UNIVERSITE de LILLE 2 – Droit et Santé

Ecole Doctorale n° 74

Faculté des sciences juridiques, politiques et sociales

MEMOIRE

présenté et soutenu par

Philippe DIMITRIOU

en septembre 2002
pour l'obtention du diplôme de DEA Défense Nationale
option Sécurité européenne et internationale

Titre :

L'application du droit de la cryptologie en matière de sécurité des réseaux informatiques.

Directeur de recherches : Madame Valérie MUTELET

Philippe DIMITRIOU, 2002. fdimitriou2@yahoo.com

UNIVERSITE de LILLE 2 – Droit et Santé

Ecole Doctorale n° 74

Faculté des sciences juridiques, politiques et sociales

MEMOIRE

présenté et soutenu par

Philippe DIMITRIOU

en septembre 2002
pour l'obtention du diplôme de DEA Défense Nationale
option Sécurité européenne et internationale

Titre :

L'application du droit de la cryptologie en matière de sécurité des réseaux informatiques.

Directeur de recherches : Madame Valérie MUTELET

Sommaire

Introduction

1. L'année 1969 figurera probablement dans les livres d'histoire comme un grand moment dans l'exploration de nouveaux mondes. Deux événements marquants à retenir : le premier homme sur la Lune et... la naissance du premier jalon d'Internet[1] : ARPAnet[2]. Comme l'aventure spatiale, Internet, le « Réseau des réseaux »[3], est d'origine militaire. Financée par l'armée américaine depuis 1969, ARPA décide de mettre sur pied un réseau d'ordinateurs. Le projet ARPAnet visait donc à relier entre eux les ordinateurs des centres de recherche et des universités, dans le but de faciliter l'échange des données[4]. Le premier réseau informatique vient de naître.

2. La conception du réseau ARPAnet par les Américains a été influencé par leurs relations avec l'Union soviétique. À la fin des années soixante, la Guerre froide bat son plein ; États-Unis et Union soviétique vivent à l'ombre de l'arme nucléaire. Pour

[1] Un vocabulaire des principaux termes de l'informatique et de l'internet est disponible en annexe (no. 1) de ce mémoire.

[2] ARPA : Advanced Research Project Agency Network. Il s'agit d'une agence du Département de la défense des Etats-Unis.

[3] En français, on utilise parfois le terme « toile ».

[4] À titre d'exemple, grâce au réseau, un chercheur pouvait enfin exploiter à distance la puissance de calcul d'un superordinateur appartenant à un autre établissement.

contrer une telle attaque, ARPAnet est conçu selon une architecture entièrement décentralisée, basée sur le principe de la « transmission par paquets »[5]. Advenant l'anéantissement d'un ou plusieurs ordinateurs du réseau, la transmission des données peut automatiquement être reacheminée vers un autre segment du réseau, évitant ainsi la rupture complète des communications[6]. En 1972, ARPAnet comprend déjà une quarantaine de « nœuds »[7].

3. Alors que des motifs militaires sous-jacents existent, l'utilité première d'ARPAnet est essentiellement d'ordre scientifique. Le réseau facilite la communication entre les chercheurs, par le courrier électronique, et leur permet d'accéder aux ressources informatiques des autres établissements. En 1972, une importante conférence internationale se tient à Washington pour traiter de l'avenir des réseaux nationaux qui avaient commencé à proliférer. La plupart des universités américaines expriment le désir de faire partie d'ARPAnet. La question du protocole à utiliser s'est donc posée, afin de permettre une compatibilité optimale entre les différents types d'ordinateurs. Un groupe de travail, l'International Network Working Group, est mis sur pied pour concevoir un protocole universel permettant de relier entre eux tous les ordinateurs et réseaux existants : il s'agit du protocole TCP/IP[8]. L'agence ARPA, au lieu de considérer le protocole TCP/IP comme un secret militaire, décide de le rendre gratuit et disponible dans le domaine public.

4. Malgré ce protocole universel, le réseau n'a pas la capacité de supporter un si grand nombre d'utilisateurs. En 1986, le National Science Foundation, un organisme subventionnaire américain, décide donc de créer son propre réseau, le NSFnet. De

[5] Une information transmise est divisée en paquets et chaque paquet arrive à destination en empruntant un chemin différent, si nécessaire. Tous les paquets sont reconstitués à l'arrivée et forment ainsi le message initial.

[6] Les Américains ont appris durant la Guerre du Golfe en 1991, à leurs dépens, l'efficacité du concept : ils ont tenté sans succès de détruire le réseau de communication iraquien.

[7] On peut citer les quatre premiers, le Stanford Research Institute (SRI), les universités de Californie à Los Angeles (UCLA) et à Santa Barbara (UCSB), et l'université de l'Utah, à Salt Lake City.

[8] Vinton Cerf et Robert Kahn, avaient mis au point en 1974 le protocole TCP (Transmission Control Protocol) et ce qui deviendra le protocole IP (Internet Protocol). On peut donc considérer Cerf et Kahn comme les créateurs de l'expression Internet ; ces deux protocoles représentent la fondation d'Internet. On y fait généralement référence en utilisant le sigle TCP/IP.

nombreux collèges, universités et centres de recherche vont se relier à NSFnet et ce réseau universitaire deviendra le plus important maillon d'Internet et finira par absorber, en 1990, le réseau ARPAnet, mis à la retraite après plus de 20 ans de service.

5. Conçu d'abord pour les superordinateurs, le système d'exploitation Unix[9] jouera aussi un rôle particulièrement important dans la diffusion du TCP/IP. En raison de sa robustesse et de sa flexibilité, Unix deviendra fort populaire dans les universités et les grandes entreprises, où il est encore fort répandu. Comme le protocole TCP/IP sera intégré à Unix, cette plate-forme sera un véhicule important pour la propagation du protocole TCP/IP, et par ricochet, de toute la technologie d'Internet. De nombreux réseaux basés sur la technologie Unix se convertiront plus tard au protocole TCP/IP. La fusion de tous ces réseaux donnera naissance à l'International Network, mieux connu sous le nom d'Internet.

6. Les informations qui circulent par voie électronique se sont multipliées depuis l' « invention » d'Internet. Celles ayant une importance militaire ou scientifique devaient être protégées lors des transmissions à travers le réseau. Cette nécessité de crypter les messages n'est pas nouvelle, mais devient cruciale à cause du fait que les informations circulant sur les réseaux (Internet) traversent plusieurs « nœuds » avant d'arriver à leur destination. Le cryptage des informations numériques[10] étant encadré par la loi, fera l'objet de notre étude. Le droit de la cryptologie tente en effet d'encadrer, entre autres, les activités basées sur les réseaux informatiques, alors que les méthodes cryptologiques sont en constante évolution. Il faut tout de suite préciser que la cryptologie est une science fort ancienne. Il convient donc, dans un premier temps, définir la notion et la placer dans son contexte historique.

7. La cryptologie est la science énonçant les principes de la cryptographie. Pour qu'il y ait cryptologie, il faut la réunion de deux éléments : une opération de transformation de

[9] Le système d'exploitation Linux, concurrent dirent de Microsoft Windows actuellement, constitue la plate-forme Unix la plus répandue actuellement.

[10] Les données informatisées, qu'elles soient stockées dans un ordinateur ou circulant sur un réseau, sont numériques : ***binaire

signaux et un caractère secret attaché à ce mode de transformation. Elle regroupe la cryptographie et la cryptanalyse.

8. Le mot « cryptographie » du grec *kryptos* (caché) et le verbe *graphein* (écrire) peut être assimilé à « étude des écritures secrètes ». La cryptographie[11], c'est l'art de dissimuler ses intentions ou ses instructions à ses ennemis et pourtant de les transmettre à ses amis au moyen d'un texte chiffré. Elle est devenue une science appliquée englobant à la fois les techniques du chiffre et de la cryptanalyse. A ne pas confondre avec la stéganographie, qui est un procédé visant à dissimuler l'existence même d'un message.

9. La cryptanalyse est la technique qui étudie les moyens de chiffrement et recherche les méthodes permettant de décrypter ; plus généralement, la science qui étudie la sécurité des procédés cryptographiques. Cette technique est généralement employée chez l'adversaire dans le but de briser le code avec lequel on a crypté un message.

10. Dans le contexte juridique actuel, la terminologie n'est pas fixée : cryptologie, cryptographie, cryptage, chiffrement, encodage…il faut par conséquent, dans l'usage, les tenir pour équivalents. Dans la langue la plus pure, le terme qu'il fallait utiliser est celui de chiffrement, opération par laquelle on chiffre (on code) un message, car si on décrypte un message, on ne le crypte point[12]. Le législateur français ne définit pas la notion elle-même et préfère citer les prestations et moyens de cryptologie. Selon l'art. 28 I, premier alinéa, de la loi no 90-1170 du 29 septembre 1990[13] , « *on entend par prestations de 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* ». Le texte définit ensuite le moyen de

[11] Ne pas confondre avec la stéganographie qui consiste en un procédé visant à dissimuler l'existence même d'un texte.

[12] Lamy Droit de l'informatique et des réseaux éd.2001, no 3014.

cryptologie : « *On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié dans le même objectif* ». Une série de dispositions juridiques viennent par la suite former le régime légal de la cryptologie[14].

11. Au long de notre étude, nous réaliserons que ce dernier reste, dans le cas français, encore surveillé par l'Etat, alors que d'autres Etats ne disposent pas encore de réglementation en la matière. Les pays puissants ont tendance à surveiller de manière assez étroite la cryptologie[15]. A travers l'histoire de la cryptologie, nous démontrerons comment cette science est devenue importante pour les Etats, qui l'ont souvent employée pour transmettre des informations importantes et préserver leur souveraineté et ce depuis une date ancienne. Ce n'est donc que depuis 1996 que, pour le cas français, la cryptologie voit son régime assoupli (V. infra).

12. Selon les historiens, l'étude de la cryptographie a débuté il y a environ 4000 ans en Egypte [16]. Les égyptiens utilisaient des hiéroglyphes moins connus ou compliqués à la place des hiéroglyphes ordinaires. Le texte résultant était assez facile à décrypter, mais l'inscription contenait quand même le premier élément essentiel de la cryptographie : une modification volontaire de l'écriture. Les chinois ont aussi pratiqué la stéganographie à l'aide de papier ou de soie qu'ils roulaient en boule et recouvraient de cire. Cette boule était ensuite dissimulée ou avalée par le porteur du message pour assurer la sécurité lors du transport.

13. La cryptologie comme nous l'entendons aujourd'hui voit le jour pendant la période de l'antiquité. Les Spartes, guerriers grecs, avaient mis au point la « scytale », un procédé de chiffrement à finalité militaire. Il s'agissait d'un axe de bois autour duquel on enroulait un ruban de papyrus, cuir ou parchemin ; le texte était écrit en lignes

[13] Texte tel que modifié par l'art. 17 de la loi 96-659 du 26 juillet 1996 sur la réglementation des télécommunications.

[14] La liste exhaustive de la réglementation française en la matière peut être consultée en annexe (no.2).

[15] La France, un des cinq membres permanents au Conseil de Sécurité de l'ONU, surveille le droit de la cryptologie pour préserver ses intérêts (V. infra, première partie).

[16] Dans la ville égyptienne Menet Khufu.

droites, parallèles à l'axe. Le destinataire du message devait ensuite ré enrouler le ruban sur un axe de même diamètre, afin de lire le texte caché[17]. Les Grecs sont aussi à l'origine de procédés stéganographiques tels que des trous représentant les lettres de l'alphabet sur un disque. Le chiffrement consistait à passer un fil de façon aléatoire dans les différents trous. Un autre procédé stéganographique était de marquer d'une piqûre d'épingle dans un livre ou tout autre document les lettres dont la succession fournit le texte secret[18]. Polybe, écrivain grec, est à l'origine du premier procédé de chiffrement par substitution. C'est un système de transmission basé sur un carré de 25 cases, chaque lettre peut être ainsi représentée par un groupe de deux chiffres : celui de sa ligne et celui de sa colonne. Les cryptologues modernes ont vu dans le "carré de 25" plusieurs caractéristiques extrêmement intéressantes , comme la conversion de lettres en chiffres, la réduction de nombres et de symboles et la représentation de chaque lettre par deux éléments séparés. Malheureusement, Polybe n' a associé aucune utilisation à son procédé révolutionnaire. Les premières utilisations confirmées du principe de substitution se sont vues dans les opérations militaires avec notamment les Romains. Le plus grand d'entre eux, César, écrivait à Cicéron en remplaçant chaque lettre claire par celle située 3 rangs plus loin dans l'alphabet.

14. Durant le Moyen Age, la cryptographie a évolué faiblement. C'est au 15e siècle que la science de l'écriture secrète sera exploitée à de fins politiques et militaires. L'Italien Léon Batista Alberti, homme d'un génie exceptionnel, a inventé la « substitution poly alphabétique » et le « surchiffrement codique », en 1467. La première technique consistait à faire correspondre un alphabet lisible à une série d'alphabets cryptés. La deuxième technique était un répertoire de 336 groupes de mots représentés par toutes les combinaisons possibles, de 11 à 4444. Le procédé de « surchiffrement codique » était tellement avancé qu' il n' a été utilisé que quatre siècles plus tard.

15. Un autre procédé de substitution poly alphabétique a été conçu, au 16e siècle, par Jean Trithème, un moine bénédictin. Un tableau appelé « Tabula Recta » chiffrait la

[17] Les historiens grecs tels que Thucydide et Plutarque mentionnent l'utilisation de ce procédé par les Spartes vers 475 av. J.-C.

[18] Procédé notamment utilisé par les Allemands pendant la première guerre mondiale.

première lettre avec le premier alphabet, la deuxième lettre avec le deuxième alphabet et ainsi de suite. Ce procédé évoluera encore avec Giovanni Batista Belaso et Giovanni Batista Porta. Ce dernier a écrit un livre résumant les éléments existants de la cryptologie[19].

16. Le premier véritable outil de cryptologie sera inventé par le français Blaise de Vigenère[20]. Il s'agit d'une révolution de la cryptologie car c'est la phrase elle-même qui était la clé de cryptage et de décryptage. Une autre méthode appelée « Carré de Vigenère » permettait de dissimuler un message dans l'image d'un champ d'étoiles[21]. Ce procédé restera inviolable jusqu'en 1917.

17. Au 17e siècle, les cryptologues insistent sur l'importance de la cryptanalyse dans la politique. Un homme appelé Antoine Rossignol intervient auprès du Roi, contre les huguenots assiégeant la ville de Réalmont en 1628. Il décrypte un message destiné aux huguenots en une heure annonçant la fin de munitions très proche des huguenots. L'armée royale a réussi de capituler la ville et depuis, Rossignol commence la carrière de celui qui allait devenir le premier cryptologue professionnel de France. Le travail de Rossignol lui donnait accès à certains des plus importants secrets de l'Etat et, de ce fait, faisait de lui un homme brillant et respecté de la cour de Louis XIV. En 1682 il décède et son fils qu'il avait formé prit sa succession. Une des plus grandes contributions des Rossignol a été de démontrer à ceux qui gouvernaient la France l'importance du décryptement dans la détermination de leur politique. C'est peut-être depuis cette date que la cryptologie trouve sa place au sein des lobbys politiques français qui souhaitent contrôler son utilisation.

18. Au 18e siècle, des bureaux spécialisés dans le chiffrement et déchiffrement des courriers se créent. Il s'agit des « Cabinets Noirs » qui s'édifient dans toute l'Europe.

[19] « De Furtivis Literarum Notis », écrit en 1563.

[20] L' « Autoclave ». C'est Cardan, un médecin et mathématicien milanais qui a inventé ce procédé, mais l'application qu'il en faisait était défectueuse.

[21] Une technique similaire est actuellement employée dans un souci de protection des droits de l'auteur d'une œuvre photographique : Le « watermarking » (V. infra, +++ 2e partie).

Celui de Vienne en Autriche passait pour être le meilleur d'Europe. Les cryptanalystes utilisaient la sténographie pour plus de rapidité et connaissaient toutes les langues européennes. Si une était inconnue alors un fonctionnaire l'apprenait. Dix personnes travaillaient et déchiffraient 80 à 100 courriers par jour et commettaient peu d'erreurs. Pour plus d'efficacité, une personne travaillait une semaine sur deux. L'Autriche possédait alors une très bonne politique extérieure du fait de sa puissance dans le domaine de la cryptologie. L'Angleterre possédait aussi son Cabinet Noir. C'est sous l'impulsion de Wallis, passionné par la science des écritures secrètes, que de nombreux décryptements sur répertoire et substitution mono alphabétique ont été réalisées, notamment des cryptogrammes américains à destination de l'Europe. C'est le père de la cryptologie anglaise comme Rossignol l'était en France.

19. Le succès des cryptanalystes étaient dus, dans une large mesure, à leur habileté. Cependant, selon François de Callière, « Les déchiffreurs célèbres ne doivent leur considération qu'à la négligence de ceux qui donnent de méchants chiffres, et à celle des négociateurs et de leurs secrétaires qui s'en servent mal ». Sa remarque est juste dans le sens où il y avait une mauvaise utilisation du chiffre facilitant ainsi la tâche du cryptanalyste. La cryptographie contemporaine n’échappe pas à ce constat : ce qui est impossible ou très difficile à décrypter aujourd’hui ne le sera plus demain. Nous verrons plus tard dans notre étude, à titre d’exemple, qu’une clé numérique de 40 bits est actuellement facile à casser, alors qu’il y a 10 ans elle nécessitait le travail de plusieurs ordinateurs liés en réseau et travaillant simultanément. Les tourments politiques de 1840 renversèrent la plus grande partie de ce qui restait en Europe d'absolutisme. Le renouveau de la liberté ne tolérait plus l'ouverture des lettres par les gouvernements. En Angleterre, une formidable clameur publique et parlementaire contre l'ouverture clandestine du courrier obligea à interrompre le Cabinet Noir. En France, il n'a cessé de dépérir depuis la révolution pour totalement disparaître.

20. Avant Internet, le télégraphe révolutionnera la cryptographie. Cette nouvelle innovation dans les flux d'information a suscité de nouvelles vocations à la cryptologie. Les hommes d'affaires utilisaient des codes commerciaux pour leurs transactions. Ils remplaçaient des mots ou des phrases par de simples groupes codiques qui offraient

une sécurité suffisante. Mais les commerçants et courtiers réalisèrent que le principal avantage de ces codes était quand même l'économie financière qu'ils procuraient. Dans le domaine militaire, le télégraphe allait offrir aux généraux et autres officiers l'occasion d'exercer un contrôle continu et instantané des forces armées. Le chef militaire, installé dans un poste de commandement loin à l'arrière et informé par le télégraphe, suivait sur des cartes l'évolution de la bataille, mieux qu'il n'aurait pu le faire sur le terrain. Le temps des généraux à cheval, surveillant la bataille du sommet d'une colline comme Napoléon, était révolu.

21. Un ouvrage fondamental a ouvert la cryptologie aux influences extérieures : Il s’agit de « la cryptographie militaire » d'Auguste Kerckhoffs von Nieuvenhof. Il a mis en relief le changement apporté aux communications militaires par le télégraphe. Les chefs des armées désiraient que le chiffrement militaire possède les qualités suivantes : sécurité, rapidité et donc simplicité. Kerckhoffs avait reçu ce nouvel ordre de chose et a souligné l'importance de la cryptanalyse mettant à l'épreuve les procédés de chiffrement. De ces principes de sélection d'un système de chiffrement opérationnel, il a déduit six conditions fondamentales :

-Le système doit être matériellement, sinon mathématiquement, indécryptable.

-Il faut qu'il n'exige pas le secret et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.

-La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée et modifiée au gré des correspondants.

-Il faut qu'il soit applicable à la correspondance télégraphique.

-Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.

-Le système doit être d'un usage facile ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

« La cryptographie militaire » se place au premier rang parmi les ouvrages fondamentaux de la cryptologie.

22. A l'aube du 20ème siècle, le savoir en cryptographie et cryptanalyse est important. C'est dans le domaine militaire que l'on verra le plus cette science des écritures secrètes. Beaucoup de cryptologues ont découvert des procédés très complexes, cependant l'utilisation par les militaires sera simplifiée car des erreurs ont été faites dans le passé pour le cryptage ou le décryptage. La France, meilleure nation cryptologique, aborde le premier conflit mondial avec de l'avance sur l'Allemagne qui pense toujours être la nation suprême et ne s'est pas rendue compte de l'importance de la cryptanalyse mettant à l'épreuve la cryptographie. Le rôle de la cryptologie va être décisif pour le destin du monde en raison de l'utilisation qu'elle a connue pendant les deux guerres mondiales.

23. La période de la Première Guerre Mondiale est à l'origine de la création, dans tous les pays, de services organisés de chiffre et de décryptement. La radio a été l'un des moyens le plus utilisés pour faire passer des messages. Les généraux se sont emparés rapidement comme instrument de guerre car elle multipliait l'avantage essentiel de la télégraphie militaire et accélérait la communication entre les quartiers généraux. Mais la probabilité d'interception était grande et la facilité d'écoute trop importante. La cryptanalyse est devenue un moyen d'action opérationnel. C'était une source valable d'informations et donc une véritable arme[22]. On peut mentionner l'exemple britannique du « Bureau 40 » dont la mission était de décrypter les messages des allemands et des espagnols. Plus de quinze mille messages secrets ont été décryptés entre 1914 et 1919. Quant aux américains, ils ont commencé à s'intéresser à l'étude du chiffre depuis 1919. Le rôle de la « American Black Chamber » était de décrypter les codes utilisés par les militaires japonais.

24. La Deuxième Guerre Mondiale marque la transition entre la cryptologie classique et la cryptologie moderne.
Les allemands ont utilisé une machine, nommée Enigma I, pour échanger des informations militaires. La marine allemande commence à l'utiliser à partir d'octobre 1934 et l'aviation à partir d'août 1935. Pendant toute la durée de la guerre, des

[22] Le Décret-loi du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions assimilait la cryptographie à une arme de guerre.

changements seront apportés à Enigma pour améliorer son efficacité. Tous les niveaux du gouvernement et de la défense on utilisé Enigma pour communiquer. Ils ont été tellement convaincus que leur codes ne peuvent être brisés, qu'ils transmettront au vu et su de tous. Malgré le haut niveau de cryptage, les secrets transmis avec la machine Enigma ont étés régulièrement déchiffrés par les cryptanalystes des alliés[23]. La résolution de ces secrets militaires qui contenaient des informations stratégiques capitales a permis de sauver la vie de centaines de personnes.

25. L'Europe ne se connecte à Internet qu'au début des années 1980. L'effondrement du bloc de l'Est à la fin de la même décennie a permis son développement ainsi que son utilisation à des fins commerciales et privées. La France était le dernier pays démocratique à limiter très strictement la cryptographie, rejoignant ainsi les pays, comme la Chine, qui ne respectent pas les droits de l'homme[24]. L'irruption d'Internet a provoqué l'évolution actuelle. Au départ, il était interdit de communiquer des informations par un moyen secret, à moins que ce moyen ait été expressément autorisé par l'Etat. A titre d'exemple, on n'avait pas le droit de brouiller ses conversations par téléphone sans fil, par conséquent n'importe qui pouvait les intercepter…ce qui était interdit, mais le matériel pour le faire se vendait légalement ! La transmission du numéro de notre carte bancaire pour un télépaiement devait se faire en clair…ce qui permettait à un tiers de capter l'information transmise et se servir à notre place. Même les mots de passe conservés sur notre ordinateur ne pouvaient pas être chiffrés ; or, il existe des logiciels[25] qui peuvent les transmettre à des pirates. La seule possibilité pour crypter des informations était de demander l'autorisation, personnelle et préalable, à un organisme spécialisé, le Service Central de Sécurité des Systèmes d'Information (SCSSI)[26]. Le développement du commerce électronique était impossible dans ces conditions. L'utilisation de la cryptologie est indispensable afin de protéger les intérêts

[23] Durant la Seconde Guerre Mondiale, Alan Turing, un anglais, a fortement contribué au décryptement des messages allemands.

[24] Les moyens de cryptologie étaient classés parmi les matériels de guerre jusqu'à la loi du 29 décembre 1990 sur la réglementation des télécommunications.

[25] Les « chevaux de Troie » (Tojan Horses) sont des logiciels qui peuvent être intégrés dans d'autres logiciels inoffensifs qui, une fois installés sur un ordinateur, activent le cheval de Troie qui peut, par exemple, transmettre des informations personnelles et/ou des codes d'accès au créateur du logiciel ou une tierce personne.

[26] Cette question sera traitée dans la Première Partie de notre étude.

des particuliers et des entreprises. Le législateur a petit à petit réalisé les enjeux en cours et a assoupli le dispositif légal.

26. La cryptologie actuelle s'applique dans des nombreux domaines : télécommunications avec ou sans fil, radio, cartes bancaires, logiciels…bref, chaque fois que l'on a besoin de confidentialité. Notre étude sur la cryptologie actuelle et le droit applicable va concerner plus spécifiquement Internet, le Réseau des réseaux.

27. Internet se développe très rapidement et remplace, dans la vie quotidienne, un bon nombre d'applications existantes[27], d'où l'actualité de la question : la cryptologie se démilitarise progressivement et s'intègre dans la vie courante de l'individu. Il s'agit d'un passage, de la science du secret à la science de la confiance. Le compromis juridique actuel, qui tend à satisfaire les besoins étatiques et ceux des citoyens, reflète bien cette situation. Par conséquent, nous étudierons, dans une première partie, la cryptologie au service des Etats puis, dans une deuxième partie, comment elle s'applique au profit des citoyens.

[27] Il suffit d'imaginer qu'en disposant d'une connexion Internet rapide, il est déjà possible d'utiliser un ordinateur à la place de la télévision, de la radio, du téléphone, du courrier classique, de régler nos factures ou d'acheter n'importe quel produit quel que soit le lieu (physique) où le vendeur est situé.

PREMIERE PARTIE

LA CRYPTOLOGIE AU SERVICE DES ETATS

28. La France se veut un pays militairement puissant et, de ce fait, encadre de manière stricte le dispositif légal portant sur la cryptologie. Les considérations de sécurité nationale se trouvent au cœur de la loi de 1990 sur la réglementation des télécommunications : « *Pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, tout en permettant la protection des informations et le développement des communications et des transactions sécurisées (…)* [28] ». Dans son discours du 19 janvier 1999, le Premier ministre M. L. Jospin, avait annoncé la libéralisation totale en France de l'utilisation de la cryptologie[29] mais a ajouté que « *le respect de la protection de la liberté individuelle et de la confidentialité des données personnelles ne doit pas aboutir à désarmer la justice et la police dans leur lutte contre la criminalité* ».

29. Il résulte un régime juridique tantôt libéral, tantôt « sécuritaire ». Ce compromis est influencé par l'idée et le besoin de sécurité, fonction appartenant essentiellement à l'Etat. En outre, les réseaux sont très fréquemment au cœur des conflits modernes. Nous analyserons cette question dans une première section. L'Etat français souhaite garder un maximum de contrôle sur cette situation, qui peut mettre en jeu ses intérêts vitaux. Il découle un régime juridique assez contraignant. Nous analyserons cette question dans une deuxième section.

---

[28] Art. 28 I, alinéa 2, de la loi no 90-1170 du 29 décembre 1990, JO 30 décembre, tel que modifié par la loi no 96-659 du 26 juillet 1996, JO 27 juillet.

[29] M. A.P., La France renonce à contrôler les communications sur Internet, Le Monde, 21 janvier 1999, p.16.

CHAPITRE 1

LES RESEAUX AU CŒUR DES CONFLITS MODERNES

30. Si l'information a toujours été au cœur de la guerre, elle acquiert aujourd'hui un rôle différent avec le développement des réseaux. Après la guerre menée au Kosovo, les certitudes héritées de la guerre froide se sont effacées et laissent la place à de nouvelles doctrines militaires. Le réseau est le système nerveux par lequel circule l'information. Cette mutation conduit les stratèges à se préparer à la « cyberguerre », où, pour dominer l'adversaire, il suffirait de perturber ses structures de commandement, de communication et de pensée, plutôt que d'entreprendre sa destruction physique. En outre, depuis les attentats du 11 septembre, la menace du « cyberterrorisme » conduit les Etats à blinder encore plus leurs réseaux, Etats-Unis en tête. Les gouvernements des pays les plus développés recourent aux différents moyens de cryptologie pour protéger les systèmes informatiques vitaux, comme ceux du trafic aérien ou ferroviaire. Mais les conflits modernes ne se limitent pas à la « cyberguerre ». Le cyberterrorisme et plus généralement la cybercriminalité sont des dangers de même importance pour les Etats. Parmi eux, les plus « vigilants », dont la France, essayent de limiter l'utilisation de la cryptologie de haut niveau en adoptant une législation contraignante. L'idée générale est que les services spécialisés de la Défense Nationale doivent être en mesure de casser les codes chaque fois que cela s'avère nécessaire.

31. Sur le plan juridique, le Conseil de l'Europe a adopté récemment une Convention sur la cybercriminalité[30]. La croissance du cyberespace a grandement favorisé le développement de la criminalité organisée, il fallait alors construire un cadre légal pour

[30] Fait à Budapest, le 23 novembre 2001. Il s'agit du premier traité international spécifique au cyberespace.

favoriser la coopération internationale en matière pénale et mener une politique pénale commune, destinée à protéger la société de la criminalité dans le cyberespace. La convention incite les pays, entre autres, à collecter en temps réel les données informatiques et à procéder au filtrage et à l'interception des informations suspectes. Sur le plan interne, la loi Godfrain de 1988 punit sur le plan pénal les attaques logiques[31] et la loi sur la sécurité quotidienne (LSQ) du 18 décembre 2001 oblige les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité de remettre aux autorités étatiques les conventions permettant le déchiffrement des données. Nous analyserons ces questions dans un premier paragraphe. Il résulte que les moyens cryptologiques doivent être juridiquement encadrés pour permettre aux différentes autorités étatiques à procéder aux contrôles nécessaires. La cryptologie de haut niveau dépend, dans le cas français, de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI, ex-SCSSI). La DCSSI examine, valide et expertise tout système informatique pouvant avoir des répercussions sur la sécurité des réseaux et des infrastructures. Et même si le dispositif juridique devient de plus en plus souple, on est loin d'être en présence d'un régime de liberté totale[32]. Cette question fera l'objet d'un deuxième paragraphe.

SECTION 1. Atteintes logiques et cryptologie

32. Les atteintes logiques peuvent prendre la forme du « cyberterrorisme » ou de la « cyberguerre », lorsque les attaques visent en particulier des acteurs étatiques. Considéré souvent comme la prochaine menace pour les Etats puissants, le cyberterrorisme peut viser aussi bien les acteurs privés de la société. Des dispositions pénales sont prises à l'égard des pirates informatiques.

§1. Les notions de « cyberguerre » et de « cyberterrorisme »

[31] C'est les attaques des pirates aux systèmes informatiques.

[32] Comme, par exemple, aux Etats-Unis, au Royaume-Uni, en Allemagne, la Suède…

33. L'OTAN, dans la récente guerre du Kosovo, a fait un usage massif de bombes venues de l'ère industrielle. Même qualifiées d'« intelligentes », en raison de leur capacité à traiter des informations de façon autonome, ces bombes n'en étaient pas moins dotées d'un pouvoir, très classique, de destruction. Derrière les drames humains et politiques immédiats se profile une question qui concerne les conflits de demain : et si les alliés s'étaient trompés de guerre ? Les bits ne sont-ils pas censés remplacer les atomes[33] ? Le problème est posé par deux chercheurs américains, spécialistes des conflits de l'ère informationnelle. John Arquilla[34] et David Ronfeldt[35] sont les inventeurs de toute une série de concepts et de formules originales : « cyberguerre » (cyberwar), « guerre en réseau » (netwar) et « noopolitique » (politique de la connaissance). Les deux chercheurs sont convaincus que « la révolution de l'information altère la nature des conflits » et « introduit de nouvelles modalités dans l'art de la guerre, le terrorisme et le crime ». Ils répondent ainsi au souhait des futurologues Alvin et Heidi Toffler de voir se développer une « compréhension nouvelle des relations entre la guerre et la société en rapide évolution[36] ». On ne peut pas, en effet, invoquer les profondes transformations de la société et ne pas s'interroger sur les bouleversements qu'elles entraînent dans la façon de faire la guerre. La Renaissance, à laquelle on compare volontiers l'ère numérique, a, elle aussi, été marquée par une façon différente de faire la guerre, avec l'invention de l'infanterie. Il en va de même de l'ère industrielle et des moyens de destruction de masse qu'elle a mis au service des armées. La cyberguerre va au-delà des bombes « intelligentes » utilisées pendant la guerre du Golfe en 1991 et des bombes au graphite capables de court-circuiter les centrales électriques, utilisées récemment contre la Serbie ; elle repose sur le concept d'information. Dans la sphère économique, cette différence réside dans le fait que « l'information, elle-même se convertit en produit du processus de production[37] ». En cas de conflit, elle devient l'objet même de l'affrontement, et non plus seulement ce qui permet de l'aborder dans des conditions avantageuses.

---

[33] Formule de M.Nicholas Negroponte, *in* L'Homme numérique, Laffont, Paris, 1995.

[34] M. Arquilla est professeur de sciences de l'information dans l'université de la Navy à Monterrey, San Francisco.

[35] M. Ronfeldt est analyste à la Rand Corporation, institut de recherche très proche de l'appareil militaire et des services de renseignement.

[36] Alvin et Heidi Toffler, Guerre et contre-guerre, Hachette, Paris, 1996.

34. Sur le terrain, on passe d'une guerre où l'essentiel pouvait se mesurer à la capacité de « destruction » à des affrontements dans lesquels la capacité de « perturbation » (disruption), c'est-à-dire de désorganisation, compte tout autant. On peut retenir deux idées des chercheurs John Arquilla et David Ronfeldt qui sont en rapport avec notre étude : la montée des organisations en réseaux et la notion domination en matière d'information.

35. Une des conséquences les plus importantes de la révolution informationnelle est la montée des organisations en réseaux. Cela vaut pour les organisations non gouvernementales (ONG) comme pour les réseaux terroristes. La technologie renforce le réseau comme structure sociale ; d'où les définitions distinctes de la « cyberguerre » (cyberwar), affrontement classique avec des armes plus « intelligentes » et selon des modes d'engagement adaptés à l'ère de l'information, et de la « guerre en réseau » (netwar), qui concerne les affrontements entre (ou avec) des acteurs « autres que des Etats ». Quant à la domination en matière d'information, l'objectif principal est de savoir plus que l'adversaire sur le théâtre d'opérations. La connaissance de la situation et des mouvements de l'autre, associée à un système de communication sophistiqué (chaque combattant est en contact avec tous les autres et les chefs d'unité communiquent avec les responsables de l'aviation et d'autres unités), permettrait d'utiliser des effectifs réduits avec une grande efficacité. John Arquilla et David Ronfeldt sont convaincus que la libre circulation de l'information sert les intérêts des Etats-Unis et que, en dernière instance, « ce n'est plus celui qui a la plus grosse bombe qui l'emportera dans les conflits de demain, mais celui qui raconte la meilleure histoire ».

36. La cyberguerre qui pourrait paraître de la science-fiction il y a quelques années, est déjà la réalité. Ceci peut aller de la robotique militaire de terrain jusqu'à la guerre en ligne. L'armée américaine possède déjà des avions sans pilote et l'armée française

[37] Manuel Castells, La Société en réseaux, Fayard, Paris, 1998.

intègre un concept similaire au « plan prospectif à 30 ans (PP30) ». Avec l'interconnexion informatique, la guerre se livre de plus en plus sur un champ de bataille numérisé.

37. Notion plus subtile que la cyberguerre, le cyberterrorisme apparaît comme la prochaine menace. Américains et Européens renforcent leurs systèmes d'information pour éviter que les pirates informatiques paralysent ces systèmes. Les attaques pirates ne constituent pas un phénomène nouveau[38]. Cependant, jusqu'à présent, les dégâts sont plutôt financiers. Deux situations sont notamment à craindre : les attaques des réseaux informatiques vitaux, comme ceux du trafic aérien ou ferroviaire, et les attaques combinées, c'est à dire les attentats classiques, suivis des attaques contre les réseaux de communication. Ce dernier cas de figure pourrait produire un niveau de terreur et de peur maximal, et les dégâts seront encore plus importants si la deuxième attaque (sur les réseaux) est menée contre les systèmes informatiques qui gèrent la réponse, c'est à dire les ordinateurs des pompiers, des hôpitaux et autres services publics.

38. La cryptologie vient donc protéger les systèmes informatiques des Etats contre ces attaques. Cependant, en étudiant la position des Etats de référence dans le domaine de la cryptologie, on s'aperçoit qu'un déséquilibre existe : certains présentent un savoir-faire technologique remarquable, alors que d'autres sont plus en retard. Par exemple, les Etats-Unis permettent l'utilisation libre de la cryptologie, cette liberté faisant partie des droits fondamentaux consacrés par la Constitution. Cependant, cette liberté connaît une limite : la cryptologie est assimilée à une arme[39] chaque fois que le moyen est destiné à l'exportation et sera utilisé à des fins militaires. La divulgation ou le transfert de données techniques à une personne étrangère, même si elle réside sur le territoire américain, est assimilée à une exportation. En même temps, la cryptologie de niveau

[38] On peut citer deux exemples à propos du piratage assimilé au cyberterrorisme : en 1999, le premier producteur de gaz en Russie, Gazprom, a perdu pendant un certain temps le contrôle de ses gazoducs ; en 2000, des pirates ont réussi à contrôler l'ordinateur central d'une centrale électrique en Californie, sans causer de dégâts.

[39] Pour les produits cryptographiques de haut niveau, qui sont classés dans la catégorie des munitions dans l'*United Stats Munition Act*, qui dépend de l' *International Trafic Arms Regulation (ITAR).*

militaire est un secret de l'Etat et les informations la concernant ne sont pas accessibles au public. Cependant, si tous les produits cryptographiques étaient classés dans la catégorie des armes de guerre et munitions et leur exportation nécessitait une autorisation de la NSA[40] et du département d'Etat, depuis 1996 le régime est assoupli[41].

39. Un autre pays très avancé est Israël : confronté aux guerres, à la guérilla et au terrorisme, il est renommé pour l'efficacité de ses services de renseignement. Les logiciels de cryptographie israéliens rencontrent un succès non négligeable et la cryptographie sert des fins militaires ainsi que les intérêts des particuliers et contribue ainsi à la sécurité de l'Etat. Sur ce point il faut préciser que les produits cryptographiques font partie, dans le commerce international, des biens considérés comme « sensibles » ou à « double usage », c'est à dire des biens susceptibles d'avoir une utilisation tant civile que militaire.

40. La France dispose du système Socrate, qui fédère tous les réseaux de communications militaires. L'armée française utilise des technologies « classiques » comme le IP[42], le routage, des adresses IP…mais le réseau reste fermé. Cela veut dire que les terminaux militaires, connectés entre eux, ne le sont pas avec Internet. Il s'agit d'un point fondamental car un pirate doit se trouver physiquement devant un de ces terminaux pour attaquer le système. La faille ne peut donc provenir que d'une complicité à l'intérieur. En outre, la stratégie de la DGA (Délégation générale pour l'armement) consiste à définir de façon précise les données à transmettre et des contrôles sont effectués sur les données qui circulent. L'armée développe aussi une structure de veille, appelée Mirador, qui lui permet de détecter les intrusions à l'échelle nationale. En revanche, les autres administrations sont plus vulnérables. Les différents ministères travaillent ensemble pour lutter contre le « cybercrime ».

[40] National Security Agency.

[41] Depuis le 15 novembre 1996, le contrôle des exportations des produits cryptologiques relève de la compétence du Commerce Department (sauf pour les produits utilisés à des fins militaires). Les raisons qui ont conduit le pays à assouplir son régime est étudié aux §85 et s.

41. Sur le plan technique, un réseau devient plus difficile à attaquer lorsque certaines mesures de sécurité sont prises, comme les *firewalls*[43], dans un premier temps, puis le cryptage des données sensibles et des codes d'accès dans un deuxième temps. Un firewall est un dispositif informatique (logiciel ou matériel, selon l'option choisie) qui filtre le flux d'informations entre un réseau local (interne à un organisme, intranet) et un réseau externe (le plus souvent Internet), en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur. On pourrait le comparer à une serrure ; il s'agit d'une mesure efficace mais non pas sans faille. Si le pirate réussit à pénétrer le réseau local, les données sauvegardées sous une forme cryptée sont beaucoup plus difficilement accessibles par la suite. De nombreux logiciels contenant des fonctions de cryptage existent dans le commerce[44] ; ils sont utilisés autant par les administrations que par les particuliers ou les entreprises privées. Nous étudierons cette question plus en détail dans notre deuxième partie.

§2. La répression des atteintes logiques

42. Les attaques pirates sont réprimées pénalement par la loi no. 88-19 du 5 janvier 1988, dite loi Godfrain[45]. La loi vise les atteintes logiques aux fichiers de programmes (les atteintes à des éléments purement matériels sont exclues de son champ d'application) d'un système informatique et s'applique quelle que soit la victime, administrations ou personnes privées.

---

[42] IP, pour *Internet Protocol*, voir annexe 1.

[43] En français on utilise aussi les termes « pare-feu » et « barrière de sécurité ». (Cf. deuxième partie).

[44] Par exemple, Microsoft Word, Winzip, Winrar, des nombreux *freeware* (logiciels distribués gratuitement sur Internet), ainsi qu'un bon nombre de logiciels *open-source* (sous licence GPL, dont chacun peut connaître gratuitement le code source et le modifier avant de le redistribuer), font partie des logiciels qui permettent à tout utilisateur de protéger un document par un mot de passe. Ils assurent donc des fonctions de confidentialité.

[45] Sur le plan communautaire, une proposition de décision-cadre du Conseil a été présentée par la Commission européenne le 19 avril 2002 (COM(2002)173). Cette proposition « *relative aux attaques visant les systèmes d'information* » vise à rapprocher les droits pénaux des Etats membres par l'institution d'incriminations communes. Son contenu ne s'éloigne pas de l'esprit de la loi Godfrain.

A. Champ d'application de la loi Godfrain

43. La loi s'applique aux STAD (systèmes de traitement informatisé de données). Le Sénat a défini en 1987 cette notion, qui coïncide avec la notion technique de système informatique : « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciels, de données, d'organes entrée-sortie, et liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* ». Par « dispositif de sécurité » on entend la volonté du détenteur de l'information d'interdire la pénétration aux tiers : il s'agit des mesures techniques de protection qui se réalisent par des moyens de cryptologie. Contrairement donc à un site Internet, qui est en principe librement accessible à tous, le fait même d'accéder à une information concernée par la loi Godfrain ouvre le droit à des poursuites pénales.

B. Peines principales

44. Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un STAD est puni d'un an d'emprisonnement et de 15000 Euros d'amende[46]. On peut définir l'accès comme une action de pénétration ou d'intrusion. En outre, pour qu'il y ait infraction, l'auteur doit avoir l'intention (avoir conscience) d'accéder anormalement dans un système…l'intention de nuire n'est pas nécessaire, ni la constatation d'un préjudice. En revanche, s'il y a préjudice (dommage), même involontaire, la peine est aggravée : deux ans d'emprisonnement et 30000 Euros d'amende[47]. Le fait d'entraver ou de fausser le fonctionnement d'un STAD, que ce soit par l'envoi de virus, la mise en place de barrages[48] ou le détournement des codes secrets ou la rétention des clés, est puni de trois ans d'emprisonnement et jusqu'à 45000 Euros d'amende[49]. La notion

[46] NCP, Art. 323-1. Le projet de loi LSI (V. *infra* §103) propose de passer de 1 à 2 ans d'emprisonnement.

[47] NCP, Art. 323-1, 2e alinéa. Le projet de loi LSI propose de passer de 2 à 3 ans d'emprisonnement.

[48] Par exemple, le déni de service sur Internet consiste à empêcher un accès normal des internautes ou de le retarder.

[49] NCP, Art. 323-2. Le projet de loi LSI propose de passer de 3 à 5 ans d'emprisonnement.

d'entrave se définit comme une influence négative sur le fonctionnement d'un système. C'est l'élément matériel de l'infraction. La même peine est prévue en cas d'introduction, de suppression ou de modification frauduleuse de données[50]. Cette falsification des données tombe également sous le coup de l'incrimination générale de faux et usage de faux (« altération de tout support d'expression de la pensée »[51]). Enfin, la participation à un groupement formé (groupe de « hackers ») est punie par l'art. 323-4 du nouveau code pénal.

C. Peines complémentaires et responsabilité des personnes morales

45. Outre les peines principales, les coupables encourent les peines complémentaires visées à l'art. 323-5 du nouveau code pénal. Ces sept peines sont :

-L'interdiction, pour cinq ans au plus, des droits civiques, civils et de famille ;

-L'interdiction, pour cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

-La confiscation[52] de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

-La fermeture, pour une durée de cinq ans au plus, des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

-L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

-L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur ;

-L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'art. 131-35 NCP.

Les personnes morales peuvent aussi être déclarées responsables pénalement[53], chaque fois que l'infraction a été commise pour leur compte, par leurs organes ou représentants

[50] NCP, Art. 323-3.

[51] NCP, Art. 441-1.

[52] L'ancien article 462-9 ne mentionnait que la seule peine de confiscation des matériels ayant servi à commettre l'infraction.

(ceci exclut les salariés). Cette responsabilité n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits. On s'aperçoit que les peines deviennent de plus en plus nombreuses et lourdes. Le législateur réalise l'importance de l'informatique dans la société contemporaine. Simultanément, au niveau international, un premier traité spécifique au cyberespace voit le jour en novembre 2001 : c'est la convention contre la cybercriminalité signée à Budapest.

SECTION 2. Cybercriminalité et interception des données

46. L'apparition de nouvelles formes de criminalité, issues des nouvelles technologies de l'information et de la communication (NTIC), notamment Internet, conduit les Etats à prendre les mesures nécessaires pour contrôler, en temps réel ou a posteriori, les données suspectes qui circulent via le réseau. Nous aborderons deux exemples très récents, l'un au niveau international[54], l'autre au niveau interne (français). Tous deux viennent armer la justice et la police dans leur lutte contre la criminalité, ce qui a soulevé de vives critiques par les ONG de défense des libertés. En effet, la liberté d'expression se voit restreinte chaque fois que des contrôles étendus sont autorisés par la loi.

§1. Les dispositions prévues par la convention sur la cybercriminalité du 23 novembre 2001

[53] Il s'agit d'une création récente et figure à l'art.121-2 NCP.

[54] Sur le plan communautaire, la Commission a aussi publié en 2000 (COM(2000)890) une communication « Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité ».

47. Les Etats[55] peuvent désormais s'appuyer sur un traité international pour préserver leurs intérêts. Il s'agit du premier traité international sur les infractions pénales commises sur les réseaux informatiques. Le texte définitif enjoint les Etats à poursuivre pénalement un certain nombre d'infractions relatives à l'usage des réseaux.

A. Les infractions prévues par la convention

48. La convention incite les Etats de prendre les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à leur droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique (art.2). L'art. 7 ajoute l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, qui engendrent des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Des dispositions concernant les atteintes à la propriété intellectuelle et les contenus immoraux (ex. pornographie pédophile) font aussi partie du texte de la convention. Enfin, le texte légalise les interceptions en temps réel, sur la base des lois existantes sur les écoutes téléphoniques (titre 5 de la convention, art. 20 et s.), institue un droit de perquisition à distance d'un système informatique (art.29) et impose aux fournisseurs d'accès (FAI[56], cf. §49 et s.) une durée de conservation des données de 90 jours au maximum, afin de permettre un contrôle éventuel, par les autorités compétentes, des opérations et des messages informatiques susceptibles de constituer des délits (art.16).

B. Le rôle du droit interne de la cryptologie à l'égard de certaines dispositions de la convention

[55] Le traité est ouvert à signature aux 43 Etats du Conseil de l'Europe, ainsi qu'aux cinq pays observateurs (Canada, Etats-Unis, Australie, Japon et Afrique du Sud).

[56] FAI : Fournisseur d'accès Internet. Ce sont des intermédiaires, qui permettent aux utilisateurs de se connecter au réseau moyennant une rémunération qui prend généralement la forme d'un abonnement mensuel.

49. Trois points de la convention sont en rapport direct avec le droit de la cryptologie des Etats signataires. Il s'agit des interceptions en temps réel, du droit de perquisition et l'obligation de conservation des données pour les FAI. *De facto*, une utilisation libre de la cryptologie de haut niveau rendrait l'application de ces dispositions de la convention illusoires.

50. La légalisation des interceptions en temps réel deviennent techniquement impossibles en pratique lorsque les messages sont envoyés cryptés, par exemple grâce à la technique du OpenPGP (cf. §54-55,134-135). En outre, les différentes techniques existantes pour garder n'anonymat (cf. §132) rendrent l'identification des coupables difficile.

51. L'institution d'un droit de perquisition à distance d'un système informatique devient aussi difficile dès lors que des firewalls de qualité sont entreposés entre les machines et le réseau externe. En plus, les bases des données et les informations chiffrées dans les mêmes machines empêchent encore plus la lecture en clair de ces dernières.

52. L'imposition aux FAI d'une durée de conservation des données « pour une durée aussi longue que nécessaire » (90 jours au maximum), quel que soit le volume des données, constitue une contrainte financière assez lourde. Inévitablement, des données qui circulent sur Internet passent par les serveurs des FAI, avant d'arriver à leur destination. Ce passage permet à ces serveurs de stocker dans leur mémoire cache[57], puis dans leurs disques durs, ces informations. Le volume d'informations qui passe tous les jours est énorme, ceci étant multiplié par 90 jours, crée le besoin de posséder d'une grande capacité de stockage. Pour ce qui est de la cryptologie, un contrôle

[57] Cache : mémoire temporaire d'un ordinateur (données stockées sur le disque dur pour une certaine durée – disk cache), qui s'efface périodiquement. Cette durée est préconfigurée par défaut dans la plupart des navigateurs Internet des PC, à moins de 30 jours.

éventuel, par les autorités compétentes, des opérations et des messages faisant partie de cette masse de données serait sans intérêt si ces données sont cryptées.

§2. Le volet cryptologique de la loi sur la sécurité quotidienne

53. Contrairement à la Convention sur la cybercriminalité, qui a nécessité quatre années d'élaboration et vingt-sept versions avant l'adoption du texte définitif, la loi sur la sécurité quotidienne (LSQ) a été votée dans l'urgence par le Parlement français. Cette loi est un ensemble fourre-tout, qui concerne aussi bien les perquisitions de véhicules que les occupations de halls d'immeuble, en passant par la pénalisation de la misère ou l'extension du fichier d'empreintes génétiques. La loi contient aussi un volet cryptologique qui mérite notre analyse.

A. LSQ et Code de procédure pénale

54. Les projets d'articles 230-1 et suivants du Code de procédure pénale disposent notamment que lorsqu'il apparaît que des données saisies ou obtenues au cours d'une enquête ou d'une instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair, « *le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations* ». Cependant, l'outil de cryptographie considéré comme le standard actuel est le format OpenPGP. Il s'agit d'une cryptographie forte, reconnue par la communauté scientifique comme incassable. C'est en raison de cette résistance à toute possibilité de cassage que le législateur français a considéré que les citoyens ne devaient pas avoir le droit de la diffuser et de

l'utiliser librement pour protéger l'intimité de leur vie privée. Demander aux services spécialisés de la Défense Nationale de casser ce qui est incassable est illogique.

B. LSQ et interceptions de sécurité

55. Le projet d'article 11-1 de la loi no.91-646 du 10 juillet 1991[58] relative au secret des correspondances émises par la voie des télécommunications, loi autorisant les écoutes téléphoniques administratives (dites interceptions
de sécurité) dispose: « *Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies* »[59]. Un tel souci de défense de la sécurité rejoint ce qui est exprimé dans la Recommandation n° R (95) 13 du Conseil de l'Europe relative aux questions de procédure pénale en lien avec les technologies de l'information : « *Des mesures devraient être examinées afin de minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales, sans toutefois avoir des conséquences plus que strictement nécessaires sur son utilisation légale* ». Mais cette disposition de la loi de 1991 nous semble inefficace pour la raison suivante : la cryptographie de type OpenPGP est liée à l'essor d'Internet et au développement des logiciels libres comme Linux. Cette cryptographie est diffusée, par des milliers de scientifiques bénévoles et de simples internautes tout autour du monde. Elle est gratuite, facile à utiliser, et surtout conçue pour ne pas dépendre d'un fournisseur précis. Paradoxalement, elle a été élaborée dès l'origine de manière à permettre aux dissidents des pays totalitaires d'échapper à la surveillance de leur Etat. La sécurité d'un message chiffré avec OpenPGP ne dépend pas d'un vendeur ou d'un

[58] JO 13 juillet 1991, p. 9167 s.

[59] Le texte actuel édicte en son article 3: « Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des télécommunications ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du

fournisseur de prestation de cryptologie, mais seulement de l'expéditeur qui a chiffré le message et du destinataire qui le déchiffrera. Pour des raisons de sécurité évidente, dans OpenPGP aucun fournisseur de cryptologie ne possède une copie de la convention secrète utilisée. Il est donc impossible techniquement de demander les conventions qui permettraient un déchiffrement éventuel. Malgré cela, le projet d'article 434-15-2 du Code pénal prévoit trois ans d'emprisonnement et 45000 euros d'amende pour le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités.

C. LSQ et surveillance des communications, échanges des données et messages électroniques

56. Il est évident que, notamment depuis les attentats du 11 septembre, les Etats se dotent de pouvoirs de plus en plus étendus en matière de surveillance des communications et des échanges des données et des messages électroniques. Une liste établie récemment par le G8 démontre que toutes les communications électroniques sont surveillées et enregistrées, ou vont l'être très bientôt. Ceci concerne les téléphones portables, les téléphones fixes, et Internet : numéros de téléphone (de connexion), lieus d'appel, données de connexion SMS, GPRS, UMTS, WAP, mots de passe, mails, web, usenet, chat, irc, ftp, adresse IP etc... Pour ce qui concerne Internet, nous citons les éléments les plus intéressants[60] :

- Système d'accès au réseau (SAR) : Journaux d'accès particuliers aux serveurs d'authentification et d'autorisation comme TACAS+ ou RADIUS (Remote Authentification Dial-in User Service) utilisés pour contrôler l'accès aux routeurs IP ou aux serveurs d'accès au réseau, date et heure de connexion du client au serveur, ID utilisateur, adresse IP assignée, adresse IP du SAR, nombre d'octets (bytes) transmis et reçus, identification de la ligne appelante (ILA).

---

maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées ».

-Serveur de courriel (email) : Journal SMTP (protocole de transfert de courrier simple), date et heure de connexion du client au serveur, adresse IP de l'ordinateur d'envoi, message-ID (msgid), expéditeur (login@domain), destinataire (login@domain), indicateur de situation, journal du POP (Post Office Protocol) ou du IMAP (Protocole d'accès message Internet), date et heure de connexion du client au serveur, adresse IP du client connecté au serveur, ID utilisateur et enfin, dans certains cas, renseignements sur le courriel récupéré.
-Serveurs de téléchargement en amont et en aval (down/upload) : Journal FTP (protocole de transfert de fichier), date et heure de connexion du client au serveur, adresse IP de la source, ID utilisateur, chemin et nom de fichier des données téléchargées vers l'amont ou l'aval.
- Serveurs web (WWW): Journal HTTP (protocole de transfert hypertexte), date et heure de connexion du client au serveur, adresse IP de la source, transaction (c'est-à-dire commande GET), chemin de la transaction (pour récupérer la page html ou l'image), dernière page visitée, codes de réponse.
- Réseau USENET : Journal NNTP (Network News Transfer Protocol), date et heure de connexion du client au serveur, ID du processus (nnrpd[NNN...N]), nom d'hôte (nom du serveur de nom de domaine (DNS) de l'adresse dynamique IP assignée), activité de base du client (sans contenu), message-ID du message livré.
- Service de bavardage internet (chat rooms) : Journal IRC, date et heure de connexion du client au serveur,durée de la séance, surnom utilisé pendant la connexion IRC, nom d'hôte ou adresse IP, ou les deux.

57. Grâce à toutes ces informations, les autorités étatiques peuvent identifier les personnes et contrôler les contenus. Par conséquent, comment s’attendre à une libéralisation totale de la cryptologie (qui ne pourrait que rendre les contrôles plus difficiles) telle qu’annoncée par le Premier ministre L. Jospin en 1999 ? Malgré un certain assouplissement du dispositif légal, cette liberté reste encore très surveillée.

[60] Source : http://news.zdnet.fr/story/0,,t118-s2111471,00.html.

CHAPITRE 2

LE REGIME LEGAL DE LA CRYPTOLOGIE : UNE LIBERTE ENCORE SURVEILLEE

58. L'Etat français souhaite conserver un quasi-monopole pour l'usage de certaines technologies cryptologiques de haut niveau, nécessaires pour assurer la sécurité de ses communications gouvernementales[61]. Ce contrôle concerne également les moyens cryptologiques employés par les personnes privées : ces moyens ne doivent pas empêcher les autorités administratives et judiciaires d'effectuer les interceptions que la loi du 10 juillet 1991 autorise[62]. Cette volonté était clairement affirmée dans l'art. 28 *I*, alinéa 2, de la loi n° 90-1170 du 29 décembre 1990 (rédaction initiale) : « *Pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, la fourniture, l'exploitation ou l'utilisation de moyens ou de prestations de cryptologie sont soumises : a) à déclaration préalable lorsque ce moyen ou cette prestation ne peut avoir d'autre objet que d'authentifier une communication ou d'assurer l'intégralité du message transmis ; b) à autorisation préalable du Premier ministre dans les autres cas.* ». Justifié par la question de sécurité[63], le dispositif légal de 1990 était très contraignant alors que le recours à la cryptologie peut constituer aussi un élément de sécurité des échanges et, à ce titre, est aussi légitime. On observe également qu'il peut être un moyen de préservation de l'intimité de la vie privée[64] :

---

[61] Notamment le cryptage militaire et diplomatique.

[62] Dans ce sens : Warusfel B., Les conditions juridiques de la sécurité sur l'Internet et le régime juridique de la cryptologie en France, *in* Internet saisi par le Droit, éd. des Parques, 1997.

[63] Sur le plan Communautaire, cette restriction procède de l'art 223 du Traité de Rome qui autorise exceptionnellement les Etats membres à s'opposer au principe de libre circulation des marchandises et « *prendre qu'ils estiment nécessaires à la protection des intérêts de leur sécurité et qui se rapportent à la production et au commerce d'armes, de munitions et de matériels de guerre* ». Au plan mondial, une recommandation du 27 mars 1997 du Conseil de l'OCDE précise que la politique de cryptographie « (…) *ne saurait affecter les droits souverains des Gouvernements nationaux* (…) ».

[64] V. *infra*, deuxième partie.

comment la France, patrie des Droits de l'homme, présentait la particularité de disposer d'une des réglementations les plus restrictives du monde quant au droit de ses citoyens à protéger leurs secrets ? Un certain assouplissement de la réglementation s'est fait avec l'art.17 de la loi n° 96-659 du 26 juillet 1996, JO 27juillet, qui vient modifier l'art.28 *I* de la loi de 1990 : « *Pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, tout en permettant la protection des informations et le développement des communications et transactions sécurisées.* ». Cette deuxième partie de la phrase fait preuve de l'évolution des mentalités. Désormais, la cryptologie est libre dans certaines hypothèses, mais nous allons observer qu'en réalité, cette liberté reste encore très surveillée.

Section préliminaire : les deux hypothèses où la cryptologie est « libre »

59. C'est l'utilisation (usage) d'un moyen ou de prestation de cryptologie qui peut être « libre », dans deux cas : Lorsque le moyen n'assure pas des fonctions de confidentialité et lorsque cette confidentialité est assurée par des conventions secrètes gérées par un organisme agréé (« tiers de confiance »). Cela résulte de la loi de 1990 et de deux décrets de 1998 et 1999.

60. La loi de 1990 dispose dans son art.28 *I*, alinéa 2, 1*o, a* que l'utilisation d'un moyen ou d'une prestation de cryptologie est libre, « *si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis* » ou si « *le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par un organisme agréés*[65] *dans les conditions définies au II* ». Dans le premier cas, un simple internaute a le droit d'authentifier, par exemple, en apposant sa signature numérique (qui prouve que c'est bien lui qui envoie le message), par un tel

[65] Il s'agit des « tiers de confiance », V. *infra*, §2.

moyen cryptologique. Le même logiciel de cryptage peut être librement utilisé pour garantir que le message envoyé n'a pas été modifié par un tiers avant d'arriver à sa destination finale. Le problème en pratique est que le plus souvent ces logiciels de cryptage permettent aussi d'assurer des fonctions de confidentialité. De nombreux sont distribués gratuitement sur Internet. Dans le deuxième cas, on a le droit de crypter le message lui-même, si on utilise une clé qui nous est fournie par un organisme agrée (tiers de confiance), qui détient donc cette clé de déchiffrement et doit à tout moment la remettre aux autorités étatiques si une telle demande est faite…

61. Le décret du 24 février 1998[66] « *définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et les prestations de cryptologie* » complète le dispositif légal dans son article 1er:

« *Est libre l'utilisation des moyens ou des prestations de cryptologie:*

a) qui ne permettent pas d'assurer des fonctions de confidentialité, notamment:

- les moyens ou prestations conçus pour protéger des mots de passe, des codes d'identification personnels ou des données d'authentification similaires, utilisés pour contrôler l'accès à des données, à des ressources, à des services ou à des locaux, sous la seule réserve qu'ils ne permettent de chiffrer que les fichiers de mots de passe ou de codes d'identification et les informations nécessaires au contrôle d'accès:

- les moyens ou prestations conçus pour élaborer ou protéger une procédure de signature, une valeur de contrôle cryptographique, un code d'authentification de message ou une information similaire, pour vérifier la source des données, prouver la remise des données au destinataire, ou bien détecter les altérations ou modifications subreptices portant atteinte à l'intégrité des données, sous la seule réserve qu'ils ne permettent de chiffrer que les informations nécessaires à l'authentification ou au contrôle d'intégrité des données concernées;

b) ou qui assurent des fonctions de confidentialité et n'utilisent que des conventions secrètes gérées selon les procédures et par un organisme agréés dans les conditions définies au II de l'article 28 de la loi du 29 décembre 1990 susvisée».

La première hypothèse suppose une stricte fonction d'authentification et / ou de préservation de l'intégrité des messages mais sans que ceux-ci soient rendus opaques

[66] D. n° 98-101, 24 févr. 1998, JO 25 févr., p. 2911.

(on ne chiffre pas le contenu, qui reste par conséquent accessible à la lecture sans avoir à décrypter). La signature électronique[67] est concernée par cette méthode.
La seconde hypothèse correspond à un cas où la confidentialité des échanges est assurée mais avec intervention d'un tiers, lui-même soumis à des nombreuses obligations.

62. Le décret du 17 mars 1999[68] « *définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable* » donne une liste concrète des moyens ou prestations « libres ». On trouve, à titre d'exemple, « *les moyens ou prestations conçus pour élaborer ou protéger une procédure de signature, une valeur de contrôle cryptographique, un code d'authentification de message ou une information similaire, pour vérifier la source des données, prouver la remise des données au destinataire, ou bien détecter les altérations ou modifications subreptices portant atteinte à l'intégrité des données, sous réserve qu'ils ne permettent de chiffrer que les informations nécessaires à l'authentification ou au contrôle d'intégrité des données concernées* », ou bien « *les moyens matériels ou logiciels spécialement conçus pour assurer la protection des logiciels contre la copie ou l'utilisation illicite, dont les fonctions de déchiffrement ne sont pas accessibles à l'utilisateur* ». Cependant, pour le premier cas, la libéralisation n'est pas totale : la fourniture est soumise à autorisation préalable[69]. Des degrés dans la « libération » subsistent alors. Pour tous les autres cas, un contrôle étroit de la part de l'Etat se présente plutôt comme le principe ; le rôle de la DCSSI, seul organisme pouvant recevoir dépôt des conventions secrètes, s'avère déterminant. Nous analyserons ces questions dans deux paragraphes.

Section 1. Un contrôle étroit de la cryptologie

[67] V. *infra*, deuxième partie §103.

[68] D. n° 99-200, 17 mars 1999, JO 19 mars, p. 4051.

[69] 11^{e} point du décret.

63. Hormis les deux hypothèses où la cryptologie est « libre », dans tous les autres cas[70], l'utilisation d'un moyen ou d'une prestation de cryptologie est soumise soit à autorisation, soit à déclaration préalable. La fourniture, l'importation de pays n'appartenant pas à la Communauté européenne et l'exportation sont en principe soumises à déclaration auprès du Premier ministre, sauf lorsqu'ils assurent des fonctions de confidentialité, où l'autorisation préalable est requise. Dans les deux hypothèses, le texte présente un caractère policier : en cas de non-respect des dispositions, des sanctions pénales peuvent être infligées.

§1. Le recours à la cryptologie soumis à autorisation

64. Les cas dans lesquels l'autorisation du Premier ministre est requise se définissent négativement. Ce sont tous les cas qui ne se trouvent pas dans le (a) de l'art. 28 *I* , alinéa 2 1*o* de la loi du 29 déc.1990 telle qu'amendée. Cependant, la déclaration peut être substituée à l'autorisation pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation n'exigent pas l'autorisation préalable.

A. Le régime de l'autorisation

65. L'autorisation doit être demandée lorsque la cryptologie est recherchée pour une fonction de confidentialité.
L'article 12 du décret du 24 février 1998[71] est venu préciser qu' « *est soumise à autorisation préalable la fourniture*[72]*, l'utilisation, l'importation*[73] *en provenance d'un*

[70] Art. 28 *I* , alinéa 2 1*o* de la loi du 29 déc.1990 telle qu'amendée.

[71] D. n° 98-101, 24 févr. 1998, JO 25 févr., p. 2911.

[72] Une réponse ministérielle (Rep. min. n° 154458, JOANQ, 5 oct. 1998, p. 5451) précise ce qu'il fallait entendre par fournisseur et fourniture: « *En cohérence avec le dictionnaire juridique, ces deux termes ont la signification suivante : fournisseur : celui qui procure un moyen ou un service à celui qui le*

Etat n'appartenant pas à la Communauté européenne ou n'étant pas partie à l'accord instituant l'Espace économique européen, ou l'exportation[74] *de tous moyens ou prestations de cryptologie autres que ceux mentionnés aux articles 1er, 2, 3 et 4* ». Le même décret indique les conditions auxquelles est soumise la demande d'autorisation. Ainsi, aux termes de ses articles 13 et 14, « *Le dossier de demande d'autorisation est adressé par envoi recommandé avec demande d'avis de réception ou déposé contre accusé de dépôt au service central de la sécurité des systèmes d'information* [SCSSI, désormais appelé DCSSI]. *Ce dernier en délivre récépissé revêtu du numéro d'enregistrement du dossier. La forme et le contenu du dossier de demande d'autorisation sont définis par un arrêté du Premier ministre, pris après avis du ministre de la Défense, du ministre de l'Intérieur et du ministre chargé des Télécommunications. Ce dossier comporte une partie technique et une partie administrative*[75] ». Concernant le délai de réponse, « *Si le dossier est complet, le Premier ministre notifie sa décision, par lettre recommandée avec demande d'avis de réception, dans un délai de quatre mois à compter de la délivrance de l'avis de réception ou de l'accusé de dépôt de la demande. Un défaut de notification dans ce délai vaut autorisation. Le dossier est réputé complet si, dans le délai d'un mois suivant la réception de la demande, le service central de la sécurité des systèmes d'information n'a pas invité, par lettre recommandée avec demande d'avis de réception, le demandeur à fournir des pièces complémentaires. Dans ce dernier cas, le*

---

distribue ou l'utilise dans le contrat de fourniture ; fourniture : contrat par lequel une personne, appelée fournisseur, s'engage à approvisionner pendant un certain temps de manière ponctuelle, périodique ou continue, en moyens ou en services, une autre personne. Par extension, l'objet même de ce contrat. Par ailleurs, concernant la notion d'intermédiaire, la définition du régime de déclaration, y compris simplifiée, n'a pas introduit cette notion, au contraire du régime d'autorisation. En effet, le régime d'autorisation, réservé aux emplois de la cryptologie les plus susceptibles de gêner le travail des services de l'Etat en charge de la sécurité du pays et du maintien de l'ordre, entraîne plus de contraintes pour les fournisseurs que le régime de déclaration. C'est pour cette raison qu'il a été jugé opportun d'introduire dans le régime d'autorisation la notion d'intermédiaire. Grâce à cette notion, une même demande d'autorisation, déposée par un fournisseur (typiquement le fabricant du produit), peut couvrir également les autres fournisseurs dont les noms sont précisés avec la demande d'autorisation (typiquement les distributeurs du produit). Ces autres fournisseurs sont alors qualifiés d'intermédiaires. La simplicité du régime déclaratif ne justifiait pas cet accommodement retenu pour le régime d'autorisation ».

[73] L'importation ne fait l'objet d'un visa spécial que si elle est en provenance d'un pays n'appartenant pas à la Communauté européenne. En fait, si la disposition a été conçue pour éviter toute discrimination entre produits / services communautaires et français, il ne faut sans doute pas lui attacher trop d'importance, dès lors que le texte vise juste auparavant la fourniture, terme bien vague qui peut englober l'hypothèse d'importation, qui ne serait qu'un préalable à la fourniture.

[74] Cela vise tout ce qui relève d'une « mise à disposition » à l'étranger ; celle-ci concerne également les transferts *online*.

[75] Art.13.

délai fixé à l'alinéa précédent part de la réception des pièces complétant le dossier[76] ». Le rôle de la DCSSI (V. *infra*) est donc décisif sur l'acceptation ou non du dossier.

66. Un arrêté du 17 mars 1999[77] définit la forme et le contenu du dossier concernant les demandes d'autorisation requises par les textes. Le dossier comporte une partie administrative et une partie technique qui doit décrire le moyen appelé à être utilisé (référence du produit, fabriquant, numéro de version, description générale du produit, description des services de cryptologie fournis-noms des algorithmes[78] utilisés...). Le dossier peut être complété par une société aussi bien que par un particulier.

B. De l'autorisation à la déclaration

67. Qu'il s'agisse d'utilisation, de fourniture, d'importation ou d'exportation, la loi prévoit un passage possible de la formule lourde de l'autorisation à la formule légère de la déclaration, lorsque l'autorisation n'apparaît pas indispensable. L'article 28 2e dans son point (b) de la loi du 29 décembre 1990 telle qu'amendée dispose que la fourniture, l'importation de pays n'appartenant pas à la Communauté européenne et l'exportation tant d'un moyen que d'une prestation de cryptologie, sont soumises à la déclaration auprès du Premier ministre dans les cas où elles n'assurent pas des fonctions de confidentialité. Un décret fixe les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations[79]. L'autorisation préalable n'est pas exigée pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation n'exigent pas un suivi particulier. Le décret n° 98-101 du 24 février 1998 instaure le régime de déclaration dans son art.3 : « *Est soumise à déclaration préalable la fourniture, l'importation en provenance d'un Etat n'appartenant pas à la Communauté européenne ou n'étant pas*

[76] Art.14.

[77] Arr. 17 mars 1999, JO 19 mars, p. 4052 ; abroge l'arrêté antérieur du 13 mars 1998 (Arr. 13 mars 1998, JO 15 mars, p. 3886).

[78] Un algorithme est un processus de calcul qui permet d'arriver à un résultat final déterminé.

partie à l'accord instituant l'Espace économique européen, ou l'exportation d'un moyen ou d'une prestation de cryptologie n'assurant pas des fonctions de confidentialité ». En outre, un autre décret n°99-199 du 17 mars 1999[80] fait sortir du régime de l'autorisation, pour les soumettre à déclaration préalable, certains matériels, logiciels ou équipements, qui, bien qu'assurant une fonction de confidentialité, ont été jugés pouvoir échapper à la politique de contrôle; ainsi en est-il, à titre d'exemple, des matériels ou logiciels offrant un service de confidentialité mis en oeuvre par un algorithme dont la clé est d'une longueur supérieure à 40 bits et inférieure ou égale à 128 bits[81].

C. Formules allégées

68. Dans le souci (!) de ne pas faire peser sur les acteurs des réseaux des obligations trop lourdes, le législateur a mis en place un régime simplifié de déclaration ou d'autorisation[82]. Certains moyens destinés aux transactions et formalités réalisées par voie électronique bénéficient de ce régime simplifié sous réserve que le déclarant certifie que l'impossibilité d'assurer des fonctions de confidentialité ne résulte pas d'un simple dispositif de verrouillage. Au titre du régime simplifié, la déclaration préalable de fourniture, d'importation en provenance d'un Etat n'appartenant pas à la Communauté européenne ou n'étant pas partie à l'accord instituant l'Espace économique européen, ou d'exportation d'un moyen ou d'une prestation de cryptologie, s'effectue par l'envoi en recommandé avec demande d'avis de réception ou le dépôt contre accusé de dépôt au service central de la sécurité des systèmes d'information, de la seule partie administrative du dossier prévu à l'article 5 du décret[83].

---

[79] Art. 28 I 3° de la loi du 29 décembre 1990.

[80] D. n°99-199 du 17 mars 1999, JO 19 mars, p. 4050.

[81] On peut citer que jusqu'à présent aucun site de vente en ligne n'offre une sécurisation supérieure à 128 bits. En outre, le seul navigateur Internet qui supporte une sécurisation supérieure est Mozilla, logiciel sous licence GPL.

[82] D. 24 février 1998, art. 38 3° (a).

[83] Art.10, D. n°98-101, 24 févr. 1998, J0 25 févr., p. 2911.

Si le moyen ou la prestation de cryptologie déclaré au titre du régime simplifié ne relève pas de ce régime, le service central de la sécurité des systèmes d'information le notifie au déclarant et l'invite, par lettre recommandée avec demande d'avis de réception, à se conformer aux dispositions du chapitre 1er du présent titre ou à celle du titre III, selon le cas. Dans le cas où le déclarant est un fournisseur, celui-ci est tenu, dès la notification du service central de la sécurité des systèmes d'information, de prévenir tous les utilisateurs auxquels il a fourni le moyen ou la prestation de cryptologie concerné de l'irrégularité de leur situation[84].

D. La dispense de toute formalité préalable

69. Enfin, une dispense de toute formalité préalable peut exister pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation sont telles que ces opérations ne sont pas susceptibles de porter atteinte aux intérêts mentionnés au deuxième alinéa de l'article 28 *I* de la loi du 29 décembre 1990. Une dispense partielle a ainsi été prévue par le décret du 24 février 1998[85] dans un cas particulier : développement, validation, démonstration d'un moyen ou d'une prestation de cryptologie :

« *Est dispensée des formalités prévues aux articles 13 et 14 l'utilisation par un fournisseur, à des fins exclusives de développement, de validation ou de démonstration, d'un moyen ou d'une prestation de cryptologie, sous réserve que celui-ci en ait informé par écrit, au moins deux semaines à l'avance, le service central de la sécurité des systèmes d'information. Si, à l'expiration de ce délai, le Premier ministre n'a pas soumis cette utilisation à des conditions particulières ou aux dispositions des articles 13 et 14, le fournisseur peut procéder librement aux opérations envisagées* ».

[84] Art.11 du même décret.

[85] D. n° 98-101, 24 févr. 1998.

70. Le droit positif de la cryptologie se veut assez complexe et lourd pour les acteurs des réseaux. En outre, ceux-ci sont sanctionnés pénalement en cas de non-respect des dispositions mentionnées ci-dessus.

§2. Les sanctions

A. Peines principales

71. La fourniture, l'importation ou l'exportation de moyens ou prestations de cryptologie sans autorisation, quand bien sûr celle-ci est requise, est sanctionnée pénalement : « *Sans préjudice de l'application du Code des douanes, le fait de fournir, d'importer de pays n'appartenant pas à la Communauté européenne ou d'exporter un moyen ou une prestation de cryptologie sans avoir obtenu l'autorisation préalable mentionnée au I ou en dehors des conditions de l'autorisation délivrée est puni de six mois d'emprisonnement et de 30000 euros d'amende*[86] ». La peine est aggravée si ces faits ont été commis « en vue de faciliter la préparation ou la commission d'un crime ou d'un délit ». La fin spécialement criminelle de la pratique conduit à une aggravation des peines. L'Art. 28 *III* (a), alinéa 3 de la loi du 29 décembre 1990 telle qu'amendée dispose : « *Le fait de fournir, d'importer de pays n'appartenant pas à la Communauté européenne, d'exporter ou d'utiliser un moyen ou une prestation de cryptologie en vue de faciliter la préparation ou la commission d'un crime ou d'un délit est puni de trois ans d'emprisonnement et de 75000 euros d'amende* ». La tentative est punie des mêmes peines.

72. L'article 28 *IV* de la loi de 1990, dispose aussi : « *Outre les officiers et agents de police judiciaire et les agents des douanes dans leur domaine de compétence, les agents habilités à cet effet par le Premier ministre et assermentés dans des conditions*

[86] Art. 28 III (a) *in limine* de la loi du 29 décembre 1990 telle qu'amendée.

fixées par le décret en Conseil d'Etat peuvent rechercher et constater par procès-verbal les infractions aux dispositions du présent article et des textes pris pour son application. Leurs procès-verbaux sont transmis dans les cinq jours au procureur de la République. Ils peuvent accéder aux locaux, terrains ou moyens de transport à usage professionnel, demander la communication de tous documents professionnels et en prendre copie, recueillir sur convocation ou sur place, les renseignements et justifications.

Ils peuvent procéder, dans ces mêmes lieux, à la saisie des matériels visés au paragraphe I sur autorisation judiciaire donnée par ordonnance du président du tribunal de grande instance dans le ressort duquel sont situés les matériels, ou d'un juge délégué par lui. La demande doit comporter tous les éléments d'information de nature à justifier la saisie. Celle-ci s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée. Les matériels saisis sont immédiatement inventoriés. L'inventaire est annexé au procès-verbal dressé sur les lieux. Les originaux du procès-verbal et de l'inventaire sont transmis au juge qui a ordonné la saisie. Est puni d'un emprisonnement de six mois et d'une amende de 30000 euros le fait de refuser de fournir les informations ou documents ou de faire obstacle au déroulement des enquêtes mentionnées au présent paragraphe ».

B. Peines complémentaires et responsabilité des personnes morales

73. Une série de peines complémentaires est également prévue, dont la confiscation de la chose qui a servi ou était destinée à commettre l'infraction[87] et l'exclusion des marchés publics[88]. Les personnes morales peuvent être pénalement responsables de ces faits[89], avec une précision : l'interdiction mentionnée à l'article L. 131-39 NCP (interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales)

[87] NCP, art. L. 131-21 et D. 98-101 du 24 févr. 1998, art. 29, V.

[88] NCP, art. L. 131-34.

[89] L. 1990, précité, art. 28 A *I* c et D. précité, art. 29, VI.

porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

C. Les sanctions vis-à-vis des tiers agréés

74. Le tiers de confiance est sous contrôle de la DCSSI. L'article 15 du décret n° 98-102 du 24 février 1998 dispose que ledit service « *peut procéder au contrôle de l'application, par l'organisme agréé, des dispositions figurant dans le cahier des charges prévu à l'article 8* ». Le tiers de confiance s'expose à des sanctions pénales s'il manque au secret professionnel qui pèse sur lui. En outre, le défaut d'agrément ou l'exercice au-delà de l'agrément obtenu, constitue un délit d'exercice illégal de l'activité de tiers de confiance : « *Le fait de gérer, pour le compte d'autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité sans avoir obtenu l'agrément mentionné au II ou en dehors des conditions de cet agrément est puni de deux ans d'emprisonnement et de 45000 euros d'amende* »[90]. La tentative est punie des mêmes peines[91]. Des peines complémentaires existent aussi et la responsabilité des personnes morales peut être engagée. Enfin, le tiers de confiance met aussi en jeu sa responsabilité civile chaque fois que, de par sa faute, la confidentialité qu'il a en charge n'est pas assurée. On applique le droit commun de la responsabilité délictuelle (art. 1382 du code civil), qui peut être très coûteux pour le tiers de confiance, si sa faute est prouvée : N'importe qui peut l'attaquer en justice, il n'y a pas de clauses limitatives de responsabilité et le préjudice doit être réparé intégralement[92].

Section 2. Le statut des tiers agréés et le rôle de la DCSSI

[90] Art. 28 *III* a, alinéa 2 de la loi de 1990.
[91] Art. 28 *III* a, de la même loi.

[92] En revanche, il faut démontrer la faute du tiers agréé, le préjudice causé et le lien de causalité entre faute et préjudice.

75. Toute une part du régime de la cryptologie repose, on l'a vu, sur le recours à des tiers agréés, tiers « de confiance » dans l'esprit du législateur[93]. Il s'agit de l'innovation principale de la loi de 1996 ; la France est le premier pays au monde à mettre en place ce mécanisme dont le caractère obligatoire est encore écarté dans la plupart des pays. Cependant, pour les besoins du commerce électronique et pour gagner la confiance des clients, le recours aux tiers de confiance est très fréquent. Ces derniers doivent, selon la législation française, présenter certaines qualités, qui ne sont pas définies par la loi de 1990 mais par le décret de 1998 : « *Un décret en Conseil d'Etat fixe les conditions dans lesquelles ces organismes sont agréés ainsi que les garanties auxquelles est subordonné l'agrément ; il précise les procédures et les dispositions techniques permettant la mise en oeuvre des obligations indiquées ci-dessus* [94]». L'art. 4 du décret de 1998[95] dispose que « *pour être agréé, l'organisme doit compter, parmi ses personnels, un nombre suffisant de personnes habilitées pour être en mesure de satisfaire aux obligations du décret du 12 mai 1981*[96] ». Pour le reste, il s'agit largement d'appréciation d'opportunité et il paraît légitime de s'attacher au sérieux, à l'honorabilité et à la compétence des postulants. Cette appréciation partiellement subjective appartient aux organismes agréés pouvant recevoir dépôt des conventions secrètes.

76. L'arrêté du 13 mars 1998[97] « fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes » utilise, curieusement, le pluriel alors que ces organismes se ramènent à un seul: le service central de la sécurité des systèmes d'information (SCSSI), actuellement appelé direction centrale de la sécurité des systèmes d'information (DCSSI). La DCSSI est donc le seul organisme pouvant recevoir dépôt des conventions secrètes et le dossier de demande doit lui être adressé. Après dépôt du dossier, la DCSSI vérifie si le cahier des charges est respecté et si c'est le cas, l'agrément est délivré par décision du Premier ministre.

---

[93] On les appelle aussi Certification Authorities ou Trusted Third Party (TTP).

[94] Art. 28 *II in fine* de la loi de 1990.

[95] D. n° 98-102, 24 févr. 1998, JO 25 févr., p.2915.

[96] D. n° 81-514 du 12 mai 1981, relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'Etat.

[97] JO 15 mars 1998, p.3886.

§1. La DCSSI et la procédure d'agrément

A. Le dépôt du dossier

77. Le déclarant doit adresser son dossier par lettre recommandée avec avis de réception ou le déposer contre accusé de dépôt à la DCSSI, au plus tard un mois avant l'action envisagée, pour le régime de déclaration, et quatre mois avant pour le régime d'autorisation. Le délai ne court qu'à compter de la réception d'un dossier complet, soit à compter de la réception des pièces complémentaires qui pourraient être réclamées par la DCSSI. En cas de silence de la part de la DCSSI, le déclarant peut procéder librement aux opérations contenues dans le dossier. Enfin, si le moyen de cryptologie déclaré relève du régime de l'autorisation, alors que le déclarant n'a rempli que les formalités de déclaration, le DCSSI l'invite, dans un délai d'un mois, à se conformer aux formalités correspondantes.

78. On a déjà vu que c'est au Premier ministre (DCSSI) qu'appartient la décision de délivrer ou pas l'agrément. Mais ceci se fait après avis du ministre de la Défense, du ministre de l'Intérieur, du ministre chargé de l'Industrie et du ministre chargé des Télécommunications. Lorsque l'agrément est donné, le déclarant devient « tiers agréé » pour quatre ans, durée renouvelable[98]. Il peut être retiré avant terme si l'organisme ne remplit plus une de ses obligations[99].

[98] Art. 5, D. n°98-102, 24 févr. 1998.

[99] Art. 16 du décret de 1998 précité.

B. Le contenu du cahier des charges

79. L'art.8 du décret de 1998[100] fixe le contenu du cahier des charges :

« *1. L'énumération des moyens ou des prestations de cryptologie dont l'organisme agréé est autorisé à gérer les conventions secrètes;*

2. L'énumération des moyens ou des prestations de cryptologie que l'organisme agréé peut utiliser ou fournir;

3. Les conditions techniques ou administratives garantissant le respect des obligations imposées à l'organisme agréé;

4. Le nombre de personnes mentionnées à l'article 4, auxquelles peuvent être demandées la mise en oeuvre ou la remise des conventions secrètes, et les dispositions prises pour respecter le décret du 12 mai 1981 susvisé;

5. Les conditions dans lesquelles sont remises à un autre organisme agréé les conventions secrètes en cas de cessation d'activité ou à la demande de l'utilisateur;

6. Les dispositions techniques prises lors de la mise en service des conventions secrètes afin de permettre, pour chaque message ou communication protégé à l'aide de ces conventions, d'identifier l'organisme agréé le gérant ainsi que les utilisateurs concernés;

7. Les conditions techniques d'utilisation des conventions secrètes, des moyens ou des prestations et les mesures nécessaires pour assurer leur intégrité et leur sécurité;

8. Le format électronique standardisé dans lequel doivent être transcrites les conventions secrètes en cas de cessation d'activité ou de retrait d'agrément, conformément à l'article 17 du présent décret. ».

Le cahier des charges comporte également une annexe classifiée précisant les modalités pratiques de remise des conventions secrètes aux autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi du 29 décembre 1990 susvisée ou de leur mise en oeuvre à la demande de ces autorités. L'art.6 du décret prévoit quelles modifications dans la situation du tiers agréé ou son activité doivent être notifiées et l'art 7 indique la façon dont le renouvellement de l'agrément doit être sollicité. Enfin, l'art.9 prévoit encore comment le cahier des charges pouvait être modifié. Sous peine

[100] D. n° 98-102, 24 févr. 1998, précité.

de sanctions, ce cahier de charges doit être respecté, mais d'autres obligations incombent aussi aux tiers de confiance.

§2. Les obligations des tiers agréés

A. L'obligation de secret

80. Les tiers de confiance détiennent les clés privées et les conventions secrètes de leurs clients. Particuliers ou commerçants, ils doivent faire confiance à ces tiers qui « (..) *sont assujettis au secret professionnel dans l'exercice de leurs activités agréées*[101]». La même loi de 1990 dispose, un peu plus loin, qu' « *ils sont tenus de conserver les conventions secrètes qu'ils gèrent* [102]». Le décret de 1998 vient préciser cette obligation : « *L'organisme agréé prend les mesures nécessaires pour préserver la sécurité des conventions secrètes qu'il gère au profit de ses clients, afin d'empêcher qu'elles ne puissent être altérées, endommagées, détruites ou communiquées à des tiers non autorisés. Il prend toutes dispositions, notamment contractuelles, vis-à-vis de son personnel, de ses partenaires, clients et fournisseurs, afin que soit respectée en permanence la confidentialité des informations de toute nature dont il a connaissance relativement à l'utilisation de ces conventions secrètes et à leur remise aux autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi du 29 décembre 1990 susvisée ou à leur mise en oeuvre au profit de ces autorités. Il notifie ces mesures et dispositions à la DCSSI*[103]». L'art.13 du même décret dispose, enfin, que « *tout organisme agréé conserve les conventions secrètes qui lui sont confiées. Toutefois, à l'issue d'un délai de quatre ans à compter de la date de signature du contrat mentionné à l'article 10, l'organisme agréé peut, après accord de l'utilisateur, déposer lesdites conventions secrètes auprès d'un autre organisme agréé choisi sur une liste*

[101] Art. 28 *II*, al. 2, de la loi de 1990.

[102] Art. 28 *II*, al. 4 *in limine.*

[103] Art.12 du décret.

d'organismes agréés fixée par arrêté du Premier ministre». On peut remarquer que le texte n'est pas très précis : il oblige le tiers à prendre des dispositions « notamment contractuelles », mais rien n'est précisé sur le plan technique. En outre, sa rédaction nous laisse croire que la priorité est accordée à la possibilité de remise aux autorités publiques des conventions secrètes, et pas à la sauvegarde des intérêts des clients. L'esprit sécuritaire de tout le dispositif juridique s'affirme encore une fois.

B. Les obligations d'ordre technique

81. Pour éviter tout risque que le tiers abuse de ses prérogatives, et pour assurer la confidentialité attendue, ce dernier ne doit fournir que les moyens ou prestations qui ont été visés dans l'agrément[104] et qui apparaissent dans le cahier des charges[105]. Cette contrainte pourrait être incompatible avec les techniques utilisées, qui sont en évolution constante ; une souplesse des procédures est indispensable. C'est un problème de niveau pratique, mais ce n'est pas le seul en matière de cryptologie…on peut donner un autre exemple, très courant dans la vie du cybercommerce. Quand on passe une commande en ligne (achat sur Internet, *via* le site d'un commerçant), au moment où on insère nos coordonnées et notre no. de carte bancaire, une session sécurisée s'ouvre entre notre terminal (notre PC) et celui du commerçant (le serveur). La clé de chiffrement doit être immédiatement disponible, afin de pouvoir se diffuser rapidement par le tiers agréé concerné. Cette clé, le plus souvent est une clé de session, c'est-à-dire une clé générée de manière temporaire et associée à un couple (client-commerçant) correspondant. Le dépôt sera rendu difficile parce qu'il faudra que la clé soit déposée avant son utilisation. En plus, l'espace nécessaire pour conserver ces clés (stockage sur disque dur) pose problème, de même que les moyens pour les récupérer[106].

[104] Art. 28 *II*, al. 3 de la loi de 1990.

[105] Art.8, D. n° 98-102, précité.

[106] En ce sens, V. Bresse P., Beaure d'Augères et Thuillier S., Paiement numérique sur lnternet, Thomson Publishing, 1997, p. 178 et s. On peut trouver le même problème d'ordre technique pour les FAI, à propos de la durée de conservation des données (V. *supra*, §50).

C. La remise des conventions secrètes

82. Peut-être l'obligation fondamentale des tiers agréés, en harmonie avec le souci de sécurité publique qui anime tout le dispositif légal, est celle formulée à l'art. 28 *II*, al. 4 *in fine*: « *Dans le cadre de l'application de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ainsi que dans le cadre des enquêtes menées au titre des chapitres premier et II et du titre II du livre premier du Code de procédure pénale, ils doivent les remettre aux autorités judiciaires ou aux autorités habilitées, ou les mettre en oeuvre selon leur demande* ». Le tiers agréé doit maintenir un service permanent de mise en oeuvre ou de remise des conventions secrètes au profit des autorités[107], doit constituer et tenir à jour une liste de ses clients[108] et avoir un registre mentionnant les demandes émanant de l'autorité judiciaire quant à la remise des conventions secrètes. Ce registre doit notamment contenir la date et l'heure de la demande, les références de la commission rogatoire ou de la réquisition judiciaire, la durée de l'autorisation, les références des conventions secrètes délivrées ou mises en œuvre etc. L'accès à ce registre est limité aux autorités judiciaires dans les conditions prévues par le Code de procédure pénale. Un registre séparé, classifié au niveau secret défense, peut se constituer pour les demandes de mise en oeuvre ou de remise des conventions secrètes effectuées dans le cadre du titre II de la loi du 10 juillet 1991. Son accès est limité au Premier ministre, à la Commission nationale de contrôle des interceptions de sécurité ainsi qu'aux agents spécialement désignés par l'une ou l'autre de ces autorités[109]. Il ne contient que la date, l'heure de la demande, la durée de l'autorisation ainsi que la référence de l'ordre de communication des conventions secrètes.

83. Nous avons démontré que le droit français de la cryptologie est très soucieux de la sécurité publique et par conséquent il est étroitement contrôlé par l'Etat. Cependant,

[107] Art. 14, D. n° 98-102, 24 févr.1998.

[108] Art. 11, *in limine*, du décret de 1998 précité.

[109] Art. 11, du décret de 1998, précité.

cette conception sécuritaire de la cryptologie tend à s'assouplir ces dernières années. La doctrine parle d'un passage « de la science du secret à la science de la confiance ». Comment cette évolution se justifie-t-elle ? Certains associent cette évolution à l'essor du commerce en ligne et l'utilisation croissante d'Internet par les ménages. D'autres considèrent que le dispositif légal de 1990 n'était pas viable, car irréaliste. Nous partageons ce deuxième point de vue, et nous devons faire la même remarque à propos du dispositif légal actuel : il reste encore irréaliste. Citons quelques exemples. Si l'importation de certains moyens cryptologiques n'est pas libre, qui peut contrôler ce que l'on télécharge chez nous par le réseau ? Pourquoi passer par les tiers agréés, système onéreux et compliqué, alors que l'on peut échapper, dans certains cas, à la législation française, en installant notre serveur dans un autre pays ? Enfin, concernant les criminels, qui peut croire qu'ils vont se plier à la loi française ? Nous imaginons mal qu'un trafiquant de drogues hésiterait à crypter sa correspondance, à l'aide d'un moyen cryptologique non déclaré, parce qu'il encourt une peine de trois ans d'emprisonnement, alors que le trafic de stupéfiants est puni de la réclusion criminelle à perpétuité…

84. On doit par conséquent s'attendre à une évolution de la législation et à une libéralisation de la cryptologie. Plus qu'aujourd'hui, une telle libéralisation sera au service des citoyens et permettra la multiplication des communications à travers le réseau. Toute personne privée (particuliers, artistes, commerçants…) a le droit de protéger ses intérêts, que ce soit la vie privée, des intérêts financiers ou la simple navigation sur le Web sans danger. Nous allons étudier ces questions dans une deuxième partie.

DEUXIEME PARTIE

LA CRYPTOLOGIE AU SERVICE DES CITOYENS

85. La limitation de l'utilisation du chiffrement pour des raisons de sécurité publique doit être traitée avec précaution. Restreindre l'usage du chiffre peut en réalité résulter à empêcher les entreprises et les citoyens de se protéger des criminels, qui, en revanche, ne se plieront jamais à la réglementation en vigueur. Le constat est le suivant : la sécurité des transmissions électroniques ne peut être garantie que par une cryptologie forte. Par conséquent, les transactions en ligne ainsi que l'échange des données personnelles nécessitent la possibilité d'importer, d'exporter et d'utiliser librement des données cryptées. Et si certains Etats préfèrent une réglementation rigoureuse, en revanche les entreprises, les associations et les particuliers souhaitent une libéralisation complète pour permettre le développement du commerce électronique et garantir le respect de la vie privée. Sous la pression notamment des entreprises[110], les Etats ont assoupli ces dernières années leur législation.

86. On a vu qu'en France, cette libéralisation n'est pas totale[111] mais les autorités se montrent de plus en plus souples quant aux autorisations[112]. En pratique, nous pouvons profiter des nouvelles techniques du chiffre (et de l'irréalisme de la législation actuelle…) dans de nombreux cas. Cette nouvelle forme de protection doit par ailleurs bénéficier à tous, et nous démontrerons qu'effectivement tous les citoyens peuvent en profiter. La cryptologie se met donc désormais au service des citoyens : d'un côté, en leur permettant d'effectuer des transactions en ligne en sécurité (section 1), de l'autre côté, en protégeant leur vie privée (section 2).

---

[110] Dans un premier temps aux Etats-Unis, les entreprises exigeaient depuis le début des années 1990 l'assouplissement du contrôle des exportations des moyens cryptologiques.

[111] Malgré l'annonce du Premier ministre M. L. Jospin en 1999, de libéraliser totalement l'utilisation de la cryptologie (cf. *supra*, §28) et la législation plus libérale applicable dans les autres pays européens.

[112] Cf, §99 et 135.

CHAPITRE 1

L'ESSOR DES TRANSACTIONS EN LIGNE

87. Les transactions en ligne ne sont devenues populaires que depuis le début des années 1990. En France, l'assouplissement du dispositif légal de 1990 avec la loi de 1996 (cf. §58 et §75) a donné un nouvel élan en encourageant les commerçants à créer de sites permettant la vente de biens et services *on line*. Du point de vue du consommateur, le commerce électronique se base sur la confiance ; ce dernier doit être convaincu que les transactions en ligne ne comportent pas de risque pour lui. On est actuellement en présence d'une véritable mutation, d'un passage d'une science secrète à la science de la confiance, qui révolutionne le monde du commerce.

88. Si l'avenir du commerce électronique est subordonné à la sécurité des paiements, ces derniers dépendent des techniques cryptologiques et la législation en vigueur. Du point de vue technique, les algorithmes actuels permettent de crypter de manière virtuellement indéchiffrable le contenu d'une transaction[113]. Il appartient donc au législateur, tant au niveau national qu'au niveau communautaire et international, de les encadrer de manière efficace. Nous étudierons ces questions dans un premier paragraphe. Par ailleurs, les ventes et les achats sécurisés en ligne ne concernent pas seulement les commerçants et les consommateurs ; le droit d'auteur est aussi concerné par la technique du chiffre. L'auteur peut ainsi contrôler l'exploitation de son œuvre chaque fois qu'il la met *on line*, à la disposition du public. Les techniques du chiffre

[113] Les clés actuellement employées sont considérées comme incassables : 128 bits pour les clés symétriques et 1024 bits pour les clés asymétriques.

viennent donc au secours du monopole de l'auteur. Cette question sera traitée dans un deuxième paragraphe.

Section 1. Commerce électronique et sécurité des paiements en ligne

89. Le commerce électronique, de par sa nature, ne connaît pas de frontières. Son impact sera important sur le développement économique au niveau mondial. Les techniques de cryptage viennent assurer la sécurité des transactions. Le droit, de son côté, encadre les opérations et précise l'étendue et les limites quant à l'application de la cryptologie. Il ne faut pas cependant oublier que la « mondialisation » et le caractère international d'Internet oblige une collaboration étroite entre les Etats. Le rapprochement des législations nationales va d'ailleurs s'accélérer dans l'avenir grâce aux réseaux. Cette démarche a déjà commencé surtout au niveau communautaire. Les Etats membres de l'Union européenne doivent transposer les directives européennes relatives aux réseaux, qui sont nombreuses. Tel est par exemple le cas en France pour le projet de loi sur la société de l'information, qui doit transposer la Directive sur le commerce électronique. Nous analyserons successivement ces questions.

§1. La contribution des techniques cryptographiques

90. C'est grâce au progrès des techniques cryptographiques que le commerce électronique a du succès[114]. On ne pourrait imaginer une transaction non-sécurisée en ligne : elle entraînerait la méfiance des internautes qui refuseraient de payer les biens ou les services en ligne. Cependant, il faut préciser sur ce point que la cryptologie ne suffit pas en tant que telle pour assurer le succès de la transaction. Il appartient aussi à

[114] On estime a plus de 10 milliards de dollars les dépenses des internautes pour des achats en ligne pour 2000, chiffre qui augmente considérablement chaque année.

l'internaute de vérifier la crédibilité du site visité, qui doit donc éviter les sites des « cybermarchands » suspects[115]. Le défaut de livraison d'un produit ouvre le droit à une action en justice, régie par les règles de droit commun, aux quelles il faut ajouter celles applicables au droit du commerce international[116].

A. Exposé des principales méthodes cryptographiques

91. Nous avons vu que le chiffrement est l'opération de transformation d'une information claire en une information incompréhensible, chiffrée. Pour chiffrer, on utilise un algorithme symétrique, soit un algorithme asymétrique. Il s'agit d'une distinction fondamentale. Les algorithmes symétriques sont aussi appelés à clé privée : une seule clé est utilisée pour chiffrer et déchiffrer l'information. Cela nécessite donc que les deux interlocuteurs connaissent au préalable la même clé. En pratique, la difficulté et le risque se situent au moment du transfert de la clé de l'un à l'autre. Les deux interlocuteurs doivent se faire mutuellement confiance et choisir un mode de transfert de la clé sécurisé. Les plus répandus sont le DES, le triple DES et l'AES[117]. Les algorithmes asymétriques s'appellent aussi à clé publique : deux clés sont utilisées. Pour crypter un message, on utilise la clé publique que l'on a reçue du destinataire du message. Le destinataire utilisera ensuite sa clé privée (qui est associée à la clé publique qui a servi pour chiffrer le message) pour décoder le message. L'avantage de cette méthode consiste au fait que l'on peut envoyer la clé publique sans risque, étant donné que le décryptage du message se fait uniquement par la clé privée associée.

92. Le DES (Data Encryption Standard) est l'algorithme à clé privée le plus répandu. Créé par IBM en 1977, il a été jugé à l'époque si difficile à décrypter qu'il a été adopté

[115] Même en présence d'un site permettant un paiement sécurisé, outre la vérification du certificat qui doit être effectuée, on doit mesurer la sériosité du site. A titre d'exemple, certains sites situés en Asie (et pas seulement) facturent mais ne livrent pas les produits commandés.

[116] Cf. *infra*, §104 et s.

[117] L'AES (Advanced Encryption Standard) est l'algorithme le plus récent et le plus puissant des trois. Il permet le chiffrement avec des clés de 128 à 256 bits.

par le ministère de la défense américain. Actuellement on utilise le triple DES, qui est un DES appliqué trois fois (avec trois clés privées différentes). Cette dernière méthode est beaucoup plus difficile à déchiffrer si on tient compte des technologies actuelles. En fait, la seule méthode pour attaquer un document chiffré avec DES est celle dite de force brute : elle consiste à essayer la totalité des différentes clés, d'où la supériorité du triple DES[118].

93. Le premier algorithme asymétrique, le RSA[119], a été créé en 1978. Il s'agit d'une technique qui utilise deux grands nombres premiers, x et y, qui donnent P une fois multipliés l'un par l'autre. P constitue la clé publique, alors que x et y forment la clé privée. Le brevet du RSA appartient à la société américaine RSA data security, mais la licence de ce cryptage asymétrique est tombée dans le domaine public depuis novembre 2000. L'algorithme est très utilisé et de nombreux certificats l'utilisent. Ces derniers servent le commerce électronique, qui a techniquement progressé grâce au protocole SSL, qui sécurise les paiements.

B. SSL : le protocole standard sur Internet

94. Si la moitié environ des internautes n'ont jamais acheté en ligne, c'est parce qu'ils ont peur de la sécurité des paiements en ligne. Cependant le protocole SSL (Secure Socket Layer), utilisé par la quasi-totalité des sites, peut garantir une transmission des données très sécurisée. Le SSL a été inventé par Netscape et est devenu un standard sur Internet. Il est facile de vérifier sa présence : c'est le « *s* » ajouté au préfixe « http » en tête des adresses Internet. Dès lors que l'URL affichée dans la barre d'adresses de notre navigateur commence par « https:// », le SSL est activé et on se trouve face à une page

[118] Le nombre de combinaisons différentes pour une simple clé DES est de 72057595037927936. Le triple DES demande trois fois cette puissance de calcul pour casser le code.

[119] Du nom de ses créateurs, les Israéliens Rivest, Shammir et Adleman.

sécurisée[120]. La fonction du SSL est d'authentifier la page et d'assurer la confidentialité des informations transmises. La longueur de la clé utilisée est aussi importante.

95. Dans un premier temps, le SSL authentifie le serveur en face de l'internaute. Par exemple, si on veut effectuer un achat sur le site http://www.fnac.com, on doit être sûr que cette adresse est bien celle de la société qui s'appelle fnac. Cette opération est réalisée grâce à un certificat numérique, sans lequel le protocole SSL ne peut pas fonctionner. Le certificat vient donc garantir l'identité de l'ordinateur distant. Les certificats sont délivrés par des sociétés appelées autorités de certification (c'est les « tiers de confiance » V. §75 s.) qui vendent ces cartes d'identité numériques. Les certificats sont valables pour une durée fixe et attestent qu'un serveur appartient bien à la société correspondante.

96. Pour utiliser le protocole SSL il faut posséder un navigateur web compatible SSL. Les versions les plus récentes de toutes les marques de navigateurs[121] le supportent. Généralement on peut remarquer l'apparition d'un cadenas verrouillé sur l'interface graphique du navigateur qui indique que l'on est en présence d'une page sécurisée. En cliquant sur ce cadenas, on obtient les informations sur le certificat : site propriétaire du certificat et société, organisme qui a émis le certificat (le tiers de confiance), date d'émission et d'expiration du certificat, algorithme de la signature du certificat…On peut sauvegarder un certificat dans notre disque dur si on le souhaite, pour consultation ultérieure.

97. La deuxième fonction du SSL consiste à assurer la confidentialité des informations transmises. Ces informations, en provenance ou à destination du serveur du commerçant, sont cryptées et par conséquent très difficiles à être lues en ligne par un tiers. Des algorithmes de chiffrement sont utilisés à cette fin.

---

[120] « https » tient pour Hyper Text Transfer Protocol *Secure.*

[121] Ainsi, Internet Explorer, Netscape Navigator, Opera et le nouveau standard open source, Mozilla, supportent tous le SSL. En outre, Mozilla permet l'utilisation de clés dépassant les 128 bits dont l'utilisation n'est pas encore libre en France.

98. La force des algorithmes est déterminée par la longueur de la clé utilisée. Cette dernière fait l'objet d'une négociation lors de l'ouverture d'une session SSL, entre les machines du client et du vendeur. La négociation repose sur les capacités des logiciels employés des deux côtés : la clé utilisée est la plus forte supportée par le logiciel le moins performant en termes de chiffrement[122]. En pratique, on rencontre des clés de 40, 56 ou 128 bits. Peut-on faire confiance aux sites ne supportant pas une longueur de clé de 128 bits, seule considérée comme incassable ? Oui, parce qu'aucun pirate n'attaquera un flux de données SSL chiffré juste pour intercepter un numéro de carte bancaire. Il est plus facile d'attaquer directement le serveur du commerçant, dans lequel de milliers de numéros de cartes peuvent être stockées. Le rôle des firewalls (cf. §41) et du cryptage des bases de données devient par la suite primordial pour les commerçants.

99. Le commerce électronique rentre de plus en plus dans les mœurs du consommateur. Les autorités étatiques deviennent de leur côté plus souples et délivrent des autorisations plus facilement. Très récemment[123] la DCSSI a autorisé le bureau français de la Free Software Foundation Europe (FSF), d'utiliser, importer et exporter le OpenSSL (version 0.9.6d et suivantes), un programme destiné aux administrateurs système désirant protéger leurs sessions, lorsqu'ils effectuent des manipulations entre des machines distantes via l'internet, version open source. Mais les autorisations nationales ne suffisent pas pour le bon fonctionnement du commerce électronique, qui ne connaît pas de frontières. Le droit doit s'harmoniser au niveau international.

§2. La contribution du droit

[122] Ainsi, un serveur supportant un chiffrement de 128 bits communiquera à 56 si le navigateur web du client ne supporte que des clés de 56 bits. En France, les navigateurs ont été limités pendant longtemps à 56 bits par la loi. De l'autre côté, les commerçants n'ont pas tous acheté de nouveaux certificats de 128 bits.

[123] Le 15 juillet 2002.

100. Le droit, on l'a déjà vu, interdit ou autorise l'utilisation de telle ou telle méthode cryptologique. En France, le développement du commerce électronique a été accéléré depuis que l'utilisation des clés de 128 bits a été autorisée ; désormais, l'internaute français peut bénéficier de ce niveau de cryptage lors de sa connexion à un site commercial, où qu'il se situe, si ce dernier offre une tel niveau de sécurité. La technique existe ; il appartient au droit de ne pas l'interdire. L'internaute-consommateur peut faire confiance aux sites commerciaux qui proposent une connexion sécurisée lors de l'achat. Ces derniers peuvent aussi offrir des garanties supplémentaires, cette fois d'ordre juridique. Ils peuvent proposer par exemple des indemnités financières ou utiliser un label, délivré par une organisation professionnelle, qui recommande leur site. Promouvoir la cryptographie consiste donc à améliorer le niveau de vie des citoyens. Les normes juridiques évoluent de façon significative, grâce à la collaboration entre les Etats, même si on est encore loin de parler d'une harmonisation. Au sein de l'Union européenne les règles juridiques offrent une protection assez élevée aux consommateurs, alors qu'au niveau international le cadre juridique se montre insuffisant.

A. Au niveau communautaire

101. Les législations nationales des pays membres de l'Union européenne sont souvent contradictoires et le développement est freiné. La volonté de coordonner et harmoniser les législations nationales doit donc s'exprimer au niveau communautaire. Cela se fait notamment à travers les différentes directives[124] applicables aussi pour Internet. On pourrait citer la directive sur la vente à distance[125], celle sur la protection des données à caractère personnel[126], celle sur la publicité trompeuse[127], la directive relative à la

[124] Les Directives lient les Etats membres destinataires quant au résultat à atteindre, tout en leur laissant le choix des moyens et de la forme.

[125] Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance.

[126] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

responsabilité du fait des produits défectueux[128], celle relative aux crédits à la consommation[129], celle concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements[130] ou celle sur les clauses abusives[131]. Enfin, la directive « commerce électronique » du 8 juin 2000[132] mérite notre attention. Cette initiative communautaire vient apporter une certaine sécurité juridique, indispensable au commerce électronique. Nous avons traité la question des tiers agréés (§75 et s.) qui apportent la confiance nécessaire aux internautes. La directive servira de cadre légal grâce auquel le commerce électronique sera harmonisé au sein de l'Union.

102. La Directive sur le commerce électronique a pour objectif de « contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les Etats membres ». Le but de la directive est d'instaurer un niveau élevé d'intégration juridique afin d'établir un espace sans frontières intérieures pour les services de la société de l'information. Elle apporte donc la sécurité juridique indispensable au commerce électronique par trois séries de dispositions[133] : harmonisation du traitement et de la formation des contrats électroniques, mise à la charge des prestataires d'obligations d'informations protectrices du destinataire et une fixation du régime de responsabilité des intermédiaires dans l'exercice de leur activité technique. Cryptage et sécurité juridique se combinent donc pour instaurer un cybercommerce européen de qualité.

---

[127] Directive 97/55/CE du Parlement européen et du Conseil du 6 octobre 1997 modifiant la directive 84/450/CEE sur la publicité trompeuse afin d'y inclure la publicité comparative.

[128] Directive 1999/34/CE du Parlement européen et du Conseil du 10 mai 1999 modifiant la directive 85/374/CEE du Conseil relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux.

[129] Directive 87/102/CEE du Conseil du 22 décembre 1986, relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de crédit à la consommation.

[130] Directive 2000/46/CE du Parlement européen et du Conseil du 18 septembre 2000.

[131] Directive 93/13/CEE du Conseil du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs.

[132] Directive 2000/31 du Parlement européen et du Conseil du 8 juin 2000 sur le commerce électronique, JOCE 17 juillet 2000, no. L 178, p.1.

[133] La directive exclut de son champ d'application les questions traitées par les directives 95/46 (protection des personnes physiques à l'égard du traitement des données à caractère personnel) et 97/66 (protection de la vie privée dans le secteur des télécommunications). Pour ces questions V. *infra*, section 2.

103. En France, le projet de loi LSI (Loi sur la Société de l'Information[134], toujours attendue), approuvé en Conseil des ministres depuis juin 2001, transpose la Directive sur le commerce électronique. Les dispositions concernant le commerce électronique se trouvent sur le Titre III de la loi. Enfin, il faut noter que le droit français donne la même valeur à la signature électronique que la signature manuscrite depuis 2000 [135]: « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État.* » . Les règles de certification d'un dispositif sécurisé de création de signature électronique relèvent des normes européennes en cours d'élaboration et s'orientent vers les CC (normes ISO)[136]. En pratique, contrairement à la signature manuscrite où la personne s'identifie directement par un signe qui lui est propre, l'auteur de la signature numérique doit recourir à un tiers qui certifie son identité (tiers de confiance).

B. Au niveau international

104. Le cadre juridique international actuel est mal adapté aux transactions électroniques et à la protection du consommateur. D'un côté, on note une absence de règles de fond internationales. De l'autre côté, la loi qui peut s'appliquer à la

[134] LSQ, loi n°2001-1062 du 15 novembre 2001, J.O. du 16 novembre 2001.

[135] Art. 1316-4 du code civil (inséré par Loi n° 2000-230 du 13 mars 2000 art. 4 . J.O. du 14 mars 2000).

[136] Au niveau interne, l'arrêté du Premier ministre prévu a été supprimé par le décret 2002-535 du 18 avril 2002 (article 20-I).

transaction internationale est régie par les conventions de La Haye[137] et la convention de Rome[138]. On constate donc une absence de convention internationale spécifique aux transactions électroniques et à la protection du consommateur. Ceci laisse subsister un cadre conventionnel mal adapté au commerce électronique. Ces questions complexes relèvent du droit du commerce international et pourraient faire l'objet d'une étude distincte. Nous limiterons notre analyse aux points relatifs à la sécurité des transactions et à la protection du consommateur.

105. Nous avons constaté qu'au sein de l'Union européenne se met progressivement en place un cadre juridique offrant une protection élevée des consommateurs, applicable aux transactions électroniques. En revanche, les règles de fond internationales protégeant les consommateurs dans le cadre de transactions électroniques sont absentes. Face à cette lacune, l'OCDE a préparé une recommandation relative aux « lignes directrices régissant la protection du consommateur dans le cadre du commerce électronique » (1999)[139]. Les orientations retenues par la cette recommandation sont ambitieuses et se basent sur le principe que les consommateurs ne devraient pas bénéficier de moins de protection dans le commerce électronique que dans les autres formes de commerce[140].

Une autre recommandation de 1997, relative aux « lignes directrices régissant la politique de la cryptographie », favorise la confiance des internautes grâce à

[137] Convention de La Haye du 15 juin 1955 sur la loi applicable aux ventes à caractère international d'objets mobiliers corporels. Elle est ratifiée par 9 Etats : France, Belgique, Danemark, Finlande, Italie, Niger, Norvège, Suède et Suisse.

[138] Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles. Elle a été signée par la majorité des Etats membres de l'Union européenne et ratifiée par la France le 1er avril 1991.

[139] Les travaux de l'OCDE sont fondés sur le principe du consensus et les textes adoptés ne sont pas juridiquement contraignants. Cependant, les 29 pays Membres ont une obligation morale de mettre en œuvre ces recommandations. Les Etats non-membres sont aussi invités à les mettre en oeuvre.

[140] On peut citer les dispositions les plus importantes : Un niveau de protection équivalent pour les consommateurs qui effectuent des transactions électroniques à celui d'une vente à distance traditionnelle ; Une information claire des consommateurs, dans une langue qu'ils comprennent, sur l'identité de l'entreprise menant des activités de commerce électronique et sur les biens et services offerts ; Une information complète concernant l'offre ; Un consentement clair et transparent du consommateur ; Un délai de réflexion approprié offert aux consommateurs ; Une information sur le droit applicable au contrat et le tribunal compétent ; Une mise en place de mécanismes d'authentification ; Une mise en place de mécanismes de réclamation et d'autodiscipline ; Enfin, un développement de la coopération internationale. On s'aperçoit que certaines orientations sont très ambitieuses et la plupart des pays ne les ont pas mises en œuvre.

l'utilisation de la cryptographie et propose une harmonisation des législations nationales en la matière.

106. Concernant la loi applicable à la transaction électronique, le cadre conventionnel actuel est mal adapté. Les deux conventions qui s'appliquent à la transaction électronique sont la convention de la Haye et la convention de Rome. Cette dernière couvre les contrats de toute nature, qu'ils portent sur des biens ou sur des services. Lorsque les deux convention sont susceptibles de régir une relation contractuelle, c'est celle de la Haye (dont l'objet est plus spécifique) qui a vocation à être appliquée. Les deux conventions ont une vocation universelle : peu importe si les parties ont choisi la loi d'un Etat non contractant, elles seront malgré tout applicables dès lors que le tribunal saisi est celui d'un Etat contractant. Ainsi, le tribunal d'un Etat ayant ratifié les deux conventions, saisi d'un litige concernant une transaction électronique, appliquera la convention de la Haye si le litige concerne des produits commandés en ligne et celle de Rome si le litige porte sur un service, sous réserve d'un texte encore plus spécifique (notamment une règle de compétence posée par une directive ou un règlement communautaires dans le cadre intra-européen). Cependant, aucune de ces deux conventions ne paraît pleinement adaptée aux échanges électroniques.

107. La convention de la Haye, outre le fait qu'elle n'est ratifiée que par peu d'Etats retient, à défaut d'accord entre les parties, la loi du pays dans lequel le vendeur a sa résidence habituelle au moment où il reçoit la commande. Toutefois, il est prévu que la loi applicable sera celle de l'acheteur «(…) si c'est dans ce pays que la commande a été reçue soit par le vendeur, soit par son représentant, agent ou commis voyageur »[141]. Cette formulation paraît inapplicable à l'Internet[142]. En outre, la convention ne réserve au juge la possibilité d'écarter la loi applicable au contrat en vertu de ces principes que si son application est manifestement contraire aux règles d'ordre public. Ainsi, en

[141] Art. 3, al.2e *in fine* de la convention.

[142] Ainsi, le professeur HUET souligne : « On mesure la difficulté que soulève à cet égard le commerce électronique, dans un processus dématérialisé où sont abolies les distances, on peut soutenir tout aussi bien que la commande est reçue dans l'établissement du vendeur, à qui elle est adressée et qu'elle est reçue au domicile de l'acheteur, d'où elle est exprimée. Néanmoins, il semble que la première interprétation soit plus respectueuse du texte et qu'il faille donc faire jouer la loi du pays du vendeur ».

pratique la convention de la Haye devrait conduire à appliquer le plus souvent la loi du vendeur, sauf si les parties en conviennent autrement, ce qui est rare en matière de vente par un site Internet : on ne négocie pas le contrat ni le prix, on insère juste nos coordonnées et le numéro de notre carte bancaire.

108. La convention de Rome, dont le champ d'application est plus large, conduit aux mêmes conclusions. La convention retient tout d'abord le principe d'autonomie de la volonté des parties (il appartient aux parties de choisir la loi applicable)[143]. En l'absence de choix de la loi applicable par les parties, le contrat sera régi par la loi du pays avec lequel le contrat présente les liens les plus étroits[144]. Un contrat est présumé présenter les liens les plus étroits avec le pays où la partie qui doit fournir la prestation caractéristique (c'est à dire l'obligation pour laquelle un paiement est dû), a, au moment de la conclusion du contrat, sa résidence habituelle ou son principal établissement[145]. En pratique le vendeur ou le prestataire de service sont favorisés par la convention au détriment du consommateur, dès lors que dans le silence du contrat c'est en principe le lieu de résidence de celui qui effectue la prestation qui détermine la loi applicable. La convention de Rome contient certes dans son article 5 des stipulations protectrices des consommateurs, mais leur rédaction les rend difficilement applicables à l'Internet. La convention prévoit dans son article 5.-2. que le choix par les parties de la loi applicable « ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle », mais dans certaines circonstances seulement, malheureusement peu compatibles avec le fonctionnement de l'Internet[146].

[143] En vertu de l'article 3.-1. de la convention, ce choix « doit être exprès ou résulter de façon certaine des dispositions du contrat ou des circonstances de la cause (…)». La seule limitation au choix des parties, qui peuvent retenir une loi étrangère, provient de l'article 3.-3 de la convention, l'impossibilité de déroger aux lois impératives (« dispositions impératives ») d'un Etat dans lequel tous les autres éléments de la situation sont localisés au moment où les parties ont fait le choix de la loi étrangère. Si les parties y dérogent, les tribunaux conservent la possibilité de faire application des lois impératives du pays dans lequel le contrat est localisé.

[144] Art. 4.-1. de la convention.

[145] Cette présomption ne peut être écartée que lorsqu'il résulte de l'ensemble des circonstances que le contrat présente des liens plus étroits avec un autre pays.

[146] Trois cas de figure exposés dans le 2 de l'art.5 : « si la conclusion du contrat a été précédée dans ce pays d'une proposition spécialement faite ou d'une publicité, et si le consommateur a accompli dans ce pays les actes nécessaires à la conclusion du contrat » ou, « si le cocontractant du consommateur ou son représentant a reçu commande du consommateur dans ce pays » ou, « si le contrat est une vente de marchandises et que le consommateur se soit rendu dans ce pays et y ait passé commande, à la condition

109. Le cadre conventionnel actuel apparaît, pour ce qui concerne le régime des transactions électroniques, à la fois ambigu et relativement défavorable au consommateur. Une adaptation ponctuelle des règles de conflit de lois concernant spécifiquement les transactions électroniques, et donc dérogeant aux conventions de portée plus générales, serait donc souhaitable. Une convention internationale relative aux transactions électroniques et à la protection du consommateur devrait voit le jour, qui protégerait les consommateurs, sans cependant défavoriser le développement des échanges électroniques internationaux. En tout état de cause, l'inefficacité des règles juridiques internationales actuelles concernant la protection du cyberconsommateur souligne encore plus l'importance des techniques du chiffre. Une cryptologie forte évite un bon nombre de problèmes d'ordre juridique même si son rôle, on l'a vu, n'est pas de remplacer le droit mais de le soutenir. Dans ce contexte, la cryptologie vient aussi au soutien du droit d'auteur, lorsqu'il s'agit d'œuvres numériques, et son importance devient cruciale chaque fois que l'œuvre fait l'objet d'une transaction ou d'un transfert en ligne.

Section 2. Le droit d'auteur à l'épreuve du chiffre

que le voyage ait été organisé par le vendeur dans le but d'inciter le consommateur à conclure une vente ». Il convient d'écarter les circonstances prévues au 2 et au 3 dont on voit mal comment elle pourraient jouer sur Internet, sauf à considérer, par une interprétation assez poussée, qu'un serveur puisse être considéré comme le représentant d'un vendeur à l'étranger. C'est donc les circonstances prévues par le premier cas de figure qui pourraient le cas échéant jouer, les deux conditions étant cumulatives. Il faudrait tout d'abord démontrer que le professionnel a pris l'initiative de la vente dans le pays du consommateur en lui adressant « une proposition spécialement faite » ou une publicité. Mais aucun critère n'est fixé, ni une définition de la publicité sur Internet n'est donnée. En outre, le consommateur pourrait éprouver des difficultés pour apporter la preuve que la transaction a bien été précédée d'une sollicitation du vendeur. La seconde condition est d'interprétation encore plus approximative dans le cas d'une transaction en ligne : que faut-il entendre par « actes nécessaires à la conclusion du contrat » dans le cas d'une transaction qui n'est pas localisable ? Il est assez difficile d'apporter la preuve d'un simple « clic ». En outre, un clic pourrait identifier un ordinateur et non le consommateur. Mais ceci est un autre débat…

110. Chiffrement et droit d'auteur peuvent aller de pair dans le monde numérique. Qu'il s'agisse de texte, d'image ou de son, le *bit*, ce binôme « 0 et 1 », constitue désormais la « molécule élémentaire[147] » de la communication. La numérisation contracte le temps et l'espace ; l'informatique, l'audiovisuel et les télécommunications se confondent. L'œuvre ne peut échapper à cette dynamique : chaque jour, des milliers de documents (normalement protégés par le droit d'auteur) circulent sur les réseaux. La structure ouverte d'Internet offre la possibilité de les télécharger[148] et de les redistribuer, et sans en dégrader la qualité[149]. Le commerce électronique d'œuvres concernées par le droit d'auteur est devenu une réalité. Cette circulation des œuvres à travers les réseaux (*on line*) devient incontrôlable et un des moyens les plus efficaces pour les protéger est l'utilisation de moyens cryptologiques[150].

111. On a vu que le régime de la cryptologie repose sur la distinction entre moyens permettant l'authentification / intégrité des données et moyens permettant la confidentialité. Nous avons étudié ces questions dans notre première partie (§58 et s.). Ce qui nous intéresse ici, c'est que le cryptage permet la protection et par conséquent une meilleure exploitation des oeuvres, ainsi qu'un meilleur respect de l'étendue de l'autorisation donnée par l'auteur pour exploiter ses œuvres. Les techniques cryptologiques viennent donc au secours du monopole de l'auteur, même si ce dernier se heurte parfois à des droits opposés.

§1. La protection du monopole de l'auteur

[147] CATALA (P.), L'information sans frontière *in* Les dossiers de la semaine juridique, n. hors série, févr.1996.

[148] Des sites privés ou des serveurs souvent localisés dans des pays ne protégeant pas les droits d'auteur offrent un téléchargement libre d'œuvres concernées par le droit d'auteur.

[149] L' « avantage » du monde numérique est qu'il permet le reproduction à l'infini des œuvres sans perte de qualité.

[150] Pour les systèmes *off line*, comme les CD-ROM (disques contenant par exemple des logiciels) ou les CD-DA (disques de musique), la technique du plombage peut être utilisée. Celle-ci peut empêcher la reproduction, mais ne peut pas s'appliquer pour les données circulant par réseau.

112. L’art. L.111-1 du code de la Propriété Intellectuelle précise que « *l’auteur jouit sur cette œuvre, du seul fait de sa création, d’un droit de propriété incorporelle exclusif et opposable à tous* ». Ce monopole lui confère aussi le droit de crypter cette œuvre, qui est considéré comme un accessoire du droit exclusif. Par ailleurs, la simple fourniture des moyens de décryptage ne peut présumer seule l’autorisation de l'auteur d’exploiter : le formalisme d’un écrit est exigé par la loi. La fonction de la technique n’est pas de remplacer le droit ; la maximalisation de la sécurité emporte cependant une minimisation des fraudes. En l’absence des moyens cryptologiques, l’ internaute peut facilement commettre une infraction, mais comment réprimer s’il ne laisse pas de trace ? Il ne reste que le cas hypothétique de flagrant délit…il est donc évident que la protection juridique devient plus efficace et couvre tous les aspects de l’œuvre lorsque la technique du cryptage vient à son secours.

A. Précisions sur la notion de monopole

113. Le droit d'auteur est le fait de la volonté du législateur. Actuellement, l’environnement juridique et socioculturel veut que l’auteur soit devenu un simple participant au résultat économique de son produit (il a n’a droit qu’à une rémunération équitable) et des intérêts industriels prennent sa place : le droit d’auteur devient donc important pour les industries du droit d’auteur, qui utilisent les procédés de cryptage de façon extensive. Les intérêts financiers étant souvent très grands, le champ d’application des techniques de chiffrement s’étend considérablement.

B. Champ d’application des techniques de chiffrement

114. De nombreuses techniques cryptologiques existent pour protéger une œuvre contre sa diffusion illégale. Nous limiterons notre analyse à celles qui peuvent s'appliquer *on line*.

115. En ce qui concerne les outils pour l'identification de l'oeuvre , il existe en matière d'enregistrement sonores et audiovisuels, le code ISRC (International Standard Recording Code) qui constitue une norme reconnue par l'ISO. Il s'agit d'un code comportant 12 caractères alphanumériques identifiant le pays d'origine de l'enregistrement, le premier propriétaire, l'année d'enregistrement et son numéro. Incorporé à l'enregistrement, ce code est inaudible à la diffusion, grâce au procédé de stéganographie, mais identifiable sur les supports numériques et la diffusion radiophonique. La majorité des CD audio dans le monde sont munis de ce code. Lors d'une transmission du contenu d'un tel CD par Internet, l'internaute peut par exemple vérifier sur une base de données l'identité de l'œuvre[151]. Un code similaire existe pour le format mp3[152] de musique, le ID3 *tag*. Celui-ci est inaudible mais permet l'identification très précise d'une œuvre musicale. Il peut en outre inclure la mention "protégé par copyright" ce qui permet aux administrateurs de sites de contrôler leur diffusion[153].

116. En ce qui concerne l'authenticité de l'œuvre, la signature numérique[154] permet de vérifier et de garantir sa provenance et facilite son *tracking* (suivi à la trace, pour localiser les trafics illicites). Pour ce qui est des outils de protection contre les copies illicites, la norme SCMS est un système de prévention, intégré dans le matériel de lecture de l'œuvre, n'autorisant qu'une seule copie numérique. Cependant ce système est limité pour l'instant aux lecteurs de cassettes numérique DAT. Pour les logiciels téléchargeables sur Internet, les industriels optent le plus souvent pour un

[151] Par exemple, le serveur www.cddb.com propose l'identification des cd audio dont la table des matières n'a pas été modifiée (CD originaux ou…copies identiques à l'original).

[152] Il ne s'agit que d'une forme compressée de données musicales, pour faciliter la transmission par le réseau.

[153] Un site devenu célèbre pour la diffusion d'œuvres musicales, www.audiogalaxy.com (actuellement hors service) utilisait le ID3 *tag* pour interdire le téléchargement des musiques sous copyright.

[154] V. aussi *infra*, 2e section.

téléchargement gratuit du produit, qui ne devient opérationnel qu'à partir du moment où on insère un code qu'il faut acheter. Cette méthode ne protège pas contre les copies illicites (on peut diffuser le logiciel avec un code fonctionnel), mais permet un contrôle *a posteriori* de la copie que l'on détient. L'article L. 335-3 al.1 CPI précise qu' « *est un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi* » . La Cour de cassation apprécie le texte de façon extensive et affirme que la contrefaçon « se constitue simplement par l'atteinte portée aux droits de l'auteur... ». Par extension, la contrefaçon peut être le fondement d'une action visant à lutter contre le décryptage de l'œuvre ; on peut qualifier le contournement du système de protection de l'œuvre en contrefaçon.

117. Dans sa fonction d'interdiction d'accès, la cryptologie peut s'appliquer à toute œuvre diffusée par Internet. Nous pouvons parler de télédiffusion dès lors que l'œuvre est accessible sur le Web. Selon le code de la propriété intellectuelle, il y a représentation lorsqu'on se trouve en présence d'une « communication de l'œuvre au public par un procédé quelconque et notamment (...) par télédiffusion [155]». La télédiffusion s'entend de la diffusion « par tout procédé de télécommunication de sons, d'images, de documents, de données et de message de toute nature ». Est ainsi visée la télématique, par conséquent les réseaux de type Internet. On trouve également des sites Web qui ne sont accessibles qu'à une partie limitée d'internautes : c'est les cas des pages réservées aux abonnés qui doivent insérer leur identifiant et un mot de passe pour accéder aux information souhaitées.

118. Une autre méthode de protection d'une œuvre est le watermarking. Le watermarking, encore appelé tatouage, est une technique destinée à protéger le droit d'auteur de manière assez efficace. Il s'agit d'une signature qui est insérée dans une image numérique (photographie, vidéo, dessin) qui prouve l'origine de la copie. Cette signature est invisible à l'œil nu et doit résister aux différentes modifications qu'une

[155] Art. L. 122-2 CPI.

personne puisse apporter sur l'image[156], mais captable pour un ordinateur ou tout autre système de lecture électronique de l'œuvre. Ce caractère invisible renvoie à l'art et la science de la stéganographie[157] mais l'opération d'insertion d'un watermark dans une image emprunte aussi de la technique du chiffre. L'algorithme du watermark, qui peut être connu par n'importe qui, est configurable par une clé sécrète qui est propre à chaque créateur. Cependant, cette clé n'est pas détenue par lui-même, mais est confiée à un tiers de confiance qui gère les clés ; ce dernier, étant tenu au secret professionnel[158], est censé la conserver et il ne doit la communiquer aux autorités étatiques que dans des cas précis.

§2. Les limites au monopole de l'auteur

119. Le droit d'auteur connaît des limites. Les unes mettent en lumière l'affrontement entre droit d'auteur et droit public, les autres se situent autour de la « trace » qu'une œuvre peut laisser une fois consultée ou remodelée.

A. Le droit à la culture

120. Les techniques de chiffrement des œuvres révèlent le rapport entre droit d'auteur et droit public. Alors que l'auteur doit pouvoir limiter la diffusion de sa création, en utilisant notamment des procédés cryptologiques dès lors qu'il s'agit d'une œuvre numérique, la communauté des internautes prétend en même temps qu'elle a un droit à la culture. En effet, la gratuité dans la navigation du réseau et l'accès sans contrôle dans la majorité des sites Internet permet d'imaginer un « cybermonde » sans limites. Au niveau européen, l'art. 128 du traité de Maastricht visant les aspects culturels de

[156] Ainsi, un watermark robuste résiste à des rotations de l'image, des changements d'échelle ou de symétries, des découpages, l'application de filtres, des changements de format…

[157] V. *supra*, §.8 de notre étude.

[158] V. *supra*, §.80 de notre étude.

l'Union incite la coopération des Etats membres pour l'amélioration de la connaissance et la diffusion de la culture. Dans la même perspective, la Déclaration Universelle des droit de l'homme de 1948 prévoit que « *Toute personne a le droit de prendre part librement à la vie culturelle de la communauté, de jouir des arts et de participer au progrès scientifique et aux bienfaits qui en résultent*[159] ». Mais l'alinéa suivant dispose que « *Chacun a droit à la protection des intérêts moraux et matériels découlant de toute production scientifique, littéraire ou artistique dont il est l'auteur* [160]». Comment peut-on conjuguer les deux textes ? Le droit positif français ne reconnaît pas en tant que telle la finalité culturelle, malgré un certain assouplissement de la loi de 1985[161]. Quelques nuances existent cependant en pratique. On peut donner l'exemple de la possibilité de passer outre l'opposition des représentants de l'auteur décédé en cas d'abus notoire dans l'exercice du droit de divulgation ou du droit d'exploitation fondé sur une sorte de droit du public d'accéder aux œuvres.

B. Les notions d'œuvre seconde et de copie privée

121. Une œuvre originale possède des caractéristiques plus ou moins uniques. Se pose donc la question de la relation entre celle-ci et l'œuvre seconde, qui possède des « traces » de la première. Dans un autre sens du terme, des traces d'une œuvre sont laissées dans un ordinateur, une fois que l'internaute l'ait consultée en ligne.

122. On a vu que le watermarking permet d'identifier un emprunt dans une œuvre existante. On pourrait se demander si cet emprunt relève du monopole de l'auteur. Cette question est en relation avec la notion de l'œuvre seconde, qui doit son existence, même partiellement, à l'œuvre première. S'il est sûr que l'auteur d'une œuvre seconde doit une partie de son bénéfice à l'auteur de l'œuvre initiale, il est difficile de délimiter

[159] DUDH, Art. 27, alinéa 1.

[160] DUDH, Art. 27, alinéa 2.

[161] Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle, telle qu'amendée.

l'étendue de ce principe. Il est admis que l'emprunt à une œuvre préexistante ne peut être subordonné à l'autorisation de l'auteur s'il est trop limité pour révéler les caractéristiques de l'œuvre originale[162], cette appréciation appartenant au juge. On peut déduire que l'auteur de l'œuvre seconde peut apposer son propre watermark, sans même demander l'accord du premier créateur, à partir du moment où œuvre originale et œuvre seconde présentent des différences fondamentales. Cette situation n'est pas à confondre avec le droit de citation, reconnu aussi sans demander une autorisation quelle conque, qui consiste à reproduire des brèves citations d'œuvres protégées dans un but éducatif, scientifique ou à titre d'information.

123. Le droit à la copie privée[163] constitue une dérogation au droit d'auteur, car en principe toute atteinte au monopole de l'auteur donne lieu à une action en contrefaçon. La loi de 1985 ne permet de porter atteinte à ce principe qu'en contrepartie d'une rémunération. L'évolution de la technologie et l'avènement des ordinateurs connectés en réseau oblige le droit à s'adapter. Dès lors qu'une œuvre est chargée sur un ordinateur, elle y est mémorisée et peut devenir accessible à tout le réseau. Deux cas de figure à distinguer, qui se ressemblent néanmoins : la sauvegarde de l'œuvre dans un ordinateur (par exemple, enregistrement sur le disque dur) et la mise en mémoire « cache » (c'est à dire la consultation temporaire, en temps réel) de l'œuvre.

124. Pour sauvegarder une œuvre, on doit avoir l'autorisation de l'auteur, sinon cette copie constitue un acte de contrefaçon. La technique du cryptage vient donc au secours du droit : pour décrypter l'œuvre on doit posséder une clé que l'on achète en général. Mais la notion juridique de copie d'usage privé est mise à mal par la suite : dès lors que l'ordinateur est connecté en réseau, cela permet aux autres membres du même réseau (à moins que l'utilisateur disposant en premier de l'œuvre ait mis des restrictions quant à l'accès à ses fichiers) de copier à leur tour l'œuvre. On pourrait comparer avec le régime applicable pour les logiciels ou les disques de musique. Pour les logiciels, une

[162] En ce sens, Lucas (A.), Droit d'auteur et multimédia *in* Mélanges Francon, Propriétés Intellectuelles, Dalloz, 1995.

[163] L'art. L.123-3 du CPI concerne indifféremment la copie privée électronique et la reprographie « traditionnelle ».

seule copie (dite de sauvegarde) est autorisée par titulaire et ne doit être utilisée qu'en cas de dommage survenu sur l'exemplaire original. Les disques de musique ne peuvent être copiés que dans un cadre strictement familial et ne doivent pas être diffusés en public.

125. La mise en mémoire « cache » d'une œuvre est une situation plus délicate. Sans que l'on se rende compte, il s'agit d'une opération qui s'effectue chaque fois que l'on consulte un document en ligne. Techniquement, pour consulter un document électronique, par conséquent une œuvre aussi, notre ordinateur le pose en mémoire, de manière temporaire, pour pouvoir l'afficher sur l'écran. Cette mémoire temporaire est censée s'effacer périodiquement, par exemple à chaque redémarrage de l'ordinateur, mais il y a des cas où l'utilisateur puisse configurer son système afin qu'il garde plus longtemps les documents en mémoire[164]. Juridiquement, si on est autorisé à décrypter *on line* et / ou consulter une œuvre, ceci ne doit pas conduire à nous permettre de garder une copie de l'œuvre en cache. Cependant, la technique veut que ceci soit le cas le plus courant…est-ce qu'on pourrait être amenés à dire que cette coutume, en réalité *conta legem*, constitue une nouvelle limite au monopole de l'auteur ? D'autant plus que cette copie privée pourrait ensuite être rediffusée par le réseau…mais ceci est un autre débat.

[164] En général, il les sauvegarde dans le disque dur, sous une forme de « fichiers temporaires ».

CHAPITRE 2

LA PROTECTION DE LA VIE PRIVEE

126. Les réseaux font circuler en permanence les informations, qui traversent de nombreux nœuds informatiques avant d'arriver à leur destination. Le risque que ces informations soient capturées, en route ou même à la source, n'existe pas seulement pour les professionnels, mais aussi pour les particuliers. Plus ils utilisent Internet, plus ils sont exposés aux dangers qu'il présente. La protection de la vie privée se met encore plus en danger depuis l'utilisation des lignes permettant une connexion permanente au réseau[165]. Comme nous fermons à clé les portes de chez –nous, il faut ainsi verrouiller l'accès à notre ordinateur aux tiers, qui peuvent l'attaquer à tout moment *via* le réseau. Cette protection de la vie privée et des données personnelles se concrétise avec les moyens cryptologiques. Le droit de son côté suit les évolutions techniques et doit s'adapter rapidement ; la protection juridique reste alors indispensable pour le monde des réseaux.

Section 1. Les solutions techniques de protection de la vie privée

[165] Tel est le cas des abonnements Internet par Câble ou DSL (Digital subscriber Line) (ADSL pour la France) qui sont proposés au grand public pour un tarif mensuel forfaitaire tout à fait attractif. L'ordinateur du consommateur reste en permanence connecté (même si l'adresse IP change tous les jours) au réseau, ce qui rend les attaques de toute sorte plus faciles pour les pirates. Il suffit d'être connecté au réseau et l'attaque devient possible. Les particuliers deviennent donc une cible, derrière les ordinateurs qui sont connectés avec une adresse IP fixe, comme ceux des grandes entreprises, des administrations et des universités. Deux solutions pour se protéger : utiliser des moyens techniques de protection et cryptologiques ou … se déconnecter du réseau !

127. Une première façon de protéger la confidentialité et l'intimité de notre vie privée et d'utiliser au maximum les solutions techniques actuelles. Ces dernières utilisent le chiffrement dans de nombreux cas, alors que dans d'autres il suffit que l'internaute optimise la configuration de ses logiciels pour être moins vulnérable. Dans les deux cas une petite connaissance des techniques est nécessaire ; il est évident que, dans la société de l'information, la connaissance dévient indispensable. Les solutions techniques protègent nos données lorsqu'on les transmet (volontairement) par le réseau, aussi bien que lorsqu'on les a stockées sur un ordinateur, sans vouloir les transmettre, ce dernier étant cependant connecté au réseau.

§1. La protection des données personnelles lors de leur transmission par le réseau

128. Notre vie privée est exposée chaque fois que l'on navigue sur Internet. Nos données personnelles peuvent être capturées à tout moment, à notre insu, par des personnes plus ou moins dangereuses. Cela peut concerner nos habitudes et préférences sur le réseau, notre identité, ou même le contenu de nos messages.

A. La traçabilité de nos préférences sur le réseau

129. Lorsqu'on visite un site, celui-ci pose le plus souvent un « cookie » dans notre disque dur. Les cookies sont des lignes d'information en format texte qui sont sauvés dans notre ordinateur dans un fichier *.txt* . Il s'agit en effet de log files qui répertorient nos préférences concernant chaque site. Ainsi, lors de la deuxième visite au même site, ce dernier peut nous identifier en lisant le cookie, nous saluer avec notre nom, présenter les pages en notre langue préférée etc. Le cookie ne présente *a priori* aucun risque pour notre ordinateur. Ce n'est qu'un bout de texte ne pouvant pas contenir une sorte de virus ou de *script* dangereux par exemple. Cependant de nombreux sites abusent de la

fonction des cookies. Ils peuvent par exemple intégrer des cookies des serveurs tiers[166] de publicité, ou collecter des informations personnelles sans notre consentement[167]. Avec un peu d'expérience, on peut paramétrer notre navigateur pour qu'il trie les cookies et nous permet de choisir quel cookie accepter ou non. Malheureusement, certains sites refusent d'accéder ou s'affichent mal si on n'accepte pas tous les cookies. Il appartient à l'internaute de faire son choix. Il faut quand même savoir que de nombreux sites commerciaux vendent les informations recueillies à des fins notamment publicitaires. On peut recevoir par la suite des emails non sollicités (*spamming*, Cf. § suivant) Se pose donc la question de la légalité des cookies, qui constituent sans doute une atteinte à la vie privée. En revanche, les cookies de session (*session cookies*), qui servent à l'identification instantanée sur un site[168] sont inoffensifs car ils ne se sauvent pas dans le disque dur.

130. L'ordre dans lequel on consulte les sites web, les préférences que l'on sauve dans nos sites préférés, l'acceptation des cookies, l'utilisation de notre boîte aux lettres sans prendre de précautions (Cf. §133), l'existence dans notre ordinateur de programmes *spyware* (Cf. §137) et les traitements « invisibles » (Cf. §138) permettent aux sociétés de publicité de nous envoyer de emails non sollicités, technique connue sous le nom de *spamming*. Les spam mails sont donc des publicités, censées correspondre à nos intérêts. Le spamming constitue une atteinte à la vie privée[169], non seulement parce qu'il nécessite une certaine surveillance de notre activité sur le réseau de la part des sociétés, mais aussi à cause du volume de ces emails que l'on peut recevoir. En outre, si on choisit en cliquant que l'on ne souhaite plus être sollicités par une telle société, le plus souvent cela prévient le serveur publicitaire que notre boîte aux lettres est active, ce qui aggravera encore plus les choses. Une protection contre ces mesures, même si elle n'est pas tout à fait efficace, est le filtrage du courrier, tel que proposé par de

[166] On les appelle « third party cookies ».

[167] Le plus souvent, les navigateurs web sont paramétrés par défaut d'accepter la plupart de types de cookies afin de faciliter la navigation (par exemple, Internet Explorer de Microsoft). D'autres optimisent la sécurité ce qui rend en revanche la navigation plus compliquée (par exemple, Opera).

[168] Par exemple, sur les sites de email, pour identifier notre boîte aux lettres.

[169] L'art. L. 121-15-1. de la loi sur la société de l'information dispose : « Il est interdit d'adresser par courrier électronique des publicités ou des offres promotionnelles non sollicitées aux personnes qui, ne souhaitant pas être rendues destinataires de telles publicités ou offres, se sont inscrites sur des registres destinés à recevoir leur opposition. »

nombreuses sociétés de messagerie. Le serveur de messagerie stocke un nombre de mots-clés et d'adresses, et nous les envoie séparément, dans un directoire *spam* ou *bulk* mail, ce qui évite le mélange avec notre véritable courrier. Enfin, si on utilise un client email sur notre ordinateur[170], on peut configurer des filtres dans le même but. Ceci nécessite encore une fois une petite connaissance en informatique.

131. Nos habitudes sur le réseau peuvent aussi être filtrées de l'intérieur, dans le cas d'un *intranet*[171]. Ceci peut être particulièrement intéressant dans le cadre d'une entreprise, lorsque l'employeur veut interdire l'accès à certains sites du web, ou dans le cadre familial, pour éviter d'exposer les enfants aux dangers de certains sites. Des filtres peuvent donc être installés sur le serveur de l'entreprise (ou de la maison) qui se connecte sur le réseau. Ceux-ci interdisent la connexion aux sites contenant[172] certains mots, par exemple « nazi ». La même fonction peut être confiée à un tiers spécialisé au filtrage des données ou être effectuée en employant un routeur ou un firewall (Cf. §140).

B. La capture de notre identité

132. Notre vie privée est contrôlée à travers notre identité sur le net. En fait, les informations en provenance ou à destination de notre ordinateur révèlent notre identité. Pour se connecter, on utilise une adresse IP, similaire aux numéros de téléphone. Cette dernière nous est accordée par notre fournisseur d'accès Internet pour un certain temps (ou de façon permanente dans le cas de location d'une adresse IP fixe), qui connaît aussi notre identité. Pour naviguer dans l'anonymat, il faut passer par un site qui nous

[170] Programme qui télécharge puis sauvegarde notre courrier. Par exemple, Outlook, Eudora ou Mozilla Mail.

[171] Intranet : un réseau local, par exemple des ordinateurs chez nous connectés entre eux. S'appelle aussi LAN (Local Area Network).

[172] Les mots-clés doivent en principe se situer au niveau de l'URL (adresse absolue) du site ou dans les mots-clés listés dans le META Tags des pages (partie spécifique du code html de la page servant à l'identification de la page au moteurs de recherche).

rend anonymes[173]. On peut par la suite se connecter au site souhaité, à travers le site *anonymiser*, avec une adresse IP aléatoire choisie par ce dernier. Cependant, ce service n'est pas gratuit dans tous les cas.

133. Un cas similaire existe pour les adresses email. Il s'agit des *remailers* qui, au moment de la transmission du courrier, masquent mon adresse. Les remailers fonctionnent donc comme l'anonymiser pour les adresses IP. Il est par ailleurs possible de modifier dans le système notre adresse, en sorte que le destinataire reçoive une autre adresse (fictive ou appartenant à une autre personne), mais cette méthode nécessite de la combiner avec une modification des détails de notre adresse IP, sinon une personne motivée peut avoir accès aux détails de l'en-tête du message pour remonter ainsi jusqu'au serveur auquel on était connecté au moment de l'envoi du message.

C. La protection du contenu de nos messages

134. Les méthodes de protection de notre vie privée exposées ci-dessus réduisent les risques et peuvent souvent suffire à elles-mêmes. Cependant le contenu de nos messages reste accessible aux tiers souhaitant l'intercepter. La solution la plus efficace reste donc le chiffrement du message. La méthode la plus efficace est le PGP (Pretty Good Privacy), qui tient pour « assez bonne confidentialité ». Le PGP est un programme qui chiffre nos messages. Malgré des rumeurs qui ont circulé en 1998, que la NSA pouvait lire ces messages grâce à un backdoor, le PGP reste encore un des moyens les plus sûrs pour crypter une information. Le PGP est une méthode de cryptage asymétrique. Développé par un chercheur américain, Phil Zimmerman, il appartient actuellement à Network Associates, une alliance entre Cisco et Lucent technologies. Le fonctionnement est similaire au SSL (Cf. §94 et s.). L'expediteur utilise la clé publique du destinataire du message qui le décrypte ensuite avec sa clé

[173] Par exemple, www.anonymiser.com. Ce genre de sites sont censés ne pas communiquer à des tiers notre adresse IP, à peu près dans la même logique que les tiers de confiance…

privée. Seul le destinataire détient la clé privée, il devient donc impossible pour un pirate qui intercepte le message de le déchiffrer.

135. Le email dévient ainsi beaucoup plus sûr que le courrier traditionnel. Par ailleurs, le feu vert officiel français a été donné pour l'utilisation du PGP open source, GnuPG[174] (sous licence GPL). Une association a obtenu la licence pour l'utiliser, importer et exporter jusqu'en 2007. Il s'agit du bureau français de la Free Software Foundation Europe (FSF), qui milite pour les logiciels libres de la mouvance GNU / Linux, qui a obtenu l'autorisation de la DCSSI. En outre, le simple utilisateur peut à tout moment modifier sa version de GnuPG et en faire profiter les autres; il devient donc, potentiellement, un « fournisseur ». Mais on a vu qu'il est toujours obligatoire, pour les « fournisseurs » de solutions, soit de faire une déclaration (systèmes dont la clé ne dépasse pas 128 bits), soit d'attendre l'autorisation formelle de la DCSSI pour des systèmes plus puissants. C'est le cas pour GnuPG et OpenSSL, car ces logiciels n'ont pas de limite dans leur force de cryptage et sont basés sur le protocole OpenPGP. Cependant la DCSSI a permis à tous les acteurs de profiter de ce logiciel libre (alors que les autorisations délivrées sont nominatives en principe)[175].

§2. La protection des données personnelles stockées sur un ordinateur connecté au réseau

136. Ce deuxième cas de figure montre bien que l'on n'a pas besoin de transmettre une information privée pour être exposé aux dangers du réseau. Dès lors que notre ordinateur est connecté à Internet, les intrusions[176] sont possibles. Le risque vient des

[174] Autorisation du 15 juillet 2002, licence pour utiliser, importer et exporter les versions 1.0.7 et suivantes de Gnu Privacy Guard (GnuPG). C'est le cas aussi pour le OpenSSL (version 0.9.6d et suivantes).

[175] La requête de la FSF a donc été formulée pour une demande de « fourniture générale », qui permet de considérer que des « intermédiaires » peuvent bénéficier de cette autorisation. Cela allégera les formalités à la fois pour les utilisateurs de base, les chercheurs et les universités, mais aussi les entreprises comme Mandrakesoft qui distribue le système Linux- Mandrake.

[176] Les personnes qui attaquent les systèmes connectés s'appellent « *intruders* ». Il s'agit en effet de *hackers* ou de *crackers*. Mais il peut aussi s'agir de sociétés qui collectent des informations à notre insu.

traitements invisibles et des logiciels installés dans notre ordinateur qui transmettent des informations. Le remède consiste essentiellement à employer les techniques du chiffre.

A. L'émission de données personnelles à notre insu

137. Certains logiciels que l'on installe dans notre ordinateur sont en effet des *spywares* (programmes espions). Ils effectuent les tâches souhaitées, mais derrière, à notre insu, envoient *via* le réseau des informations personnelles ou concernant la configuration de notre système. Généralement, c'est dans les sites pirates que l'on trouve la liste de ces programmes[177]. L'utilisateur averti ne doit pas par conséquent les installer. Dans la même logique, dans le cas d'un intranet cette fois-ci, on trouve les *sniffers*, logiciels ayant leurs propres pilotes de notre carte réseau qui affichent tout ce qui reçoit celle-ci[178].

138. Les traitements invisibles constituent un sujet d'irritation pour les internautes encore plus délicat. Il s'agit de traitements qui restent cachés à l'utilisateur mais perçus par les entreprises concernées. Contrairement aux spywares, ils sont déjà dans notre ordinateur lorsqu'il est livré, sous forme de logiciels[179]. On pense immédiatement au système d'exploitation de Microsoft, Windows. Microsoft s'est octroyée le droit, lorsque l'on utilise son service de mise à jour du système ou de dépannage à distance, d'explorer notre ordinateur, sa configuration, de répertorier les logiciels installés et vérifier les licences correspondantes. Et s'il paraît obligatoire de détenir les licences des logiciels installés, la constitution par Microsoft de bases de données sur nos

[177] Le créateur du programme ne le mentionne pas. C'est par exemple le cas du GetRight, du Gator, de Kazaa…des programmes qu'on télécharge sur Internet.

[178] Si le réseau interne est constitué avec des hubs et pas avec des switch, toutes les informations passent par toutes les cartes réseaux, et c'est seulement grâce à l'adresse contenue dans chaque paquet que la carte décide de la transférer ou non au système. Le sniffer lit tout, même si l'adresse du destinataire est différente.

habitudes porte sans doute atteinte à notre vie privée. Microsoft avait promis en 1998 de retirer ce mouchard pour les prochaines versions de Windows. Cependant, la dernière version de Windows (XP, home et pro) possède sans doute beaucoup plus de flexibilité d'exploration et il est possible qu'elle envoie des informations personnelles même si on utilise jamais les services du site de Microsoft.

B. Les solutions techniques

139. Dans un premier temps, l'internaute doit choisir les logiciels qu'il installe avec précaution. Il ne faut pas télécharger du net de programmes dont on ne connaît pas la provenance ou la qualité. Quant au système d'exploitation…notre sort est dans les mains de Bill Gates[180], à moins que l'on installe un autre système d'expoitation[181].

140. Dans l'attente du nouveau protocole IP V6[182], les routeurs et les firewalls protègent de manière très efficace contre les attaques en provenance du réseau extérieur. Les routeurs acheminent les messages vers les serveurs ou les PCs. En choisissant le chemin le plus court, ils optimisent les débits. Ils peuvent aussi analyser les « en-tête » des paquets IP et refuser les adresses qui ne correspondent pas à celle du serveur de destination. Ils assurent donc des fonctions de filtrage. Certains modèles de routeurs proposent aussi des fonctions NAT[183] qui rendent les machines connectées derrière ce routeur invisibles au réseau extérieur. L'utilisateur peut aussi choisir pour le filtrage, à la place du routeur, un firewall (Cf. aussi §41 et 98), et laisser au routeur le

[179] Intel, fabricant de matériel, avait aussi inclus sur la puce du processeur Pentium III (et ultérieurs ?) un numéro permettant l'identification de chaque PC à distance. Malgré les protestations des différentes associations privées de protection de la vie privée, il est redoutable que Intel ait arrêté ce procédé.

[180] Fondateur et PDG de Microsoft.

[181] Par exemple Linux, système gratuit, très stable et open source, pour ce qui concerne les PC. Il ne faut pas négliger en outre les ordinateurs de Apple, les Macintosh, longtemps considérés comme les ordinateurs les plus performants.

[182] En cours de normalisation, les adresses IP V6 étendent l'espace d'adressage (pour faire face aux demandes accrues d'accès sur Internet) et apportent des mécanismes de sécurité aux couches les plus basses du réseau (qui ne sont installés actuellement que dans les couches supérieures).

[183] Network Address Translation.

seul travail d'acheminement des messages. Le firewall peut filtrer les adresses IP, les virus et parfois est même configurable pour contrôler l'utilisation du réseau. Une fois notre système protégé, les techniques du chiffre viennent renforcer ce dispositif en cachant le contenu de nos informations privées.

141. Si la protection du système n'est pas une tâche facile pour le simple utilisateur, il est pour autant d'une importance fondamentale lorsqu'il s'agit de protéger notre vie privée. Cela est dû au fait que des informations personnelles se trouvent dans le système entier et il est techniquement impossible de crypter tout ce qu'un ordinateur contient. Dans un deuxième temps, le chiffrement des nos données personnelles le plus importantes paraît plus simple lorsqu'on utilise des logiciels conçus à cet effet (V. *supra*). Les mots de passe constituent enfin une solution facile (mais pas très fiable) pour protéger nos données. Word, Excel et d'autres logiciels très répandus proposent ce genre de fonction.

142. Les difficultés que les techniques présentent pour le simple utilisateur, la méconnaissance des solutions les plus efficaces ainsi que les failles dans les logiciels spécialisés, conduisent à un moment ou un autre à la révélation de certains aspects de notre vie privée. Il est donc normal que le droit vienne au secours du citoyen, en prévoyant des dispositions protectrices de la vie privée. Malgré un certain retard constaté quant à son adaptation aux nouvelles technologies, il reste l'ultime source de protection efficace.

Section 2. Le droit, outil indispensable à la protection de la vie privée

143. Internet et les réseaux constituent un domaine « obscur » pour la plupart de particuliers, souvent même pour ceux qui maîtrisent les questions informatiques. Cette science « invisible » devient encore plus difficile à comprendre à cause de l'évolution

des technologies : une solution qui protège efficacement aujourd'hui ne protégera plus demain. L'internaute est obligé de mettre à jour ses logiciels de protection[184], voire ses connaissances, assez souvent, ce qui donne l'impression que seule la technique la plus récente peut nous protéger. S'il est vrai que les solutions techniques protègent la vie privée de manière assez efficace, des failles subsistent toujours et le besoin d'appliquer le droit redevient évident. Ce dernier, outre le fait qu'il agit *a priori* pour harmoniser les droits nationaux et anticiper les conflits, il agit aussi *a posteriori* pour punir[185] les atteintes à la vie privée. Cependant, ce droit connaît aussi des limites. Il appartient donc au législateur de trouver le juste équilibre entre libertés et besoin de sécurité.

§1. Un droit fondamental du citoyen

144. Plusieurs textes consacrent ce droit à la vie privée. Au niveau transnational, on pourrait citer l'art. 12 de la Déclaration universelle des droits de l'homme de 1948[186], ou l'art. 8 de la Convention européenne des droits de l'homme de 1950[187]. En outre, la CEDH est d'applicabilité directe dans les Etats membres de l'Union et a une valeur supérieure aux normes nationales. Au niveau interne, l'art. 9, al. 1er du code civil dispose que « *Chacun a droit au respect de sa vie vie privée* ». Ces textes si fondamentaux s'appliquent bien évidemment au droit du cyberespace. Plus précisément, la Loi[188] de 1978 relative à l'informatique, aux fichiers et aux libertés dispose dans son article premier : « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de*

[184] Souvent on a besoin de la dernière version d'un logiciel pour être suffisamment protégé ; des *bugs* (défauts) sont régulièrement découverts ce qui nécessite des mises à jour. D'autres logiciels, comme les programmes antivirus nécessitent des mises à jour au moins deux fois par mois pour qu'ils soient efficaces.

[185] Pour un exposé des différentes peines applicables lors des atteintes logiques ainsi que pour l'analyse des questions de sécurité publique, voir Première partie.

[186] Article 12 DUDH : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. ».

[187] Article 8 – 1 CEDH : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. ».

l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. ». Il découle que le citoyen a, par exemple, le droit d'avoir accès aux informations le concernant et de demander leur modification, le cas échéant. Les personnes qui collectent les informations de leur part ont l'obligation de les conserver pour qu'elles ne soient pas endommagées ou communiquées à des tiers non autorisés.

A. Les droits du citoyen face à ses informations personnelles

145. La loi de 1978 dispose dans son article 3 que « *Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés* [189] *dont les résultats lui sont opposés.* ». Un projet de loi récent, intitulé « Protection des données personnelles et de la vie privée » viendra modifier la loi de 1978. Entre autres, l'art.3 est concerné [190]. Ce projet constitue une transposition de la Directive européenne 95/46/CE relative à la protection des données personnelles, adopté en Conseil des ministres le 18 juillet 2001[191]. Celle-ci impose notamment un droit d'accès des individus aux données les concernant, un droit de correction, un droit de refus dans certaines circonstances (telles que la prospection commerciale), un droit d'information sur l'origine des données, l'identité des utilisateurs et la finalité de l'usage et enfin, un droit de recours.

---

[188] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[189] Par « traitement automatisé » on entend les opérations d'enregistrement, d'élaboration d'informations nominatives. Cela peut par exemple concerner une base de données de clients dans le serveur d'un cybercommerçant, que celle-ci soit enregistrée de manière permanente sur un seul serveur ou qu'elle fasse l'objet de transferts fréquents *via* le réseau.

[190] Le projet de loi dispose : « Art. 3. - I. - *Est responsable d'un traitement de données à caractère personnel, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine ses finalités et ses moyens.* »
« II. - Est destinataire d'un traitement de données à caractère personnel toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires. ».

146. Par ailleurs, les citoyens ont le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives les concernant fassent l'objet d'un traitement[192]. Le droit d'accès à ces informations se concrétise par l'interrogation des services ou organismes chargés, de mettre en oeuvre les traitements automatisés dont la liste est accessible au public en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication[193].

147. Concernant la durée[194] de conservation de ces informations, celle-ci ne doit pas excéder la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou traitées. Pour les informations qui restent quand même conservées, elles ne peuvent faire l'objet d'un traitement à d'autres fins qu'à des fins historiques, statistiques ou scientifiques, à moins que ce traitement n'ait reçu l'accord exprès des intéressés. Par ailleurs, cette dernière disposition semble ne pas s'appliquer au commerce électronique. La fin publicitaire ou la revente des informations à des tiers est notamment concernée. La durée de conservation du numéro de la carte bancaire qui a servi à la transaction ne doit donc pas excéder ce qui est nécessaire à cette transaction, même si en pratique, certains sites les gardent dans leurs bases de données pour faciliter les transactions ultérieures. Mais ceci est un risque pour le commerçant, qui doit préserver la sécurité des ces informations.

B. L'obligation de conservation des informations

---

[191] Directive 95/46, JOCE 23 nov. 1995, no L 281 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Elle est entrée en vigueur le 25 oct. 1998.

[192] Art. 26 de la même loi.

[193] Art. 34.

[194] Art. 28.

148. Le cybercommerçant ou tout autre propriétaire d'une base de données contenant des informations personnelles des citoyens, a l'obligation de les conserver soigneusement. L'article 29 de la loi de 1978 dispose que « *Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés* ». Le texte est en conformité avec les dispositions communautaires, à savoir avec les Directives 95/46 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et 97/66 sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et enfin le Règlement (CE) no 45/2001[195]. Ces textes contiennent des dispositions visant à garantir que les fournisseurs de services de télécommunication accessibles au public soient tenus de prendre les mesures techniques et organisationnelles appropriées pour assurer la sécurité et la confidentialité de leurs services. Cette confidentialité se réalise grâce à l'utilisation, on l'a vu, de moyens cryptologiques.

149. Enfin, l'article 27 de la loi de 1978 oblige les personnes qui collectent ces informations d'informer les citoyens par rapport au caractère obligatoire ou facultatif des réponses, aux conséquences à leur égard d'un défaut de réponse, aux personnes physiques ou morales destinataires des informations et à l'existence d'un droit d'accès et de rectification. La collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est bien évidemment interdite (art.25 de la loi) ; on pourrait penser aux pratiques des compagnies comme Microsoft, ou le fonctionnement des spywares (cf. §137-138).

§2. Les limites du droit à la protection de la vie privée

[195] Règlement (CE) no 45/2001 du 18 décembre 2000, JOCE 12 janvier 2001, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

150. Malgré les nombreux textes protégeant la vie privée, les droits du citoyen-internaute connaissent, comme on peut l'imaginer, plusieurs limites. Parmi ces limites la toute première, on l'a vu, tient à la nature même d'Internet qui ne connaît pas de frontières. Selon quel droit interpréter, par exemple, le silence de l'internaute ? La non-réponse à une question ou à une publicité peut suivre la règle « le silence vaut acceptation » ? Le système juridique Anglo-Saxon préfère la règle du *opt-out*, alors que les « européens » mettent plutôt l'accent sur le consentement (*opt-in*). D'autres limites peuvent aussi se rencontrer à cause des conflits entre droit à la vie privée et d'autres droits. On peut citer par exemple le droit d'auteur ou encore le droit public et plus précisément les questions de sécurité publique ou les intérêts de la défense nationale.

151. En ce qui concerne le droit d'auteur, on a vu (§ 118, 121 et s.) que ce droit à la copie privée connaît des limites. Les questions de sécurité publique et les intérêts de la défense nationale on été étudiés dans la première partie. On peut sur ce point ajouter la limite apportée par la loi de 1978. Concernant l'art.29, sa limite est posée à l'art. 29-1[196] : « *Les dispositions de la présente loi ne font pas obstacle à l'application, au bénéfice de tiers, des dispositions du titre Ier de la loi no 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal et des dispositions du titre II de la loi no 79-18 du 3 janvier 1979 précitée. En conséquence, ne peut être regardé comme un tiers non autorisé au sens de l'article 29 le titulaire d'un droit d'accès aux documents administratifs ou aux archives publiques exercé conformément aux lois no 78-753 du 17 juillet 1978 précitée et no 79-18 du 3 janvier 1979 précitée.* ». La primauté des intérêts de l'Etat est encore une fois confirmée[197].

[196] Inséré par la loi n° 2000-321 du 12 avril 2000, article 5, 2°.
[197] Le texte est en conformité avec l'alinéa 2 de l'art.8 de la CEDH : « *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.* ».

152. On doit constater que les techniques cryptologiques actuelles et le droit applicable en la matière constituent deux matières complexes qui s'interpénètrent. Notre seul regret est que le droit, tant au niveau interne que transfrontalier, accuse une lenteur quant à son adaptation aux nouvelles technologies, et cela est partiellement dû au fait que le juriste ne les maîtrise pas suffisamment. L'apport des juristes formés aussi en informatique sera donc considérable, notamment pour le cas d'Internet qui présente des lacunes en matière de sécurité.

153. La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives[198]. Ce besoin de sécurité se concrétise dans le nouveau monde numérique à travers les moyens cryptologiques. La cryptologie devient par conséquent la science protectrice de notre société mondialisée, satisfaisant ainsi un besoin bientôt ressenti par tous les citoyens. Parce que s'ouvrir au monde grâce au Réseau implique aussi de s'exposer à de nouveaux risques.

[198] Entre autres, une loi très récente (no. 2002-1094 du 29 août 2002) d'orientation et de programmation pour la sécurité intérieure emploie cette même phrase pour souligner l'importance de la sécurité. La notion de sécurité, dans tous ses aspects, est par ailleurs à la une des journaux actuellement.

BIBLIOGRAPHIE

OUVRAGES JURIDIQUES SPECIFIQUES POUR INTERNET

BAILLET (F.), *Internet, le droit du cybercommerce, le guide pratique et juridique*, Issy les Moulineaux : Stratégies, 2001, 217 pages.

BENSOUSSAN (A.) et LE ROUX (Y.), *Cryptologie et signature électronique : aspects juridiques*, Paris : Hermès science publication, 1999, 175 pages.

BOURCIER (D.), HASSETT (P.) et ROQUILLY (C.), *Droit et Intelligence artificielle, une révolution de la connaissance juridique*, Paris : Romillat, 2000, 303 pages.

CACHARD (O.), *La régulation internationale du marché électronique*, Paris : LGDJ, 2002, 622 pages.

CHARMOT (C.), L'échange de données informatisé (EDI), Coll. Que sais-je ? Paris : PUF, décembre 1998, 127 pages.

DELFS (H.) et KNEBL (H.), *Introduction to Cryptography, principles and applications*, Paris: Springer, 2002, 315 pages.

FERAL – SCHUHL (C.), *Cyberdroit, le droit à l'épreuve de l'internet*, 3 édition, Paris : Dalloz, 2002, 353 pages.

GUERRIER (C.) et MONGET (M.-C.), *Droit et Sécurité des Télécommunications*, Paris : Springer, 2000, 458 pages.

KAUFMAN et GAUTIER, *Noms de domaine sur Internet : Aspects juridiques*, Paris : Vuibert, 2001, 230 pages.

LAMY, *Droit de l'informatique et des réseaux*, Paris : Lamy, 2001, 1940 pages.

LUCAS (A.), DEVEZE (J.), et FRAYSSINET (J.), *Droit de l'informatique et de l'internet*, Paris : PUF, 2001, 748 pages.

PIETTE – COUDOL (T.), *Echanges électroniques, certification et sécurité*, Paris : Litec, 2000, 237 pages.

ROSENOER (J.), *Cyberlaw, the law of the internet*, New York: Springer, 1997, 362 pages.

STINSON (D.), Traduction de VAUDENAY (S.), *Cryptographie, Théorie et pratique*, Paris : Vuibert, 2002, 394 pages.

TABATONI (P.) (sous la direction de), *La protection de la vie privée dans la société d'information*, Tome 1, Paris : PUF, 2000, 65 pages.

TABATONI (P.) (sous la direction de), *La protection de la vie privée dans la société d'information*, Tome 2, Paris : PUF, 2000, 58 pages.

VERBIEST (T.) et WERY (E.), *Le droit de l'internet et de la société de l'information, Droits européen, belge et français*, Série création information communication, Bruxelles : Larcier, 2001, 648 pages.

VIER (C.), (sous la coordination de), *L'internet et le droit, droit français, européen et comparé de l'internet*, Coll : Légipresse, Paris : Victoires, 2001, 486 pages.

OUVRAGES JURIDIQUES GENERAUX

AUDIT (B.), *Droit international privé*, 2e éd. 1997, Paris : Economica, 944 pages.

JACQUET (J.-M.) et DELEBECQUE (Ph.), *Droit du commerce international*, 2e éd. 2000, Paris : Dalloz, 413 pages.

TERCINET (A.), *Droit européen de la concurrence, opportunités et menaces*, Les cours du haut enseignement de gestion, Bonchamp-Lès-Laval : Montchréstien / Gualino, février 2000.

OUVRAGES NON JURIDIQUES

BERNSTEIN (T.), BHIMANI (A.), SCHUKTZ (E.) et SIEGEL (CA.), *Sécurité internet pour l'entreprise*, Paris : International Thomson publishing, 1997, 425 pages.

COLE (E.), *Hackers beware, defending your network from the wiley hacker*, Indianapolis: New Riders, 2001, 778 pages.

GUISNEL (J.), *Guerres dans le cyberespace, services secrets et Internet*, Paris : La découverte, 1997, 349 pages.

MARTIN – LALANDE (P.), *L'internet, un vrai défi pour la France*, Paris : La documentation française, 1998, 111 pages.

ARTICLES SPECIALISES

BARBRY (E.), *Le droit du commerce électronique : de la protection…à la confiance*, Computer & Telecoms law review, 1998/2, p.14.

BARBRY (E.) et OLIVIER (F.*), Des décrets tant attendus : quel droit pour la cryptologie ?*, Etude, I 124, JCP éd. G., no 14, 1er avril 1998, p.591.

BARESCH (D.), *Sécurité et confiance dans la communication électronique – pour une approche européenne*, Revue du Marché commun et de l'Union européenne, no 420, juillet-août 1998, p.437.

BARESCH (D.) et SCHLECHTER (R.), *La Directive européenne pour les signatures électroniques*, Revue du Marché commun et de l'Union européenne, no 439, juin 2000, p.387.

BENSOUSSAN (A.), *Centre certificateur, authentification, preuve et contrôle*, Les petites affiches, 29 mai 1996, no 65, p.28.

BISCHOFF (P.), *L'Union européenne et la protection des données, la société de l'information à l'épreuve des droits de l'homme*, Revue du Marché commun et de l'Union européenne, no 421, sept.1998, p.537.

BREBAN (Y.) et POTTIER (I.), *Sécurité, authentification et dématérialisation de la preuve dans les transactions électroniques*, 1ère Partie : Gazette du Palais, Doctrine, 4 avril 1996, p.276.

BREBAN (Y.) et POTTIER (I.), *Sécurité, authentification et dématérialisation de la preuve dans les transactions électroniques*, 2ème Partie : Gazette du Palais, Doctrine, 1er août 1996, p.863.

CAPRIOLI (E.), *Sécurité et confiance dans le commerce électronique. Signature numérique et autorité de certification*, La semaine juridique éd. G., no 14, 1er avril 1998, p. 583.

CAPRIOLI (E.), *La directive européenne no 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques*, Gazette du Palais, Doctrine, 29-31 oct. 2000, p.5.

CAPRIOLI (E.), *Les lignes directrices de l'OCDE régissant la politique de cryptographie*, Cahiers du Lamy droit de l'informatique, no 92, mai 1997,p.1.

CATINAT (M.), *La politique européenne de promotion d'internet*, Revue du Marché commun et de l'Union européenne, no 435, févr. 2000, p.81.

COSTES (L.), *Les nouveaux principes « safe harbor » régissant les flux transfontières de données entre l'Union européenne et les Etats-Unis*, Lamy droit de l'informatique et des réseaux, no 130 - nov. 2000, p.1.

COSTES (L.), *Une proposition de décision – cadre de la Commission visant à renforcer la sécurité des réseaux et des systèmes d'information*, Lamy droit de l'informatique et des réseaux, no 147 – mai 2002, p.1.

DE BOTTINI (R.), *La Directive « commerce électronique » du 8 juin 2000*, Revue du Marché commun et de l'Union européenne, no 449, juin 2001, p.368.

FERAL (P.-A.), *Un pas supplémentaire vers la reconnaissance et la protection d'un droit fondamental dans l'Union européenne – Le règlement (CE) no 45/2001*, Revue du Marché commun et de l'Union européenne, no 450, juillet-août 2001, p.475.

GAVALDA (Ch.), *La cryptologie*, Juris PTT, dossier no 55, 1er semestre 1999, p.3.

GOLIARD (F.), *Télécommunications et réglementation française du cryptage*, Chronique, Recueil Dalloz 1998, 11e cahier.

GRYNBAUM (L.), *La preuve littérale et la signature à l'heure de la communication électronique*, Chroniques, Communication-Commerce électronique, Editions du Juris-Classeur, nov.1999, p.9.

IGGLEZAKIS (I.), *La convention EDI, étude comparative des droits grec-américain-européen*, EempD, 1997, p.239.

LEFER (S.), *Sécurité et confiance : maîtres mots du commerce électronique*, Lamy droit de l'informatique, no 99-janvier 1998, p.1.

MAISL (H.), *Communications mobiles, secret des correspondances et protection des données personnelles*, Computer & Telecoms law review, 1995/2, p.13.

NICOLEAU (P.), *La protection des données sur les autoroutes de l'information*, Recueil Dalloz 1996, chroniques, p.111.

OLIVIER (F.) et BARBRY (E.), *Aperçu rapide sur la loi du 26 juillet 1996 sur la réglementation des télécommunications*, La semaine juridique, éd. G., no 38, 18 sept. 1996.

PENNARU (S.), *De Gutenberg à Bill Gates : Commentaire du projet de loi relatif à l'adaptation du droit de la preuve aux technologies de l'information et à la signature électronique*, Petites Affiches, 27 janvier 2000, no 19, p.4.

PIETTE-COUDOL (T.), *L'échange de données informatisé (EDI)*, Gazette du palais, Doctrine, 2e sem. 1991,p.551.

PIETTE-COUDOL (T.), *Un nouveau décret applicable à la signature électronique*, Bulletin d'actualité, Lamy droit de l'informatique et des réseaux, no 147 - mai 2002, p.6.

SEDALLIAN (V.), *Les préoccupations de la CNIL : transposition de la directive européenne, données personnelles sur Internet…(Rapport d'activité pour 1996)*, Computer & Telecoms law review, 1997/3, p.57.

SEDALLIAN (V.), *Les problèmes posés par la législation française en matière de chiffrement*, Computer & Telecoms law review, 1998/4, p. 23.

STROWEL (A.), IDE (N.) et VERHOESTRAETE (F.), *La Directive du 8 juin 2000 sur le commerce électronique : un cadre juridique pour l'internet*, Journal des tribunaux, éd. Larcier (Bruxelles), no 6000, 17 février 2001, p.133.

SWETENHAM (R.), *Le plan d'action pour une utilisation sûre d'internet*, Revue du Marché commun et de l'Union européenne, no 436, mars. 2000, p.160.

THIEFFRY (P.), *L'émergence d'un droit européen du commerce électronique*, RTD eur., 36 (4), oct.-déc. 2000, p.649.

ARTICLES DE PRESSE

BAUDOIN (P.) et FREYSSINET (E.), *Cybercriminalité*, L'internet, Cahiers de la documentation française, no 295, mars-avril 2000, p.31.

CATTIEUW (A.) et HEBRARD (P.), *L'origine des codes secrets*, Pour la science (édition française du Scientific American), La cryptographie, l'art du secret, dossier hors-série juillet-oct. 2002, p.8.

FONTAINE (C.), *Le tatouage des images numériques*, Pour la science (édition française du Scientific American), La cryptographie, l'art du secret, dossier hors-série juillet-oct. 2002, p.72.

GILBERT (H.) et GIRAULT (M.), *Cryptographie des télécommunications*, Pour la science (édition française du Scientific American), La cryptographie, l'art du secret, dossier hors-série juillet-oct. 2002, p.80.

NGUYEN (H.), *Cyberterrorisme : Comment les Etats blindent leurs réseaux*, Le Monde informatique, no 917, 23 nov. 2001, p.8.

PATARIN (J.), *La cryptographie à clé secrète*, Pour la science (édition française du Scientific American), La cryptographie, l'art du secret, dossier hors-série juillet-oct. 2002, p. 38.

PATARIN (J.), *La cryptographie des cartes bancaires*, Pour la science (édition française du Scientific American), La cryptographie, l'art du secret, dossier hors-série juillet-oct. 2002, p. 66.

REMI (F.), *La cryptographie à clé publique*, Pour la science (édition française du Scientific American), La cryptographie, l'art du secret, dossier hors-série juillet-oct. 2002, p. 44.

WEGRZYNOWZSKI (E.), *Peut-on casser les clés ?* , Pour la science (édition française du Scientific American), La cryptographie, l'art du secret, dossier hors-série juillet-oct. 2002, p. 32.

LIENS INTERNET

SITES OFFICIELS

http://www.ssi.gouv.fr (Service Central de Sécurité des Systèmes d'Information, ancienne adresse : http://www.scssi.gouv.fr/)

http://www.fbi.gov (Federal Bureau of Investigation – en anglais)

http://www.certa.ssi.gouv.fr (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques)

http://www.internet.gouv.fr/francais/textesref/pagsi2/accueil.htm
(Projet de loi « Protection des données personnelles et de la vie privée »)

http://csrc.nist.gov/encryption/aes/index2.html#overview (computer security ressource center ; AES – en anglais)

http://www.oecd.org/pdf/M000014000/M00014341.pdf (OCDE; lignes directrices FAQ)

http://www.internet.gouv.fr/francais/index.html (l'action de l'Etat pour le développement de la société de l'information)

http://europa.eu.int/ (le site de l'Union européenne)

SITES NON-OFFICIELS

http://www.droit-technologie.org/dossiers/JT6000_directive_080600_commerce_electronique.pdf (commentaire de la directive commerce électronique)

http://news.zdnet.fr/story/0,,t118-s2111111,00.html (news site)

http://fr.news.yahoo.com/020725/7/2ot4k.html (news site)

http://www.defense-consommateur.org/ (protection du consommateur)

http://www.fit.qut.edu.au/ISRC

http://www.monde-diplomatique.fr/1999/08/PISANI/12382 (penser la cyberguerre)

http://www.ifrance.com/Scpolundi/Cyberguerre/Cyber-guerre.htm (Cyberguerre et sécurité nationale)

http://perso.wanadoo.fr/fiweb/secuforces.htm (La sécurité française : les organismes officiels)

http://www.scpp.fr/SCPP/SCPPWeb.nsf/zIDPrint/99480D3D7C4F3CFDC1256841004D02AD?OpenDocument (code ISRC)

http://www.cybersciences.com/Cyber/1.0/1_29_52.asp (histoire de l'internet)

http://library.thinkquest.org/28005/flashed/timemachine/courseofhistory/egypt.shtml (Menet Khufu & hiéroglyphes – en anglais)

http://histoirecrypto.ifrance.com/histoirecrypto (histoire de la cryptologie)

http://www.branchez-vous.com/actu/00-11/04-332103.html (La cyberguerre aux États-Unis)

http://press.coe.int/dossiers/107/f/f-sommaire.htm (Convention internationale contre la cybercriminalité)

http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm **(convention** du Conseil de l'Europe sur la **cybercriminalité)**

Table des annexes

ANNEXES

Annexe 1 : Abréviations et termes Internet

ABREVIATIONS :

SEFTI : Service d'Enquête des Fraudes aux Technologies de l'Information
DCPJ : Direction Centrale de la Police Judiciaire
BCRCI : Brigade Centrale de Répression de la Criminalité Informatique
IRCGN : Institut de Recherches Criminelles de la Gendarmerie Nationale
SGDN : Secrétariat Général de la Défense Nationale
DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information
SCSSI : Service Central de la Sécurité des Systèmes d'Information
DSSI : Directoire de la Sécurité des Systèmes d'Information
DISSI : Délégation Interministérielle pour la Sécurité des Systèmes d'Information
CISSI : Commission Interministérielle pour la Sécurité des Systèmes d'Information
DSTI : Direction des Systèmes Terrestres et d'Information
DST : Direction de la Surveillance du Territoire
GIC : Groupement Interministériel de Contrôle
IHESI : Institut des Hautes Etudes de la Sécurité Intérieure
DGCCRF : Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes
DCRG : Direction Centrale des Renseignements Généraux
DGSE : Direction Générale de la Sécurité Extérieure
DG13 : Direction Générale chargée des télécoms et de la sécurité informatique (DG 13)
DSN : Direction de la Sûreté Nationale
CNCIS : Commission Nationale de Contrôle des Interceptions de Sécurité
CCSDN : Commission Consultative du Secret de la Défense Nationale
SCTIP : Service de Coopération Technique Internationale de Police
CLUSIF : Club de la Sécurité informatique des systèmes d'information français
CIGREF : Club Informatique des GRandes Entreprises Françaises
HCFDC : Haut Comité Français pour la défense civile
IHEDN : Institut des Hautes Etudes de Défense Nationale
RECIF : Recherches et Etudes sur la Criminalité Informatique Française
DAS : Délégation aux Affaires Stratégiques
INPS : Institut National de Police Scientifique
OCLCTI : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la communication
OSSIR : Observatoire de la Sécurité des Systèmes d'Information & des Réseaux
CERT-RENATER : Groupement d'Intérêt Public
CyberCrimInstitut : Institut International des Hautes Etudes de la Cybercriminalité

TERMES INTERNET :

administrateur de site, de serveur
Domaine: Informatique / Internet
Définition : Personne chargée de la maintenance et du suivi d'un site ou d'un serveur sur la toile d'araignée mondiale.
Voir aussi: toile d'araignée mondiale.
Equivalent étranger: webmaster.

adresse réticulaire
Domaine : Télécommunications / Internet.
Voir: adresse universelle.

adresse universelle
Domaine : Télécommunications / Internet.
Synonyme: adresse réticulaire.
Définition : Dénomination unique à caractère universel qui permet de focaliser une ressource ou un document sur l'internet, et qui indique la méthode pour y accéder le nom du serveur et le chemin à l'intérieur du serveur.
Note: Par exemple, l'adresse universelle de la page d'accueil de la Délégation générale à la langue française est « http ://www.culture.gouv.fr/culture/dglf/accueil.htm ». Elle comprend trois parties : « http » indique la méthode d'accès; «www.culture.gouv.fr» est le nom du serveur du ministère de la culture et de la communication en France sur la toile d'araignée mondiale; « culture/dglf/accueil.htm » est le chemin d'accès au document.
Voir aussi: domaine, internet, page d'accueil, système d'adressage par domaines.
Equivalent étranger: uniform ressource locator, universal resource locator, URL.

annuaire des domaines
Domaine: Télécommunications / Internet.
Voir: système d'adressage par domaines.

appliquette n.f.
Domaine: Informatique / Internet.
Définition : Petite application indépendante du matériel et du logiciel utilisés, qui est téléchargée depuis un serveur de la toile mondiale et qui est exécutée localement au sein d'un logiciel de navigation.
Note: Les appliquettes sont surtout employées dans le langage de programmation Java.
Voir aussi: logiciel de navigation, toile d'araignée mondiale.
Equivalent étranger: applet.

article de forum
Domaine: Informatique / Internet.
Synonyme: contribution n.f.
Définition: Document similaire à un message électronique, destiné à alimenter un ou plusieurs forums.
Voir aussi: forum.
Equivalent étranger: news item, news posting, news article.

Autoroutes de l'information
Domaine: Télécommunications / Réseaux - Internet.
Définition: Structure constituée par des moyens de télécommunication et d'informatique interconnectés, qui permet d'offrir à un très grand nombre d'usagers de multiples services, en général à débit élevé, y compris des services audiovisuels.
Note: On rencontre aussi le terme «inforoute», qui n'est pas recommandé.

Equivalent étranger: information highway (ang.), information superhighway (ang.), infobahn n.f. (all.).

barrière de sécurité
Domaine: Télécommunications / Réseaux - Internet.
Définition: Dispositif informatique qui filtre les flux d'informations entre un réseau interne à un organisme et un réseau externe en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur.
Note: Dans cette acception, on dit aussi «pare-feu » (n.m.).
Equivalent étranger: firewall.

cadre n.m.
Domaine: Informatique / Internet.
Définition: Sous-fenêtre de la fenêtre principale d'un logiciel de navigation, qui peut afficher un document différent de ceux affichés dans les autres sous-fenêtres.
Voir aussi: fenêtre, logiciel de navigation.
Equivalent étranger: frame.

causette n.f. *fant.*
Domaine: Informatique / Internet.
Définition: Communication informelle entre plusieurs personnes sur l'internet, par échange de messages affichés sur leurs écrans.
Voir aussi: internet.
Equivalent étranger: chat.

concentrateur n.m.
Domaine: Télécommunications / Réseaux - Internet.
Définition: Dispositif informatique placé au nœud d'un réseau en étoile, qui concentre et distribue les communications de données.
Note: Un concentrateur n'assure ni routage ni commutation.
Equivalent étranger: hub.

contribution n.f.
Domaine: Informatique / Internet.
Voir: article de forum.

diffusion réticulaire systématique ou, ellipt., **diffusion réticulaire**
Domaine: Télécommunications / Internet.
Voir: diffusion systématique sur la toile.

diffusion sélective
Domaine: Télécommunications / Internet
Voir: distribution sélective.

diffusion systématique sur la toile ou, ellipt., **diffusion sur la toile**
Domaine: Télécommunications / Internet.
Synonyme: diffusion réticulaire systématique.
Définition: Envoi systématique de données ou de documents à des utilisateurs de la toile mondiale.
Voir aussi: distribution sélective.
Equivalent étranger: webcasting, netcasting.

disque numérique polyvalent
Domaine: Informatique.
Définition: Disque numérique optique de grande capacité, à usages divers (audio, vidéo, multimédia, mémoire vive, mémoire motte).
Note: La capacité des disques numériques polyvalents est supérieure à celle des cédéroms et nécessite des lecteurs appropriés.
Equivalent étranger: Digital Versatile Disk (DVD).

distribution personnalisée
Domaine: Télécommunications / Internet

Voir: distribution sélective.

distribution sélective
Domaine: Télécommunications / Internet.
Synonyme: distribution personnalisée, diffusion sélective.
Définition: Technique utilisée pour faire bénéficier automatiquement un utilisateur de la toile mondiale, à sa demande, d'un envoi de données d'un type choisi.
Note: La distribution sélective se distingue de ta recherche individuelle.
Equivalent étranger: push technology.

domaine n.m
Domaine: Télécommunications / Internet.
Définition: Ensemble d'adresses faisant l'objet d'une gestion commune.
Voir aussi: système d'adressage par domaines.
Equivalent étranger: domain.

dorsale n.f.
Domaine.: Télécommunications / Réseaux - Internet.
Définition: Partie principale d'un réseau de télécommunication ou de téléinformatique, caractérisée par un débit élevé qui concentre et transporte les flux de données entre des réseaux affluents.
Equivalent étranger: backbone.

extranet n.m.
Domaine : Télécommunications / Réseaux – Internet.
Définition: Réseau de télécommunication et de téléinformatique constitué d'un intranet étendu pour permettre la communication avec certains organismes extérieurs. par exemple des clients ou des fournisseurs.
Voir aussi: intranet.
Equivalent étranger: extranet.

FAQ
Domaine: Télécommunications / Internet.
Voir: foire aux questions.

fenêtre n.f.
Domaine: Informatique.
Définition: Partie rectangulaire de l'écran d'un ordinateur à l'intérieur de laquelle sont affichées les informations relatives à une activité déterminée.
Note: Plusieurs fenêtres peuvent êtres ouvertes simultanément: elles peuvent être juxtaposées ou se recouvrir totalement ou partiellement.
Equivalent étranger: window.

fichier des questions courantes
Domaine: Télécommunications / Internet.
Voir: foire aux questions.

fil (de I. discussion)
Domaine: Informatique / Internet.
Définition: Dans les échanges au sein d'un forum ou entre utilisateurs du courrier électronique. enchaînement des commentaires à un article donné.
Voir aussi: article de forum, forum.
Equivalent étranger: thread.

foire aux questions
Domaine: Télécommunications / Internet.
Abréviation: FAQ.
Synonyme: fichier des questions courantes, questions courantes.
Définition: Rubrique présentant par sujets les questions les plus fréquemment posées par les utilisateurs, accompagnées des réponses correspondantes.
Note: La foire aux questions a, en particulier, pour but de faciliter l'intégration des internautes novices

dans un groupe de discussion et de diminuer le nombre des messages diffusés dans le réseau.
Equivalent étranger: frequently asked questions (file), FAQ.

forum n.m.
Domaine: Informatique / Internet.
Définition: Service permettant l'échange et la discussion sur un thème donné: chaque utilisateur peut lire à tout moment les interventions de tous les autres et apporter sa propre contribution sous forme d'articles.
Voir aussi: article de forum.
Equivalent étranger: newsgroup.

fouineur n.m
Domaine: Informatique / Internet.
Définition: Personne passionnée d'informatique qui, par jeu, curiosité. défi personnel ou par souci de notoriété, sonde, au hasard plutôt qu'à l'aide de manuels techniques, les possibilités matérielles et logicielles des systèmes informatiques afin de pouvoir éventuellement s'y immiscer. *(Source:* Office de la langue française du Québec.)
Voir aussi: pirate.
Equivalent étranger: hacker.

fournisseur d'accès
Domaine: Télécommunications / Internet.
Définition: Organisme offrant à des clients d'accéder à l'internet, ou, plus généralement, à tout réseau de communication.
Note: Le fournisseur d'accès peut aussi offrir des services en ligne.
Equivalent étranger: access provider.

frimousse n.f. *fam*
Domaine : Informatique / Internet.
Définition: Dans un message, association facétieuse de quelques caractères typographiques qui évoquent un visage expressif.
Note: 1.Les deux frimousses les plus connues sont: -) pour la bonne humeur et: - (pour le dépit, où les deux points représentent les yeux, le trait représente le nez et les parenthèses la bouche.
2.Le terme « binette » est recommandé au Québec. « Frimousse » doit être préféré à «binette ».
Equivalent étranger: emoticon, smiley.

glisser-déposer n.m.
Domaine: Informatique / Internet.
Définition: Action par laquelle l'utilisateur sélectionne un objet à l'écran, le déplace jusqu'à une autre position, puis le lâche pour déclencher une action sur cet objet.
Equivalent étranger: drag and drop.

hypertexte n.m.
Domaine: Informatique / Internet.
Définition: Système de renvois permettant de passer directement d'une partie d'un document à une autre, ou d'un document à d'autres documents choisis comme pertinents par l'auteur.
Equivalent étranger: hypertext.

hypertextuel adj.
Domaine: Informatique / Internet.
Définition: Relatif à l'hypertexte.
Equivalent étranger: hypertext.

internaute n.
Domaine: Télécommunications / Réseaux - Internet.
Définition: Utilisateur de l'internet.
Note: On rencontre aussi le terme « cybernaute ».
Equivalent étranger: cybernaut.

Internet n.m. sg.
Domaine: Télécommunications / Réseaux - Internet.
Définition: Réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants.
Note: L'acheminement est fondé sur le protocole IP *(internet: Protocol),* spécifié par l'Internet Society (ISOC). L'accès au réseau est ouvert à tout utilisateur ayant obtenu une adresse auprès d'un organisme accrédité. La gestion est décentralisée en réseaux interconnectés.
Equivalent étranger: Internet network, Internet, Net.

intranet n.m.
Domaine: Télécommunications / Réseaux - Internet.
Définition: Réseau de télécommunication et de téléinformatique destiné à l'usage exclusif d'un organisme et utilisant les mêmes protocoles et techniques que l'internet.
Equivalent étranger: intranet.

liaison numérique à débit asymétrique
Domaine: Télécommunications / Réseaux - Internet.
Voir: raccordement numérique asymétrique.

logiciel de navigation
Domaine: Informatique / Internet.
Synonyme : navigateur *n.m.*
Définition: Dans un environnement de type internet. logiciel qui permet à l'utilisateur de rechercher et de consulter des documents et d'exploiter les liens hypertextuels qu'ils comportent.
Voir aussi: hypertextuel.
Equivalent étranger: browser.

logiciel médiateur
Domaine: Informatique.
Définition: Logiciel qui permet le fonctionnement de plusieurs ordinateurs en coordination, en attribuant à chacun une tâche spécifique, comme les échanges avec les utilisateurs, l'accès aux bases de données ou aux réseaux.
Note: Le terme. « logiciel médiateur » désigne aussi un logiciel qui permet de coordonner le fonctionnement de plusieurs logiciels au sein d'un même ordinateur.
Equivalent étranger: middleware.
mandataire n.m.
Domaine: Télécommunications / Réseaux - Internet.
Voir: serveur mandataire.

module d'extension n.m,
Abréviation: extension n.f.
Domaine: Informatique / Internet.
Définition: Elément logiciel que l'on adjoint à une application pour en étendre les fonctions.
Equivalent étranger: plug-in.

mouchard n.m.
Domaine : Informatique / Internet.
Voir: témoin (de connexion)

navigateur n.m.
Domaine: Informatique / Internet.
Voir: logiciel de navigation.

page d'accueil
Domaine: Informatique / Internet.
Définition : 1. Page de présentation d'un site sur la toile mondiale.
2. Page de tête affichée par un logiciel de navigation.
Voir aussi: logiciel de navigation.

Equivalent étranger: home page.

page sur la toile
Domaine: Informatique / Internet.
Equivalent étranger: webpage, web page.

pare-feu n.m.
Domaine: Télécommunications / Réseaux - Internet.
Voir: barrière de sécurité.

passerelle n.f.
Domaine: Télécommunications / Internet
Définition: Dispositif destiné à connecter des réseaux de télécommunication ayant des architectures différentes ou des protocoles différents, ou offrant des services différents.
Note: Une passerelle peut par exemple connecter un réseau local d'entreprise avec un autre réseau local ou un réseau public de données.
Equivalent étranger: gateway.

pirate n.m.
Domaine: Informatique / Internet.
Définition: Personne qui contourne ou détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique.
Equivalent étranger: cracker.

questions courantes
Domaine: Télécommunications / Internet,
Voir: foire aux questions.

raccordement numérique asymétrique
Abréviation: RNA.
Domaine: Télécommunications / Réseaux - Internet.
Synonyme: liaison numérique à débit asymétrique.
Définition: Technique de transmission numérique offrant deux canaux de données à haut débit sur une ligne téléphonique ordinaire en paire symétrique, le débit dans le sens du réseau vers l'utilisateur étant très supérieur au débit dans l'autre sens.
Note: 1. Dans le sens du réseau vers l'utilisateur, le débit est suffisant pour permettre la distribution de programmes de télévision ou de documents multimédias, notamment en provenance de l'internet. Il est de l'ordre de 600 à 800 kbit/s dans l'autre sens. En outre, le canal téléphonique est conservé.

2. L'expression «ligne numérique à paire asymétrique » ne doit pas être utilisée car il s'agit d'une transmission asymétrique sur paire symétrique.

Equivalent étranger: asymetric (bit rate) digital subscriber line, ADSL.

recherche Individuelle
Domaine: Télécommunications / Internet.
Définition: Technique utilisée sur la toile mondiale lorsque internaute recherche des données par une démarche active au moyen de son logiciel de navigation, qui lui présentera ensuite le résultat de cette recherche.
Note: La recherche individuelle se distingue de la distribution sélective.
Equivalent étranger: pull technology.

serveur n.m.
Domaine: Informatique.
Définition: Système informatique destiné à fournir des services à des utilisateurs connectés et, par extension, organisme qui exploite un tel système.
Note : Un serveur peut par exemple permettre la consultation et l'exploitation directe de banques de données,
Equivalent étranger: server, on-line data service.

serveur mandataire

Abréviation: mandataire.
Domaine: Télécommunications / Réseau x- Internet.
Définition: Dispositif informatique associé à un serveur et réalisant, pour des applications autorisées, des fonctions de médiation, telle que le stockage des documents les plus fréquemment demandés ou l'établissement de passerelles.
Voir aussi: passerelle, serveur.
Equivalent étranger : proxy server, proxy.

signet n.m.
Domaine : Informatique / Internet.
Définition: Moyen d'accéder rapidement à une adresse universelle préalablement stockée en mémoire par l'utilisateur.
Voir aussi: adresse universelle.
Equivalent étranger: bookmark.

site (de la toile, sur la toile)
Domaine: Informatique / Internet.
Equivalent étranger: website, web site.

système d'adressage par domaines
Abréviation: adressage par domaines.
Domaine: Télécommunications / Internet.
Synonyme : annuaire des domaines.
Définition: Système de basés de données et de serveurs assurant la correspondance entre les noms de domaine ou de site utilisés par les internautes et les adresses numériques utilisables par les ordinateurs.
Note : Ce système permet aux internautes d'utiliser, dans la rédaction des adresses, des noms faciles à retenir au lieu de la suite de chiffres du protocole IP.

Exemple: Le nom du serveur sur la toile mondiale du ministère de la culture et de la communication est « www.culture.gouv.fr ».
Voir aussi: adresse universelle, domaine, internaute.
Equivalent étranger: domain name system, DNS

témoin (de connexion)
Domaine: Informatique / Internet.
Définition: 1. Appliquette envoyée par un serveur de la toile mondiale à un utilisateur, parfois à l'insu de celui-ci, au cours d'une connexion, afin de caractériser cet utilisateur.
2. Par extension, information que l'appliquette peut enregistrer sur le disque de l'utilisateur et à laquelle le serveur peut accéder ultérieurement.
Note: Dans cette acception, on dit aussi « mouchard » (n.m.).
Voir aussi: appliquette, toile d'araignée mondiale.
Équivalent étranger: cookie.

toile d'araignée mondiale ou, ellipt, **toile mondiale**, **toile** n.f. sg.
Abréviation: TAM.
Domaine: Informatique / Internet.
Définition: Dans l'internet, système, réparti géographiquement et structurellement, de publication et de consultation de documents faisant appel aux techniques de l'hypertexte.
Voir aussi: hypertexte, internet.
Equivalent étrange : cookie

visionneur n.m.
Domaine: Informatique / Internet.
Définition: Logiciel permettant d'afficher un document sans disposer du logiciel qui a servi à le produire.
Equivalent étranger: viewer.

Tables d'équivalence

Terme étranger

access provider
Domaine : Télécommunications / Internet.
Equivalent français : fournisseur d'accès.

applet
*Domaine :*Informatique / Internet.
Equivalent français : appliquette, n.f.

asymetric (bis rate) digital subscriber line (ADSL)
Domaine : Télécommunications / Réseaux – Internet.
Equivalent français : dorsale, nf.

bookmark
Domaine : Informatique / Internet.
Equivalent français : signet, n.m.

browser
Domaine : Informatique / Internet.
Equivalent français : logiciel de navigation, navigateur, n.m.

chat
Domaine : Informatique / Internet.
Equivalent français : causette. n.f.fam.

cookie
Domaine : Informatique / Internet.
Equivalent français : témoin (de connexion), mouchard, n.m.

cracker
Domaine : Informatique / Internet.
Equivalent français : pirate, n.m.

cybernaut
Domaine : Télécommunications / Réseaux / Internet.
Equivalent français : internaute, n.

Digital Versatile Disk (DVD)
Domaine : Informatique
Equivalent français : disque numérique polyvalent

domain
Domaine : Télécommunications / Internet
Equivalent français : domaine, n.m.

domain name system (DNS)
Domaine : Télécommunications / Internet
Equivalent français : système d'adressage par domaines, annuaire des domaines

drag *and* drop
Domaine : Informatique / Internet
Equivalent français : glisser-déposer *n.m.*
emoticon
Domaine : Informatique / Internet
Equivalent français : frimousse n.f. fam.

extranet
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : extranet, nf.

firewall
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : barrière de sécurité, pare-feu, n.m.

frame
Domaine : Informatique / Internet
Equivalent français : cadre n.m.

frequently asked questions (file) (FAQ)
Domaine : Télécommunications / Internet
Equivalent français : foire aux questions, FAQ, fichier des questions courantes, questions courantes

gateway
Domaine : Télécommunications / Internet
Equivalent français : passerelle n.f.

hacker
Domaine : Informatique / Internet
Equivalent français : fouineur, n.m.

hotlist
*Domaine :*Informatique / Internet
Equivalent français : liste de signets

homepage
Domaine : Informatique / Internet
Equivalent français : page d'accueil

hub
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : concentrateur, n.m.

hypertext
Domaine : Informatique / Internet
Equivalent français : hypertext, n.m ; hypertextuel, adj.

infobahn (all)
Domaine : Télécommunications / Réseaux / Internet

Equivalent français : autoroutes de l'information

information high-way
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : autoroutes de l'information

information superhighway
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : autoroutes de l'information

Internet network
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : internet, n.m. sq.

Intranet
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : intranet, n.m.

middleware
Domaine : Informatique
Equivalent français : logiciel médiateur.

Net
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : internet, n.m. sq.

netcasting
Domaine : Télécommunications / Internet
Equivalent français : diffusion systématique sur la toile, diffusion réticulaire systématique, diffusion réticulaire

newsgroup
Domaine : Informatique / Internet
Equivalent français : forum, n.m.

news article
Domaine : Télécommunications / Internet
Equivalent français : article de forum, contribution, n.f.

new item
Domaine : Télécommunications / Internet
Equivalent français : article de forum, contribution, n.f.

news posting
Domaine : Télécommunications / Internet
Equivalent français : article de forum, contribution, n.f.

on-line data service
Domaine : Informatique
Equivalent français : serveur, n.m.

plug-in

Domaine : Informatique / Internet
Equivalent français : module d'extension.

proxy server, proxy
Domaine : Télécommunications / Réseaux / Internet
Equivalent français : serveur mandataire, mandataire, n.m.

pull technology
Domaine : Télécommunications / Internet
Equivalent français : recherche individuelle.

push technology
Domaine : Télécommunications / Internet
Equivalent français : distribution sélective, diffusion sélective, distribution personnalisée.

server
Domaine : Informatique
Equivalent français : serveur, n.m.

smiley
Domaine : Informatique / Internet
Equivalent français : frimousse, n.f.fam.

thread
Domaine : Informatique / Internet
Equivalent français : fil (de la discussion)

uniform resource locator (URL)
Domaine : Télécommunications / Internet
Equivalent français : adresse universelle, adresse réticulaire.

universal resource locator (URL)
Domaine : Télécommunications / Internet
Equivalent français : adresse universelle, adresse réticulaire.

viewer
Domaine : Informatique / Internet
Equivalent français : visionneur, n.m.

webcasting
Domaine : Télécommunications / Internet
Equivalent français : diffusion systématique sur la toile, diffusion réticulaire systématique, diffusion sur la toile, diffusion réticulaire.

webmaster
Domaine : Télécommunications / Internet
Equivalent français : administrateur de site, de serveur.

webpage, web page
Domaine : Informatique / Internet
Equivalent français : page sur la toile.

website, web site
Domaine : Télécommunications / Internet
Equivalent français : site (de la toile, sur la toile)

window
Domaine : Informatique
Equivalent français : fenêtre, n.f.

World Wide Web
Domaine : Informatique / Internet
Equivalent français : toile d'araignée mondiale, toile, n.f.sg., TAM

Termes français

admnistrateur de site, de serveur
Domaine : Informatique / Internet
Equivalent étranger : wedmaster

adressage par domaines
Domaine : Télécommunications / Internet
Equivalent étranger : domain name system, DNS

adresse réticulaire
Domaine : Télécommunications / Internet
Equivalent étranger : uniform resource locator, universal resource locator, URL.

adresse universelle
Domaine : Télécommunications / Internet
Equivalent étranger : uniform resource locator, universal resource locator, URL

annuaire des domaines
Domaine : Télécommunications / Internet
Equivalent étranger : domain name system, DNS

appliquette, n.f.
Domaine : Informatique / Internet
Equivalent étranger : applet

article de forum
Domaine : Informatique / Internet
Equivalent étranger : news item, news posting, news article

autoroutes de l'information
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : information highway (ang.), information superhighway (ang.), Infobahn (all.).

barrière de sécurité
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : firewall

cadre, n.m.
Domaine : Informatique / Internet
Equivalent étranger : frame

causette, n.f. fam**.**
Domaine : Informatique / Internet
Equivalent étranger : chat

concentrateur, n.m.
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : hub

contribution, n.f.
Domaine : Informatique / Internet
Equivalent étranger : hub

diffusion réticulaire
Domaine : Télécommunications / Internet
Equivalent étranger : webcasting, netcasting

diffusion réticulaire systématique
Domaine : Télécommunications / Internet
Equivalent étranger : webcasting, netcasting

diffusion selective
Domaine : Télécommunications / Internet
Equivalent étranger : push technology

diffusion sur la toile
Domaine : Télécommunications / Internet
Equivalent étranger : webcasting, netcasting

diffusion systématique sur la toile
Domaine : Télécommunications / Internet
Equivalent étranger : webcasting, netcasting

disque numérique polyvalent
Domaine : Informatique
Equivalent étranger : Digital Versatile Disk, DVD.

distribution personnalisée
Domaine : Télécommunications / Internet
Equivalent étranger : push technology

distribution sélective
Domaine : Télécommunications / Internet
Equivalent étranger : push technology

domaine, n.m.
Domaine : Télécommunications / Internet
Equivalent étranger : domain

dorsale, n.f.
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : backbone

extension, n.f.
Domaine : Informatique / Internet
Equivalent étranger : plug-in

extranet, n.f.
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : extranet

FAQ
Domaine : Télécommunications / Internet
Equivalent étranger : frequently asked questions (file), FAQ

fenêtre
Domaine : Informatique
Equivalent étranger : window

fichier des questions courantes
Domaine : Télécommunications / Internet
Equivalent étranger : frequently asked questions (file), FAQ

fil (de la discussion)
Domaine : Informatique / Internet
Equivalent étranger : thread

foire aux questions
Domaine : Télécommunications / Internet
Equivalent étranger : frequently asked questions (file), FAQ

forum, n.m.
Domaine : Informatique / Internet
Equivalent étranger : newsgroup

fouineur, n.m.
Domaine : Informatique / Internet
Equivalent étranger : hacker

fournisseur d'accès
Domaine : Télécommunications / Internet
Equivalent étranger : access provider

frimousse, n.f.fam
Domaine : Informatique / Internet
Equivalent étranger : emoticon, smiley

glisser-déposer, n.m.
Domaine : Informatique / Internet
Equivalent étranger : drag and drop

hypertext, n.m.
Domaine : Informatique / Internet
Equivalent étranger : hypertext

hypertextuel adj.
Domaine : Informatique / Internet
Equivalent étranger : hypertext

internaute, n.
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : cybernaut

internet, n.m.sg.
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : Internet, network, Internet, Net

intranet, n.m.
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : intranet

liaison numérique à débit asymétrique
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : asymetric (bit rate) digital subscriber line, ADSL

liste de signets
Domaine : Informatique / Internet
Equivalent étranger : hotlist

logiciel de navigation
Domaine : Informatique / Internet
Equivalent étranger : browser

logiciel médiateur
Domaine : Informatique
Equivalent étranger : middleware

mandataire, n.m.
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : proxy server, proxy

module d'extension
Domaine : Informatique / Internet
Equivalent étranger : plug-in

mouchard, n.m.
Domaine : Informatique / Internet
Equivalent étranger : cookie

navigateur, n.m.
Domaine : Informatique / Internet
Equivalent étranger : browser

page d'acceuil
Domaine : Informatique / Internet
Equivalent étranger : home page

page sur la toile
Domaine : Informatique / Internet
Equivalent étranger : webpage, web page

pare-feu, n.m.
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : firewall

passerelle, n.f.
Domaine : Télécommunications / Internet
Equivalent étranger : gateway

pirate, n.m.
Domaine : Informatique / Internet
Equivalent étranger : cracker

questions courantes
Domaine : Télécommunications / Internet
Equivalent étranger : frequently asked questions (file), FAQ

raccordement numérique asymétrique, RNA
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : asymetric (bit rate) digital sudscriber line, ADSL

recherche individuelle
Domaine : Télécommunications / Internet
Equivalent étranger : pull technology

serveur, n.m.
Domaine : Informatique
Equivalent étranger : server, on-line data service

serveur mandataire
Domaine : Télécommunications / Réseaux / Internet
Equivalent étranger : proxy server, proxy

signet, n.m.
Domaine : Informatique / Internet
Equivalent étranger : bookmark

site (de la toile, sur la toile)
Domaine : Télécommunications / Internet
Equivalent étranger : wedsite, wed site

système d'adressage par domaines
Domaine : Télécommunications / Internet
Equivalent étranger : domain name system, DNS

témoin (de connexion)
Domaine : Informatique / Internet
Equivalent étranger : cookie

toile, n.f. sg.
Domaine : Informatique / Internet
Equivalent étranger : World Wide Web

toile d'araignée mondiale (TAM)
Domaine : Informatique / Internet
Equivalent étranger : World Wide Web

toile mondiale
Domaine : Informatique / Internet
Equivalent étranger : World Wide Web

visionneur, n.m.
Domaine : Informatique / Internet
Equivalent étranger : viewer

Annexe no 2
La réglementation française en matière de cryptologie

Législation française

Décrets du 31 juillet 2001
Décret de création de la Direction centrale de la sécurité des systèmes d'information (DCSSI), décret de création de la Commission interministérielle pour la sécurité des systèmes d'information.

Recommandation n° 901 du 2 mars 1994
Recommandations pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.

Recommandation n° 600 de mars 1993
Protection des informations sensibles ne relevant pas du secret de défense
Recommandations pour les postes de travail informatiques

Recommandation n°400 du 18 octobre 1991 d'installation des sites et systèmes traitant des informations sensibles ne relevant pas du secret de défense

Le décret n°2002-535 du 18 avril 2002, relatif au schéma d'évaluation et de certification vient renforcer les bases juridiques du schéma français qui reposait jusqu'ici sur un avis du Premier ministre de 1995 ; il complète également le décret de signature électronique du 31 mars 2001, en fixant les règles de certification des procédés de signature.

L'arrêté du ministre de l'économie, des finances et de l'industrie relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation, annoncé dans le décret relatif à la signature électronique du 31 mars 2002 a été signé le 31 mai 2002, JO 132 du 8 juin 2002.

Article 28 de la loi sur la réglementation des télécommunications 90-1170 du 29 12 90, modifiée par la loi 91-648 du 11 juillet 1991, modifiée par la loi 96-659 du 26 juillet 1996

Décret n°98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, J.O. du 25 Février 1998 page 2911, modifié par le décret n°2002-688 du 2 mai 2002, JO du 3 Mai 2002 page 8055

Décret n°99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation, J.O. Numéro 66 du 19 Mars 1999 page 4050.

Décret n°99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable, J.O. Numéro 66 du 19 Mars 1999 page 4051.

Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie, J.O. Numéro 66 du 19 mars 1999 page 4052.

Arrêté du 13 mars 1998 définissant le modèle de notification préalable par le fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis à autorisation, J.O. du 15 mars 1998 page 3888.

Décret n°98-102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, J.O. du 25 février 1998 page 2915.

Arrêté du 13 mars 1998 définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie, J.O. du 15 mars 1998 page 3888.

Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes, J.O. du 15 mars 1998 page 3888.

Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes, J.O. du 15 mars 1998 page 3891.

Arrêté du 13 mars 1998 fixant le tarif forfaitaire pour la mise en œuvre des conventions secrètes au profit des autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, J.O. du 15 mars 1998 page 3891.

Décret 2001-1192 du 13 décembre 2001, relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage, J.O. du 15 décembre 2001, page 19905.

Arrêté du 13 décembre 2001, relatif au contrôle à l'exportation vers les pays tiers et au transfert vers les États membres de la Communauté européenne de biens et technologies à double usage, J.O. du 15 décembre 2001, page 19911.

Arrêté du 13 décembre 2001, relatif à la délivrance d'un certificat international d'importation et d'un certificat de vérification de livraison pour l'importation de biens et technologies à double usage, J.O. du 15 décembre 2001, page 19914.

Législation communautaire

Règlement (CE) n°1334/2000 du Conseil du 22 juin 2000, instituant un régime communautaire de contrôle des exportations de biens et technologies à double usage, JOCE L 159 du 30 juin 2000, p. 1.

Règlement (CE) n° 2889/2000 du Conseil du 22 décembre 2000, modifiant le règlement (CE) n°1334/2000 en ce qui concerne l'exportation et les transferts intracommunautaires des biens et technologies à double usage, JOCE n° L 336 du 30 décembre 2000, p. 14.

Action commune du Conseil du 22 juin 2000 relative au contrôle de l'assistance technique liée à certaines destinations finales militaires.

Décision du Conseil du 22 juin 2000 abrogeant la décision 94/942/PESC relative à l'action commune concernant le contrôle des exportations de biens à double usage.

INDEX

(renvoi aux numéros de paragraphes)

Table des matières