juin 2002.

- MEEUS E., Legal – Signature électronique : où va-t-on ?, *Inside Internet*, Best of publishing, n°42, mai 2001, pp.72-74.

- MEUNIER C., La loi du 28 novembre 2000 relative à la criminalité informatique, *in* Actualités du droit des technologies de l'information et de la communication, *Commission Université-Palais, Formation permanente CUP*, février 2001, vol.45, pp.35-160.

- PEETERS K., E-mail : l'application killer, *Internet Addict* (http://www.internetaddict.be), *Marketing*, 23 avril 2002.

- PEETERS K., Spam : que le pollueur paie !, *Internet Addict* (http://www.internetaddict.be), *e-Business*, 24 juin 2002.

- RAPHAEL L., Ras-le-bol des e-mails publicitaires !, *La Libre Belgique* (http://www.lalibre.be), 24 juin 2002.

- RIMMER S. W., Death to spam, - : http://www.mindworkshop.com/alchemy/nospam.html

- SACRE J.-F., Compromis pour le marketing en ligne, *La Vie du net - Le Soir en ligne* (http://www.laviedunet.be/), 22 juin 2002.

- SALVAGGIO S., Interview – Anthropologie de la société digitale, *Inside Internet*, Best of publishing, n°47, novembre 2001, pp.64-66.

- SIRINELLI P., *"Exceptions et limites aux droit d'auteur et droits voisins"*, Atelier

sur la mise en oeuvre du Traité de l'O.M.P.I. sur le droit d'auteur et du Traité de l'O.M.P.I. sur les interprétations et exécutions et les phonogrammes, 1999 (http://www.wipo.int/fre/meetings/1999/wct_wppt/pdf/imp99_1.pdf), p.13.

- SIX N., De l'art de choisir le bon mot de passe, *JDNet Solutions* (http://solutions.journaldunet.com/), actualité *Sécurité*, 27 mai 2002.

- SIX N., Trop de mots de passe inefficaces sur les réseaux, *JDNet Solutions* (http://solutions.journaldunet.com/), actualité *Sécurité*, 24 mai 2002.

- SMITH R., Serious privacy problems in Windows Media Player for Windows XP, 2002 : http://www.computerbytesman.com/privacy/wmp8dvd.htm

- SOSNOWIEZ N., La vague des SMS rose profite d'une belle pagaille juridique, *ZDNet.fr* (http://www.zdnet.fr/), *actualités Business*, 18 juin 2002.

- STIENAERS M., Augmentation des budgets de l'e-mail marketing, *Internet Addict* (http://www.internetaddict.be), *Marketing*, 03 juillet 2002.

- SZAFRAN E., La cryptographie sur Internet : aspects techniques et réglementaires, *Auteurs & Media*, Larcier, 1998 (2), pp.120-133.

- VAN POUCKE F., Marketing – La veille : tout savoir sur vos marchés, *Inside Internet*, Best of publishing, n°48, décembre 2001, pp.58-60.

- VILLARS D., Society History – Aux origines de l'Internet - 1ère partie : plongée dans la Guerre froide, *Inside Internet*, Best of publishing, n°23, mai 1999, pp.112-113.

- VILLARS D., Society History – Aux origines de l'Internet - 2ème partie : à la recherche d'un ordinateur qui soit autre chose qu'un outil de calcul, *Inside Internet*, Best of publishing, n°24, juillet 1999, pp.85-86.

- VILLARS D., Society History – Aux origines de l'Internet - 3ème partie : les pièces du premier réseau s'emboîtent, *Inside Internet*, Best of publishing, n°25, septembre 1999, pp.86-87.

- VILLARS D., Society History – Aux origines de l'Internet - 4ème partie : une plomberie numérique mais… vide!, *Inside Internet*, Best of publishing, n°26, octobre 1999, pp.88-89.

- VILLARS D., Society History – Aux origines de l'Internet - 5ème partie : la fin de l'Arpanet, *Inside Internet*, Best of publishing, n°27, novembre 1999, pp.88-89.

- VILLARS D., Society History – Aux origines de l'Internet européen - 6ème partie : l'Europe se connecte, *Inside Internet*, Best of publishing, n°28, décembre 1999, pp.98-99.

- WEARDEN G., THOREL J., Spam et cookies : le Parlement européen arrondit les angles, *ZDNet.fr* (http://www.zdnet.fr/), *actualités internet*, 03 juin 2002.

C.– Autres

- Anti-Spam ! (http://members.hostedscripts.com/antispam.html)
- Break the chain – *stop junk e-mail and misinformation* (http://www.breakthechain.org/)
- CASPAM – *le collectif anti-spam* (http://caspam.org/)
- CAUCE – The Coalition Against Unsolicited Commercial Email (http://www.cauce.org/)
- L'encyclopédie e-Business – L'encyclopédie du Journal du Net, *JDNet Solutions* : http://encyclopedie.journaldunet.com/
- MAPS – Mail Abuse Prevention System (http://www.mail-abuse.com)
- SPAM (http://www.spam.com)
- SpamCop (http://spamcop.net/)
- Spam Laws (http://www.spamlaws.com/)