Université Montpellier I

Faculté de Droit, des Sciences Économiques et de Gestion
Institut de Recherche et d'Étude pour le Traitement de l'Information Juridique

Droit de la cryptographie : une approche pour la protection des informations sur l'internet

Mémoire de D.E.A Informatique et Droit

Sous la direction de M. le professeur J. FRAYSSINET

Par Yannick Spegels et Hughes-Jehan Vibert

Formation doctorale : Informatique et Droit
Équipe de Recherche Informatique et Droit (E.A 718)
Section du CNU : 01 Droit privé et sciences criminelles.
71 Science de l'information et de la communication.

Université de Montpellier 1
IRETIJ
39 rue de l'université 34060 Montpellier CEDEX

Nous tenons à remercier Monsieur le professeur Jean Frayssinet de l'Université d'Aix en Provence pour avoir accepté d'être le directeur de notre mémoire, ainsi que pour ses conseils.

Nous remercions également Monsieur le professeur Michel Bibent de l'Université Montpellier I ainsi que tous les enseignants et chargés de cours pour l'excellente année que nous avons passé dans le cadre du DEA Informatique et Droit de la faculté de droit de Montpellier

Monsieur le Professeur Daniel Poulin de l'Université de Montréal nous a donné des conseils bibliographiques et nous l'en remercions vivement en regrettant de ne pas avoir pu le rencontrer à Montréal.

Nous avons une pensée particulière pour Romaric et Nicolas qui nous ont gentiment permis de bénéficier de leurs connexions à l'internet.

Nous remercions Quicklaw system Inc. pour nous avoir permis d'utiliser ses bases de données juridiques au Canada ainsi que celles de Westlaw pour les États-Unis

Enfin, merci à l'Université du Québec À Montréal et à sa Faculté de droit pour la formation dispensée par ses différents enseignants, notamment en informatique juridique.

À Sophie

Table des matières

Rien n’est plus digne d’un capitaine que de savoir deviner les desseins de l’ennemi.

Machiavel,
Discours sur la première décade de Tite-Live
Livre troisième, chapitre XVIII

Chapitre introductif

Au nom de la raison d'État, Machiavel préconisait tout un arsenal de recettes utiles au Prince pour que ce dernier se préserve et par là même préserve sa principauté. Les conspirations intérieures, les guerres furent autant de faits menaçant la permanence de l'État et ce, quelque soit son statut. Tout naturellement, les démocraties comme les dictatures ont alors développés un arsenal pour se préserver. Se préserver pour elles mêmes, contre les autres, contre les menaces intérieures et extérieures. Le secret est devenu ainsi la clé de voûte de tout un arsenal militaire et administratif. Le secret est donc un enjeu pour les uns et un obstacle pour les autres : un obstacle qu'il s'agira, pour ces derniers, de renverser pour une stratégie qui restera toujours la même : s'assurer un monopole, quelqu'il soit (savoir, pouvoir, religion).

Dès que les échanges d'information apparurent, le cryptage est devenu le plus sûr moyen de s'assurer du secret entre deux personnes ou deux groupes de personnes, contre les tiers. Notre sujet est relatif à la cryptologie, du grec *kryptos* (caché) et *logos* (science), ce terme peut être assimilé à « la science du secret »[1] ou à l'art de coder un message de façon à le rendre incompréhensible sauf pour son destinataire. Si ce mémoire traitera de la cryptologie sous le prisme d'une réflexion juridique, il sera nécessaire de donner dans cette introduction une large part à une étude historique et contemporaine de la cryptographie (du grec *graphein*, écrire), de ces écritures secrètes qui sont à la base de cette cryptologie dont l'actualité souligne l'importance. Cette étude faite, il sera également utile de décrire les moyens de cryptographie moderne afin de pouvoir donner au lecteur tous les éléments pour saisir l'aspect juridique de la cryptologie. La science du secret est aussi un domaine modulable selon les objectifs à atteindre, d'ailleurs pour Bruce Schneier,

> *« il existe deux types de cryptographie dans le monde : la cryptographie qui empêche votre petite sœur de lire vos fichiers, et la cryptographie qui empêche les principaux gouvernements de lire vos fichiers »*[2]

[1] STERN, Jacques, *La science du secret*, Paris, Éditions Odile Jacob, 1998, 204 pages

[2] SCHNEIER, Bruce, *Applied Cryptography*, New York, 2nd Ed., John Wiley & sons Inc., 1998
VIENNOT, Laurent, (trad.), *Cryptographie appliquée*, Paris, 2ème Éd., International Thomson Publishing France, 1997, 846 pages pour l'édition francophone.

En effet, quelque soient les moyens utilisés, c'est l'objectif de secret qui donne à la cryptographie tout son sens, la personne devant rester dans l'ignorance importe peut. Il existe de multiples moyens pour s'assurer du secret. Les chuchotements, les gestes, une connaissance des langues étrangères, ou même les « sanglots longs… » de la BBC avant le débarquement Alliés en Normandie, sont autant de moyens qui nous éloignent de l'image du cryptanalyste qui décortique péniblement une masse de documentation illisible. Et pourtant nous sommes bien devant une succession de faits, volontaires ou non, qui rendent l'information opaque à ceux qui en écoute la représentation « cryptée ».

Pour revenir à notre propos, et selon l'encyclopédie Universalis,

> *« Tout système de cryptage est composé d'un algorithme de codage plus ou moins compliqué utilisant ou non une ou plusieurs clés de sécurité et il est, en principe, conçu de manière à être inviolable. En fait, un code peut être " cassé " soit par la technique d'essai et erreur en se laissant guider par certaines caractéristiques du message codé, soit en tentant de retrouver l'algorithme et/ou les clés utilisés pour le codage. Pour casser un code, un très grand nombre de tentatives doivent être effectuées et, depuis l'utilisation d'ordinateurs par les casseurs de code, on peut dire qu'aucun code n'est inviolable, sauf à nécessiter un nombre de tentatives tel que le plus puissant des ordinateurs mettrait plusieurs centaines ou plusieurs milliers d'années à les réaliser. »*

Bref, la cryptologie est un jeux qui se joue à deux.

Nous verrons dans ce chapitre introductif la cryptologie sous une approche historique (Section I) pour traiter ensuite d'une approche moderne, une approche « computerisée » (Section II)

Section I : La cryptographie : une approche historique[3]

Historiquement la cryptographie peut s'appréhender de plusieurs façon. En effet nous sommes passé d'une cryptographie tenant aux divinités à une cryptographie tenant aux intérêts personnels et, plus tard étatiques; mais nous sommes également passés d'une cryptographie mécanique à une cryptographie mathématique, ces éléments se combinant parfois. Cela dit, nous respecterons des règles chronologiques classiques quand à l'approche des sciences et techniques, nous séparerons cette historique à la fin de moyen âge pour voir que nous sommes passé d'une cryptologie rudimentaire (I), à une cryptologie plus élaborée (II)

I - D'une cryptographie rudimentaire…

Des éléments pouvant se rapporter à la cryptologie se retrouvent au cours de toute l'histoire de l'humanité. L'art d'interpréter les mystères, et donc de décrypter le sens donné à tel ou tel événement fantastique est le fondement de toutes les religions ayant accompagné l'être humain dans son évolution. Cette évolution à finalement conduit, les États naissant à développer leurs propres mystères pour leur sécurité, une sécurité parfois assurée par l'agression. Nous passerons donc chronologiquement d'une cryptographie naissante (A) à une cryptographie appliquée

A- <u>Cryptographie naissante</u>

Il ne semblerait pas absurde de faire remonter la cryptographie à l'ère des hiéroglyphes dont certains furent utilisés sur des tombeaux alors que parfaitement inusités. Car le hiéroglyphe à également un aspect symbolique, et le sens donné à certain signe nous échappe mais, semble t'il échappait également aux contemporains de ceux qui marquaient ainsi les pierres. Nous entrons ainsi dans la phase mystique de la cryptologie. Le secret est en effet mystérieux et les religions se nourrissent de mystère. La boucle est ainsi bouclée.

[3] Pour une approche historique complète voir KAHN, David, *La guerre des codes secrets*, Paris InterÉditions, 1980

Il n'est donc pas surprenant de voir certains moyens de cryptographie repris dans la Bible, ainsi la substitution qui par un système hébraïque traditionnel (le Atbash), permet de remplacer chaque lettre le l'alphabet par celle qui est dans le même ordre si l'on récite l'alphabet à l'envers (a=z, b=y, etc.), SHESHAK devenant ainsi BABEL.

Dans la Chine antique ont avait recours à la stéganographie qui vise à dissimuler le message secret. Les Chinois recouvraient de cire des messages que le porteur dissimulait sur lui ou avalait. Ce procédé se retrouvait également en Grèce où l'on pouvait tout aussi ingénieusement cacher l'existence d'un message en tondant un héraut sur le crâne duquel on tatouait l'information. Une fois la repousse des cheveux faite, une seconde « tonte » était nécessaire pour que le destinataire du message soit informé. Les encres sympathiques furent également un autre moyen de dissimulation du message qu'il est inutile de détailler ici.

B- Cryptographie appliquée

C'est sans doute à Sparte que l'on doit la première utilisation militaire[4] de la cryptographie grâce à la scytale. Ce système consistait en un axe de bois autour duquel on enroulait, de façon à le recouvrir, un ruban. Le texte était écrit dans la hauteur de l'axe sur le ruban qui était ensuite déroulé tel quel par le destinataire. Ce dernier réenroulait la bande sur un bâton de même diamètre que le premier et le message se reformait. Que le bâton soit trop large ou trop étroit et le message devenait illisible. En d'autre terme, cette scytale est une clé sans laquelle il est impossible de déchiffrer un message, une clé à la disposition des généraux et haut magistrats : nous sommes au cinquième siècle avant Jésus-Christ et cette cryptographie rudimentaire est déjà un symbole de pouvoir.

Jules César utilisait quant à lui un procédé de substitution rudimentaire : chaque lettre de l'alphabet était décalée de 3 caractères par rapport à l'alphabet. Il s'agit ici d'un système simple qui s'apparente à nos cryptages modernes dans le sens où

> *« [cette substitution] traite un message sous forme symbolique, c'est à dire comme une suite de lettres, et qu'elle défini une transformation sur ces lettres, que l'on nomme un chiffrement »*[5]

[4] Nous développerons cet aspect militaire dans la partie consacrée à la raison d'État (I)
[5] STERN, Jacques, *La science du secret*, Paris, Éditions Odile Jacob, 1998, page 25

II - …à une cryptographie plus élaborée

La cryptologie est une science qui respecte son temps, c'est donc tout naturellement que la fin du moyen-âge annonça l'arrivée d'une cryptographie entrant dans l'ère de la modernité. On pourra remarquer que cette modernité fut d'abord le fait d'individus alors que les initiatives de l'époque contemporaine proviennent plutôt des États. Le caractère stratégique de la cryptographie ne fut pourtant jamais ignoré, c'est en fait l'accélération des progrès techniques appliqués à la guerre qui suscita ce développement, littéralement exponentiel en puissance, de la cryptographie, un développent suivant les mêmes règles que celui de l'armement. C'est donc toujours avec la même approche chronologique que nous aborderons la période de la modernité naissante (A), pour voir ensuite celle de la modernité en marche (B)

A- La modernité naissante

Jusqu'au moyen âge l'intérêt pour la cryptographie n'évolua pas et finalement, c'est avec une certain respect pour l'air du temps qu'en 1477 un italien, Leon Batista Alberti, fit évoluer la science des écritures secrètes en inventant la substitution polyalphabétique, procédé permettant la correspondance de nombreux alphabets cryptés en un seul clair.

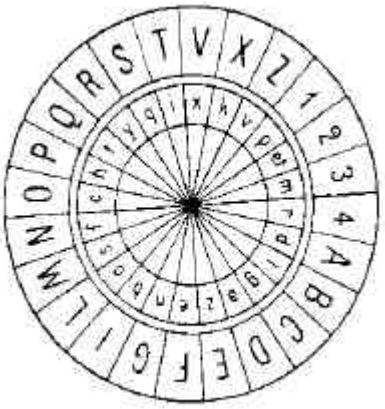

figure 1 : Le cadrant chiffrant d'Alberti

Le procédé consiste à utiliser 2 disques : l'un est mobile l'autre étant fixe. L'utilisateur à recours à une lettre indice prise dans le cercle interne mobile (ici x=v), il suffit de faire communiquer les autre lettres entre elles. Il faut convenir d'une lettre indice dans le cercle interne, k, avec le correspondant puis l'on peut débuter le cryptogramme par la lettre de

l'anneau placée en face de la lettre indice. Mais là où Alberti engage la cryptographie sur la voie de la complexité, est quand il écrit : « Après avoir écrit 3 ou 4 mots, je peux changer la position de la lettre indice en tournant le disque de façon que k soit, par exemple, sous le D. Donc dans un message, j'écrirai un D majuscule et à partir de ce point k ne signifiera plus B mais D et toutes les lettres du disque fixe auront de nouveaux équivalents. »

> *« Alberti ira plus loin quand il complétera]sa découverte par une autre invention déterminante dans l'histoire de la cryptologie : le surchiffrement codique. En effet il constitua un répertoire de 336 groupes de mots représentés par toutes les combinaisons allant de 11 à 4444. Mais le génie d'Alberti était trop en avance sur son temps et ce n'est que 400 ans plus tard que les puissances mondiales utiliseront ce procédé de surchiffrement codique mais bien plus simplement. »*[6]

Les procédés cryptographiques évoluèrent pour arriver deux siècles plus tard à faire de la cryptologie une science de mathématiciens…

B- La modernité en marche

C'est un mathématicien milanais, Jérôme Cardant, qui le premier, développa au XVIème siècle, l'idée du système de l'autoclave qui consiste à considérer le message en lui même comme la clé. On pourrait également traiter de la substitution polyalphabétique mais il sera plus intéressant de se référer directement à l'ouvrage de David Kahn[7] et, de la même façon, nous ferons un bond chronologique jusqu'à notre siècle puisque le réel développement de la cryptologie est venu avec le nécessaire traitement de donnés à transmettre en quantité…industrielles : comme toutes les sciences, la cryptologie est étroitement liée à l'air du temps.

L'entrée dans la modernité s'est développée de façon remarquable à l'issue des deux conflits mondiaux. Chaque guerre apportant les enseignements nécessaires pour préparer la suivante. Ainsi la célèbre machine Enigma fut utilisée (et cassée) lors de la seconde guerre mondiale et préparée à l'issue de la première. La chance fut dans le camps de alliée puisqu'avant de saborder un sous-marin allemand quasiment détruit, les anglais eurent la présence d'esprit de le visiter. Un exemplaire de la machine secrète fut trouvé facilitant ainsi le décryptage des communications allemandes.

[6] MARIE, Fabrice, *Histoire de la cryptologie*, http://wwwmutimania.com/marief

La machine Enigma ressemble à une machine à écrire et fonctionne sur le principe du rotor où 26 contacts apparaissent sur la face interne et sur la face externe et sont reliées les uns aux autres, elle est de plus composée de 3 rotor choisis parmi 5 ce qui permettait de développer un cryptage de plus d'un millions de combinaisons. Le décryptage consistant à utiliser un cheminement inverse.

Figure 2 : La machine Enigma

La guerre froide à développé tous ces systèmes mécaniques et l'informatique militaire à amélioré les possibilités et la rapidité des outils de cryptographie.

[7] KAHN, David, op. cit.

Section II - La cryptographie : une approche « computerisée »[8]

« Computerisée » c'est à dire (vous excuserez l'anglicisme) que le cryptage ne peut plus désormais se passer d'une utilisation de la puissance et rapidité de calcul des ordinateurs. Nous sommes entré, dans cette matière aussi, dans un domaine qui dépasse les capacité d'analyse de l'être humain. La numérisation, en transformant toutes les informations (textes, images, sons) en 1 et en 0 permet de rationaliser la cryptographie en donnant le même outils pour toutes les sortes de communication. Deux systèmes de cryptage constituent la base de la cryptologie moderne les cryptographies symétriques et asymétriques visent à un échange de clés.

Les clés de chiffrement sont basées sur la difficulté de factoriser des grands nombres, il est donc logique de voir ici que plus la clé est longue, plus le décryptage devient complexe. Nous allons détailler ces notions grâce aux deux grands systèmes de cryptage : il s'agit des systèmes de cryptage symétrique (I) et de type asymétrique (II). Différents, ces deux systèmes peuvent néanmoins être complémentaires, il s'agit à présent de les étudier.

I- Le cryptage symétrique

Deux exemples servirons à décrire cette forme de cryptage, ils obéissent d'ailleurs aux mêmes règles mais offrent des garanties de sécurité différentes. Nous verrons ainsi successivement le DES (A) et l'IDEA (A)

A- DES (Data Encryption Standard)

Nous sommes au début des années 1970, à cette époque seule la cryptographie militaire à droit à des budgets conséquents. Cela dit pour des raisons de… secret, rien ne transparaissait et la cryptographie était un espace protégé. L'Agence nationale de sécurité américaine (NSA pour National Securiy Agency) n'existait même pas pour le public, cet organisme n'avait donc

[8] En plus d'autre sources, l'ouvrage de référence sera ici sans conteste celui de Schneier qui à l'avantage d'être assez accessible pour celles et ceux qui ne sont pas mathématiciens :
SCHNEIER, Bruce, *Applied Cryptography*, New York, 2nd Ed., John Wiley & sons Inc., 1998
VIENNOT, Laurent, (trad.), *Cryptographie appliquée*, Paris, 2ème Éd., International Thomson Publishing France, 1997, 846 pages pour l'édition francophone.

aucune existence officielle. La cryptographie non militaire était quant à elle éparpillée, il n'existait aucune norme ou quasi norme dans ce domaine et, surtout, aucune garantie quant à la réelle sécurité de ces procédés cryptographique. Selon un rapport du gouvernement des États-Unis,

> *« Les implications profondes du lien entre les différentes variantes de mécanismes de clefs, ainsi que les principes de fonctionnement et la force réelle des équipements de chiffrement et déchiffrement étaient, et sont encore, virtuellement inconnus de presque tous les acheteurs, et il est très difficile de faire des choix bien informés quant au type d'équipement –en ligne, hors ligne, génération de clef, etc.- qui satisfassent les besoins en sécurité des acheteurs. »*[9]

Il fut donc lancé un appel d'offre pour développer un algorithme standard de cryptographie unique, susceptible de protéger les données numérisées tant lors de leurs transmissions que lors de leurs stockages. Les conditions pour valider un tel standard devaient être un haut niveau de sécurité, une facilité d'utilisation, disponible à tous les utilisateurs, une sécurité dépendant de la clé, adaptabilité à diverses application (messageries, transferts financiers…), efficacité, exportabilité, rentable économiquement.

C'est finalement IBM qui fut chargé du développement du DES par la NSA et le DES fut adopté au niveau fédéral le 23 novembre 1976. Le DES est un système de cryptographie symétrique à clé secrète unique. Cette même clé permet à la fois de crypter et de décrypter un message.

Pour donner une brève description technique, le DES permet de découper un message en tranches traités séparément. Contrairement à un système de type Enigma, l'intérêt est que le programme de chiffrement n'est pas secret, l'outil importe peu car c'est de la clé que dépend le secret (et nous nous rapprochons finalement du système de la scytale lacédémonienne dont le secret dépendait du bâton utilisé). La confidentialité de ce système repose sur « l'utilisation d'une clé secrète de 64 bits dont 56 sont utilisés lors de nombreuses opérations de manipulation de données . […Le DES opère d'abord un découpage du texte clair en segments de 64 bits]. À l'intérieur de ce segment, il permute les 32 premiers bits avec les 32 suivants » [10], suivent alors de multiples permutations qui rendent le décryptage impossible.

---

[9] DAVIS, R.M., « The Data Encryption Standard in perspective », *Computer Security and the Data Encryption Standar. National Bureau of Standards* , Washington DC, fevrier 1978. Special publication 500-27, cité par Schneier page 282.

[10] Voir Pirate mag, hors série n°1, juillet 1999, p.17

Le DES est capable de résister à la plupart des attaques et en 1993 on estimait à un coût de un millions de dollars US le développement d'un ordinateur capable de casser la clé DES en 3 heures et demi. Le coût d'un tel système est donc prohibitif et ne rend le décryptage possible qu'aux États ou aux grandes compagnies.

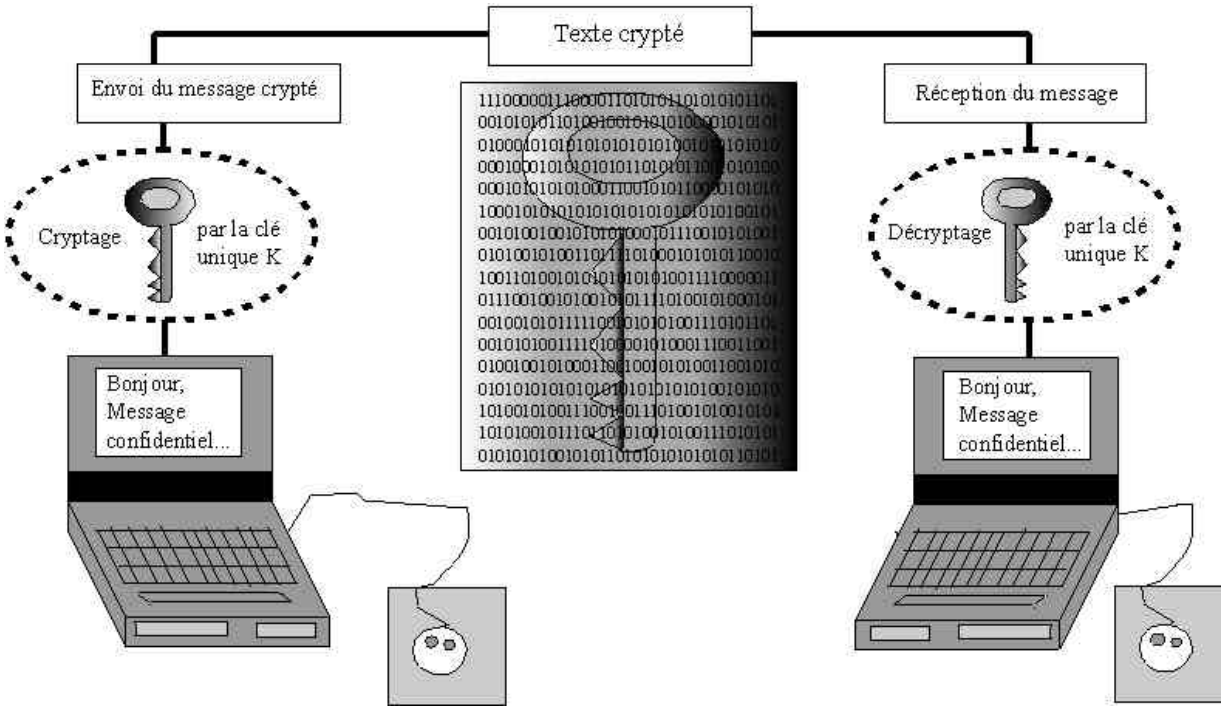

figure 3 : le système DES

Reste qu'il faut s'interroger sur la fiabilité du DES de nos jours. Des rumeurs persistent à affirmer que la NSA aurait caché une brèche secrète dans l'algorithme. Peut-être… Cela dit, selon des estimations de 1997[11], s'il fallait trois millions de dollars américains pour casser le DES en 1993, les coûts sont divisés par 5 tous les 10 ans. À cela s'ajoute la rapidité croissante des ordinateurs qui permettront rapidement de casser la protection des documents; enfin la possibilité de mettre les ordinateurs en réseaux permettent d'améliorer encore ce résultat. Il n'en demeure pas moins que le DES est une « assez bonne protection » contre les individus et

[11] SCHNEIER, Bruce, op. cit., p 318

compagnies au budget plus modestes. Enfin, il est toujours possible de démultiplier les algorithmes.

En effet, la solution du triple DES semble satisfaisante, il s'agit de chiffrer chaque bloc du message sous 2 (deux) clés différentes de 56 bits : « on chiffre par la première, applique le déchiffrement correspondant à la seconde, et chiffre de nouveau avec la clé initiale »[12]. Cela étant de grands problèmes demeures dans ce système à clé unique et ce quelque soit sa force:

- l'échange des clés est nécessaire comme préalable à toute communication sécurisée d'un secret
- Cet échange se démultiplie quant il s'agit de communiquer plusieurs secrets différents à plusieurs personnes différentes. Dans ce cas il y a un sérieux problème dans la gestion des clés, à moins de donner à tous la même clé au risque de tuer le secret, ce qui devient absurde.

Contre les attaques plus puissantes, il est généralement admis que le DES est périmé ou, tout au moins en voie de l'être. Pour Philip Zimmermann,

> *« Même les très bons logiciels, qui utilisent le DES dans le mode d'opération correct présentent encore des problèmes. Le standard DES utilise une clé de 56- bit, ce qui est trop petit pour les normes actuelles, et peut maintenant être aisément cassée par des recherches exhaustives de la clé sur des machines ultra rapides spéciales. Le DES a atteint la fin de sa vie utile, et voilà pourtant encore des logiciels qui y font appel. »*[13]

Les systèmes de cryptage asymétrique visent à régler ces problèmes, mais un algorithme comme IDEA règle avec efficacité l'obsolescence du DES

B- L'IDEA (International Data Encryption)

Si l'IDEA est beaucoup moins populaire que le DES ou le RSA, il n'en demeure pas moins qu'il semble être l'algorithme de cryptage le plus puissant et le plus sûr[14]. Son utilisation est d'ailleurs popularisée par PGP qui l'utilise dans sa fonction de chiffrement. Pour l'histoire il a été inventé en 1990 par Xuejia Lai et James Massey. Si l'on tarde pour remplacer le DES

[12] STERN, Jacques, op. cit., page 176
[13] ZIMMERMANN, Philip, *Mode d'emploi de PGP freeware version*, document pdf disponible à cette adresse, http://www.cl.cam.ac.uk/~fapp2/pgpenfrancais/doc.htm
[14] Tout au moins selon Bruce Schneier, op. cit. p 339

pour l'IDEA cela tient au fait qu'il soit breveté et nécessite une licence pour ses applications commerciales…
L'IDEA dispose d'une clé de 128 bits ce qui suppose 2^{128} chiffrements pour retrouver la clé[15] :

> *« Concevez une puce qui peut tester un milliard de clés par secondes et mettez en un milliard à la tâche, cela prendrait 10^{13} années, c'est plus que l'âge de l'univers. Une matrice de 10^{24} puces pourrait trouver la clé en un jour mais il n'y a pas assez d'atomes de silicium dans l'univers pour construire une telle machine. »*[16]

Il s'agit donc d'un des algorithmes les plus puissant qui soit. Il semble ainsi démontré que le cryptage s'approche d'une certaine perfection puisque le décryptage deviendrait impossible.

II- La cryptographie asymétrique (exemples du RSA et de PGP)

L'objectif ayant conduit au cryptage asymétrique est de régler le problème du transfert des clés. Nous l'avons vue implicitement plus haut : avec une même clé symétrique il est possible de déchiffrer et de déchiffrer. Aussi, Whitfield Diffie et Martin Hellman découvrirent une solution simple : en cryptologie l'intérêt d'est pas vraiment d'empêcher l'ennemi de chiffrer (encore que, nous le verrons, les limitations à l'exportation des algorithmes de chiffrement reviennent à cette solution); en fait l'intérêt de cryptage est seulement d'empêcher le seul déchiffrage. Nous détaillerons donc le système RSA qui reprend ce principe (A), pour voir ensuite le système PGP qui ne comprend pas seulement du chiffrement asymétrique mais qu'il fallait toutefois décrire puisqu'il semble constituer une norme de fait sur l'internet.

A- L'exemple du RSA

Le système RSA fut développé à l'origine après que ses auteurs s'aperçurent qu'ils n'arriveraient pas à démontrer l'infaillibilité de la théorie de Diffie et Hellman… Le cryptage asymétrique RSA (des professeurs Rivest, Shamir et Adelman) fonctionne sur le principe de factorisation d'entiers par des entiers premiers (divisibles uniquement par 1 et eux-mêmes). Globalement le système de cryptage du RSA repose sur un postulat simple : s'il est facile de déterminer que 52 X 84 = 4368, il devient complexe de déterminer quels nombres aboutissent à

[15] à peut près 340 282 366 920 938 463 463 374 607 431 770 000 000 de chiffrements…

[16] SCHNEIER, Bruce, op. cit., p. 342

ce résultat, qui plus est en factorisant des nombre premiers difficiles à retrouver dans le cas de grand nombres… Pour la description technique il serait utile encore une fois de consulter les documentations pertinentes[17]. Nous décrirons par contre concrètement le fonctionnement de ce système…

Alice[18] désire communiquer avec Robert. Pour que leurs correspondances soient cryptées, elle informe Robert de l'existence d'une clé publique grâce à laquelle Robert pourra crypter son message. Alice recevra le message crypté par la clé publique et le décryptera grâce à sa clé privée qui reste, quant à elle, confidentielle.

Le système fonctionne donc avec 2 clés complémentaires :

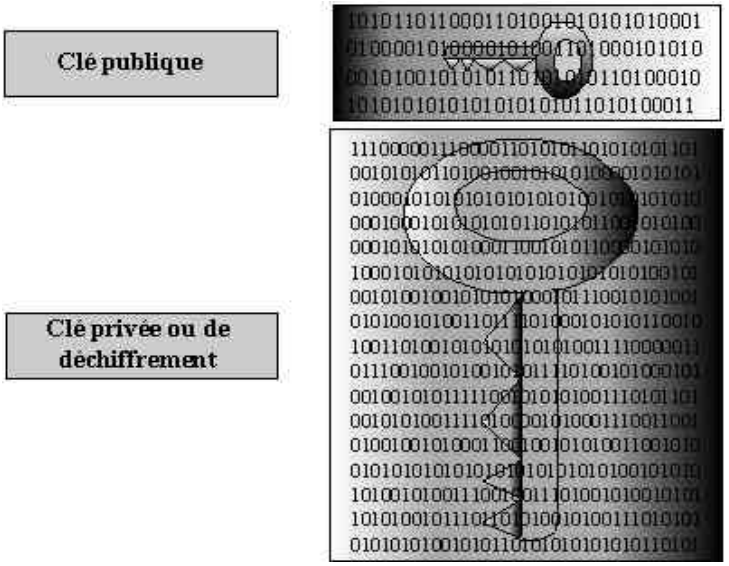

Figure 4 : le système des clés RSA

Le procédé reste confidentiel car la seule utilité de cette clé est de crypter un message. Une fois en possession de la clé publique Robert n'a plus qu'à l'utiliser pour transmettre un message (figure 5) et, si possible, en profiter pour y insérer sa propre clé publique pour qu'Alice puisse lui répondre à son tour en toute confidentialité :

[17] SCHNEIER, Bruce, op. cit., p. 491, ou encore Pirate Mag, Hors-Série n°1, juillet 1999 qui reprend les mêmes explications pour seulement 12 francs

[18] Parmi tous les ouvrages consultés les prénoms Alice et Robert (ou Bob) reviennent systématiquement. Nous serons plus original la prochaine fois.

L'avantage du système utilisant des clés asymétriques réside dans le fait que la clé privée n'a pas besoin d'être connue par celui qui envoie un message. Il s'agit donc d'une sérieuse amélioration par rapport au système DES. Par contre ce système est lourd à gérer pour des fichiers de grande taille ,

> *« À titre de comparaison, installé sous forme de logiciel, le DES permet de réaliser des fonctions 100 fois plus rapidement que le logiciel RSA, alors que dans le cas du « hardware », le DES s'avère cette fois de 1000 à 10000 fois plus rapide. »*[19]

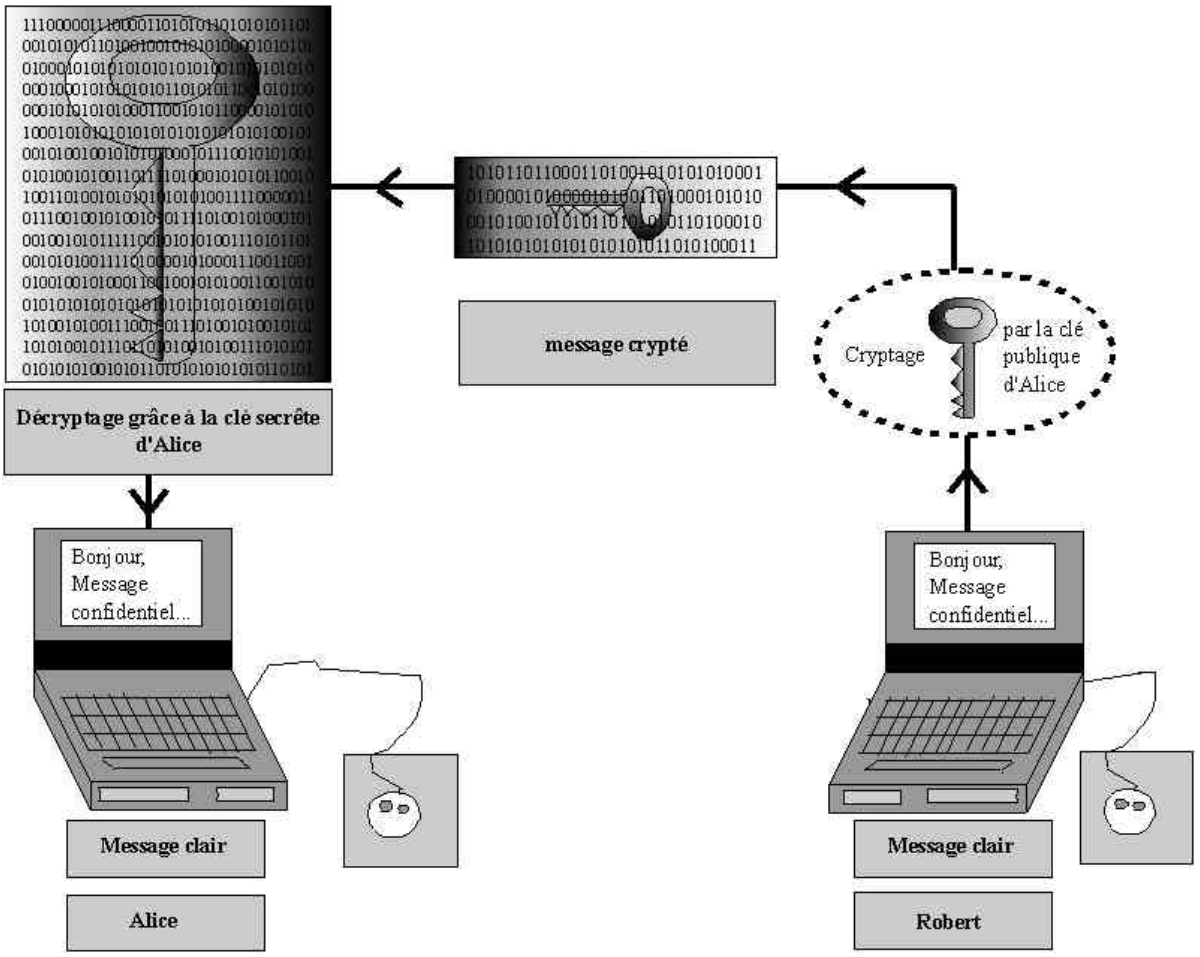

figure 5 : le système RSA

Devant ces lenteurs, la solution consisterait à utiliser conjointement les deux formats de protection. En effet, il peut être utile de combiner les avantages du RSA sur le secret des clefs et ceux du DES (ou triple DES) pour la rapidité d'exécution. Ainsi rien n'empêche de transférer une clé DES grâce au RSA et de crypter ensuite le message grâce à l'algorithme DES. Ce

[19] RSA, RSA, http://www.rsa.com/rsalabs/faq/faq_rsa.html, cité par Pierre Trudel : Trudel, Pierre et autres, Droit du cyberespace, Montréal, Éditions Thémis, 1997, chap. 19, page 20

système s'appelle « l'enveloppe numérique ». C'est d'ailleurs le type de système qu'utilise PGP en combinant l'IDEA avec le RSA.

Mais le système RSA permet également une authentification de l'expéditeur du message : si Alice décide de coder la signature de son message à l'aide d'un autre jeux de clés, elle sera la seule à pouvoir crypter des messages avec une clé de déchiffrage, il suffira alors aux destinataires de vérifier l'authenticité de la signature à l'aide de le clé de décryptage que seul Alice peut leur avoir donné. Les deux clés sont bel et bien complémentaires.

L'authentification garantie, il importe également de s'assurer que le document envoyé n'a pas été corrompus. En effet dans ce mémoire, nous traiterons de la cryptologie à la lumière du droit. La preuve électronique entre tout naturellement dans le cadre de ce travail car la cryptographie, à l'aide des clés asymétriques, permet d'empêcher toute modification des documents et ce d'une façon plus sûre qu'avec le format papier.

L'intégrité du document est assurée grâce à la fonction de hachage qui établit une correspondance entre une chaîne binaire de longueur arbitraire et une chaîne binaire de longueur fixe et qui a les propriétés suivantes :

- il est impossible sur le plan calcul de trouver une donnée d'entrée qui correspond à une donnée de sortie préétablie;
- il est impossible sur le plan calcul de trouver deux données d'entrée distinctes qui correspondent à la même donnée de sortie.[20]

Par le hachage il est impossible de modifier un document sans modifier l'emprunte du message. L'intégrité du document est ainsi vérifiée sans le moindre doute. Le système s'apparente à la clé des cartes bancaires qui se contente d'attribuer une courte valeur à la chaîne

[20] Groupe de travail sur le commerce électronique Industrie Canada, *Politique cadre en matière de cryptographie aux fins du commerce électronique, Pour une économie et une société de l'information au Canada Politique cadre en matière de cryptographie aux fins du commerce électronique* Février 1998, http://strategis.ic.gc.ca/crypto

Lire aussi RIVEST, R.L., « The MD4 Message digest Algorithm. », *Advances in cryptology*, CRYPTO'90 Proceedings, p. 303-311 à propos du logiciel MD4, spécifique au hachage par emprunte de la source de 128 bits

des chiffres composant le numéro de la carte. Cette fonction est par contre améliorée par la fonction de hachage puisqu'à un document correspond une valeur de hachage bien précise.

B- Le cas de PGP : *Pretty Good Privacy* (assez bonne confidentialité)

PGP tient sa principale qualité de sa grande popularité : il semble *de facto* être devenu une norme dans tout ce qui concerne l'échange de courrier électronique. Son fonctionnement est semblable à celui du RSA pour ce qui est de la gestion des clés :

> *« PGPfreeware est basé sur un système de cryptographie à clé publique largement accepté et hautement éprouvé, comme montré dans la Figure 5, par lequel vous et les autres utilisateurs de PGP générez une paire de clés consistant en une clé privée et une clé publique. Comme son nom l'implique, vous êtes le seul à avoir accès à votre clé privée, mais de façon à correspondre avec les autres utilisateurs de PGP vous avez besoin d'une copie de leur clé publique, et eux besoin d'une copie de la vôtre. Vous utilisez votre clé privée pour signer les messages e-mail et les fichiers attachés que vous envoyez aux autres et pour décrypter les messages et fichiers qu'ils vous envoient. Inversement, vous utilisez les clés publiques des autres pour leur envoyer un e-mail crypté et vérifier leurs signatures numériques. »*[21]

PGP comprend également un algorithme de cryptage s'inspirant d'IDEA, ce logiciel crypte également la clé privé de l'utilisateur en utilisant plutôt qu'un mot de passe une *phrase de passe…* Enfin, PGP dispose d'une méthode originale de certification des clés distribuées : chaque utilisateur contribue à promouvoir la certification des clés distribuées (voir la figure 6)

La puissance de PGP semble désormais admise : elle est considérable.

> *« Si tous les ordinateurs personnels du monde – 260 millions – étaient mis à travailler sur un seul message crypté avec PGP, cela prendrait encore un temps estimé à 12 millions de fois l' âge de l'univers, en moyenne, pour casser un simple message. »*
>
> William Crowell, Directeur délégué, National Security Agency, 20 Mars 1997.

[21] Mode d'emploi de PGP freeware, disponible à cette adresse : http://wwwcl.cam.ac.uk/~fapp2/pgpenfrancais/doc.htm

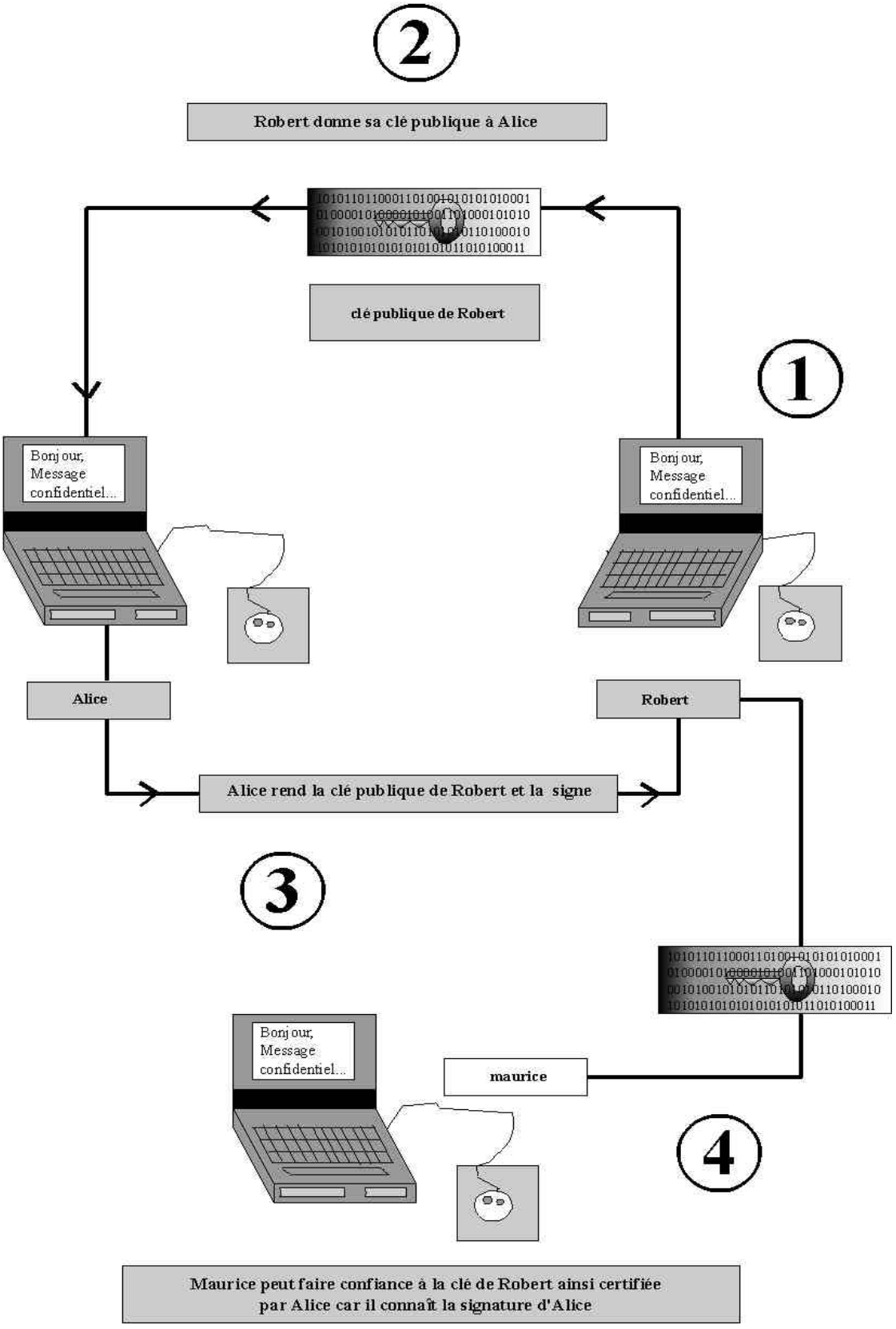

Figure 6 : le système de certification des clés publiques par PGP

Nous avons vu que la cryptographie est un jeux qui se joue à deux. PGP est un logiciel ouvertement destiné à contrer les attaques puissantes (et notamment gouvernementales). Nous profitons donc de cette partie consacrée à ce logiciel pour parler de cette autre versant de la cryptologie : le décryptage agressif. Si aucun algorithme de cryptographie n'est incassable, le temps nécessaire à détruire sa résistance est par contre un sérieux élément de dissuasion. La solution au décryptage forcé n'est donc pas raisonnablement un seul travail de cryptographe.

Des moyens détournés existent comme la contamination d'un logiciel de cryptage par un virus afin de pouvoir récupérer les mots de passe de l'utilisateur. Un autre moyen intéressant est le Tempest[22] qui permet de capter à distance les champs électromagnétique de tout appareil électrique. Ces appareils émettent des parasites, par exemple l'écran de l'ordinateur se met ainsi à scintiller avant même que la sonnerie d'un téléphone cellulaire ne tinte. L'ordinateur rayonne comme un émetteur radio. Il semble alors inutile de dépenser des fortunes et des siècles à décrypter ce que l'on peut lire en clair à la source ou chez le destinataire, le cryptage n'est en effet qu'une phase intermédiaire[23]. Des protections existent (tout local revenant à réaliser une cage de Faraday) mais elles sont onéreuses, de plus les fils électriques constituent autant d'antennes propageant les signaux électro-magnétiques… Toutes ces raisons sont résumés par le nom même de PGP, qui n'assure qu'une assez bonne confidentialité dans le cryptage pur, en attendant qu'un jour un cryptanalyste n'en casse la clé.

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: PGPfreeware 6.0 for non-commercial use <http://www.pgp.com>

LQFvBDeIhYMRAwDGQFk9/InS6eFX1T1ct+pz2+azLjVowc46nZ6ge6QZ10oaw9eBZCK+iDMY89/VkMJqtURPbalNhBPHX/t3hPJWyJF
mAzMgtoCip50G+qSay2H0hBBMw+jUYq9hQqV9X60AoP/Y3ZXsHUFN9gRtuTj6cab4Ua91Av9c+0BGnjGGG1AVgl7G
4QKZYAg02wiFndzg2Qie4zDpfdVApSQz64pTX7i/ft9RPuuc1SthweAbqs0GJyEm2er+NhfWHuGppbA1y4cbaSmnGAn6me3DZiKgBn/Gh
0ZfjHMC/Asu41TzHEWe1TdixCQq4czgHugBR9r+GSKKRETuQkGdpEeLRkY5LrDBG+tH5JQLgF3YfnW97MNpZtI3
fU4SmwA1100NZMl0YjlD6Ncsg2aRBsJjMR3LfejdkGNmEpEepv8DAwIKoFAfj5rZV2BzHNFZ5UssZZqT9XxZ3BPgFPdOO73ws88CQt8
TefJ/PbQXdGVzdCA8dGVzdEBob3RtYWlsLmNvbT6dAQQEN4iFlBADAQEErx02pZsgEoJLDUV4PQ0QkgXYJ2hnqUC0
sc+3Zuc21ahzvE0qvvgvyqTP8sRwfMe2k66wu4hz5wpXmipD3pUvtN0h2UHmHwjlZlu3aN/5bKmW2Ij/tWPQpLTHSuzifr8AAgIC/0cFCM
+iDyTkAkp1ppsW47CxVC9vTZsMlyTOoFDarFvpRq/1ckK5Go8z9Kn1mSYKajfn8b/A5rF/a+bQzEp7ScNByaYq8FWf4j+6HUyG4jK+hIS
ACdAE1Grz2oLiB9096v8DAwLR+Lf6eLNCnmAxJrT8PO+O8RvX+noiU94H9Sfckm5GTDQyWeUxeUWSND3nbkuSIayB3w===fpfV
-----END PGP PRIVATE KEY BLOCK-----

[22] Transient Electromagnetic Pulse Emanation Surveillance Technology (Technique de surveillance des impulsions électromagnétique transitoires), voir le dossier sur le Hors série de Pirates Mag' op. cit, p. 10

[23] Lire l'étude de Ross J. Anderson, financée par Microsoft dans le but de pouvoir vérifier à distance la validité des licences des logiciels utilisés…, http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf, visionné le 20 juillet 1999

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0 for non-commercial use <http://www.pgp.com>

MQFCBDeIhYMRAwDGQFk9/InS6eFX1T1ct+pz2+azLjVowc46nZ6ge6QZ10oaw9eBZCK+iDMY89/VkMJqtURPbalNhBPHX/t3hPJWyJ
FmAzMgtoCip50G+qSay2H0hBBMw+jUYq9hQqV9X60AoP/Y3ZXsHUFN9gRtuTj6cab4Ua91Av9c+0BGnjGGG1AVgl7G4QKZYAg02wi
Fndzg2Qie4zDpfdVApSQz64pTX7i/ft9RPuuc1SthweAbqs0GJyEm2er+NHfWHuGppbA1y4cbaSmnGAn6me3DziKgBn/Gh0ZfjHMC/Asu4
1TzHEWe1TdixCQq4czgHugBR9r+GSKKRETuQkGdpEeLRkY5LrDBG+tH5JQLgF3YfnW97MNpZtI3fU4SmwA1100NZMl0YjlD6Ncsg2
aRBsJjMR3LfejdkGNmEpEeprQXdGVzdCA8dGVzdEBob3RtYWlsLmNvbT6JAEsEEBECAAsFAjeIhYMECwIDAQAKCRAHqW7IP8u1f
tDKAJ4mTnCsEyJ3T6ATCJcMZ0q/LhBkMgCePLq0zgKCNznA+1G90Q5FdqfPBVu5AM4EN4iFlBADAQEErx02pZsgEoJLDUV4PQ0Qk
gXYJ2hnqUC0sc+3Zuc21ahzvE0qvvgvyqTP8sRwfMe2k66wu4hz5wpXmipD3pUvtN0h2UhmHwjlZlu3aN/5bKmW2Ij/tWPQpLTHSuzifr8A
AgIC/0cFCM+iDyTkAkp1ppsW47CxVC9vTZsMlyTOoFDarFvpRq/1
ckK5Go8z9Kn1mSYKajfn8b/A5rF/a+bQzEp7ScNByaYq8FWf4j+6HUyG4jK+hISACdAE1Grz2oLiB9096okARgQYEQIABgUCN4iFlAA
KCRAHqW7IP8u1fnObAKDtMx+Nza/mDRNejN9TvePCekrpjQCgukc/5/e2brKsVIZvmMbTyGf8H5w==sjJo
-----END PGP PUBLIC KEY BLOCK-----

Figure 6 : Format de clés publique et privée PGP à 768 bits

Dans ce long chapitre introductif nous avons détaillé la cryptographie dans toutes ses approches, principalement historiques et techniques. Depuis une trentaine d'années la cryptographie n'est plus un domaine spécifiquement réservé aux gouvernements, les enjeux commerciaux ont également développé la recherche du secret. Le développement du commerce électronique et la mise à disposition de l'internet au grand public ont incontestablement créé un besoin de confidentialité pour les données échangées. Il apparaît alors que deux réalités se présentent dans toute approche contemporaine de la cryptologie. En effet, la seule raison d'État n'est plus suffisante pour justifier un monopole gouvernemental dans l'utilisation et le développement de moyens cryptographiques. La raison commerciale est désormais une justification devenue légitime. Pour James Massey, [24]

> « Ce n'est que depuis 10 ans, en fait, que la recherche cryptographique ouverte (non militaire, non secrète) se répand. Il y a eu, et il continuera d'y avoir, des conflits entre les deux communautés de recherche. La recherche ouverte est une quête commune de la connaissance qui dépend de façon vitale du libre-échange des idées par le biais des présentations lors des conférences ou des publications dans les journaux scientifiques ».

Une opposition s'installe alors entre les intérêts privés et les intérêt gouvernementaux. La cryptogologie est la science visant à protéger le secret des informations, aussi dans ce mémoire, nous porterons notre intérêt sur la protection des informations afin d'explorer le double aspect « raison d'état » (chapitre I) et « raison commerciale » (chapitre II), le tout pris dans une approche chronologique.

Chapitre I : La protection des informations face à la raison d'État

Les années 1990 sont marquées par l'entrée de la société de l'information. Les réseaux génèrent un grand nombre de données. Ces gisements d'information, considérables et détaillés, peuvent être utilisés à l'insu des personnes pour constituer des profils individuels ou surveiller la navigation d'un internaute. L'exploitation des informations circulant sur Internet, ainsi que la mémorisation des données peut transformer l'internaute en objet de surveillance, le citoyen en individu épié.

> *"Peut-on admettre que le monde de l'Internet renvoie à celui des Incas où portes et fenêtres devaient être en permanence ouvertes pour que les inspecteurs puissent voir à tout instant ce qui se passait à l'intérieur des foyers ?*[25]*"*

Face à ces caractéristiques, s'oppose l'intérêt de la nation. Le désire d'écouter tout ce qui peut ce dire, prévenir l'imprévisible et protéger l'État contre toute agression.

La science du chiffrement est fortement marquée par un passé militaire. D'ailleurs, à l'origine, il a été inventé et développé pour et par ces institutions militaires. La marque du "secret-défense" est présente dans toutes réglementations concernant la cryptologie (section I). Mais la communication des individus, se fait de plus en plus par l'intermédiaire de réseaux complexes que l'individu ne maîtrise plus. Aussi, il ne peut avoir confiance en ce qui se passe sur ces réseaux. Donc, il recherche un moyen de protection adapté à ces nouvelles circonstances et naturellement il se tourne vers la cryptologie. Malheureusement, son utilisation par des particuliers n'est pas favorablement perçue par tous les Etats (section II). Mais, la protection de la sphère privée de chacun passe par une nécessaire confidentialité (section III).

[24] MASSEY, J.L., An introduction to contempory cryptology. Proceedings of the IEEE, vol. 76, n°5, mai 1988, p. 533

Section I : La cryptologie considérée comme une arme de guerre

Un des rôles de l'État est la défense voire la promotion de certaines valeurs, mais aussi assuré le maintien des intérêts de la sécurité nationale. Contre cet intérêt national, la cryptologie représente un véritable danger. En effet, issu des méthodes militaires, popularisé par le développement fulgurant de la puissance des ordinateurs, le cryptage garantit si bien la confidentialité des échanges qu'il met la police et les services de renseignement en difficulté. Trop puissant, il rend indéchiffrable de manière exploitable, les messages électronique.

En revanche, pour le particulier, la cryptologie constitue le premier outil de protection efficace de sa vie privée. De même, pour celui ayant des intentions malveillantes, c'est une aubaine. La cryptologie permet d'échapper aux fameuses écoutes et autres interceptions.

Aussi, réglementer la cryptologie met en présence deux intérêts antagonistes. Mais toute réglementation est nécessairement un compromis entre les besoins de protection demandés par les utilisateurs des nouvelles technologies (II) et les nécessités de la sécurité publique qui réclame un contrôle absolu (I).

I - Des réglementations pour un contrôle absolu…

Devenus accessibles au plus grand nombre, les outils cryptographiques sont très vite apparus comme le véhicule d'une opposition entre ceux que l'on appelle les crypto-anarchistes (favorable à une liberté de l'accès et de l'utilisation des outils cryptographiques) et les autres, plutôt favorables à un maintient de la tutelle étatique. Les lois et décrets concernant la cryptographie de tous les pays du monde sont devenus caractéristiques d'une certaine idéologie des États ou de leurs responsables politiques.

Globalement trois grands soucis préoccupent les partisans de la raison d'État ou, tout au moins de la restriction dans l'usage et dans la dissémination des outils cryptographiques. D'une part, il y a principalement des raisons de sécurité nationale, en effet, il y a un contrat social entre l'État et ses sujets, ces derniers attendant de leur Léviathan paix, ordre et sécurité. Or, si

[25] 18ème rapport d'activité de la CNIL.

elle est libéralisée, la cryptographie, en empêchant la lecture et l'analyse des communications interceptées, rend le rôle de l'État difficile à tenir : le contrat social risque de n'être plus assuré. D'autre part, libéraliser la cryptographie c'est peut être aussi le risque de voir se développer plus encore les cas de trafics financiers, de blanchiment d'argent, l'espionnage ou le terrorisme ; nous pouvons d'ailleurs noter sur ce point que ces risques sont ceux généralement pointés du doigts lorsque l'on traite habituellement des problèmes tenant à l'applicabilité du droit sur l'internet. Enfin, et dans une optique plus interne aux États, la libéralisation des outils cryptographiques serait aussi le moyen de créer un crypto-terrorisme ou un crypto-chantage contre les projets scientifiques publiques ou privés, en effet on peut imaginer une intrusion dans certains systèmes et un cryptage agressif des disques dur des ordinateurs. Tous ces cas ne sont pas théoriques,

> « For exemple the Italian Mafia apparently uses PGP, as did an employee of a software compagny who has been accused of stealing multimillion-dollar software. Also, Aldrich Ames, while spying for the Soviet Union, used very weak encryption which was easily cracked » [26].

Les mêmes auteurs donnent d'ailleurs sept autres exemples notamment celui de l'attentat de la secte Aun au gaz Sarin dans le métro de Tokyo. Dans cette affaire les autorités japonaises ont réussis à décrypter des informations prévoyant un massif déploiement d'armement contre le Japon et les États-Unis. Il est toutefois des cas où le décryptage pose des problèmes. Selon Louis J Freeh[27], le directeur du FBI, il n'y eu que peut de cas où le cryptage à empêché la justice d'opérer, cela dit nous sommes dans un sujet sensible où le secret est la règle.

Pour traiter des réglementations nationales, nous avons artificiellement découpé cette section entre l'Europe (A) et l'Amérique du Nord (B) du fait que ces deux zones regroupent l'essentiel des intermédiaires prenant part à l'internet. Il est à noter que l'article de Wayne Madsen pour l'Electronic Privacy Information Center[28] est une source intéressante sur l'état du droit en matière de cryptage, il donne ainsi un bref état de la situation dans 76 États du monde en ajoutant un code de couleurs :

---

[26] Pour des cas concrets : DENNING, D.E . et W.E. Baugh JR, *Cases Involving encryption in crime and terrorism,* http://guru.cosc.georgetown.edu/~denning/crypto/cases.html, visionné le 20 juillet 1999

[27] Cité par ACKERMAN, Wystan M., « Encryption : a 21st century national security dilemma », *International review of law computer & technologie*, volume 12, number 2, pages 371-394, 1998

[28] http://www.epic.org

« a "green" designation signifies that the country has either expressed support for the OECD guidelines on cryptography (nous en reparlerons), which genaraly favor unnhindered legal use of cryptography, or has no cryptography control. A "yellow" designation signifies that the country has proposed new cryptography controls, including domestic use controls, or has shown a willingness to treat cryptographic-enabled software as a dual-use item under the Waasenaar Arrangement. A "red" designation denotes countries that have instituted sweeping controls on cryptography, including domestic controls. Some countries do not fit neatly into one of the three cathégories, but trends may show them as being bordeline, i.e., "yellow/red ". »[29]

A- Les normes européennes

Les méthodes cryptographique utilisées l'étaient surtout par des militaires ou des diplomates [30]. C'est ce caractère d'armes de guerre qui a valu à la cryptographie d'être réglementée de façon très sévère, notamment en France et au niveau européen. En revanche, pour la Belgique, l'approche fut moins draconienne[31].

La réglementation belge :

Le 21 décembre 1994, le législateur belge a voté une loi portant sur des dispositions sociales et diverses[32]. Au sein de cette loi, trois articles, assez nébuleux, étaient censés réglementer la matière de la cryptographie en Belgique.

Grâce à ces trois articles, la loi du 21 décembre 1991[33], dite «*loi portant réforme de certaines entreprises publiques économiques* », a été enrichie d'un nouvel article 70bis. D'autre part, ce dernier est venu compléter l'article 95 alinéa premier de cette même loi. Cette dernière réglemente le cadre légal de toute la matière des télécommunications diffusées à partir

---

[29] MADSEN, Wayne et aut, « Cryptography and liberty : an international survey of encryption policy », *The John Marshall Journal of computer & information law*, Chicago, spring 1998, p. 482

[30] SYX, D : «Vers de nouvelles formes de signature ? le problème de la signature dans les rapports juridiques électroniques», *in Droit de l'informatique*, 1986/3, p133 et s.

[31] BALTHAZAR Géraldine, «application et réglementation de la cryptologie en Belgique et en France » Wintersemester 1996-1997-seminarabeit.

[32] Loi du 21 décembre 1994, moniteur belge du 23 décembre 1994 ; BONAVENTURE Olivier : « encryptage en Belgique : La loi », http://pgp.netline.be/cryptage/loi.html .

[33] Loi du 21 mars 1991, MB du 27.03.1991 pp 6196-6197 et pp 6202-6203

d'appareils terminaux[34]. Certains politiciens ont considéré que cette loi s'appliquait également aux logiciels informatiques et par conséquent à l'internet.

La loi du 21 mars 1991 a vu son article 95 alinéa 1° complété comme suit :

> «*Le Ministre peut, sur proposition de l'Institut [Belge des services postaux et des télécommunications - IBPT] retirer un agrément ou imposer une interdiction de maintenir le raccordement à l'infrastructure publique de télécommunications lorsqu'il s'avère que*
> (...)
> *5° l'appareil terminal rend inefficace les moyens permettant, dans les conditions prévues aux articles 88bis et 90ter à 90decies du Code d'instruction criminelle, le repérage, les écoutes, la prise de connaissance et l'enregistrement des télécommunications privées* ».

De ce fait, l'IBTP peut proposer des clés de cryptage au gouvernement. Donc, il n'a qu'un rôle de conseiller du gouvernement.

Le nouvel article 70bis fut rédigé comme suit :

> «*Le Roi fixe, par arrêté délibéré en conseil des ministres, les moyens techniques par lesquels Belgacom et les exploitants des services non réservés*[35] *qu'il désigne doivent permettre, le cas échéant, éventuellement conjointement, le repérage, les écoutes, la prise de connaissance et l'enregistrement des télécommunications privées dans les conditions prévues par la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées* ».

De cette façon, cet article prévoit que, moyennant un arrêté d'application délibéré en conseil des ministres, l'utilisation de dispositifs de cryptage, pourrait être totalement interdite. Donc, le gouvernement a le pouvoir d'interdire l'utilisation d'un mécanisme de cryptage, et ce quel qu'il soit, à quelque moment que ce soit et selon son bon vouloir.
Étant donné les incertitudes engendrées par cette loi, l'IBTP[36], suivis par quelques auteurs[37], a interprété cet article comme ne s'appliquant pas aux logiciels. Mais ce n'est qu'une

[34] Définis dans la loi du 21 mars 1991 comme « *toutes installation qui peut être raccordée directement à l'infrastructure de télécommunication par un point de raccordement pour transmettre, traiter ou recevoir les informations visées au 4°* ».

[35] Selon les articles 83 et 87 de la loi du 27 mars 1991, les services non réservés sont définis comme étant tous les services de télécommunications qui ne sont pas les services de téléphonie, les services de télex, de mobilophonie et de radiomessagerie, les services de commutation de données, le service télégraphique et enfin, la mise à disposition de liaisons fixes.

[36] IBTP, Avenue de l'Astronomie, 14, B-1030 Bruxelles

[37] DUMORTIER, jos, « Cryptogrfie is niet verboden », http://www.kuleuven.ac.be/ck/archief/ck-7-3/forum/fforu.htm .

interprétation doctrinale confortée par aucun texte légal. En effet, aucun arrêté d'application n'a été pris depuis la promulgation de la loi.

Face à cet aspect flou de l'article 70 bis, la classe politique a interrogé directement le ministre de la justice belge, sur l'éventualité d'une prohibition totale de la cryptographie[38]. Ce dernier a répondu que :

> « *Rendre obligatoire le dépôt des clés des terminaux auprès des autorités de manière à pouvoir lire en cas d'enquête des messages cryptés ne résoudra pas tous les problèmes* », d'autant que «*l'interdiction de la cryptographie s'est avérée irréalisable sur les plans juridique et technique dans d'autres pays* »[39].

Ici, le ministre c'est montré prudent. Au regard des enjeux économiques, auxquels nuirait l'interdiction de tous procédés de cryptage, et en pratique, cette interdiction est peu réaliste sauf si elle est suivis au niveau mondial. Étant donné que l'internet est un phénomène international, sans une certaine cohérence entre les politiques nationales aucun résultat tangible n'est réalisable. De plus, des arrêtés permettant d'accéder à des informations touchant essentiellement à des libertés individuelles seraient contraire à la constitution belge. Tout ceci pourrait expliquer l'interprétation de cette loi, selon laquelle elle ne s'applique pas aux logiciels.

Mais, même si l'idée d'une prohibition totale de la cryptologie est exclue (pour des raisons pratiques et juridiques), la réglementation de son utilisation reste une façon d'éviter des abus ou au moins de les minimiser.
Pour cela, diverses propositions furent lancées dont une pouvant apporter une solution satisfaisante.

Parmi les propositions avancées par les parlementaires, une envisageait la suppression des articles posant problèmes, en y substituant un nouveau régime. Celle-ci adoptait l'idée d'une accessibilité maximale aux clés de cryptage. Mme Bribosia (à l'origine de cette proposition) proposait de compléter les dispositions du code d'instruction criminelle Belge, afin

[38] Question posée au sénat le 9 mai 1996, par Mme Bribosia-Picard (PSC) à M. De Clerck, ministre de la justice belge, http://pgp.netline.be/crytpage/question-complète-bribosia.html

[39] Ibidem

de prévoir un cadre légal à l'accès par les autorités judiciaires aux informations sur le réseau Internet[40]. Ce système ressemblait fortement à celui prévu en matière d'écoutes téléphoniques, mais adapté à l'internet.

Ainsi, le juge d'instruction pourra obliger toute personne susceptible de l'aider à le faire, dans la mesure où cette aide est nécessaire pour son investigation. Il est nécessaire qu'il y ait des indices sérieux d'une infraction grave et que les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité. Bien évidemment, l'aide ne pourra être demandée et ordonnée qu'à l'égard des messages envoyés à ou par des personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, et à l'égard des messages envoyés à ou par des personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.

Toute personne susceptible de l'aider sera donc citée en justice et sera tenue de comparaître, à défaut de quoi elle se verra infliger une amende.

Les conditions du décryptage seront très strictes ; le juge ne pourra en faire usage que pour procéder au décryptage des messages faisant l'objet de l'instruction. Son «mandat», c'est-à-dire son accès à un site, ne sera valable que pour une période déterminée qui ne pourra jamais dépasser six mois. La conservation des messages ne pourra se faire que sous les conditions très strictes de l'article 90septies du Code d'instruction criminelle et le juge sera obligé de détruire la clé de cryptage une fois la période de surveillance passée.

Dans l'hypothèse où la surveillance concerne des personnes ayant la qualité de médecin ou d'avocat, le respect du secret professionnel devra être garanti. D'autre part, le bâtonnier ou le représentant de l'ordre des Médecins devra en être averti. (Articles 91septies et 91octies)

Les sanctions qui toucheront les personnes refusant de coopérer seront des peines pénales sévères : emprisonnement d'un à cinq ans ou amende de 100 à 5.000 FB[41].

---

[40]BONAVENTURE Olivier, «*Question posée par Mme Bribosia-Picard (PSC) à M De Clerck, Ministre de la Justice, question posée au sénat le 9 mai 1996*», http://pgp.netline.be/cryptage/proposition-Bribosia-100696-bribosia.html

[41] Au regard des peines d'emprisonnement qui sont également prévues dans cet article, le montant des amendes peut paraître dérisoire mais il faut savoir que les montants des amendes pénales en droit belge doivent être majorés de 1990 décimes, montant prévu par une loi du 5 mars 1952, modifiée la dernière fois par une loi du 24 décembre 1993. En réalité donc, les peines varient d'un montant d'environ 20.000 FB à 1.000.000 FB

Ainsi, la proposition de Mme Bribosia semblait une alternative sérieuse même si elle ne prévoyait pas le cas d'une fuite d'information au niveau de l'État ou encore si le nom de la personne susceptible d'aider le juge d'instruction était lui-même crypté. Mais cette proposition n'est toujours pas votée, et on peut supposer que la Belgique attend de consulter la position européenne en la matière afin d'aligner ses textes sur celle-ci. Dans ce cas, il est fort probable que la future réglementation belge sur la cryptographie sera certainement plus libérale.

La réglementation française :

Depuis un décret du 18 avril 1939, une prohibition de principe de la cryptographie était édictée. Mais, il prévoyait également des possibilités d'obtenir des dérogations administratives ponctuelles[42].

Face à l'apparition et au développement de l'internet, cette législation s'est révélée insuffisante (surtout au vu de la lourdeur administrative du régime et de l'accroissement de la demande privée en produit de sécurité). Aussi, une loi du 29 décembre 1990[43], est venu simplifier et élargir les procédures antérieures.

Même si cette loi a été édictée dans le but de simplifier la procédure, l'article 28.I de cette même loi soumet l'utilisation de toutes techniques de chiffrement à des conditions très précises : toutes utilisations, fournitures et exportations d'un moyen de cryptographie devaient être précédées de l'obtention d'une autorisation préalable, hormis certains cas précis où une déclaration préalable était exigée. Ces principes étaient tellement stricts que la loi réservait ces techniques aux militaires, policiers et dans une certaine limite aux banquiers. Le simple citoyen, l'université ou la petite entreprise étaient exclus des utilisateurs potentiels, car pour chaque utilisation de procédé de cryptage, il était nécessaire de passer par une procédure administrative aussi rébarbative que dissuasive.

[42]MEILLAN Eric, «le contrôle juridique de la cryptographie», *Droit de l'informatique & des télécoms*, 1993/1, pp78 et s.

[43]BORTMEYER Stéphane, «L'Utilisation du chiffrement en France», http://web.cnam.fr/Network/Crypto/ (décembre 1996); Loi 90-1170 du 29 décembre 1990, Journal Officiel du 30 décembre 1990 ; loi modifiée par la loi 91-648 du 11 juillet 1991, Journal Officiel du 13.7.91

L'article 28 de cette loi édictait que les moyens ou prestations de cryptographie ayant pour but d'être fournis ou utilisés par des particuliers, utilisés par des banques ou exportés à l'étranger étaient soumis à une déclaration préalable ou à une autorisation préalable :

- La déclaration préalable était requise quand le moyen ou la prestation de cryptage n'avait pour objet que d'authentifier une communication ou assurer l'intégrité du message transmis (exemple du code secret bancaire).
- L'autorisation préalable, du Premier ministre, était nécessaire dans les autres cas. C'est à dire pour tout ce qui sort du champ d'application de l'alinéa premier de l'article 28 de la loi du 29 décembre 1990[44]. (Exemple de particulier qui souhaite crypter ses messages.).

Mais certains outils de cryptage n'avaient pas besoin de déclaration ou d'autorisation préalable pour être mis en circulation. Ainsi les cartes à microprocesseur ne permettant pas le chiffrement par elles-mêmes étaient totalement libres d'usage. De même pour les techniques conçues spécialement pour les logiciels qui ne permettent pas le chiffrement. Ils n'étaient pas considérés comme des moyens de cryptologie car, dans ces cas le codage n'est connu que par le fabricant (la cryptologie suppose une codification tenant lieu de convention secrète). Enfin, en raison du caractère non rétroactif de la loi de 1990, les moyens qui étaient permis, par l'intermédiaire d'autorisations délivrées avant la publication de la loi étaient dispensées d'une autorisation préalable. Elles conservaient leurs effets jusqu'à l'expiration de leurs termes prévus initialement.

A l'inverse, d'autres outils de cryptographie ne pouvaient bénéficier de ce régime parce qu'ils étaient interdits ou soumis à d'autres réglementations. Ainsi, aucune autorisation n'était accordée pour un usage destiné à dissimuler la teneur des communications obtenues à partir des installations radioélectriques libres ou amateurs et des postes émetteurs récepteurs fonctionnant sur des canaux banalisés (article 11 du décret 92-1358[45]).

[44]Loi n° 90-1170, Journal Officiel de la République française, 30 décembre 1990, p16439, http://www.urec.fr :80/Ftp/securite/Lois.France/90.12.30.crypto.txt

[45] Décret français n°92-1358 du 28 décembre 1992, JO du 30 décembre 1990

De plus, l'exportation de matériel de cryptographie pouvait parfois être régie par un système autre que celui de la loi de 1990. Les moyens de cryptographie qui étaient «*spécialement conçus ou modifiés pour permettre ou faciliter l'utilisation ou la mise en œuvres des armes*» relevaient du régime visant le matériel de guerre, armes et munitions, prévu par les articles 12 et 13 du décret-loi du 18 avril 1939[46].

Enfin, un régime particulier était édicté pour les exportations des biens pouvant avoir une utilisation civile et militaire (dit biens à double usage). La loi du 31 décembre 1992[47] a, dans son article 2, traité du transfert de produits et technologie à double usage au sein de la CEE[48]. Il y était précisé que ces produits et technologies seraient soumis à une autorisation préalable et devraient toujours être présentés aux douanes avant leurs expéditions (article 2). Ici, le but recherché était de maintenir un contrôle intérieur qui pouvait être éventuellement assouplis[49].

Il existait donc trois régimes distincts d'exportation des moyens de cryptologie sous l'empire de la loi de 1990 (déclaration préalable, autorisation préalable et autorisation d'exportation de matériel de guerre).

Sous cette loi de 1990, deux institutions étaient compétentes: la DISSI (Délégation Interministérielle pour la Sécurité des Systèmes d'Information) et le SCSSI (Service Central de la Sécurité des Systèmes d'Informations).

---

[46]Décret toujours en vigueur ; WARUSFEL Bertrand, «exportation de cryptologie : des régimes juridiques difficiles à concilier», *Droit de l'Informatique & des Télécoms*, 1993/1, pp.72 à 74 ; Article 2, § 4d du décret 95-598 du 6 mai 1995

[47] loi n°92-1477 du 31 décembre 1992 relative «*aux produits soumis à certaines restrictions de circulation et à la complémentarité entre les services de police, de gendarmerie, et de douane*», publiée au journal officiel le 05 janvier 1993

[48] Voir également les textes : Décret 95-613 du 5 mai 1995 relatif au contrôle à l'exportation de biens à double usage, JO du 7 mai 1995, page 7547 ; Arrêté du 5 mai 1995 relatif au contrôle à l'exportation vers les pays tiers et au transfert vers les États membres de la Communauté européenne de biens à double usage, Journal officiel du 7 mai 1995, page 7561 ; Arrêté du 5 mai 1995 définissant la licence générale de G.502 d'exportation des moyens de cryptologie et fixant les modalités d'établissement et d'utilisation de cette licence, JO du 7 mai 1995, page 7578

[49] WARUSFEL, Bertrand, «contrôle des exportations de technologie à double usage : le droit français réagit face au marché unique», in *Droit de l'Informatique & des Télécoms*, 1993/2, p83 et s.

- La DISSI fut crée par décret le 3 mars 1986 et supprimée en février 1996. Elle fut remplacée par le SGDN (Secrétariat Général à la Défense Nationale[50]) dans ses attributions. Elle était compétente dans le domaine de la sécurité des communications, de la protection contre les rayonnements compromettant et la sécurité logique (surtout contre les intrusions). Ses fonctions étaient la mise en œuvre de la politique définie par l'État, proposer des mesures d'intérêt générales et arbitrer les éventuels litiges en la matière[51].

- Le SCSSI était le seul interlocuteur pour la procédure de demande d'autorisation préalable ou celle de la déclaration. Il appréciait le niveau de sécurité des systèmes, évaluait les procédés cryptologiques et les autres procédés (TEMPEST), faisait des audits de sécurité, formait des experts et entretenait des relations avec les industriels concernés. En matière de cryptologie son rôle fondamental était surtout son évaluation de la teneur des procédés de cryptographie[52]. Pour cela, le déclarant ou demandeur devait prendre toutes les dispositions nécessaires afin que le SCSSI puisse vérifier la concordance entre le dossier technique fourni est l'objet de la déclaration ou de la demande.

En fonction de ce dossier et de ses annexes, le SCSSI décidait d'avaliser ou non le moyen objet de la demande. Mais les critères d'acceptation ou de refus n'étaient pas publics, ce qui pouvait aboutir à des refus abusifs de la part du SCSSI. Surtout qu'il semblerait que la politique du SCSSI était de n'autoriser que des systèmes de chiffrement peu fiables, afin qu'une personne disposant de moyens importants puisse casser ce code et déchiffrer les messages.

[50] Le secrétariat du département ministériel de la Défense, dépendant directement du Premier ministre et du ministre qui a la Défense dans ses attributions

[51] MALHEY Bruno, «Législation sur la cryptographie», http://ns.urec.fr:70/00/Securite/Docs/Lois/chiffrement.txt

[52] article 14 du décret du 28.12.1992

Quel que soit l'objet de la demande (déclaration ou demande), le début de la procédure était la même. Dans les deux cas (articles 1à 3 ou 4 à 9 du décret 92-1358 du 28 décembre 1992) un dossier était déposé au SCSSI qui en délivrait récépissé. Ce dossier était divisé en deux parties, une administrative et une technique. Toutes deux devaient être fournies en quatre exemplaires selon une forme et un contenu fixé par un arrêté du 28.12.1992 :

- La partie technique devait indiquer les objectifs de sécurité et décrire en détails les fonctions et les mécanismes de sécurité.
- La partie administrative permettait de s'assurer de l'identité du déclarant ou du demandeur.

À la vue de ce dossier le SCSSI pouvait demander des informations complémentaires pendant toute la procédure. Si tel était le cas, le déclarant ou le demandeur était tenu de coopérer avec le SCSSI afin que celui-ci puisse vérifier que le moyen ou la prestation de cryptographie était bien conforme au dossier fourni (article 14 du décret du 28 décembre 1992). La suite de la procédure différait selon la demande.

Pour le régime de la déclaration obligatoire[53], il existait trois types de déclarations différentes selon que le but recherché était l'utilisation, l'exportation ou la fourniture de système d'encryption.

- En premier lieu, la déclaration de fourniture devait être effectuée une seule fois, un mois avant la première livraison du système.

- Ensuite, la déclaration d'utilisation devait être effectuer par l'utilisateur au moins un mois avant la première utilisation (article 2 alinéa 2). Mais un régime de déclaration simplifié a été institué par l'article 1er, alinéa 3 :

> *«La déclaration de fourniture peut être accompagnée d'une déclaration d'utilisation générale[54], qui précise le domaine d'utilisation prévu du moyen ou de la prestation ainsi que les éventuelles catégories d'utilisateurs auxquelles le moyen ou la prestation est destinée».*

[53]Titre I[er] du décret 92-1358

Dans ce cas, la déclaration d'utilisation générale dispensait l'utilisateur d'une nouvelle déclaration.

- Enfin, la déclaration d'exportation requerrait le dépôt d'un dossier de déclaration de fourniture en vue d'exportation, un mois au minimum avant la première prestation. Une copie du récépissé de cette déclaration devait être présentée lors de chaque exportation, à l'administration des douanes (article3). Pour certains produits, toute déclaration de fourniture tenait lieu de déclaration d'exportation temporaire d'un échantillon. Donc ils n'étaient pas soumis à cette procédure, de même pour la déclaration concernant un usage strictement personnel (article 13). En effet, ce régime dérogatoire, s'expliquait par la nécessité pour l'utilisateur de pouvoir voyager hors de ses frontières avec son ordinateur personnel et de continuer à l'utiliser.

Pour le régime de l'autorisation préalable [55], il existait aussi une triple distinction suivant qu'il était recherché une utilisation, une exportation une fourniture de moyens de cryptage.

Ainsi, pour une autorisation de fourniture de moyens de cryptographie une demande était déposée auprès du SCSSI. Cette demande devait préciser la durée qui ne pouvait excéder cinq ans (article 4 du décret du 28.12.1992). De plus la prestation fournie devait satisfaire à diverses obligations[56] :

- Conformité aux normes nationales des interfaces avec les utilisateurs.
- Sécurité de la gestion de la prestation.
- Conservation des éléments secrets pendant 10 jours ouvrables pour une communication précise et ponctuelle, et 4 mois dans les autres cas.
- Aménagement de possibilités techniques pour faciliter les investigations judiciaires.
- Déclaration aux autorités de police judiciaire des accès illicites au système de gestion ou des atteintes à sa sécurité. Et dans ce dernier cas, le fournisseur devrait aussi informer le SCSSI.

---

[54] On entend par déclaration générale toute déclaration qui est formulée par un fournisseur, a contrario de la déclaration individuelle, émanant d'un particulier

[55]Titre II du décret 92-1358 du 28 décembre 1992

[56]Arrêté du 28.12.92

Dans le cas de l'autorisation d'utilisation, la demande était déposée auprès du SCSSI mais ici, la durée était de 10 ans au maximum (article 6 alinéa 1et 4). La demande pouvait être générale ou personnelle.

- Quand elle était générale, elle était formulée par le titulaire de l'utilisation de fourniture (régime simplifié). Ce système constituait une simplification pour les futurs utilisateurs car ils étaient dispensés du dépôt d'une demande d'autorisation. Mais uniquement s'ils remplissaient les conditions de l'autorisation d'utilisation générale. Par exemple, une fois l'autorisation obtenue, le banquier, auquel le fournisseur avait vendu le produit, n'avait plus besoin de redemander une autorisation pour utiliser le produit.

- Quand l'autorisation était individuelle, elle était demandée par l'utilisateur. C'était une situation exceptionnelle pour le cas d'une absence d'autorisation générale. De cette façon, la fabrication ou l'exportation ne valait que pour l'utilisateur demandeur. Cette autorisation pouvait être assortie de conditions pour réserver l'utilisation de ces moyens ou prestations à certaines catégories d'utilisateurs (téléphone de voiture, produits bancaires comme des distributeurs de billets automatiques…). Mais cette autorisation pouvait également être retirée, de façon temporaire ou définitive, en cas de fausse déclaration, faux renseignements, de modifications, de non-respect des réglementations ou obligations prescrites par l'autorisation (article 8 du décret du 28.12.1992).

Enfin, une autorisation d'exportation pouvait être attribuée. Dans ce cas, le dossier de demande devait, en plus de la partie technique et administrative, comporter une demande de licence d'exportation déposée auprès de l'administration douanière (SE.TI.C.E). Cette licence n'était délivrée qu'après accord du Premier ministre.

Les sanctions étaient différentes selon que l'on contrevenait au régime de déclaration ou d'autorisation. Elles étaient constituées d'amendes de quatrième ou cinquième classe et de peine d'emprisonnement pouvant aller jusqu'à 3 mois.

Enfin, des peines complémentaires éventuelles pouvaient être possibles (confiscation des moyens de cryptologie, interdiction de solliciter une nouvelle autorisation…).

Au travers toutes ces procédures nous pouvons remarquer que la réglementation française était extrêmement restrictive en ce qui concernait la cryptographie et que tous manquements à ces prescriptions étaient sévèrement sanctionnés (décret 92-1358 du 28 décembre 1992).

La réglementation communautaire :

La cryptologie fut réglementé au niveau européen sous trois aspects différents. Elle fut réglementée comme outil pour la sécurité des systèmes d'informations, comme instrument de la criminalité informatique et comme bien à double usage (civil et militaire).

- L'aspect sécurité des système d'informations a été abordé par le Conseil de l'union européenne dans sa décision adopté le 31 mars 1992 [57]. Cette décision comprenait l'élaboration de stratégies globales pour la sécurité des systèmes d'information (plan d'action) et la création d'un groupe de hauts fonctionnaires (SOG-IS), dont le rôle était de conseiller la Commission sur les actions à entreprendre. Le but de cette décision était

> *«la mise au point de stratégies permettant à l'information de circuler librement à l'intérieur du marché unique, tout en assurant la sécurité de l'utilisation des systèmes d'information dans l'ensemble de la Communauté »*[58].

Par ce biais, le but était de promouvoir une interopérabilité des systèmes ainsi que réduire les barrières existantes et éviter l'apparition de nouvelles entraves entre les États membres et les autres pays.

Avec l'aide du SOG-IS, la commission a pu mettre en place un plan d'action cohérent qui s'est traduit par la publication de deux livres verts[59]. Au travers de ces documents, il apparaît que le but recherché est la protection adéquate des informations et des personnes physiques et non une volonté de réglementer la cryptographie ou de réduire son application. Cette vision se trouve confortée par la directive du 24 octobre 1995 relative à la protection des personnes

[57] Décision n° 92/242/CEE en matière de sécurité des systèmes d'informations, JO L 123, 8 mai 1992, p19

[58] Décision du Conseil du 31 mars 1992, JOCE 92/242/CEE

[59] the Green Book on the Security of Information Systems (18 octobre 1993) et, the Green Paper on Legal Protection for Encrypted Services in the Single Market, (le 6 mars 1996) : http://info.risc.uni-linz.ac.at/1/misc-info/crypto/green-paper.txt .

physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données[60]. En effet, le but est la protection des personnes par la cryptographie, et par-là même permettre la libre circulation des données concernées par cette directive.

Mais afin de limiter l'utilisation à des fins criminelles de la cryptologie, un compromis est recherché et il semble se diriger vers la mise en place d'un réseau de tiers de confiance, de certification chargée de la gestion des clés, de la certification, de la constitution de répertoire,…. [61]. Cependant des divergences sont apparus au moment de déterminer qui seront ces tiers de confiance. L'Allemagne proposait un « centralized escrow key from Brussel » alors que la France et le Royaume-Uni voyaient plutôt des tiers privés. Choix qui a été privilégié par la France[62].

- L'aspect criminalité informatique au travers de la cryptologie a été l'objet de la recommandation du 11 septembre 1995 concernant les problèmes de procédure criminelle dans le domaine de la technologie et de l'information[63]. Ce texte recommande particulièrement en matière de cryptographie :

> «*Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, whitout affecting its legitimate use more than is stricly necessary*. »[64]

Au sein de cette recommandation il n'y a aucune précision sur les mesures ou sur l'équilibre qu'il faut trouver entre sécurité publique et protection des individus. Selon le « C*ommunication Weeks International* », il faut interpréter ce texte comme interdisant les

[60]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, http://www2.echo.lu/legal/fr/dataprot/directiv/direct.html

[61]KOOPS, Bert-Jaap, «Crypto Law Survey», http://cwis.kub.nl/~frw/people/koops/lawsurvy-html

[62] voir *supra*

[63]Recommandation n° R (95) 13 of the Commitee of Ministers to Member States concerning Problems of criminal Procedure Law connected with Infornation Technology, http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html

[64]Appendix to Recommandation n° R (95)13, point V

moyens de cryptage trop performants, c'est à dire, ceux qui ne permettraient pas au gouvernement d'accéder aux clés de cryptage[65].

- Enfin, une réglementation sur la cryptographie envisagée en tant que bien à double usage (c'est à dire comme une arme de guerre), découle de deux textes communautaires. Ces textes réglementent l'exportation de biens à double usage. Il s'agit du règlement[66] et de la décision du 19 décembre 1994[67].

Le premier texte institue un régime communautaire de contrôle des exportations de biens à double usage et le second est relatif à l'action commune concernant le contrôle des exportations de biens à double usage.

Le règlement définis les biens à double usage comme :

> *« les biens susceptibles d'avoir une utilisation tant civile que militaire »*[68]

Le principe est que l'exportation des biens à double usage figurant sur l'annexe I de la décision du 19 décembre 1994, est soumise à autorisation individuelle. Celle-ci est octroyée par les autorités compétentes de l'État membre où est établi l'exportateur (article 3 et 6). Mais les États membres peuvent accorder le bénéfice de formalités simplifiées dans différents cas :

> *« - Une autorisation générale pour un bien ou un groupe de biens à double usage.*
> *- Une autorisation globale à un exportateur spécifique pour un bien ou un groupe de biens à double usage qui peut être valable pour les exportations à destination d'un ou de plusieurs pays déterminés.*
> *- Des procédures simplifiées dans le cas d'une exigence d'autorisation de la part d'un État membre au titre de l'article 5. »*

A contrario, un État membre pourrait interdire ou soumettre à autorisation l'exportation des biens à double usage qui ne figure pas sur la liste de l'annexe I (article 5).

---

[65] «Euro-clipper chip scheme proposed » in *Communications Week International*, daté du 18 septembre 1995

[66] Règlement du conseil n°3381/94 du 19 décembre 1994, JO CE L367/1 du 31 décembre 1994

[67] Décision du conseil n°94/942/PESC du 19 décembre 1994, JO CE L 367 du 31 décembre 1994 et notamment ses annexes I (pages 109 à 111) et IV (pages 156 et 157)

[68] Article 2, a) du règlement (ce) n ° 3381/94 du Conseil du 19 décembre 1994, JOCE N° L 367/1

De plus, pour garantir une application correcte de ce dernier, le règlement prévoit des procédures douanières particulières à l'exportation de ces biens (articles 10 et 11) et des mesures de contrôles assez strictes (articles 14 et 15).

Enfin, un groupe de coordination est institué (composé d'un représentant de chaque État et présidé par un membre de la Commission) afin d'examiner toute question concernant l'application du règlement ainsi que les mesures à prendre pour informer les exportateurs de leurs obligations (article 16).

Malgré tout, certains outils sont exclus du contrôle communautaire par l'annexe IV. Il s'agit de tous les procédés de cryptage utilisés dans des machines servant des transactions bancaires ou monétaires (distribution de billets automatiques….)[69]. De même sont exclus les radiotéléphones portatifs ou mobiles, les équipements de contrôle d'accès et les équipements d'authentification des données[70].

Étant donné que les instances européennes sont des institutions supranationales, le but recherché au travers de la réglementation de la cryptographie, n'est pas le même que pour ses États membres. En effet, même si ces instances considèrent encore la cryptologie comme un bien à double usage, elles ne perdent pas de vue les libertés présentes dans le traité de Rome ou de Schengen notamment la liberté de circulation (surtout en ce qui concerne les données). De plus, même si les instances européennes ne négligent pas les dangers de la cryptologie, elles n'oublient pas non plus l'importance de l'individu et de ses droits au sein de l'Europe. D'ailleurs en toute logique les réglementations françaises et belges devront s'aligner sur les prescriptions européennes.

B- Les normes Nord-américaines

Les normes Nord-américaines ne sont pas uniformes dans leurs appréciations de la cryptologie. Nous verrons principalement les États-Unis et le Canada. Cela dit, et pour évoquer le cas du Mexique, c'est l'institut du commerce extérieur qui régit les importations et

[69] Annexe IV, JOCE, N° L 367/157

[70] Ib.

exportations mexicaine. Or, il n'existe actuellement aucun contrôle sur l'importation et l'exportation des technologie de cryptage au Mexique.[71]

Les États-Unis

En 1996, la responsabilité de l'exportation de la cryptographie fut transférée du Département d'État au Département de commerce. Cela dit la NSA (National Security Agency) veille et conserve toutes ses prérogatives puisqu'elle dispose d'une équipe présente dans tous les ministères et services administratifs travaillant de près ou de loin sur le cryptage (Y compris les Département d'État et de la Justice…).

On ne peut en effet parler de la cryptographie et oublier la NSA qui semble être l'organisme contre lequel tous les libéralistes semblent s'acharner. La NSA fut crée en 1952 par Henry Truman et son existence fut longtemps gardé secrète. L'objectif de la NSA est d'écouter (et de décoder la cas échéant) toutes les communications entrant et sortant des États-Unis et susceptibles d'avoir de l'importance au regard de la sécurité de ce pays. Selon le STOA,[72]

> « toutes les communication électroniques, téléphoniques et toutes les télécopies en Europe sont quotidiennement interceptées par la National Sécurity Agency Des États-Unis, qui transfèrent toutes les informations provenant du continent européen via le centre statégique de Londres, puis par satellite vers Fort Meade au Maryland via le centre crucial de Menwith Hill dans la région des North York Moors au Royaume-Uni. Le système a été mis à jour pour la première fois dans les années soixante-dix par un groupe de chercheurs au Royaume-Uni (Campbell, 1981). Des travaux menés récemment par Nicky Hager (Secret Power, Hager, 1996) fournissent des détails extrêmement précis sur un projet nommé ECHELON. Hager a interrogé plus de 50 personnes travaillant dans le renseignement pour découvrir un système de surveillance qui s'étend au monde entier pour former un système pointé sur tous les satellites clés Intelsat utilisés pour transmettre l'essentiel des communications téléphoniques, Internet, le courrier électronique, les télécopies et télex transmis par satellite dans le monde entier. Les sites de ce système sont basés à Sugar Grove et Yakima aux États-Unis, à Waihopai en Nouvelle-Zélande, à Geraldton en Australie, à Hong Kong et à Morwenstow au Royaume-Uni. »

On peut alors facilement comprendre la puissance de cet organisme dont le budget, secrètement gardé, s'élèverait à 13 milliards USD par an pour un personnel qui serait composé de seize mille personnes. Pour la NSA, la technologie cryptographique est vitale aux intérêts

---

[71] ibid., p 506

[72] Étude intérimaire STOA, Une évaluation des techniques de contrôle politique, résumé analytique disponible à cette adresse http://www.europarl.eu.int/dg4/stoa/fr/publi/166499/execum.htm , visité le 20 juillet 1999

nationaux de sécurité. Ceux-ci comprennent les intérêts économiques, militaires et des affaires étrangères.

Le contrôle à l'exportation des produits de cryptographie est régi par le *Arms Export Control Act* (AECA) qui donne un large pouvoir à l'administration :

> *(a) (1)… The President is authorized to designate thoses items which shall de considered as defense articles and defense services for purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall constitute the US Munitions List.*
> *(2)… Decisions on issuing export licences under this section shall be made in coordination with the director of US Arms Control and Disarmament Agency, taking into account the Director's assessment as to whether the export of an article would contribute to an arm race, aid in the developpement of weapons of mass destruction, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreement or other arrangements.*[73]

Aux États-Unis les outils de cryptographie sont regroupés en cinq catégories qui déterminent comment et quelle autorisation donner à l'exportation, cela dit, comme le dit Schneier, toutes les autorisations à l'exportation sont faite après un avis de la NSA, avis toujours suivi :

> *« en réalité, la NSA à le contrôle de l'exportation des produits cryptographiques. Si vous voulez une "Commodity Juridiction" (CJ), vous devez soumettre votre produit à l'approbation de la NSA et soumettre votre demande de CJ au Département d'État. Après avoir obtenu l'autorisation de Département d'État, l'affaire passe dans la juridiction du département du Commerce, qui ne s'est jamais vraiment préoccupé de l'exportation de la cryptographie. Toutefois, le Département d'État n'accordera jamais une CJ sans l'approbation de la NSA et, pour autant que l'on sache, il n'a jamais refusé une licence après l'approbation de la NSA »*[74]

Concrètement les restrictions à l'exportation concerne les produits de chiffrement d'une puissance supérieure ou égale à 56 bits qui doivent obtenir une licence d'exportation. Les produits d'authentification peuvent être exporté après une seule approbation du Département d'État sans passer par les autres services. Cela étant il existe une exception réciproque entre les États-Unis et le Canada, puisque Les États-Unis autorisent l'exportation vers le Canada de toute quantité de logiciels de chiffrement personnalisés ou de matériel comportant un logiciel de chiffrement intégré.

[73] 22 US Code § 2778 (1997)

[74] ibid.

La NSA est aussi un organisme scientifique regroupant un nombre impressionnant de cryptananalyste. C'est dans ses services qu'ont été développé certaines puces visant à garantir la sécurité nationale et à satisfaire les utilisateurs privé en permettant l'utilisation d'outils cryptographique. Deux types de puces furent été ainsi créés :

- La puce Clipper est dédiée au chiffrement des conversations vocales. Le problème est ici que cela revient à déposer les clés au gouvernement qui aurait ainsi la possibilité d'espionner les citoyens :

> *« Chaque puce a un clé spéciale, qui n'est pas nécessaire pour les messages. Cette clé est utilisée pour chiffrer une copie de la clé utilisée par chaque utilisateur pour chiffrer ses messages. Lors du processus de synchronisation, la puce Clipper émettrice génère et envoie un champ d'accès de respect de la loi (LEAF pour Law Enforcement Access Field) à la puce Clipper réceptrice. Le LEAF contient une copie de la clé de scéance courante, chiffrée avec une clé spéciale (la clé d'unité). Ceci permet au Gouvernement (US) de découvrir la clé de séance et ainsi d'écouter le contenu de la conversation. »*[75]

Cela dit, des erreurs ont été décelés dans le Clipper, et permettraient à des pirates « de déjouer le système »[76]

- La puce Capstone vise quant à elle à fournir les outils cryptographiques nécessaires pour un commerce électronique sécuritaire. Ici également les intrusions possibles du gouvernement américain dans la vie privée des citoyens sont perçues par certain comme inacceptable, légitime pour d'autre. Cela dit, Capstone n'est applicable qu'au gouvernement et aux entités privées prenant contact avec lui. L'utilisation de cette puce entre personnes privés n'a aucun caractère obligatoire, ce qui donne à ce système une constitutionnalité évidente mais un applicabilité plus que douteuse puisque les criminels ne l'utiliseront jamais.

Nous le voyons les États-Unis constituent un intéressant terrain d'observation, regroupant en son sein une administration lourde en contrainte et les associations les plus radicales pour ce qui est de la libéralisation de la cryptographie. Cela dit, pour ce qui est de l'utilisation de

[75] Schneier op. cit., p 620 et s

[76] KING, Henry R., « Big Brother, the holding compagny : a review of Key-escrow Encryption Technologie » (1995) 21 Rutgers Comp. & Tech. L.J. 224, 234, cité par Pierre Trudel : Trudel, Pierre et autres, Droit du cyberespace, Montréal, Éditions Thémis, 1997, chap. 19, page 20

moyens de cryptographie à l'intérieur de son territoire, les États-Unis permettent une utilisation de moyens puissant, il faut bien distinguer cette situation de celle qui existe en France où cet usage interne de la cryptographie est réglementé.

Le Canada

Le cas du Canada ressemble à celui des autres pays signataires de l'Arrangement de Wassenaar. Ici aussi la réglementation sur la cryptographie a été dictée par la raison d'État et ce pays procède à un contrôle des exportations de la cryptographie en limitant l'exportation du matériel ou des logiciels personnalisés. Les lois concernant l'exportation au Canada sont similaires à celle des États-Unis. Cependant,

> *« le 24 décembre 1996, le Canada a modifié sa politique pour une période d'essai de 12 mois, et autorisé l'exportation, vers la plupart des pays, de logiciels de chiffrement personnalisés de 56 bits et de matériel comportant un logiciel de chiffrement. Cette période a été prolongée jusqu'au 30 juin 1998 […]L'exportation de produits cryptographiques aux fins d'utilisation par des citoyens canadiens ou des firmes canadiennes à l'étranger, quoique contrôlée, est habituellement autorisée..»*[77]

Concernant les atteintes aux libertés, La *Charte canadienne des droits et libertés*[78] justifierait une atteinte raisonnable dans le cadre d'une société libre et démocratique :

> ***1.*** *La Charte canadienne des droits et libertés garantit les droits et libertés qui y sont énoncés. Ils ne peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique.*

Mais nous voyons au travers de cette Charte que tout l'intérêt d'un individus s'estimant lésé, sera d'établir que les agissements de l'État, écoutes et surveillances en l'espèce, ne sont pas conforme à ce test constitutionnel.

II… face à des revendications libertaires

Le développement exponentiel des télécommunications et de l'informatique depuis une trentaine d'années a donné à l'individu de nouveaux outils et ainsi, l'occasion de développer

[77] Groupe de travail sur le commerce électronique, *Politique cadre en matière de cryptographie aux fins du commerce électronique, Pour une économie et une société de l'information au Canada*, Industrie Canada, Février 1998, http://strategis.ic.gc.ca/crypto, visionné le 20 juillet 1999

une cryptologie à vocation civile. Les discours sur une autoroute de l'information annoncés il y a 10 ans se sont effectivement réalisés à grande vitesse et ce principalement en Amérique du nord. Il est d'ailleurs manifeste que ce soit dans ces pays que la réaction des individus fut la plus intransigeante contre les menaces portées contre la vie privée et/ou la *privacy*. Il semble en effet que les citoyens européens n'ont pas pris conscience des enjeux de la cryptographie sur les libertés individuelles. En effet, si le gouvernement Français a assouplis ses lois sur la cryptographie ce n'est nullement suite à une pression des citoyens français mais plutôt pour répondre aux inquiétudes des sociétés intéressés par le commerce électronique face à l'avance des pays nord américains dans ce domaine. Cela dit nous évoquerons cet aspect commercial dans la seconde partie de ce mémoire.

Les États-Unis ont incontestablement une approche quasi religieuse[79] en matière de liberté individuelle et le premier amendement de la Constitution[80] est un des enseignements de base donné dans les petites classes. Il suffit d'avoir à l'esprit la porté relative des scandales d'écoutes téléphoniques illégales faites par des présidents français et américain pour comprendre toute la nuance entre nos deux États pour ce qui est de l'appréciation de l'intolérable et de l'excusable.

Nous entrons ici dans la sphère purement individuelle de la cryptographie. La cryptographie est en effet le moyen pour tout individu de se protéger contre les tentatives de l'État, de toute organisation ou de tout autre individu, d'avoir accès aux information qu'il désire garder secrètes. Nous nous porterons pour cette partie sur la protection contre les instances étatiques mais il est bien entendu qu'au delà du Roman de Georges Orwell[81], *Big Brother* peut également prendre une forme privée (A). Devant l'état des lieux que nous proposons ici, il sera utile de traiter des tentatives réalisés pour s'assurer une assez bonne protection. Nous sortirons donc ici du droit tel qu'il est pratiqué pour traiter plutôt du droit tel qu'il se construit (groupes de pression, pétitions électroniques etc.) (B).

---

[78] L.R.C. (1985), App. II, n°44

[79] Les notions de « Pères Fondateurs de la Constitution américaine » comme la devise « In God we trust » sont manifestes de ce caractère religieux.

[80] amendement sur la liberté d'expression, dont l'application rend, par exemple, constitutionnels les excès xénophobe dans la discours du Klu Klux Klan, idée impensable dans une Europe marquée par la Shoah.

[81] *1984, Paris, 1984, éditions Folio*

A- La crainte du *Big Brother*

Sans doute peut-on dire avec Pierre Trudel que les préoccupations que prennent la vie privée sont parfois démesurés par rapport au nombre d'incidents rapportés[82]. En effet, dans l'hypothèse (vérifiée selon le rapport du STOA, voir *supra*), où l'ensemble des informations sont interceptés, il n'en demeure pas moins qu'il est extrêmement difficile de trier autant de données.

Sur l'Internet, les États sont dans cette situation où ils ont exactement la même possibilité de diffuser de l'information que les individus. Il y a une certaine concurrence évidente entre l'État et le particulier dans le cas d'oppositions exprimée en ligne contre le pouvoir en place dans des pays restreignant la liberté d'expression : les deux entités disposent des mêmes moyens techniques et de diffusion. Ici réside une augmentation du pouvoir individuel sur tous les autres pouvoirs. Concernant le pouvoir étatique, cela peut-être intolérable.

Au sujet des pays démocratiques, il est de leurs responsabilités d'assurer les individus contre toute dérive futur d'un régime en place. La liberté d'expression est une notion fluctuante et relative à chacun des pays, elle n'était pas la même qu'aujourd'hui sous Mac Carthy ou sous Vichy. La cryptographie permet d'éviter toute analyse des contenus de messages qui pourraient, le temps passant, ressortir et être opposé à certains individus.

La crainte d'un État observant les faits et gestes des individus n'est pas infondée. Grâce à l'informatique et aux possibilités que cette outils permet dans le traitement et le croisement des informations personnelles, l'individu peut-être littéralement suivis et observé. Techniquement, l'espace de réelle confidentialité n'existe pratiquement plus. Un ensemble d'éléments recense exhaustivement tous nos faits et gestes, par exemple :

---

[82] Trudel, Pierre et autres, Droit du cyberespace, Montréal, Éditions Thémis, 1997, chap. 1, page 19

- L'augmentation soudaine de la consommation électrique suppose une présence dans son domicile de la personne, voir même l'heure de son réveil (consommation d'eau, d'électricité encore…).
- L'utilisation des différentes clés d'accès électronique donnent ces mêmes informations à la seconde près.
- L'utilisation des moyens de paiement autres que les espèces permet d'être informer et des déplacement et des types de consommations.
- Les communications téléphoniques peuvent être écoutées, de même que peut être située la position géographique des correspondants dans le cas de l'utilisation de téléphone cellulaires…

Bref, à moins de vivre en dehors de son temps, tous les actes de la vie courante peuvent être autant d'éléments pour surveiller un individu. La cryptologie ne règle pas tous ces problèmes et ne concerne l'individu que dans le cas d'informations que celui-ci désire envoyer.

La crainte du *Big Brother* n'est pas farfelue ni destinée aux paranoïaques pris de délire. L'histoire récente révèle souvent, après que les accès aux dossiers soient autorisés, des pratiques révoltantes que les politiques contemporains expliquent par le fait d'une autre époque et d'autres nécessités ou mœurs sociales. En fait, à moins d'une révolution dans la manière d'aborder l'État, il n'y a aucune raison pour que ces pratiques aient cessé car la surveillance et le renseignement sont des éléments incontournables de la raison d'État.

B- Et la recherche d'une protection

Il est incontestable que le développement de l'internet à permis la mise à disposition du public de moyens de cryptographie qui n'était pas vraiment, avant cela, une préoccupation pour les individus. Dans son ouvrage, Jacques Stern évoque ce rapport d'une commission de la chambre des représentants au États-Unis dans lequel il a été démontré qu'il ne fallait que « 3 minutes et 14 secondes (!) pour localiser sur le réseau, la copie d'un programme permettant d'exécuter l'algorithme de chiffrement DES »[83]. Nous l'avons vu, les craintes sont sans doute démesurées mais il n'en demeure pas moins que le droit de disposer et d'utiliser les logiciels de

[83] STERN, Jacques, op. cit. p.128

cryptographie est devenu un élément incontournable d'un « droit de l'internaute » du fait de la rapidité des questions tournant autour de ces problèmes de confidentialité. De par certaines maladresse des États (des États-Unis, de la France…, en fait de tous les États tentant d'imposer certaines règles) et de par la réaction de certaines organisations privées ayant rapidement compris les réalités de l'internet, la cryptographie à bénéficiée d'une incroyable publicité. La première maladresse se nomme Philip Zimmermann, la première réaction fut l'utilisation judicieuse de l'internet par des groupes de pressions.

PGP et Zimmermann

Nous l'avons vu, Philip Zimmermann inventa un logiciel qui reprend certains éléments d'autre algorithme de cryptage connus par ailleurs (RSA pour la gestion des clés, IDEA pour le chiffrement et MD5 pour ce qui concerne la fonction de hachage à sens unique). Il semble à l'heure actuelle que PGP soit le logiciel de chiffrement grand public le plus proche de la classe militaire. Nous avons hésité à mettre l'explication des motivations ayant poussé Philip Zimmermann à développer PGP dans le corps de ce mémoire plutôt qu'en annexe, mais il semble que son explication illustre parfaitement un certain état d'esprit impensable en France et il serait vain de chercher artificiellement à réduire son propos. Sans doute l'auteur désire t'il se fabriquer une légende mais il faut garder à l'esprit les réelles pression que le gouvernement américain lui a fait subir[84] :

> « *"Quoi que vous ferez, ce sera insignifiant, mais il est très important que vous le fassiez." –*
>
> Mahatma Gandhi
>
> C'est personnel. C'est privé. Et cela ne regarde personne d'autre que vous. Vous pouvez être en train de préparer une campagne électorale, de discuter de vos impôts, ou d'avoir une romance secrète. Ou vous pouvez être en train de communiquer avec un dissident politique dans un pays répressif. Quoi qu'il en soit, vous ne voulez pas que votre courrier électronique (e-mail) ou vos documents confidentiels soient lus par quelqu'un d'autre. Il n'y a rien de mal dans la défense de votre intimité. L'intimité est dans le droit fil de la Constitution.
>
> Le droit à la vie privée est disséminé implicitement tout au long de la Déclaration des Droits. Mais quand la Constitution des États-Unis a été établie, les Pères Fondateurs ne virent aucun besoin d'expliciter le droit à une conversation privée. Cela aurait été ridicule. Il y a deux siècles, toutes les conversations étaient privées. Si quelqu'un d'autre était en train d'écouter, vous pouviez aller tout simplement derrière la grange et avoir une conversation là. Personne ne pouvait vous écouter sans que vous le sachiez. Le droit à une conversation

[84] Les douanes américaines se sont « intéressées » à Zimmermann pour exportation irrégulière par la biais de l'internet. Le dossier semble actuellement classé du fait notamment du soutient et de la colère de nombreux internautes.

privée était un droit naturel, non pas seulement au sens philosophique, mais au sens des lois de la physique, étant donnée la technologie de l'époque.

Mais avec l'arrivée de l'âge de l'information, commençant avec l'invention du téléphone, tout cela a changé. Maintenant, la plupart de nos conversations sont acheminées électroniquement. Cela permet à nos conversations les plus intimes d'être divulguées sans que nous le sachions. Les appels des téléphones cellulaires peuvent être enregistrés par quiconque possède une radio. Le courrier électronique, envoyé à travers Internet, n'est pas plus sûr que les appels de téléphone cellulaire. L'e-mail est en train de remplacer rapidement le courrier classique, devenant la norme pour tout le monde, et non plus la nouveauté qu'il était dans le passé. Et l'e-mail peut être systématiquement et automatiquement fouillé à la recherche de mots-clés, sur une grande échelle, sans que cela soit détecté. C'est comme la pêche aux filets dérivants.

Peut-être pensez-vous que le courrier électronique que vous recevez est assez légitime pour que le cryptage ne se justifie pas. Si vous êtes vraiment un citoyen au dessus de tout soupçon, pourquoi n'envoyez-vous pas toujours votre correspondance papier sur des cartes postales? Pourquoi ne vous soumettez-vous pas aux tests de consommation de drogue sur simple demande? Pourquoi exigez-vous un mandat de perquisition pour laisser la police fouiller votre maison? Essayez-vous de cacher quelque chose? Si vous cachez votre courrier dans des enveloppes, cela signifie-t-il que vous êtes un [élément] subversif ou un trafiquant de drogue, ou peut-être un paranoïaque aigu? Est-ce que les citoyens honnêtes ont un quelconque besoin de crypter leurs e-mails?

Que se passerait-il si tout le monde estimait que les citoyens honnêtes devraient utiliser des cartes postales pour leur courrier? Si un non-conformiste s'avisait alors d'imposer le respect de son intimité en utilisant une enveloppe, cela attirerait la suspicion. Peut-être que les autorités ouvriraient son courrier pour voir ce que cette personne cache. Heureusement, nous ne vivons pas dans ce genre de société car chacun protège la plupart de son courrier avec des enveloppes. Aussi personne n'attire la suspicion en protégeant son intimité avec une enveloppe. La sécurité vient du nombre. De la même manière, ce serait excellent si tout le monde utilisait la cryptographie de manière systématique pour tous ses e-mails, qu'ils soient innocents ou non, de telle sorte que personne n'attirerait la suspicion en protégeant l'intimité de ses e-mails par la cryptographie. Pensez à le faire comme une forme de solidarité.

Jusqu'à aujourd'hui, si le Gouvernement désirait violer l'intimité de citoyens ordinaires, il devait consentir une certaine dépense d'argent et de travail pour intercepter, ouvrir et lire les lettres. Ou il devait écouter et si
possible transcrire le contenu des conversations téléphoniques, du moins avant que la technologie de la reconnaissance vocale automatique soit disponible. Cette méthode, coûteuse en travail, n'était pas praticable sur une grande échelle. Cela était fait seulement dans les cas importants, quand cela en valait la peine.

En 1991 aux États-Unis, le projet de loi 266 du Sénat, un texte anti-criminalité, comportait une disposition troublante cachée à l'intérieur du texte. Si cette résolution était devenue une véritable loi, cela aurait contraint les fabricants d'équipements de communications sécurisées à insérer des "portes dérobées" spéciales dans leurs produits, de telle sorte que le gouvernement puisse lire les messages cryptés par n'importe qui. Le texte disait: "La recommandation du Sénat est que les fournisseurs de services de communications électroniques et les fabricants d'équipements de communication électronique devront s'assurer que les systèmes de communication permettent au gouvernement d'obtenir le contenu en clair des communications vocales, des données, et des autres communications dans les cas prévus par la loi". Ce fut cette loi qui m'a conduit à publier PGP électroniquement de manière gratuite cette année-là, peu de temps avant que la mesure ne soit retirée après de vigoureuses protestations des
groupes de défense des libertés civiles et des groupes industriels.

Le “Digital Telephony bill” de 1994 a fait obligation aux compagnies de téléphone d’installer des dispositifs d’interception à distance dans leurs commutateurs centraux, créant une nouvelle infrastructure technologique pour cette interception “pointer-et-cliquer”, de telle sorte que les agents fédéraux n’auront plus à sortir et attacher des pinces crocodiles sur les lignes de téléphone. Maintenant, ils auront la possibilité de rester assis dans leur quartier général à Washington et d’écouter vos appels téléphoniques. Bien sûr, les lois requièrent encore une réquisition judiciaire pour une interception. Mais alors que les infrastructures technologiques peuvent durer pendant des générations, les lois et politiques changent du jour au lendemain. Une fois que l’infrastructure des communications est optimisée pour la surveillance, une modification dans les conditions politiques peut conduire à abuser de ce pouvoir fondé sur de nouvelles bases. Les conditions politiques peuvent se modifier avec l’élection d’un nouveau gouvernement, ou peut-être même de manière plus abrupte après l’attentat à la bombe contre un immeuble fédéral.

Un an après que le “Digital Telephony bill” de 1994 soit passé, le FBI dévoila des plans pour exiger des compagnies de téléphone d’intégrer dans leurs infrastructures la capacité d’intercepter simultanément 1 % de tous les appels téléphoniques dans toutes les grandes villes américaines. Cela représenterait une multiplication par plus de mille par rapport au niveau précédent dans le nombre d’appels qui peuvent être interceptés. Dans les années précédentes, il y avait eu seulement à peu près un millier de réquisitions d’interceptions judiciaires par an aux États-Unis, à la fois au niveau fédéral, au niveau des États et au niveau local. Il est difficile de savoir comment le gouvernement pourrait ne serait-ce qu’employer assez de juges pour signer assez d’ordres d’interception pour intercepter 1 % de tous les appels téléphoniques, encore moins embaucher assez d’agents fédéraux pour s’asseoir et écouter tout ce trafic en temps réel. La seule façon plausible de traiter toute cette quantité de trafic est une application massivement Orwellienne de la technologie de reconnaissance vocale pour passer au crible tout cela, à la recherche de mots clés intéressants ou de la voix d’un interlocuteur particulier. Si le gouvernement ne trouve pas la cible dans le premier échantillon de 1 %, les interceptions peuvent être étendues à un 1 % différent jusqu’à ce que la cible soit trouvée, ou jusqu’à ce que la ligne de téléphone de chacun ait été inspectée à la recherche de trafic subversif. Le FBI dit qu’ils ont besoin de cette capacité pour prévoir le futur. Ce plan a provoqué un tel scandale qu’il a été retiré au Congrès, en peu de temps, en 1995. Mais le simple fait que le FBI ait été jusqu’à demander ces pouvoirs élargis révèle leur programme. Et la défaite de ce plan n’est pas si rassurante quand vous considérez que le “Digital Telephony bill” de 1994 avait aussi été retiré la première fois qu’il a été introduit, en 1993.

Les avancées technologiques ne permettent pas le maintien du statu quo, à partir du moment où la vie privée est concernée. Le statu quo est instable. Si nous ne faisons rien, des nouvelles technologies donneront au gouvernement des nouvelles capacités de surveillance dont Staline n’aurait jamais pu rêver. La seule façon de garder la haute main sur la vie privée dans l’âge de l’information est la cryptographie sûre.

Vous ne devez pas avoir à vous méfier du gouvernement pour vouloir utiliser de la cryptographie. Vos affaires peuvent être interceptées par les concurrents, le crime organisé, ou des gouvernements étrangers. Plusieurs gouvernements, par exemple, admettent utiliser leurs services d’écoutes contre les compagnies d’autres pays pour donner à leurs propres sociétés un
avantage sur la concurrence. L’ironie est que les restrictions du gouvernement des États-Unis sur la cryptographie ont affaibli les défenses des entreprises américaines contre les services de renseignement étrangers et le crime organisé.

Le gouvernement sait quel rôle pivot la cryptographie est destinée à jouer dans le rapport de force avec son peuple. En Avril 1993, l’Administration Clinton dévoila une audacieuse nouvelle initiative dans la politique cryptographique, qui avait été préparée à l’Agence de Sécurité Nationale (“National Security Agency” NSA) depuis le début de l’Administration Bush. La pièce centrale de ce dispositif est le microprocesseur construit par le gouvernement et appelé puce “Clipper”, contenant un algorithme de la NSA classé top

secret. Le gouvernement est en train d'encourager l'industrie privée à l'insérer dans leurs équipements de communications sécurisées, comme les téléphones sécurisés, les fax sécurisés, etc. AT&T insère dès à présent la "Clipper" dans ses équipements vocaux sécurisés. Ce que cela cache: au moment de la fabrication, chaque puce "Clipper" sera chargée avec sa propre clé, et le gouvernement en gardera une copie, placée entre les mains d'un tiers. Il n'y a pas à s'inquiéter, cependant: le gouvernement a promis qu'il utiliserait ces clés pour lire le trafic des citoyens uniquement dans les cas dûment autorisés par la loi. Bien sûr, pour rendre la "Clipper" complètement efficace, la prochaine étape devrait être de mettre hors-la-loi toute autre forme de cryptographie.

Le gouvernement avait déclaré au début que l'utilisation de Clipper serait volontaire, que personne ne serait forcé de l'utiliser à la place d'autres types de cryptographie. Mais la réaction du public contre le Clipper a été forte, si forte que le gouvernement a anticipé. L'industrie informatique a affirmé de manière monolithique son opposition à l'usage de Clipper. Le directeur du FBI, Louis Freeh, répondit à une question lors d'une conférence de presse en 1994 en disant que si Clipper n'arrivait pas à obtenir le soutien du public, et que les interceptions du FBI étaient réduites à néant par une cryptographie non contrôlée par le gouvernement, son Bureau n'aurait pas d'autre choix que de chercher une solution législative. Plus tard, dans les suites de la tragédie d'Oklahoma City, M. Freeh témoignant devant la Commission Judiciaire du Sénat, déclara que la disponibilité publique de cryptographie sûre devait être restreinte par le gouvernement (bien que personne n'eût suggéré que la cryptographie avait été utilisée par les auteurs de l'attentat).

L'Electronic Privacy Information Center (EPIC) a obtenu des documents révélateurs par le biais du "Freedom of Information Act" [loi sur la liberté de l'information]. Dans un document de travail intitulé "Encryption: The Threat, Applications and Potential Solutions" [Cryptage: la menace, les applications, et les solutions possibles], et envoyé au Conseil national de sécurité en Février 1993, le FBI, la NSA, et le Ministère de la Justice (DOJ) concluaient que "Les solutions techniques, telles qu'elles existent, marcheront seulement si elles sont incorporées dans tous les produits de cryptage. Pour s'assurer que cela a lieu, une loi obligeant à l'utilisation de produits de cryptage approuvés par le Gouvernement ou l'adhésion aux critères de cryptage du Gouvernement est requise."

Le Gouvernement a eu un comportement qui n'inspire pas confiance dans le fait qu'il n'abuseront pas de nos libertés civiles. Le programme COINTELPRO du FBI avait ciblé les groupes qui s'opposaient aux politiques du Gouvernement. Ils ont espionné les mouvements pacifistes et le mouvement des droits civils. Ils ont intercepté le téléphone de Martin Luther King Jr. Nixon avait sa liste d'ennemis. Et ensuite il y a eu la pagaille du Watergate. Le Congrès paraît maintenant prêt à faire passer des lois restreignant nos libertés civiles sur Internet. A aucun moment dans le passé la méfiance envers le Gouvernement n'a été si largement partagée sur tout le spectre politique qu'aujourd'hui.

Si nous voulons résister à cette tendance inquiétante du gouvernement pour rendre illégale la cryptographie, une mesure que nous pouvons adopter est d'utiliser la cryptographie autant que nous le pouvons actuellement pendant que c'est encore légal. Quand l'utilisation de cryptographie sûre devient populaire, il est plus difficile pour le gouvernement de la criminaliser. Par conséquent, utiliser PGP est bon pour préserver la démocratie.

Si l'intimité est mise hors la loi, seuls les hors-la-loi auront une intimité. Les agences de renseignement ont accès à une bonne technologie cryptographique. De même les trafiquants d'armes et de drogue. Mais les gens ordinaires et les organisations politiques de base n'avaient pour la plupart pas eu accès à une technologie cryptographique de "qualité militaire" abordable.

Jusqu'à présent. PGP donne aux gens le pouvoir de prendre en main leur intimité. Il y a un besoin social croissant pour cela. C'est pourquoi je l'ai créé. »[85]

Aujourd'hui, PGP est le standard en matière de protection du courrier électronique.

Les groupes de pression

Cette pression est le fait de plusieurs organisations. Elle n'est pas seulement américaine aussi nous tiendrons compte des avis de la CNIL sur la cryptologie.

- Les groupes de pression américains

L'Electronic Frontier Foundation est devenu rapidement un acteur incontournable pour ce qui est de la protections des droits civils dans le cyberespace. Ils sont d'ailleurs à l'origine de la campagne du ruban bleu qui illustrait (et illustre encore) de nombreux sites de la Toile.

Pour l'EFF, l'utilisation et l'accès à l'information relative à la cryptographie est un droit fondamental dans lequel le gouvernement n'a pas à intervenir. Avec le Digital Privacy and Security Working Group qu'elle a organisé, l'EFF à fait opposition contre le projet de loi sur le téléphone digital et à la puce Clipper que l'EFF considère comme une machine à écoute téléphonique.

En dehors de son aspect de groupe de pression, l'EFF est toujours représenté dans les procès relatif au contrôle de l'exportation des outils de cryptographie. Inutile de préciser que son soutient à Philip Zimmermann fut total.

Selon le Monde diplomatique[86], l'EFF dispose d'une influence réelle auprès des membres du Congrès. Les bureaux de l'EFF sont d'ailleurs situés à Washington[87] ce qui illustre très

[85] ZIMMERMANN, Philip, « Pourquoi j'ai écrit PGP », Mode d'emploi de PGP freeware version, http://www.cl.cam.ac.uk/~fapp2/pgpenfrancais/doc.htm

[86] EUDES, Yves, « Bataille pour la liberté sur les résaux », *Le monde diplomatique*, hors série, collection manière de voir, Octobre 1996, p.37

[87] Electronic Frontier Foundation, 1001 G Street NW, Suite 950E, Washington D.C. 20001, USA, http://www.eff.org

justement son activité. Quant au budget de cette fondation, il est assuré par de nombreuses sociétés impliquées dans la création informatique comme Microsoft, IBM, AT&T, APPLE[88]. Le paradoxe est ici intéressant puisque Microsoft n'est pas vraiment en phase avec la privacy quant à ses logiciels et qu'AT&T est la première société à introduire la puce Clipper dans le dispositif de sécurité du téléphone TSD (Telephone Security Device) modèle 3600…

L'Electronic Privacy Information Center[89] (EPIC) est également un groupe actif, poursuivant les mêmes objectifs que l'EFF et localisé lui aussi à Washington…

- La France, La Commission Nationale Informatique et Libertés

Autorité administrative indépendante, il semble en effet indiscutable qu'en matière de cryptographie, la CNIL a exercé ce qui pourrait s'apparenter à des pressions sur les derniers gouvernements. En effet, dès 1996[90] la CNIL estimait que

> *« l'élaboration d'un cadre juridique protégeant le droit de l'individu au respect de sa vie privée et de l'anonymat s'avère indispensable, notamment par la création de procédures de cryptage fiables, lesquelles nécessiteront des directives européennes et des dispositifs de certification à l'échelle européenne. »*

En 1996 les procédés de cryptage n'avaient rien de fiable puisque les décrets d'application de la Loi de réglementation des télécommunications[91] ne sont sortis qu'en 1998, ils étaient donc tout simplement interdits en France sauf un avis favorable du SCSSI, organisme militaire qui n'a pas désiré répondre à nos appels.

Autorité indépendante, la CNIL n'en est pas moins respectueuse des lois. Peut-être avec le recul il semble clair que la Commission a fait preuve d'ironie en soulignant le rôle exagéré que la Loi donnait au SCSSI. Elle tenta toutefois la concertation dans le cas d'un projet télémédecine via l'internet.

---

[88] TORRÈS, Astrad, « Faut-il brûler Internet », *Le monde diplomatique*, hors série, collection manière de voir, Octobre 1996, p.57

[89] http://www.epic.org

[90] CNIL, *17ème rapport d'activité 1996*, Documentation Française, ISBN : 2 11 003757-1.

[91] Loi n° 96-659 du 26 juillet 1996, JO 27 juill. 1996, p. 11384

« Aussi, la CNIL n'a-t-elle délivré un avis favorable qu'après s'être assurée de l'efficacité des solutions de sécurité proposées. Aussi, après concertation avec le Service central de la sécurité des systèmes d'information (SCSSI), compétent pour autoriser l'éventuel chiffrement des données, la CNIL a estimé que le recours à la cryptologie était indispensable pour assurer une protection efficace des données à caractère personnel circulant sur les réseaux. Il en résulte qu'il doit être procédé au chiffrement des données transmises par Internet, par un algorithme de cryptage autorisé par le SCSSI. »[92]

Autorité administrative, la CNIL est, contrairement aux groupes de pression américain, à l'abris des politiques industrielles et commerciales.

Section II : Le présent : Les antagonismes en présence

Les réseaux informatiques ont créé de nouvelles possibilités en ce qui concerne les communications personnelles et commerciales. Mais cela n'a pas été sans répercussions néfastes sur la capacité des organismes d'application des lois de protéger le public. La nouvelle technologie à également produit de nouvelles façon de commettre d'anciens crimes et de nouvelles façons de dissimuler des preuves. Son utilisation soulève des inquiétudes (I) mais elle peut contribuer à protéger l'individu (II).

I- La protection de l'État

La sécurité publique, la lutte contre la criminalité, la sécurité nationale et la conformité aux règlements, exigent une réglementation adaptée. La justification d'une réglementation sévère, n'est pas moins que de :

"*préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État*"
(article 28 alinéa 2 de la loi du 26 juillet 1996).

En effet, le maintien de l'ordre public est une des rationalités les plus anciennes du droit. Cette notion d'ordre public peut être comprise comme l'ensemble des normes et valeurs perçues comme fondamentales au sein d'une société et dont la protection et le maintien incombent à une autorité publique détenant un pouvoir de coercition. Ce sont des normes qui ne peuvent être transgressées sans qu'il n'y ait sanction (réelle ou appréhendée)[93]. Ainsi, le thème

[92] CNIL, 18ème rapport d'activité 1997, Documentation Française, ISBN : 2 11 004033-5.
[93] Trudel, Pierre et autres, "Droit du cyberespace", Montréal, *Éditions Thémis*, 1997, p.54

de la sécurité est impliqué à deux niveaux : la sécurité publique qui est une volonté de maintenir l'ordre public (B) et la sécurité nationale qui concerne la protection contre les menaces extérieures (invasion ou terrorisme) (A).

A- La sécurité « extérieure »

La sécurité nationale vise à assurer la sécurité des États et des institutions publiques. De tous temps, les services secrets ont utilisé toutes sortes de codages et de moyens cryptographiques pour communiquer entre agents et gouvernements, de telle sorte que les « ennemis » ne puissent pas comprendre les informations échangées. La cryptologie a alors évolué dans ces milieux fermés qu'étaient les gouvernements, les services secrets et les armées. Aussi, très peu de gens, voire personne n'utilisait la cryptographie à des fins personnelles. C'est pourquoi, pendant tant d'années, la cryptologie est restée une science discrète. La cryptologie fut longtemps considérée comme un instrument de sécurité et de protection pour les *États Nations*.

Le droit de la cryptologie opposait les « libéraux » et les « sécuritaires ». Le principe de liberté triomphait dans la majorité des pays membres des organisations internationales, mais pas dans l'ex-URSS et aux États-Unis, où les exportations étaient sévèrement limitées.

En France, le bien du pays est mis en avant afin de protéger «l'État-Roi ». Pour cela l'État se réserve le droit d'intervenir à tout moment et de contrôler tout ce qui se passe sur son territoire. Mais, la France ne se borne pas à intercepter et déchiffrer les messages d'autrui, comme le font d'autres pays. Elle se particularise par une interdiction assez stricte de crypter tout message, d'user, fournir et exporter tout moyen de cryptologie. Ainsi, la France est l'un des pays les plus sécuritaires en cryptologie, cela est conforme à sa tradition juridique et militaire. Depuis la loi du 26 juillet 1996[94], ainsi que des décrets[95] et des arrêtés de 1998[96] , le

[94] Loi n°96-659 du 26 juillet 1996 sur la réglementation des télécommunications

[95] Décret n°98-206 du 23 mars 1998 relatif aux opérations dispensées de toute formalité préalable, JO du 25 février 1998, p.4448 et 4449

[96] Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande des organismes gérant pour le compte d'autrui des conventions secrètes. , JO du 15 mars 1998, p.3886 à 3891

chiffrement est libre en France pour l'utilisation des clefs d'une longueur inférieure ou égale à 40 bits. Mais, un régime de déclaration ou d'autorisation s'applique dans la plupart des cas.

Cela est justifié par le fait que les procédés de cryptage inviolables peuvent être utilisés par des gouvernements ou d'autres organisations hostiles pour cacher des informations subversives. À ce titre ils constituent une menace potentielle pour la sécurité nationale[97], ils peuvent encourager le terrorisme et faire craindre des agissements perfides d'États étrangers ou de groupes organisés.

Ainsi, l'État invoque le fait qu'il doit avoir accès à certains types d'informations pour pouvoir contrer les réseaux terroristes et les autres types d'activités illégales[98]. En effet, les États craignent les actions de "crypto-anarchistes"[99], militants purs et durs d'une généralisation et d'une liberté totale de la cryptographie. Aussi, bien évidemment, l'État cherche à ralentir ou à stopper la diffusion de cette technologie, invoquant les impératifs de sécurité nationale. Mais cette position semble extrémiste car les terroristes, les trafiquants d'armes et les espions n'ont pas attendu la cryptographie pour prospérer.

B- La sécurité intérieure

La sécurité publique doit protéger les valeurs reconnues comme fondamentales au sein d'une société. Or, pour les États, une protection trop forte de l'information porte atteinte à leurs sécurités et profite au crime organisé. Cela constitue à ce titre une menace potentielle pour l'ordre public.

[97] Livre Vert de la Commission européenne, La sécurité des systèmes d'information, DG XIII 4/1994, points 4.2.5.1 et 5.1.3.

[98] GUISNEL Jean, "Guerres dans le cyberespace", éditions la Découverte, p. 31 et s. 69 et s.

[99] TIMOTHY C.May, "The Crypto Anarchist Manifesto" disponible à : http://www.quadralay.com/Crypto/crypto-anarchist.html ; Sur le sujet voir : GUISNEL Jean, "Guerres dans le cyberespace", éditions la Découverte, p.57.

L'État avance le fait qu'il doit avoir accès à certains types d'informations pour pouvoir contrer la mafia, les narco-trafiquants, le blanchiment de l'argent sale et d'autres types d'activités illégales[100].D'ailleurs, pour l'Américain James Kallstrom, agent du FBI *:*

> *"Nous ne voulons pas créer de sanctuaire pour les criminels*" ou encore : *"Un cryptage inviolable aurait pour seul effet d'assurer l'impunité aux criminels"*[101].

En effet, l'efficacité des organismes chargés de détecter l'activité criminelle, à mener leurs enquêtes et à poursuivre les délinquants, dépend souvent de leur capacité d'assurer une surveillance électronique des communications et de perquisitionner dans des endroits où certaines informations pertinentes peuvent être conservées. Dans de nombreux cas, la rapidité d'accès à l'information est indispensable pour mener à bien des enquêtes. Cette observation est particulièrement valable pour les systèmes informatiques, qui peuvent être utilisés pour déplacer, dissimuler ou effacer d'importantes quantités d'informations par une simple pression sur une touche. Dans certains cas, c'est la rapidité d'action qui peut permettre d'empêcher qu'un crime ou un acte terroriste soit commis.

L'essor des télécommunications a créé de nouvelles possibilités d'infractions ainsi que de nouveaux obstacles à l'efficacité des contrôles. La possibilité d'avoir recours à des télécommunications protégées facilitera toute forme d'activité illégale. En effet, l'ordinateur et les télécommunications peuvent être utilisés à des fins de transfert illégal ou de trafic de stupéfiants, d'armes et autres produits dangereux ou illégaux et faire l'objet de poursuites. De même, ces nouvelles technologies peuvent permettre le blanchiment de fonds provenant d'activités criminelles ou encore le transfert illégal d'informations (comme la pornographie infantile, la propagande haineuse, la propriété intellectuelle, les secrets commerciaux ou d'État). Les délinquants peuvent utiliser les ordinateurs et la technologie des réseaux pour commettre, sous une nouvelle forme, des crimes qui existaient déjà. Or, l'efficacité des organismes chargés de la sécurité public peut être entravée par un usage libre de la cryptographie.

---

[100] GUISNEL Jean, "Guerres dans le cyberespace", éditions la Découverte, p. 31 et s. 69 et s.

[101] ZIMMERMAN Philip, "Vie privée, vie cryptée", *Libération, cahier multimédia*, 23 février 1996.

Le point V. (*Use of Encryption*) de la Recommandation du 11 septembre 1995 relative aux problèmes de procédure pénale liés à la technologie de l'information est le signe de cette défiance des États vis à vis de la cryptographie :

> "*Des mesures pour minimiser les effets négatifs de l'utilisation de la cryptographie dans l'investigation des crimes et délits doivent être envisagées, sans préjudicier à son usage légitime plus qu'il n'est nécessaire*" [102].

En effet :

> *«la technologie informatique est sur le point de fournir aux individus et aux groupes la possibilité de communiquer et d'interagir les uns avec les autres d'une manière totalement anonyme, et ces développements vont complètement modifier la nature de la réglementation étatique, la possibilité de taxer et de contrôler les interactions économiques, la possibilité de garder l'information secrète, et affectera même la notion de confiance, de réputation...*
> *la crypto-anarchie pourrait permettre le libre commerce de secrets nationaux et la commercialisation de produits illicites ou volés. Un marché informatique anonyme rendrait même possible l'émergence de marchés d'assassinats et d'extorsions. Divers éléments criminels et étrangers seront des utilisateurs actifs du CryptoNet . Mais cela n'empêchera pas la progression de la crypto-anarchie.»* [103]

L'utilisation de la technologie par les trafiquants de drogue, pour la fraude fiscale, pour le crime (organisé ou non) peut soulever le spectre de la crainte de la désintégration sociale. De plus, à côté de la lutte contre la mafia et la drogue, la petite et moyenne délinquance est également au cœur des préoccupations gouvernementales. Or l'usage de la cryptographie peut empêcher l'application de la loi et de réaliser des interceptions légales.

Aussi, Le Conseil de l'Europe a adopté une recommandation le 11 septembre 1995 qui valorise le concept libéral tout en proclamant la nécessité de s'opposer à la criminalité induite par la cryptographie. Un comité d'experts du crime dans le cyberespace, établi en janvier 1997, envisage les diverses formes de coopération pour limiter les délits, les atteintes à la sécurité et au patrimoine[104].

---

[102] Recommandation du comité du Conseil de l'Europe n° R(95)13, disponible à : http://www2.echo.lu/legal/en/crime/crime.html.

[103] C.MAY Timothy, "The Crypto Anarchist Manifesto"disponible à : http://www.quadralay.com/Crypto/crypto-anarchist.html ; Sur le sujet voir : GUISNEL jean, "Guerres dans le cyberespace", éditions la Découverte, p.57.

[104] GUERRIER Claudine, Maître de conférences, spécialisée dans le droit des TIC,"Le droit actuel de la cryptologie est-il adapté aux utilisateurs d'Internet ?" , ***Lex Electronica*** *- ISSN 1201-7302 - Vol.4 No.1,* INT (Institut National des Télécommunications)Rue Charles Fourier – 91011 Evry, France, 1998.

Ainsi, le développement des réseaux informatiques voit émerger de nouvelles préoccupations : la sécurité informatique, la protection des données, la preuve. La cryptographie, même si elle n'est pas la solution à tous ces problèmes en représente néanmoins un pivot essentiel et indispensable. Donc, dans le contexte d'Internet, le droit de la cryptologie est appelé à évoluer. En effet, pour beaucoup d'habitués des réseaux [105](y compris des réseaux ouverts comme l'internet) renforcer la sécurité n'est pas un problème techniquement délicat. Il suffirait de pouvoir chiffrer ses données avec un algorithme maison, dont la complexité pourrait varier en fonction du degré de sensibilité des informations qui sont envoyées. L'idée, est que l'on ne sécurise plus le réseau, accessible à tous, mais les informations qui y transitent. Il s'agit d'un renversement de l'approche traditionnelle de la sécurisation. Malheureusement, aussi simple que soit cette méthode, comme dans beaucoup d'autres États, chiffrer ses données s'avère difficile. En effet, le SCSSI a toujours tendance à considérer le chiffrement comme une arme de guerre. Ainsi, l'État estime qu'il doit être en mesure de surveiller les communications qui transitent sur son territoire pour des impératifs d'ordre public. Ceci afin d'éviter, en théorie, à des activistes sur écoute d'élaborer un plan à l'insu des services de surveillance.

II- La protection de l'individu

Le respect de la vie privée est une des préoccupations majeures à l'encontre des environnements électroniques. Même si le mythe du Big Brother est souvent démesuré si l'on se réfère au faible taux d'incidents rapportés ou de violation effective. De plus, dans la réalité actuelle des réseaux de communication, il semble impossible (sinon par des moyens démesurés) de contrôler le flux d'informations[106]. Mais la nécessité de protéger la vie privée, l'honneur et la réputation des individus au sein des environnements électroniques semble faire un consensus général[107].

---

[105] BLANCHARD Philippe , "Pirates de l'informatique, enquête sur les Hackers français", France, édition Addison Wesley, juillet 1995.

[106] KATSH Ethan, "law in a Digital World", New York, Oxford University Press, 1995

[107] Conférence ministérielle du G-7 sur la société de l'information, conclusions de la présidence, Bruxelles, 27 février 1995, http://info.ic.gc.ca/ic-data/ppd/g7/concluding.remarks.txt et Commission européenne, livre blanc : croissance, compétitivité, emploi, les défis et les pistes pour entrer dans le XXI e siècle, Bruxelles, 1994

A- La vie privée

Actuellement le droit à la vie privée et les droits qui y sont rattachés sont assurés par plusieurs normes. La notion de vie privée est apparue comme une catégorie juridique autonome vers le 19e siècle. Son importance s'est accrue dans plusieurs systèmes juridiques comme conséquence de la multiplication des technologies permettant de traiter plus d'informations et de ce fait rendant des intrusions ou des divulgations plus faciles.

La première reconnaissance de la vie privée comme un droit de l'homme, se trouve dans la déclaration universelle des droits de l'Homme[108]. Depuis, ce droit a été reconnu à la fois par la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales[109], par le pacte international relatif aux droits civils et politiques[110] et par la convention américaine relative aux droits de l'Homme[111].

Malgré la reconnaissance de la protection de la vie privée, ses contours restent flous. La plupart des auteurs constate qu'il est impossible d'arriver à une définition qui fait l'unanimité[112]. En général, la vie privée est entendue comme étant une notion qui participe aux principes d'autonomie de la personne. Normalement elle est «définie de deux façons : le droit de vivre en paix sans intrusion ni interruption et le droit de contrôler les renseignements qui touchent sa personne »[113]. Pour établir s'il y a atteinte à la vie privée, il est nécessaire de déterminer si une divulgation d'information porte sur un élément de la vie privée.

[108] Article 12 de la *Déclaration universelle des droits de l'Homme*, proclamé le 10 décembre 1948 par l'assemblée générale des Nations Unis.

[109] Article 8 de la *Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales*, signée le 4 novembre 1950, entrée en vigueur le 3 septembre 1953

[110] Article 17 du *Pacte international relatif aux droits civils et politiques*, adopté le 16 décembre 1966 par l'assemblée générale des Nations Unis.

[111] Article 11 de la convention américaine, adoptée le 22 novembre 1969.

[112] LINDON Raymond, « protection de la vie privée : champ d'application », 1971, 2, JCP.6734

[113] Industrie Canada, *la protection de la vie privée et l'autoroute canadienne de l'information : une nouvelle infrastructure de l'information et des télécommunications*, Ottawa, 1994, p5.

La vie privée comprend deux grands axes principaux qui permettent de l'identifier. En premier, la vie privée s'oppose à la vie publique. Ce sont des informations qui ont pour caractéristique d'identifier un sujet. Ici, il y a un rattachement à la notion d'intimité. Ensuite, il existe un axe contextuel. Le champ de protection de la vie privée varie en fonction des personnes et des époques. En effet, ce qui est une information assimilable à un aspect de la vie privée pour un inconnu, ne le sera peut être pas pour une personnalité publique[114].

En France, le droit au respect de la vie privée est reconnu au travers de l'article 9 du Code civil. Il est constitué de l'identité, du domicile, de la vie sentimentale, de la vie familiale. Mais de temps en temps, un débat resurgit afin de déterminer si la notion de vie privée s'entend comme un tout ou juste l'intimité de la vie privée. En effet, alors que l'alinéa premier de l'article 9 du Code civil parle de vie privée, l'alinéa second semble ne prendre en compte que l'intimité de la vie privée. Mais la plupart des tribunaux français ne font pas la différence et visent aussi bien l'une que l'autre de ces notions, en les assimilant toutes les deux. En effet, la Cour de cassation a une jurisprudence assez fluctuante sur la notion. Tantôt elle se réfère à l'intimité de la vie privée dans un but restrictif[115], tantôt elle se réfère à la notion de vie privée sans autre précision[116]. Afin de permettre une prévention des atteintes à la vie privée des utilisateurs d'environnement électronique, le législateur français a assoupli sa réglementation en matière de cryptologie.

La loi du 26 juillet 1996[117] a introduit des cas où l'usage de la cryptographie peut être libre, et où les formalités de déclaration et d'autorisation sont allégées. Cependant, un examen des nouvelles dispositions et de leurs implications pratiques montre qu'en réalité, le système qui existe depuis 1990 n'est pas bouleversé dans ses fondements. Désormais, l'utilisation de procédés de cryptographie à des fins d'authentification et d'intégrité est libre.

---

[114] MICHAUD Martin, *Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandeis à l'inforoute*, Montréal, Edition Wilson &Lafleur, 1996, pp.45 et s.

[115] Arrêt de la 1er chambre civil du 20 octobre 1993, B.I, n°295, relatif à la publication de renseignements relatifs aux revenus

[116] Arrêt du 13 avril 1988, B.I, n°98, relatif à l'impératrice d'Iran.

[117] Loi n°96-659 du 26 juillet 1996 sur la réglementation des télécommunications

Il y a toutefois une précision importante: le procédé de cryptographie ne devrait pas permettre d'assurer des fonctions de confidentialité. Pour assurer la confidentialité l'usage de la cryptographie est libre, à condition que les conventions secrètes soient gérées selon certaines procédures et par un organisme agréé : « le tiers de confiance ». L'instauration de ce que l'on appelle les « tiers de confiance » est la principale innovation de la loi.

Ce tiers de confiance est un organisme auquel l'utilisateur confie sa clé privée de cryptage et qui en cas de nécessité remet ladite clé à l'autorité judiciaire ou à la police. Les Anglo-saxons désignent ce système sous le terme de "*key-escrow*" ou de "*GAK*" pour *Gouvernement Access to Keys* (Accès du Gouvernement aux Clés). Dans le système imaginé par le législateur français, le tiers de confiance ne se limite pas à être le dépositaire des clés privées, il en assure la gestion pour le compte de l'utilisateur : c'est en fait un tiers de séquestre.
L'organisme passe un contrat avec l'utilisateur et lui transmet les clés à utiliser pour chiffrer son information. Le tiers de confiance devient le garant de la fiabilité des moyens de cryptographie utilisés. L'utilisateur n'est donc pas autorisé à utiliser des logiciels qui lui permettent de générer lui-même sa clé privée.

Ces tiers de confiance devront être agréés par le 1er Ministre. Le décret du 23 mars 1998[118], complété par un arrêté du 13 mars 1998[119], définit les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie. La France est le premier pays au monde à se doter d'un tel système (et le seul jusqu'à présent).
Un tiers de confiance[120] est un organisme chargé de gérer les clés privées de chiffrement (les conventions secrètes) utilisées pour garantir la confidentialité d'une information, les transmettre à l'utilisateur et qui doit remettre ladite clé à l'autorité judiciaire ou aux services chargés des écoutes administratives dans les cas prévus par la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

[118] Décret n°98-206 du 23 mars 1998 relatif aux opérations dispensées de toute formalité préalable, JO du 25 février 1998, p.4448 et 4449

[119] Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande des organismes gérant pour le compte d'autrui des conventions secrètes, JO du 15 mars 1998, p.3886 à 3891

[120] La loi emploie le terme d'organisme agréé.

La notion de gestion exclut que l'on puisse utiliser des logiciels qui permettent de générer de manière autonome sa propre clé privée : c'est le tiers de confiance qui transmet à l'utilisateur les clés à utiliser pour chiffrer ses données. D'ailleurs, l'article 10 du décret indique bien que l'organisme délivre «copie de ses conventions secrètes » à l'utilisateur.

L'organisme sera agréé par le Premier ministre, dans les conditions fixées par le décret du 24 février 1998. Il devra notamment remettre un cahier des charges conforme au modèle fixé par l'arrêté du 13 mars 1998 et décrivant ses obligations et notamment, détaillant les mesures prises en matière de sécurité. Les mesures de sécurité concernent aussi bien les prestations offertes, que le personnel, les locaux physiques, et la sécurité informatique.
L'organisme agréé devra compter un nombre suffisant de personnes habilitées, pour être en mesure de connaître les informations classées, intéressant la défense nationale et la sûreté de l'État[121]. Les personnes appelées à remettre, (c'est-à-dire à délivrer les conventions secrètes à une autorité habilitée) ou à mettre en œuvre (c'est-à-dire à restituer en clair des données fournies chiffrées par une autorité habilitée), les conventions secrètes doivent être habilitées au niveau secret-défense, et doivent être deux disponibles 24 H/24 pour la remise des clés. L'agrément sera accordé après avis de 4 ministres (défense, intérieur, industrie, télécommunications) et pourra être refusé pour des motifs liés aux intérêts de la défense nationale ou de la sécurité intérieure ou extérieure de l'État : autant dire que l'État dispose d'un large pouvoir discrétionnaire. Il est possible, même si les références à la nationalité qui figuraient dans le projet de décret ont été enlevées, que seules des entreprises françaises en outre déjà agréées «secret-défense » puissent remplir les conditions exigées. L'organisme agréé devra exercer ses activités sur le territoire national (article II de la loi). Il devra disposer d'une infrastructure en moyens humains, matériels et logistiques importants pour être en mesure de satisfaire aux conditions requises par l'arrêté : procédures administratives et techniques de sécurité décrites dans des guides et manuels de la sécurité, désignation d'un responsable de la sécurité, personnel habilité techniquement et soumis à des obligations strictes de respect du secret professionnel et des correspondances privées, activités relatives aux conventions secrètes exercées dans des locaux à zone à accès contrôlé, utilisation d'un système informatique dédié à la gestion des conventions secrètes (ce qui signifie notamment que ce système ne devra pas être relié à un réseau d'ordinateur ou de télécommunication donc à

Internet). Aucune personne ne doit détenir directement l'accès aux conventions secrètes, le déchiffrement devant s'opérer avec un dispositif détenu par des opérateurs différents. Or, dans un système informatique classique, l'administrateur système a en principe accès à toutes les données, cela est inhérent à la technique. La seule exception concerne les systèmes militaires hautement sécurisés. D'une manière générale, c'est bien une sécurité de type militaire que devra mettre en œuvre l'organisme agréé. Enfin, le contrôle des mesures et procédures de sécurité prises est assuré par le SCSSI (article 15 du décret).

Entre le tiers de confiance et l'utilisateur un contrat sera passé. A la différence des questions relatives à la sécurité et à la remise de conventions secrètes, la question des obligations du tiers de confiance envers ses clients est évoquée de manière très générique dans le décret et l'arrêté qui renvoient au contrat entre l'utilisateur et l'organisme. Cependant, les obligations à la charge du tiers de confiance en matière de sécurité sont précisées dans le décret. Il est prévu notamment que le contrat comprend un engagement de l'organisme relatif à la sécurité des conventions secrètes qu'il gère dont la portée n'est toutefois pas précisée. Les mesures nécessaires doivent être prises par l'organisme agréé pour préserver la sécurité des conventions secrètes, afin d'empêcher qu'elles ne puissent être altérées, endommagées, détruites ou communiquées à des tiers non autorisés. L'organisme agréé doit prendre 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. Les mesures prises pour préserver la sécurité des conventions secrètes doivent être notifiées au SCSSI par le tiers de confiance.

Le contrat doit contenir également les modalités selon lesquelles l'utilisateur ou une personne mandatée par lui, pourra se faire délivrer copie de ses conventions secrètes durant son contrat ou après son terme (article 10 3° du décret), et selon l'article 9 du modèle de cahier des charges: les règles du moyen d'emploi et des conventions secrètes distribuées, les sanctions encourues par le client en cas de mauvais usage ou de détournement du moyen, les sanctions encourues par le gestionnaire en cas de perte, vol ou altération des conventions secrètes.

[121] Article 4 du décret renvoyant au décret n°81-514 du 12 mai 1981, abrogé et remplacé par le décret n°98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale.

Bien que la loi indique que l'utilisation de moyens de chiffrement fournie par un tiers de confiance est libre, les utilisateurs de ces produits sont «suivis » par l'administration. En effet, le décret indique que le tiers de confiance doit tenir à jour et communiquer au moins deux fois par an au SCSSI une liste de ses clients. Des dispositions techniques doivent être prises afin de permettre pour chaque message ou communication protégée à l'aide d'une convention secrète, d'identifier l'organisme agréé et l'utilisateur concerné. La valeur de l'identifiant permettant cette identification doit également être communiquée au SCSSI pour chaque client.

Mais l'obligation principale du tiers de confiance est la remise des clés privées aux autorités habilitées. Il doit maintenir un service permanent de mise en œuvre ou de remise des conventions secrètes au profit des autorités. Il doit tenir à jour deux registres distincts : l'un concernant les demandes présentées par les autorités judiciaires, l'autre concernant les demandes effectuées dans le cadre du titre II de la loi du 10 juillet 1991 (interceptions de sécurité dites écoutes administratives), et classé secret défense. Les deux registres doivent être conservés dans une armoire forte placée dans la zone d'accès contrôlé. Les modalités pratiques de remise des conventions secrètes ou de mises en œuvre sont classifiées, ce qui s'explique par les mesures de contrôle d'accès exigées, mais pourrait être de nature à gêner l'exercice des droits de la défense.

En ce qui concerne les moyens de cryptographie, un décret fixe les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations :

a) un régime simplifié de déclaration ou d'autorisation pour certains types de moyens ou de prestations ou pour certaines catégories d'utilisateurs. Cette disposition concerne par exemple les banques qui bénéficient déjà d'autorisations pour assurer la sécurité de leurs transactions financières ou encore les services de l'État comme l'armée ou la police.

b) la substitution de la déclaration à l'autorisation pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation, tout en justifiant, au regard des intérêts sus mentionnés, un suivi particulier, n'exigent pas l'autorisation préalable de ces opérations.

c) la dispense de toute formalité préalable 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.

Les intérêts auxquels ces textes font référence sont les intérêts de la défense nationale et de la sécurité intérieure et extérieure de l'État. Il sera intéressant de connaître les procédés de cryptographie dont les caractéristiques techniques ou les conditions d'utilisation sont telles que ces opérations ne sont pas susceptibles de porter atteinte aux intérêts précités, c'est-à-dire les procédés de chiffrement aisément cassables par les services de renseignement français.

Ensuite, cette réglementation (loi du 26 juillet 1996) aggrave les peines de prison encourues qui passent de 3 à 6 mois et l'importation d'un produit de cryptologie venant d'un pays n'appartenant pas à la Communauté européenne est désormais passible de sanctions pénales, ce qui n'était pas le cas auparavant (cette nouvelle incrimination ne va pas manquer de poser certains problèmes d'application. En effet, on peut télécharger sur l'Internet des logiciels incorporant des fonctionnalités de cryptage qui n'ont pas été autorisés en France, mais qui peuvent être utilisés et fournis dans d'autres pays. Or les sites qui proposent ces logiciels peuvent être indifféremment situés dans des pays de l'union européenne comme la Suède, ou dans des pays n'appartenant pas à l'union comme la Norvège.).

La loi crée également le délit d'exercice illégal d'une 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 est puni de deux ans d'emprisonnement et de 300 000 francs d'amende*".
>
> Enfin, "*le fait de fournir, d'importer de pays n'appartenant pas à la Communauté européenne, d'exporter 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 500 000 francs d'amende*".

Finalement, le texte prévoit que le tiers de confiance est soumis au secret professionnel. Les dispositions de l'article 226-13 du Code pénal qui précisent que :

"la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 100 000 francs d'amende."

Ces dispositions pourront donc être invoquées. En revanche, l'article 432-9 sur l'atteinte au secret des correspondances qui punit de trois ans d'emprisonnement le fait par une personne dépositaire de l'autorité publique, l'exploitant d'un réseau de télécommunications ou le fournisseur d'un service de télécommunications, agissant dans l'exercice de ses fonctions d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances, ne semble pas applicable, sauf à considérer que le tiers de confiance est dépositaire de l'autorité publique ou chargé d'une mission de service public.

En cas de non respect de ses obligations, le tiers de confiance risque toujours le retrait de l'agrément et la cessation d'activité. L'agrément peut être retiré à tout moment en cas de non respect des conditions fixées dans le cahier des charges. Le titulaire de l'agrément dispose d'un très court délai (8 jours) pour faire ses observations, délai qui peut être supprimé en cas d'urgence. En cas de cessation d'activité ou de retrait d'agrément, l'organisme doit communiquer à ses clients la liste des organismes agréés offrant les mêmes services afin de pouvoir leur confier les conventions secrètes. Les délais et les difficultés pour changer d'organisme ne sont pas évoqués. Que se passe-t-il par exemple si les moyens proposés par les tiers de confiance ne sont pas compatibles avec les moyens du nouveau tiers de confiance ? Dans une telle hypothèse, il n'y aurait sans doute pas d'autre possibilité que de déposer les clés auprès du SCSSI, organisme désigné par arrêté pour recevoir les clés à l'issue d'un délai de 4 ans à compter de la date de signature du contrat ou en cas de défaut de choix d'un nouvel organisme par l'utilisateur en cas de cessation d'activité ou de retrait

Malgré les allégements annoncés, la cryptographie restait en France très sévèrement réglementée. Les peines ont été aggravées et de nouvelles infractions ont été créées. En revanche, la clé privée restait en possession de l'utilisateur. Ainsi, la cryptographie n'est plus réservée aux seuls militaires. En effet, ses applications civiles sont aujourd'hui indispensables au développement des réseaux. L'article 28 modifié de la loi fait lui-même référence "à la protection des informations et le développement des communications et des transactions sécurisées".

Ainsi, en rénovant sa politique en matière de cryptographie, le législateur français, n'a fait qu'harmoniser sa réglementation avec les politiques en matière de cryptologie de l'union européenne et de l'OCDE.

Au niveau européen, la Commission européenne estime que les considérations en matière de protection de la vie privée ne limitent pas l'usage de la cryptographie en tant que moyen d'assurer la sécurité des données et la confidentialité. En effet le droit fondamental à la préservation de la vie privé doit être assuré, mais peut être limité pour d'autres raisons légitimes, telles que la sauvegarde de la sécurité nationale ou la lutte contre le crime, si ces restrictions sont appropriées, efficaces, nécessaires et proportionnées afin d'atteindre ces autres objectifs. De cette façon, la Directive communautaire sur la protection des données[122] harmonise les conditions selon lesquelles l'accès aux données personnelles, leurs traitements et leurs transferts vers un pays tiers sont légales.

En ce qui concerne la sécurité des données, la directive oblige les États membres à assurer qu'un contrôleur de données mette en œuvre des mesures techniques et organisationnelles appropriées, afin de protéger les données contre une destruction accidentelle ou illégale, une perte accidentelle, une altération, une révélation ou un accès non autorisé (en particulier quand le traitement nécessite la transmission de données sur des réseaux) et contre toute autre forme illégale de traitement.

La cryptographie est un moyen technique important permettant d'assurer l'intégrité des données et leur confidentialité. Afin d'assurer également la circulation de données personnelles dans le Marché intérieur, de tels moyens techniques doivent pouvoir "voyager" avec les informations personnelles qu'ils protègent. Ainsi, toute réglementation entravant l'usage de produits et de services de chiffrement à travers le Marché intérieur entrave donc la circulation

[122] Directive 95/46/CE du 24.10.95 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 ; JO L 281/31 du 23.11.95. Voir aussi la Position Commune 57/96 du 12.9.96 visant à l'adoption d'une Directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de services (RNIS) et des réseaux mobiles numériques publics (JO C315 du 24.10.96), qui établi les règles spécifiques pour la protection des données et le droit à la vie privé en rapport avec les réseaux de télécommunications.

sécurisée et libre des informations personnelles, et la fourniture des biens et services qui y sont liés.

De même, l'OCDE au travers de ses lignes directrices, sur une politique de cryptographie[123], reconnaît que les droits fondamentaux des individus au respect de leur vie privée, notamment au secret des communications et à la protection des données de caractère personnel, devraient être respectés dans les politiques nationales à l'égard de la cryptographie et dans la mise en œuvre et l'utilisation des méthodes cryptographiques. En effet, l'OCDE admet que ces méthodes peuvent être un instrument précieux pour protéger la vie privée, notamment en ce qui concerne tant la confidentialité des données et les communications que la protection de l'identité des personnes. Ainsi, pour cette organisation, la cryptologie offre aussi de nouvelles possibilités de limiter le recueil de données personnel, en permettant des paiements, transactions et échanges sûrs mais anonymes. Cette prise de conscience n'est pas récente, l'OCDE avait déjà, en 1980[124] et en 1992[125] mis en évidence des besoins de moyens techniques, pour assurer la protection des données personnelles et de la vie privée ainsi que la sécurité des systèmes d'information. Depuis 1989 le comité de la politique de l'information, de l'informatique et des communications (PIIC) de l'OCDE a inclus les technologies et politiques de cryptographie dans ses travaux sur la sécurité et la vie privée. Cette prise de conscience, de l'importance de la cryptographie dans la protection de la vie privée des individus, a abouti les 27 et 28 février 1997 à l'élaboration de ces lignes directrices en matière de cryptographie. Et après soumission au conseil celui-ci a adopté ces lignes directrices en tant que recommandation du conseil relative aux lignes directrices régissant la politique de cryptographie du 27 mars 1997.

Mais, la notion de vie privée n'a pas une signification unanime dans le monde et la vision française de cette notion n'est peut être pas celle qui paraît la plus adaptée à un environnement électronique.

---

[123]" La politique de cryptographie : les lignes directrices et les questions actuelles "(les lignes directrices régissant la politique de cryptographie de l'OCDE et le rapport sur la politique de cryptographie : contexte et questions actuelles), OCDE/GD (97) 204, le 27.03.1997

[124] Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

[125] Lignes directrices régissant la sécurité des systèmes d'information

B- La *privacy*

La notion de *privacy* est beaucoup plus large que notre notion de vie privée. Il peut être intéressant de se pencher ici sur le Québec qui est une société distincte du reste du Canada non seulement de part sa langue officielle mais aussi de part son Code civil. Cela dit, isolé dans un espace très majoritairement anglo-saxon, le Québec est influencé par des règles de *common law* et d'*equity*. Enfin il y a un rôle unificateur de la Cour suprême du Canada dans lequel 9 juges (dont trois québécois) unifient, en tenant compte des particularismes (du droit civil mais aussi des droit amérindiens et de l'influence des États-Unis) pour l'ensemble du Canada .

Le juge Baudoin de la Cour d'appel du Québec nous a donné une illustration de cette différence par rapport à l'interprétation de la Charte québécoise des droits et libertés[126] qui, dans son article 5 dispose que « toute personne à droit au respect de sa vie privée » :

> « c) Le respect de la vie privée (art. 5)
> Le contenu exact de ce qu'est la vie privée, selon l'article 5 de la charte, reste encore à définir. Plusieurs auteurs se sont efforcés d'en préciser l'étendue et les contours.
> Il convient toutefois, contrairement à ce qui a été plaidé oralement devant nous, de ne pas confondre le droit à la vie privée, concept de droit civil, et le "Right of Privacy", notion de common law et plus particulièrement du droit américain. Au périmètre beaucoup plus large et dont les tribunaux des U.S.A. et des autres provinces canadiennes se sont servis pour définir non seulement le droit à l'intimité stricto sensu, mais aussi certaines libertés publiques. »[127]

La notion de *privacy* ne peut pas vraiment être cerné sous une définition stricte et figée : ce concept évolue en permanence avec le développement des techniques (et la cryptographie à usage privée est un exemple flagrant de cette évolution), mais également avec le développement des mentalités, cela dit cette évolution s'est toujours faite vers une meilleure garantie offerte aux individus.

Pour illustrer ce propos nous traiterons de l'arrêt *Reine* c. *Edwards* de la Cour suprême du Canada (annexe 5) relatif à une affaire s'étant déroulée dans la province anglophone de l'Ontario. Cet arrêt concerne les fouilles et le respects du domicile et on peut facilement ici faire une analogie avec la cryptologie qui, précisément limite l'efficacité de ce pouvoir de

[126] *Charte des droits et libertés de la personne*, L.R.Q., C-12

[127] *Godbout* c. *Longueuil (ville de)*. C.A. [1995] R.J.Q. p. 2569.

l'État régalien. Par ailleurs cet arrêt illustre bien la richesse de la notion de *privacy*, il mérite donc de figurer intégralement en annexe de ce mémoire.

Ainsi, le juge Cory de la Cour suprême du Canada, à propos des droits qu'un accusé à de contester l'admission d'éléments de preuve obtenus à la suite d'une perquisition dans des lieux occupés par un tiers s'est penché sur l'application à donner à l'article 8 de la Charte canadienne des droits et libertés[128] qui dispose que « chacun à droit à la protection contre les fouilles, les perquisitions ou les saisis abusives » . Pour la Cour suprême du Canada,

> *«Un examen des arrêts récents de notre Cour et de ceux de la Cour suprême des États-Unis, que j'estime convaincants et applicables à bon droit à la situation dont nous sommes saisis, indique qu'il est possible de dégager certains principes quant à la nature du droit à la protection contre les fouilles, les perquisitions ou les saisies abusives, garanti par l'art. 8. J'estime qu'ils peuvent être résumés de la façon suivante:*
>
> *1.* *Une demande de réparation […] ne peut être présentée que par la personne dont les droits garantis par la Charte ont été violés. Voir R. c. Rahey, [1987] 1 R.C.S. 588, à la p. 619.*
>
> *2.* *Comme tous les droits garantis par la Charte, l'art. 8 est un droit personnel. Il protège les personnes et non les lieux. […]*
>
> *3.* *Le droit d'attaquer la légalité d'une fouille ou perquisition dépend de la capacité de l'accusé d'établir qu'il y eu violation de son droit personnel à la vie privée. […]*
>
> *4.* *En règle générale, deux questions distinctes doivent être posées relativement à l'art. 8. Premièrement, l'accusé pouvait-il raisonnablement s'attendre au respect de sa vie privée? Deuxièmement, si tel est le cas, la fouille ou la perquisition a-t-elle été effectuée de façon raisonnable par la police? […]*
>
> *5.* *L'existence d'une attente raisonnable en matière de vie privée doit être déterminée eu égard à l'ensemble des circonstances. […]*
>
> *6.* *Les facteurs qui peuvent être pris en considération dans l'appréciation de l'ensemble des circonstances incluent notamment:*
>
> *(i)* *la présence au moment de la perquisition;*
> *(ii)* *la possession ou le contrôle du bien ou du lieu faisant l'objet de la fouille ou de la perquisition;*
> *(iii)* *la propriété du bien ou du lieu;*
> *(iv)* *l'usage historique du bien ou de l'article;*
> *(v)* *l'habilité à régir l'accès au lieu, y compris le droit d'y recevoir ou d'en exclure autrui;*
> *(vi)* *l'existence d'une attente subjective en matière de vie privée;*
> *(vii)* *le caractère raisonnable de l'attente, sur le plan objectif.*
>
> *Voir United States c. Gomez, 16 F.3d 254 (8th Cir. 1994), à la p. 256.*
>
> *7.* *Si l'accusé établit l'existence d'une attente raisonnable en matière de vie privée, il faut alors, dans un deuxième temps, déterminer si la perquisition ou la fouille a été effectuée de façon raisonnable. »*[129]

[128] L.R.C. (1985). App. II, n°44
[129] *R.* c. *Edwards*, [1996] 1 R.C.S. 128, § 45

Les juges de la Cour suprême s'expriment nominalement[130]. Il est alors intéressant de constater que si ces juges ne contestent pas les conclusions de la majorité, ils peuvent éprouver la nécessité de se manifester pour donner des nuances ou exprimer une dissidence. Les décisions étant rendue à la majorité des juges. Le juge La Forest argumenta contre l'interprétation faite par le juge Cory sur la porté de l'article 8 de la Charte canadienne.

> *« À [son] avis, le texte de l'art. 8 ne limite pas la protection qu'il garantit aux fouilles ou perquisitions dans des lieux sur lesquels un accusé possède un droit personnel à la vie privée, au sens qu'il existe un lien direct de contrôle ou de propriété. La disposition vise plutôt à nous protéger tous contre l'intrusion de l'État ou de ses représentants par des fouilles, perquisitions ou saisies abusives; elle ne vise pas seulement à protéger les criminels, quoique la réparation la plus efficace -- et c'est le prix à payer pour assurer la liberté de tous et chacun -- protégera inévitablement le criminel. »*[131] [nous soulignons]

Le contrôle consiste ici à apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi. En fait, il n'y a pas interdiction des fouilles mais plutôt une garantie offerte aux individus d'être protégé contre les fouilles. D'ailleurs dans l'arrêt *R.* c. *Dyment*[132], le juge La Forest estime avec le reste de la Cour suprême de Canada que

> *« Le point de vue qui précède est tout à fait approprié dans le cas d'un document constitutionnel enchâssé à une époque où, selon ce que nous dit Westin, la société a fini par se rendre compte que la notion de vie privée est au cœur de celle de la liberté dans un État moderne; voir Alan F. Westin, Privacy and Freedom (1970), aux pp. 349 et 350. Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Ne serait-ce que pour cette raison, elle mériterait une protection constitutionnelle, mais elle revêt aussi une importance capitale sur le plan de l'ordre public. L'interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'État démocratique. »*

Pour cet arrêt Canadien, et pour éviter l'ambiguïté, nous rappelons que la vie privé dont il est question est, dans la version anglaise de l'arrêt, la *privacy*. Ces articles des chartes québécoise et canadienne regroupent des notions également présentes dans le quatrième amendement à la Constitution Des États-Unis qui assure « le droit des citoyens d'être garantis dans leurs personnes, domicile, papiers et effet, contre des perquisition et saisies déraisonnables… ». Nous le voyons, les notions de *privacy* dégagés ici sont pertinentes par

---

[130] les seuls cas où les arrêts ne portent aucune mention des juges sont les décisions qui auraient de très fortes conséquences politique (comme sur la sécession du Québec ou sur la politique linguistique au Manitoba)
[131] *R.* c. *Edwards*, [1996] 1 R.C.S. 128, § 59
[132] [1988] 2 R.C.S. 417

rapport au sujet de ce mémoire : la cryptographie permet aux individus d'assurer pour eux même le respect de leur *privacy*.

De part le nombre d'utilisateurs, l'internet est dominé par les anglo-saxons et donc, indirectement, les notions nord américaines tendent à s'imposer comme de véritables normes sur l'internet. La notion de *privacy* commence à apparaître dans nos raisonnement continentaux. On traite ainsi de plus en plus souvent d'un critère de raisonnabilité dans les matières du droit de l'informatique comme solution aux problèmes[133]. Ainsi on pourrait considérer comme raisonnable le fait de décrypter ou d'écouter les conversations d'une personne sérieusement soupçonnée de terrorisme mais complètement hors de proportion, le fait d'espionner les conversations d'une actrice sans justification aux yeux de l'intérêt de l'État…

Sans aucun doute la notion de *privacy* est importante dans toute approche juridique de la cryptologie. Son importance correspond, en France, à un légitime soucis de comprendre la philosophie de l'internet. Elle correspond surtout à un légitime soucis des individus d'assurer leur épanouissement à l'abris des écoutes indiscrètes. Ce droit est donc devenu, ou deviendra inévitablement, celui de l'internaute et, peut-être par un effet de mimétisme, celui de l'utilisateur des autres outils de télécommunication puisque les algorithmes de cryptages s'appliquent également à toutes les communications[134].

Section III : Le futur : La protection de la vie privée

Confronté au phénomène sociétaire révolutionnaire que représente les réseaux, notamment la dislocation des frontières, de l'espace et du temps, le droit étatique, expression de la régulation sociale des comportements, est présent. Ce droit ne peut se contenter de déplorer la difficulté de son application. Il doit trouver dans une expression normative plurielle la manière adéquate d'agir. Le législateur doit peser le pour et le contre de chaque mesure prise.

[133] VIVANT, Michel et Christian LE STANC, Lamy droit de l'informatique, 1998

[134] Voir par exemple le logiciel net2phone (http://www.net2phone.com), permet de téléphoner partout dans le monde via l'internet, ou les logiciels de visioconférences, qui peuvent ou pourront également être cryptés lorsque les ordinateurs et débits de communication seront assez rapides pour que n'apparaisse aucune attente dans les communications.

En effet, il revient aux États de réaliser les adaptations juridiques nécessaires pour que les individus puissent évoluer dans un cadre inspirant confiance. L'utilisation de la cryptologie oscille entre deux mondes : celui des libertés sans contrôle et celui fondé sur les lois (l'intérêt de l'État). C'est en tenant compte de ces deux paramètres que le rôle essentiel du droit réalisera sa fonction réglementaire pour le maintien d'une société libre. Pour cela, le législateur a adopté une nouvelle politique normative (I) qui va engendrer un nouveau rôle pour l'État (II).

I- L'aboutissement des nouvelles orientations normatives

La nécessité de développer, pour des raisons de protection de la vie privée, le droit de l'utilisateur d'utiliser des techniques d'anonymisation de ses transmissions amène l'État à éviter un excès de réglementation (A). Mais, à l'heure de la mondialisation des réseaux, il doit veiller à ce que sa politique nationale ne soit pas isolée (B).

A- Une libéralisation totale

Derrière la grande réforme de la sécurité sociale annoncée par le Premier ministre, se profile un grand chantier informatique. L'axe principal, en sera le "codage" des actes, des pathologies et des médicaments, qui devrait permettre de mieux cerner les dépenses de santé. Un codage qui nécessitera une numérisation des prestations médicales, d'où la création d'une multitude de réseaux informatiques entre les différents acteurs de la sécurité sociale. Le problème, est que sur ces réseaux vont transiter des informations sensibles liées au secret médical.

Pour assurer sa confidentialité, il faudra sans nul doute utiliser un chiffrement puissant. C'est à dire, un chiffrement suffisamment puissant, pour que le gouvernement ne puissent pas espionner. Ainsi, entre en scène le SCSSI, le service de Matignon chargé de distribuer (avec parcimonie) les autorisations de cryptage des données.
Pour préparer ce passage à l'informatique, toute la santé publique, médecins, pharmaciens, responsables ministériels, de la sécurité sociale et des caisses d'assurance maladie, ainsi que les industriels et vendeurs de carte à puce, se sont retrouvés pendant deux jours pour un colloque organisé à l'hôtel Méridien de Paris (*Economie et Santé*, 21 et 22 novembre 1995).

Il en ressort que tous les remboursements s'effectueront par télétransmission. Qu'en est-il de la garanti du secret médical ? Du risque d'intrusion informatique ? Du risque de contrôle des assurés en fonction de leur pathologie ?

En effet, les réseaux numériques de prestations sociales existent déjà. D'ailleurs dans un des ateliers, un représentant des pharmaciens est venu dire à l'audience qu'un grand nombre des officines étaient déjà connectés à leur caisse primaire pour enregistrer les transactions de remboursement. Questionné en privé après le débat, cet expert a pris soin de souligner que tout cela était «sécurisé» : une enveloppe électronique scelle l'opération de manière à ce que l'on sache si quelqu'un l'a modifié. Mais, est-ce réellement une sécurité ? C'est plutôt ce qu'on appelle une «signature électronique» : l'intégrité du message est respectée, mais pas sa confidentialité. Donc, ce n'est pas vraiment une sécurité.

Tout cela fût confirmé par un représentant de la branche santé du groupe Schlumberger. Toutes ces transmissions ne sont pas sécurisées. D'ailleurs, un représentant de la CNIL a confirmé que seules certains types d'échanges étaient vraiment sécurisés. Le reste passe presque en clair, donc avec la même « sécurité » (c'est à dire aucune) que sur support papier.

Ainsi, si la liste des médicaments que l'on achète peut être considérée comme sensible, que dire de notre fiche d'identité thérapeutique appelée «le carnet médical ». C'est l'autre élément sensible avancé par le gouvernement, la mise en place à terme, du carnet médical sur support informatique. Ce « carnet », qui retracera tout le parcours médical et thérapeutique du patient, se retrouvera sur une carte individuelle. Cela recoupe le projet de carte « Sesam-Vitale », qui fait l'objet de tests et d'essais entre professionnels et assurés. Le but est d'obtenir une carte pour l'assuré, une autre pour le médecin, le pharmacien, le laboratoire d'analyse ou l'infirmière en ambulatoire ; Un lecteur de carte ; un PC ; et l'acte médical est inscrit sur les deux supports ; puis transmis par réseau au centre de remboursement d'assurance maladie. Le carnet médical devrait être confondu avec la carte de sécurité sociale à puce de l'assuré.
Alors il faudra sécuriser cette information numérique, dans le stockage et la transmission. Il faut reconnaître que la notion de vie privée fut mise en avant par la plupart des intervenants. Aussi, le chiffrement paraît résoudre une partie du problème. Mais de quels degrés de sécurité

le secret médical est-il censé bénéficier ? Le SCSSI[135] avait, seulement, accepté de constituer un groupe de travail avec certains conseils de l'ordre (dont celui des médecins), l'assurance maladie et la CNIL pour réfléchir à des solutions acceptables pour tout le monde. Mais l'État va-t-il se réserver une possibilité afin d'intercepter les communications ?

L'exemple britannique peut laisser présager le pire: en octobre 1995, la *British Medical Association* annonçait qu'elle boycotterait le futur réseau de la sécurité sociale de Sa Majesté (le *National Health Service*). En effet, le gouvernement, sous la pression du *Général Communications Headquarters* (GCHQ), l'équivalent du SCSSI, a décidé d'interdire l'usage du chiffrement sur ce réseau.

Ce détail inquiète les informaticiens de l'assurance maladie. Notamment le CESSI (curieusement absent du colloque), le Centre d'étude et de sécurité informatique de la CNAM, chargé de construire le réseau interne qui connectera l'ensemble des caisses primaires. Ainsi, un responsable du CESSI fit cette réflexion :

> *"Nous ferons tout pour obtenir le plus haut degrés de sécurité dans la transmission, le stockage et le traitement des informations médicales pris en charge par la CNAM. La notion de secret doit rester intacte. Il est pour moi hors de question que les clés des serrures qui protégeront ce secret soient mis entre les mains d'organismes du type du GCHQ britannique..."*[136] .

Mais la mise en place de ces réseaux constitue pour la CNIL une de ses préoccupations majeures. Surtout s'il est question d'utiliser un réseau ouvert tel que Internet. Aussi, le 4 février 1997, la CNIL adoptait une recommandation de portée générale sur le traitement des données de santé à caractère personnelles[137]. La CNIL exige :

> *«le chiffrement des données de santé à caractère personnel circulant sur les réseaux, par un algorithme de cryptage autorisé par le SCSSI. »* [138]

---

[135] Le service central de la sécurité des systèmes d'informations, service de Matignon chargé de donner des autorisations à tout système de cryptage des données.

[136]" Le secret médical à la merci du SCSSI", netizen - 22 nov. 1995, ngroups : fr.network.divers, fr.comp.infosystemes

[137] J.O du 12 avril 1997.

[138] 18e rapport d'activité de la CNIL, *cahiers Lamy droit de l'informatique et des réseaux*, N°105, juillet 1998

De cette façon, le niveau de sécurité des données médicales est encore soumis à l'appréciation du SCSSI donc du gouvernement.

De plus, la CNIL rappelle entre autre, l'obligation de sécuriser les messageries médicales professionnelles et de chiffrement des données de santé nominatives transférées[139].

La politique française de cryptographie ne pouvait pas rester en l'état. Elle devait s'adapter aux nouveaux besoins de notre société de l'information. Surtout que cette nécessité n'était pas que nationale mais aussi communautaire. La Directive européenne sur les traitements de données à caractère personnel[140] requiert que les États membres protègent les droits et les libertés des personnes physiques à l'égard du traitement des données à caractère personnel, notamment le droit au respect de leur vie privée, pour assurer la libre circulation des données à caractère personnel dans la Communauté.

L'article 17 de la directive indique que le responsable d'un traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction, la perte, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau. L'article précise que :

> *« Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. »*

Les régimes établis pour l'utilisation et la fourniture des moyens et des prestations de cryptographie pourraient affecter l'application de la directive, dans la mesure où, selon la Commission :

> *«les moyens appropriés nécessaires pour sécuriser les données personnelles ne seraient pas disponibles en France et/ou ne pourraient pas «voyager» avec les données qu'elles sécurisent provenant d'autres États membres ».*

[139] ibidem

[140] Directive n°95/46 du 24 octobre 1995, JOCE 23/11/95 L 281/30.

De même, les régimes d'autorisation et d'intervention de tiers de confiance risquent d'entraver l'utilisation et la libre circulation des moyens de chiffrement appropriés aux risques pour les données.

Une autre directive du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[141] prévoit que les États membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessibles au public.

Les deux directives prévoient que des limitations puissent être portées à des obligations et des droits institués par lesdites directives, lorsque ces limitations constituent une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales. La «mesure nécessaire » fait référence au principe de proportionnalité.

La législation française est évidemment justifiée par des motifs de sécurité publique (article 36 du Traité de Rome). Mais prend-elle suffisamment en compte les besoins légitimes de chiffrement et remplie-t-elle le test de proportionnalité ?

La loi française ne remplie certainement pas ce test de proportionnalité dans la mesure où elle peut être considérée comme trop limitative de droits garantis par le Traité de Rome et la directive sur les données personnelles. Les limitations prévues par l'État français ne peuvent pas être considérées comme appropriées, efficaces et nécessaires au regard des objectifs poursuivis.

En effet, la libéralisation française de l'utilisation des procédés de cryptologie découlant de la loi de 1996 ne paraît pas suffisante. Cette loi permettait l'utilisation du chiffrement à des fins de confidentialité, à condition de passer par un «tiers de confiance ». Or, ce système de tiers de confiance est-il réellement compatible avec les réglementations sur la vie privée ?

Les traités internationaux, la Convention Européenne des Droits de l'Homme et les lois garantissent le droit fondamental à la vie privée, y compris le caractère secret des

[141] Directive n°97/66/CE du 15/12/97, JOCE 30/01/98 L24/1.

communications. Le recours à la confidentialité contribue à la liberté de communication, droit également garanti par les traités internationaux et la Constitution.

D'autres lois garantissent le secret de certaines informations. On peut citer le secret médical ou le secret professionnel.

En conséquence, dans le contexte du passage vers la circulation de l'information en ligne, le public doit avoir accès à des outils techniques lui permettant une protection efficace de la confidentialité des données et des communications contre les intrusions arbitraires. Le chiffrement des données est très souvent le seul moyen efficace, et d'un bon rapport coût-efficacité, pour répondre à ces exigences. Si l'on reconnaît l'importance du droit à la vie privée et à la liberté de communication, on doit reconnaître également la possibilité d'en assurer l'effectivité.

Or, si le système des tiers de confiance n'est pas d'un bon rapport coût-efficacité, il empêche l'application effective d'autres droits garantis par la loi.

Et l'examen du décret sur les tiers de confiance montre que l'obligation principale qui pèse sur le tiers de confiance est d'assurer l'accès aux clés privées. Donc, toute communication protégée par une convention secrète doit permettre d'identifier l'organisme agréé et l'utilisateur concerné.

Aussi, l'économie générale du décret sur les tiers de confiance créée un sentiment de suspicion à l'égard de la confidentialité. Or, ce système qui touche à l'exercice de libertés publiques n'est pas transparent quant à son dispositif opératoire. Par exemple, les modalités pratiques de remise des clés privées aux autorités ou de leur mise en œuvre font l'objet d'une annexe classifiée qui ne pourra donc pas être communiquée.

L'OCDE dans ses lignes directrices sur la cryptographie indiquait sur ce point que :

> *« le processus par lequel l'accès légal est obtenu devrait être consigné, afin que la divulgation des clés cryptographiques ou des données puisse être vérifiée ou examinée dans le respect des dispositions du droit national…. Les modalités de l'accès légal devraient être énoncées clairement, et publiées de telle manière qu'elles soient aisément disponibles pour les utilisateurs, détenteurs de clés et fournisseurs de méthodes cryptographiques.»*[142]

Il peut arriver que la régularité des enregistrements d'écoutes téléphoniques soit contestée et une expertise doit alors pouvoir être ordonnée afin de rechercher si des manipulations ont été pratiquées[143]. Or ceci est impossible si les modalités de remise ou de mise en œuvre des conventions secrètes sont classifiées.

L'article 8-2 de la Convention européenne des droits de l'homme admet que l'on peut prévoir des exceptions au droit au respect à la vie privée et de sa correspondance pour des motifs liés à la sécurité publique et nationale, à condition que les ingérences de l'autorité publique soient prévues dans la loi (entendue au sens large). Comme pour le droit communautaire, les exceptions de l'article 8-2 sont d'interprétation étroite et doivent être proportionnées au but légitime poursuivi. Selon la jurisprudence de la Cour européenne des droits de l'homme, la pratique et la législation doivent offrir des garanties adéquates et suffisantes contre les abus : il doit exister des contrôles destinés à garantir les droits individuels. C'est en application de ces principes que la France avait été condamnée dans un arrêt Kruslin[144] du 24 avril 1990 dans une affaire d'écoutes téléphoniques.

Alors que l'usage des communications électroniques est appelé à se développer, il ne faudrait pas que la loi sur la cryptographie et son application restreigne le champ de la protection de la confidentialité.

Face à ces difficultés posées par la législation sur la cryptographie, comme elle était régie par la loi de 1996, le gouvernement français a adopté un véritable tournant dans son attitude envers la cryptographie.

---

[142] Point 6 « accès légal ».

[143] Jur. Classeur Proc. Pén. Art. 100 à 100-7 n°122

[144] CEDH, Kruslin, série A, n°176 A ; D. 1990 p.353 note PRADEL

Le 19 janvier 1999, Monsieur Lionel JOSPIN, Premier ministre, à l'issue du comité interministériel pour la société de l'information, fit une conférence de presse. Au cours de celle-ci, il devait constater, qu'avec « la généralisation progressive de l'usage des technologies et des réseaux d'information, les conditions de garantie de la protection de la vie privée et de la sécurité des transactions deviennent déterminantes. Elles supposent, comme l'a souligné le remarquable rapport récent du Conseil d'État[145], une adaptation de notre droit. »[146]

Pour ce faire un ensemble de propositions et d'engagements ont été annoncé ce jour là. Entre autres mesures, une concernait plus particulièrement la cryptologie. Ainsi, le gouvernement français reconnaissait que la cryptologie apparaissait comme un moyen essentiel pour protéger la confidentialité des échanges et la protection de la vie privée. Et de ce fait, il reconnaissait que la législation de 1996 n'était plus adaptée. Donc, une série de mesures, pour un changement radical d'orientation de la législation française en matière de cryptologie, fut annoncée par le gouvernement :

«- offrir une liberté complète dans l'utilisation de la cryptologie ;
- *supprimer le caractère obligatoire du recours au tiers de confiance pour le dépôt des clefs de chiffrement ;*
- *compléter le dispositif juridique actuel par l'instauration d'obligations, assorties de sanctions pénales, concernant la remise aux autorités judiciaires, lorsque celles-ci la demandent, de la transcription en clair des documents chiffrés. De même, les capacités techniques des pouvoirs publics seront significativement renforcées et les moyens correspondant dégagés.* »

Ici, la politique française en matière de cryptage passait d'un encadrement strict à une utilisation future totalement libre. En attendant la mise en place de cette nouvelle politique, le Premier ministre proposait de relever le seuil de cryptographie, dont l'utilisation libre était de 40 bits à 128 bits. En effet, ce niveau est considéré par les experts comme assurant une grande sécurité.

Le 17 mars 1999, le gouvernement français joignait les actes à la parole. Lors d'une intervention, M. Lionel JOSPIN, Premier ministre, à l'occasion de la fête de l'Internet, annonçait la publication de décret relevant de 40 à 128 bits le seuil en deçà duquel l'utilisation

[145] CONSEIL D'ÉTAT, Section du rapport et des études Internet et les réseaux numériques, *Etude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998,* 2ème partie Favoriser les échanges par une confiance accrue des acteurs

[146] http://www.intrenet.gouv.fr/francais/frame-actualité.html

des moyens de cryptologie est entièrement libre[147]. Cette étape, n'est que la première qui amènera la France vers une libéralisation totale de la cryptologie.

Le 19 mars 1999, deux décrets et un arrêté ont été publiés au journal officiel. Ces textes ont pour but d'assouplir les conditions d'utilisations des moyens ou des prestations de cryptologie.

Le décret n°99-199[148] énumère une série de matériels, de logiciels ou d'équipements de cryptologie pour lesquels la procédure de déclaration préalable est substituée à la procédure d'autorisation[149].

Ensuite, le décret n°99-200[150] énumère les catégories de moyens ou de prestations de cryptologie pour lesquels il y aura, désormais, dispense de toute formalité préalable[151]. Enfin, l'arrêté du 17 mars 1999[152] détermine la forme et le contenu des dossiers concernant les déclarations ou demandes d'autorisation (partie administrative et partie technique) et fournit un modèle en annexe[153].

Même s'il reste des efforts à fournir avant de rendre la cryptologie totalement libre, La France montre des signes de bonne volonté et lie les actes au discours. Mais cette politique nationale risque de se confronter à un obstacle persistant que représentent les réglementations internationales.

---

[147] op. cit

[148] Décret n°99-199, 17 mars 1999 : JO 19 mars 1999, p. 4050 ; JCP G 1999, III, 20059, et http://www.internet.gouv.fr/francais/textesref/cryptodecret99199.htm

[149] Voir annexe 3

[150] Décret n°99-200, 17 mars 1999 : JO 19 mars 1999, p. 4051 ; JCP G 1999, III, 20060, et http://www.internet.gouv.fr/francais/textesref/cryptodecret99200.htm

[151] Voir annexe 2

[152] Arrêté du 19 mars 1999 : JO 19 mars 1999, p. 4052 ; JCP G 1999, III, 20061, et http://www.internet.gouv.fr/francais/textesref/cryptoarrete4.htm

[153] Voir annexe 1

B- Une limitation persistante

Le constat est le suivant : la sécurité des transmissions électroniques ne peut être garantie que par une cryptographie forte. Or le développement de ces transmissions (comme pour le commerce électronique qui par sa nature est international), suppose la possibilité de pouvoir importer et exporter librement des données cryptées.

Les normes techniques doivent être reconnues sur le plan international et permettre l'interopérabilité des systèmes.

Toutefois, ces besoins se heurtent à diverses restrictions à la libre exportation des produits de chiffrement. En effet, les produits de cryptographie font partie dans le commerce international des biens considérés comme « sensibles » ou dit « à double usage », c'est-à-dire les biens susceptibles d'avoir une utilisation tant civile que militaire. Le régime de la cryptographie française concernant l'importation et l'exportation s'inscrit dans une réglementation internationale et européenne.

Une réglementation communautaire :

Un règlement communautaire du 19 décembre 1994[154] institue un régime communautaire de contrôle des exportations de biens à double usage afin d'établir des normes communes dans le cadre de la réalisation du marché commun. En revanche, le règlement ne prévoit pas de restrictions dans le domaine de l'utilisation ou de l'importation des produits de cryptographie.
Mais la politique générale tend vers un certain assouplissement des contrôles à l'exportation des produits dits « sensibles ». Cet assouplissement est justifié par les progrès de la technologie et par la forte pression des industries exportatrices européennes et des pays tiers.

L'objectif de ce texte est de créer une procédure de contrôle harmonisée pour les exportations hors de l'Union et d'édicter un principe général de libre circulation des biens à

[154] Règlement (CE), n°3381/94 du Conseil, du 19.12.1994, instituant un régime communautaire de contrôle des exportations de biens à double usage, JOCE, n°L367/1, du 31.12.1994 ; modifié par le règlement Conseil CE n°837/95 du 10.04.1995, JOCE du 21.04.1995,n°L90 ; décision du Conseil du 16.02.1996,JOCE du 1.03.1996,n°L52 ;décision du Conseil du 22.10.1996,JOCE 30.10.1996,n°L278 ; JOCE du 28.02.1997,n)C64 p.1 ; décision du Conseil du 20.01.1997,JOCE 4.02.1997, n°L34

double usage dans la Communauté. Le règlement européen repose sur la mise en place d'une barrière extérieure commune par l'adoption d'une liste identique de biens et de technologies à double usage dont l'exportation est soumise à autorisation (liste commune).

Ce régime, applicable depuis le 1er juillet 1995, est marqué par les principes directeurs du marché commun, notamment celui de libre circulation des biens à l'intérieur du marché commun ainsi que celui de reconnaissance mutuelle des licences d'exportation entre les États membres. Néanmoins, des restrictions temporaires aux transferts intra-communautaires subsistent pour certains biens considérés comme particulièrement sensibles, parmi lesquels figurent les produits et logiciels de cryptographie.

Les produits concernés sont énumérés dans l'annexe I du texte communautaire. En ce qui concerne la cryptologie, sont ainsi visés les télécommunications, logiciels et matériels informatiques de haute technologie et la sécurité de l'information[155] .
Toutefois, les logiciels qui sont couramment à la disposition du public c'est-à-dire qui *« rendus accessibles sans qu'il ait été apporté de restriction à leur diffusion ultérieure »* ne sont pas soumis au contrôle à l'exportation, prévus par la réglementation européenne. Tel est le cas, également, des radiotéléphones mobiles destinés à l'usage civil ou de certains équipements assurant la sécurité de l'information tels que les cartes à microprocesseurs ou encore des équipements d'authentification des données, sans permettre de les chiffrer, des équipements cryptologiques spécialement conçus, mis au point ou modifiés pour servir dans des opérations bancaires ou financières.

Pour faire respecter cette réglementation, des modalités de contrôle ont été instituées. Elles varient selon que les exportations concernent un État membre ou un État tiers à l'Union européenne.

[155] La catégorie 5 « télécommunications » de l'annexe I comprend une partie 2 sécurité de l'information définie comme « *tous les moyens et toutes les fonctions réglant l'accessibilité ou assurant la confidentialité ou l'intégrité de l'information ou des télécommunications, à l'exclusion des moyens et des fonctions prévues pour la protection contre les défaillances »*. Par conséquent, sont compris la cryptologie, la crypto-analyse, la protection contre les émanations compromettantes et la sécurité des ordinateurs.

- Au niveau intra-communautaire, le principe est celui de la libre circulation des marchandises[156]. Cependant, pendant une période transitoire de trois ans, l'exportation des biens figurant sur la liste de l'annexe IV du règlement, qui inclut les produits et logiciels de cryptographie, restent soumis à autorisation. Cette période est achevée depuis le 1er juillet 1998. Le chiffrement apparaît donc comme une exception au principe de libre circulation des marchandises posé par le Traité.

- Vers les pays tiers tous les biens visés à l'annexe I du règlement sont soumis à autorisation d'exportation, quel que soit le pays tiers de destination. Les formalités peuvent être allégées pour certains produits (article 3 du règlement). L'exportation est définie par le règlement comme :

> *"le régime permettant la sortie temporaire ou définitive de marchandises communautaires du territoire douanier de la communauté conformément à l'article 161 du Code des douanes communautaires ; ce régime inclut la réexportation, c'est-à-dire l'opération au sens de l'article 182 dudit code consistant en la sortie du territoire douanier de la Communauté de marchandises non communautaires".*

Les équipements de sécurité de l'information et les logiciels de chiffrement ne peuvent donc pas être exportés hors de la communauté sans licence[157].

Actuellement, ce règlement est en cours de révision par les institutions communautaires. En effet, depuis le 1er juillet 1998, les exportations des produits de chiffrement à destination de l'Union Européenne auraient du être libres.

La Commission a présenté le 15 mai 1998, un rapport[158] dressant le bilan de l'application du règlement du 19.12.1994 et une proposition[159] de règlement visant à remédier aux lacunes

---

[156] L'article 9 du Traité Rome dispose que « *La Communauté est fondée sur une union douanière qui s'étend à l'ensemble des échanges de marchandise, et qui comporte l'interdiction, entre les États membres, des droits de douanes à l'importation et à l'exportation (…)*»

[157] De façon générale, les États membres ne respectent pas cette procédure de licences. Tel est le cas notamment du Royaume-Uni qui a récemment modifié sa législation dans ce domaine.

[158] Selon l'article 18 du règlement du 19.12.1994, la Commission adresse « *tous les deux ans au parlement européen et au Conseil un rapport concernant l'application du règlement* »

[159] Proposition de règlement du Conseil, 15 mai 1998, COM(98)257 final, instituant un régime communautaire de contrôle des exportations des biens à double usage, JOCE, 15.05.98, n°L257.

recensées dans le règlement précité. La Commission reconnaît qu'il a contribué à faciliter les échanges intra-communautaires. En effet, le régime mis en place en 1994 a permis de réduire les formalités d'exportation et de faciliter la libre circulation de la quasi-totalité des biens à double usage dans la Communauté. Cependant, il existe un manque de convergence et de cohérence entre les différentes politiques et pratiques nationales.

La France ne respecte pas encore le principe communautaire de la reconnaissance mutuelle, du fait de la survivance de régimes d'autorisations et de la difficulté des reconnaissances entre États membres, alors que l'administration des douanes devrait être capable de reconnaître et d'accepter les autorisations délivrées par les autres États membres. Il persiste donc une entrave aux principes de reconnaissance mutuelle et de libre circulation des marchandises.

Dans la proposition faite par la commission en ce qui concerne les produits de cryptologie, les restrictions existantes aux transferts intra-communautaires seraient supprimées, et remplacées par la procédure de notification (ce qui nécessiterait de modifier la loi française qui ne distingue pas entre les exportations vers des pays membres et des pays non-membres). Dans ces conditions, un paradoxe risque d'apparaître, les exportations de produits de chiffrement à destination de l'Union européenne seraient libres, alors que la fourniture en France des mêmes produits resterait soumise aux formalités de déclaration.

Enfin, la période transitoire étant arrivée à échéance il y a un an, et le nouveau règlement n'ayant pas encore été adopté, doit-on considérer que les transferts intra-communautaires des biens de l'Annexe IV sont désormais libres ou au contraire qu'ils restent soumis à licence ? Le règlement européen n'est pas vraiment explicite sur ce qui se passe à la fin de la période transitoire et reste ouvert à interprétation divergente[160].

Mais, il ne faut pas perdre de vue que la proposition de règlement émise par la Commission, s'inscrit dans un cadre d'ensemble d'une politique communautaire qu'il convient de garder à l'esprit. En effet, l'Union s'est fixée comme objectif de parvenir en l'an 2000 au

[160] Le règlement dit bien que les restrictions ont une durée limitée et sont transitoires, mais l'article 19-5 du règlement indique : « *La nécessité des mesures prévues par le présent article est réexaminée dans un délai de*

développement d'une politique de libre circulation des produits et services de cryptographie ainsi qu'à la création d'une zone homogène de sécurité à l'intérieur de l'Union[161].

Même, si la France doit respecter une réglementation européenne commune aux 15 États membres, elle doit aussi remplir ses engagements internationaux et notamment, l'Arrangement de Wassenaar.

L'Arrangement de Wassennaar.

Ces dernières années, le contexte international a connu de grands bouleversements, d'une part sur le plan politique, suite à la fin de la guerre froide; d'autre part, pour des raisons économiques avec la volonté de faciliter les échanges commerciaux.

Dans ce contexte, les contrôles à l'exportation des biens dits sensibles n'ont pas été oubliés. Ainsi, la fin de la guerre froide a entraîné la disparition du COCOM[162] (Coordinating Committee for Multilateral Export Controls) qui était une organisation internationale permettant le contrôle et la surveillance mutuelle des exportations concernant les biens stratégiques et les données techniques à destination de pays tiers. Le but de la réglementation COCOM était d'éviter, de prévenir l'utilisation, l'exportation des produits sensibles dans des pays « ennemis ».

Le COCOM a disparu en mars 1994, et a été remplacé en 1995 par l'Arrangement de Wassenaar sur les contrôles à l'exportation pour les armes conventionnelles, les biens et technologies à double usage. Le but de cet accord est de prévenir la paix internationale et régionale, en limitant l'acquisition de moyens à double usage pour des pays qui représentent

---

trois ans à compter de la date d'entrée en vigueur du présent règlement. »

[161] Voir Communication de la Commission européenne, « Assurer la sécurité et la confiance dans la communication électronique », COM (97) 503.

[162] Ses membres étaient pour l'essentiel les pays membres de l'OTAN ainsi que d'autres pays tels le Japon et l'Australie.

une menace pour la sécurité mondiale. (suite à cet accord, il est par exemple plus difficile de vendre et d'exporter des moyens de cryptographie vers l'Iran, la Libye[163].)

L'accord dit de Wassenaar[164] adopté définitivement les 11 et 12 juillet 1996 prévoit à l'instar de la réglementation du COCOM une politique axée sur la destination finale. Ainsi, sont toujours en vigueur des listes de contrôle de ces biens et de leurs utilisations, des procédures concernant l'information lors de l'exportation d'un des produits hors des pays membres de l'accord (dont fait partie la France).

Les trente-trois États signataires de Wassenaar cherchent à assurer que le transfert d'armes conventionnelles et de produits et technologies à double usage ne viennent pas, par accumulation, produire un effet déstabilisateur au niveau mondial. Cet arrangement n'est pas dirigé à l'encontre d'un État précis et donc, il n'empêche pas des transactions civiles menées de bonne foi. Mais depuis l'application des arrangements de Wassenaar, tous les produits conçus ou modifiés pour utiliser une méthode de cryptographie de n'importe quelle longueur de clé, en vue d'assurer la sécurité de l'information, ont été contrôlés, à moins qu'ils ne relèvent d'une exemption particulière ou de note générale sur les logiciels.

Or, afin de suivre la technologie et le commerce électronique tout en conservant une bonne sécurité, les États signataires de Wassenaar ont décidé lors de la réunion de Vienne le 3 décembre 1998, de modifications concernant l'exportation de produits et technologies de cryptographie[165]. Ces modifications apportent des assouplissements en établissant une équivalence pour les produits matériels et logiciels, imposent des contrôles sur certains produits de très grande diffusion et suppriment les contrôles sur une série de produits.

---

[163] « The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies », http://www.acda.gov/wmeat95/wasarr95.htm (février 1997), pp32-33.

[164] Le texte de l'Arrangement est disponible à : http://ideath.parrhesia.com/wassenaar/ et le site en ligne du secrétariat qui se trouve à : http://www.wassenaar.org/.

[165] Détails sur, http://www.wassenaar.org

Ainsi, les contrôles sont supprimés, entre autres, sur :

- les produits qui exécutent la fonction d'authentification de données.
- les produits qui exécutent la fonction de signature de données.
- Les produits utilisant un algorithme symétrique d'une longueur de clé ne dépassant pas 56 bits…

Donc, même si les signataires de l'Arrangement de Wassenaar ont adopté un infléchissement de leurs politiques envers la cryptographie, cette libéralisation n'est que modérée. En effet, la suppression des contrôles sur un algorithme, ne concerne que ceux d'une longueur de 56 bits, ce qui n'est pas très fiable[166].

De plus, même si les États parties à cet arrangement, se sont entendus pour accorder, dès que possible, « une licence générale d'exportation pour les logiciels de très grande diffusion utilisant un algorithme asymétrique d'une longueur de clé ne dépassant pas 128 bits », pour le moment, l'exportation de tels produits est soumise à contrôle.

Or, si en France, l'utilisation de moyen de cryptographie est autorisée jusqu'à 128 bits, il n'existe pas encore de produits, sur le marché national, permettant de chiffrer à ce niveau[167]. Il est donc possible de se fournir qu'à l'étranger, cela sous-entend une exportation. Mais, si les industriels capables de fournir ce matériel se situent dans un pays refusant l'exportation de moyen de cryptographie, ce droit de crypter des informations jusque 128 bits n'est que théorique. Par exemple, les programmes de cryptage, supérieurs à 56 bits, de Nestcape ou Microsoft sont interdits d'exportation par le gouvernement américain[168], donc théoriquement inaccessible en France.

[166] « Le DES à 56 bits brisé en 56 heures », *Revue expertises*, p.286, octobre 1998

[167] DELBECQ Denis , « Comment cacheter les e-mails », *le monde interactif*, le 03.02.1999,p.VI

[168] « Quand le 128 bits se réduit à 56 bits », *le monde interactif*, le 03.02.1999, p14

II Les nouveaux rôles de l'État

Pour toutes les raisons vues auparavant, il existe des motifs légitimes d'assurer, dans certains cas, à l'État un accès à des données chiffrées. Dans les faits, pour assurer cet accès, on peut généralement limiter l'utilisation de produits cryptographiques à ceux qui peuvent être déchiffrés et lus au besoin ou exiger de ceux qui possèdent les clés, qu'ils déchiffrent les messages sur demande. Les solutions politiques fondamentales et les moyens pratiques de les mettre en œuvre soulèvent des préoccupations concernant les droits fondamentaux, principalement en ce qui a trait à la vie privée. En fin de compte, il convient d'évaluer les coûts et les avantages de chaque politique possible en matière de cryptographie. Surtout en ce qui a trait aux droits fondamentaux, aux intérêts commerciaux, à la sécurité publique et à la lutte contre la criminalité. De cette façon, il faudra évaluer quels seront les avantages de la limitation du chiffrement sur le plan de la sécurité et déterminer si elle l'emporte sur des dommages susceptibles d'être causés par la non-réglementation du chiffrement. Mais, il est difficile de savoir si ces mesures permettent une application de la loi et un maintien de la sécurité. Au cours des dernières décennies, les nouvelles technologies ont sensiblement amélioré la capacité technique d'assurer diverses formes d'accès légitime. Aussi, les mode contrôle des États doivent s'adapter (A) et leurs politiques doivent se mondialiser(B).

A- Vers des modes de contrôle « revisités »

Aujourd'hui, personne ne peut être totalement empêché de chiffrer des messages et notamment pas les criminels ou les terroristes qui peuvent également avoir recours au chiffrement dans leurs activités. L'accès aux logiciels de chiffrement est relativement aisé, par exemple en les chargeant simplement à partir d'Internet. En effet, aujourd'hui, chacun peut se procurer sur l'internet le logiciel PGP (Pretty Good Privacy), réputé inviolable. Peut-on imaginer sérieusement que la mafia ou un réseau pédophile utilisera un logiciel de cryptage fourni par un « centre de confiance » et de plus, lui remettre spontanément des clefs de codage qu'il ne changera jamais ? De plus, la circulation des informations concernant la cryptologie ne peut être empêchée, sachant en outre que des livres sur le thème sont en vente libre, y compris en France.

De même, profitant du fait que l'exportation de la version imprimée de codes sources de produit de cryptographie n'est pas soumise aux même restrictions à l'exportation que la même version sous forme numérique, des hackers, à l'occasion d'une conférence internationale qui se tenait en Europe, ont emporté le code source de la dernière version de PGP, qui après avoir été scannée et compilée est désormais disponible en Europe, y compris sur des sites situés dans des pays de l'Union européenne[169]. D'ailleurs, divers procès en inconstitutionnalité de la loi américaine à l'exportation sont actuellement en cours devant les tribunaux américains, ce qui pourrait encore augmenter la disponibilité de produits de cryptographie sur Internet, selon le résultat de ces procédures.

Ensuite Il est, difficile de prouver qu'une personne déterminée a envoyé un message chiffré non-autorisé. Le contrôle du respect de la loi supposerait d'intercepter des volumes d'informations considérables, selon des protocoles variés, dans lesquels la présence d'une information chiffrée n'est pas facilement décelable.

De plus, il est même possible de dissimuler une information chiffrée de manière à ce qu'elle semble anodine, à travers les méthodes stéganographiques. Ces méthodes permettent de cacher un message dans d'autres données (par exemple une image), de telle manière que l'existence même d'un message secret, et donc du recours même au chiffrement, ne puisse être détectée.

Le système des tiers de confiance pouvait sembler un pas dans la bonne direction, mais on peut rester sceptique sur la possibilité d'une mise en œuvre qui offre toutes les garanties de sécurité souhaitable, qui permette de répondre rapidement à l'évolution des besoins, qui soit compatible avec les communications internationales, et d'un coût abordable.

Le système projeté risque bien de n'être mis en œuvre que par les citoyens honnêtes, vis à vis desquels les autorités n'auront justement jamais besoin de décrypter les messages. Il est revanche fort à parier que ce système entraînera de nouvelles formalités et surtout de nouveaux coûts pour les particuliers ou les entreprises. En revanche, restreindre l'usage du chiffrement pourrait en réalité empêcher les entreprises et les citoyens respectueux des lois de se protéger des criminels.

[169] Voir le site : The international PGP Home page, http://www.ifi.uio.no/pgp/

En fait, on ne peut réellement empêcher les criminels d'avoir accès à un chiffrement puissant et de contourner le chiffrement avec dépôts des clés privées obligatoire. Si des mesures de contrôle peuvent rendre le recours au chiffrement à des fins criminelles plus difficiles, les bénéfices de la réglementation en termes de lutte contre la criminalité sont difficiles à évaluer, et sont souvent exprimées en termes généraux.

Pour la Chambre de Commerce Internationale, la limitation de l'utilisation du chiffrement en raison de la lutte contre la grande criminalité est sujette à caution, car les auteurs d'actes délictueux ne se sentiront pas obligés de se plier aux règlements applicables à la communauté économique[170].

De plus, en l'absence d'étude sur la question de l'interception de communication, on ignore leur effectivité et leur utilité réelle. L'ampleur des écoutes illégales, émanant tant de personnes privées que de fonctionnaires outrepassant leurs pouvoirs, est dénoncée dans les rapports de la CNCIS. L'État n'est pas une entité abstraite, mais un organisme composé d'individus qui ont leurs faiblesses et leurs tentations. L'objectif des administrations chargées de la lutte contre la délinquance et le crime n'est pas seulement d'avoir accès aux clés, mais d'avoir accès à un texte non-chiffré, en temps réel, de manière discrète. Or la mise en œuvre dans un cadre légal de ce type d'accès en temps réel dans le cadre des nouvelles formes de communication, est rendu plus difficile en pratique par la multiplicité des intervenants : les services concernés n'ont plus affaire à un opérateur unique organisme de service public (France Télécom).

L'interception des communications doit être considérée au regard des autres moyens d'investigation pouvant être mis en œuvre dans la lutte contre la délinquance : analyse du trafic et des informations diffusées en clair (surveillance des forums et listes publiques par exemple). En effet, comme le recours aux télécommunications électroniques et aux radiocommunications ainsi que la capacité technique de les surveiller ont évolué, on a reconnu dans l'ensemble des pays industrialisés la nécessité légitime pour les organismes de l'État d'être autorisé à surveiller les communications, pour autant que des mécanismes de

[170] Prise de position de la CCI sur une politique internationale du chiffrement, *Droit de l'informatique et des télécoms*, 1994/2 p.70.

protections judiciaires et légales soient en place. Ainsi, en France, la loi du 10 juillet 1991[171] reconnaît le secret des correspondances émises par voie de télécommunications (donc, celles émises par Internet). Mais dans son article premier, elle admet une dérogation en permettant de « porter atteinte à ce secret que par l'autorité publique, dans les cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par elle-même ». Mais, bien que l'on puisse obtenir des autorisations judiciaires afin d'intercepter les renseignements chiffrés, ceux qui les interceptent se révèlent parfois incapable de les lire. Donc deux difficultés se posent :

- Il pourrait devenir difficile, voire impossible de déterminer si l'information interceptée est vraiment visée par l'autorisation qui a été donnée de l'intercepter

- Il pourrait devenir difficile pour les autorités de déchiffrer l'information ou encore de le faire à temps pour l'utiliser efficacement.

Donc, Un système de contrôle, *a posteriori*, serait beaucoup plus simple et beaucoup moins coûteux à mettre en place. En effet, parfois l'information, même chiffrée à des fins de communication, peut souvent être trouvée non-chiffrée à la source, comme dans les formes de communication traditionnelles, par exemple auprès des banques, magasins et agences de voyage qui sont parties prenantes dans une communication avec un suspect ou à certaines étapes d'une communication. De plus, les clés privées des produits de chiffrement puissants sont difficilement mémorisables et doivent être conservées quelque part. D'ailleurs, l'efficacité des autorités judiciaires à détecter l'activité criminelle, à mener leurs enquêtes et à poursuivre les délinquants dépend souvent de leur capacité d'assurer une surveillance et de perquisitionner dans des endroits où de l'information pertinente peut-être conservée. De cette façon, les fouilles et les perquisitions, à la source des informations, peuvent permettre de retrouver en claire les données recherchées. Mais des mécanismes de protection judiciaires doivent s'appliquer aux fouilles et aux inspections des lieux, qui s'étendent maintenant à la fouille ou à l'inspection d'ordinateur et des réseaux, afin de respecter les droits fondamentaux des individus[172].

---

[171] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie des télécommunications, JO du 13 juillet 1991

[172] Pour la France, articles 56 s., 76 s. et 92 s. du Code de procédure pénale.

Ainsi, on pourrait laisser la liberté de crypter aux utilisateurs en leurs laissant, surtout, le choix des moyens, en compensant par l'obligation de communiquer les systèmes et clés de cryptage à la requête de toute autorité judiciaire. Le refus explicite de communiquer serait très sévèrement réprimé, comme la perte ou l'oubli des clés, qui seraient présumés de mauvaise foi. Donc, il paraît nécessaire d'adapter notre législation pénale afin de compenser une libéralisation totale de la cryptologie tout en permettant à notre justice de rester efficace. Cette optique, fut celle choisit par le gouvernement canadien qui propose une modification de son code criminel et d'autres lois pour :

- Criminaliser la divulgation illicite des clés ;
- Décourager l'utilisation du chiffrement à des fins criminelles ;
- Décourager l'utilisation de la cryptographie pour dissimuler des éléments de preuve
- Appliquer au contexte de la cryptographie les procédures existantes d'interception, de recherche, de saisie et d'aide.

Enfin, les services spécialisés du renseignement disposent d'autres moyens d'investigation qui sont soit plus classique (comme la surveillance, l'analyse des indices, le recours à des informateurs), soit plus sophistiqués (ex : interception du rayonnement électromagnétique moyens de surveillance électronique sophistiqués, en passant par les réseaux de surveillance par caméra, les appareils permettant de détecter des conversations à distance ou derrière des vitres fermées, la caméra stroboscopique danoise « Jai » capable de prendre des centaines de photographies en quelques secondes et les systèmes de reconnaissance automatiques de véhicule. Le Parlement européen s'est même inquiété récemment des risques que font peser ces systèmes de surveillance sur les libertés publiques et sur la nécessité de mettre en place des procédures de contrôles[173]).

- Pour le Canada article 1, 8 et 24 (2) de la charte canadienne qui autorise les fouilles, les perquisitions et les saisies « *dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique*" et qui permet l'utilisation des preuves,*" sauf si leurs utilisations est susceptible de déconsidérer l'administration de la justice* ».

[173] la Fondation Omega de Manchester, « Une évaluation des techniques de contrôle politique », PE 166.499, résumé analytique est disponible à :
http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm

En réalité, la loi a sans doute pour but que les systèmes non décryptables ne se répandent dans le grand public : s'il n'existe pas d'outils conviviaux commercialisés, il faut faire plus d'effort pour se procurer les outils non commercialisés et les utiliser. Mais, l'utilisation d'outils cryptographiques semble nécessaire à la protection de l'individu sur les réseaux. Aussi, le rôle de l'État n'est-il pas également d'apporter une certaine garantie de sécurité quant a l'utilisation de la cryptographie ?

En effet, l'utilisation croissante de la cryptographie robuste engendrera certains avantages sur le front de la lutte contre la criminalité en assurant une protection technique des renseignements. Dans un contexte où les échanges d'information dématérialisés se développent, il est indispensable de pouvoir bénéficier de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel, assurer la sécurité des transactions financières et commerciales.

Il ne faut pas perdre de vue que l'utilisation d'un réseau de communication expose les échanges à certains risques, qui nécessitent l'existence de mesures de sécurité adéquates. Il est donc nécessaire d'avoir accès à des outils techniques permettant une protection efficace de la confidentialité des données et des communications contre les intrusions arbitraires. Le chiffrement des données est très souvent le seul moyen efficace pour répondre à ces exigences.
Les technologies cryptographiques sont ainsi reconnues comme étant des outils essentiels de la sécurité et de la confiance dans les communications électroniques. Elles vont être amenées à jouer un rôle croissant en matière de protection contre la fraude informatique, de sécurité des données, de protection de la confidentialité des correspondances, de protection du secret professionnel et de commerce électronique. Encore faut-il que ces moyens de protection soient fiables.

Un des problèmes évoqués par les techniciens est celui de l'évaluation de la sécurité du produit de cryptage offert. Les procédures et algorithmes offerts à la vente sont la propriété du fournisseur. Donc, il ne sera donc pas possible pour le public et les experts en cryptographie d'apprécier le degré de fiabilité du logiciel de cryptage, ni le risque qu'il soit cassé par un professionnel du chiffre, comme cela peut se faire pour des logiciels développés à partir de systèmes connus comme RSA ou DES. Aussi, une des solutions serait de passer par un tiers de

confiance. En effet, il doit recevoir l'agrément du SCSSI et ce, selon des conditions strictes. L'organisme qui souhaite devenir tiers de confiance[174] adresse une demande auprès du Service Central de la sécurité des systèmes d'information. L'agrément est accordé *intuitu personæ* par le Premier Ministre ou son représentant, pour une durée de quatre ans, avec possibilité de renouvellement. Ce « parrainage » devrait impliquer une certaine confiance dans le produit fourni par ce tiers de confiance. Mais, Le rapport de force international semble moins favorable aux tiers de confiance et des utilisateurs potentiels émettent des réserves.

Les protagonistes du *lobbyng « tiers de confiance »* perdent en crédibilité. Certains membres de l'exécutif américain ont fait savoir que les techniques de « séquestre de clés » par un tiers de confiance sont plus chères et moins efficaces que les produits sans séquestre. Les adversaires des tiers de confiance ont développé une thématique fédératrice. D'ailleurs, La Commission européenne finalise en 1998 un projet, de directive sur les signatures digitales et la sécurité des communications électroniques, où elle exclut le recours aux tiers de confiance, ainsi qu'au séquestre ou à la récupération des clés de chiffrement. La Commission est persuadée que le système des tiers de confiance n'est pas fiable.

En effet, Les tiers de confiance vont être chargés de gérer pour le compte d'autrui les clés de chiffrement, et vont donc avoir accès potentiellement à de nombreuses données confidentielles. Aussi, le système de séquestre peut devenir une cible privilégiée des espions industriels et du crime économique et une analogie avec les banques peut être faite à ce titre. Il y a des risques physiques, logiques et humains qui impliquent que la sécurité tant intérieure qu'extérieure, soit contrôlée à tous les niveaux.

En France, le décret et l'arrêté de 1998[175] montrent que des conditions administratives et techniques strictes sont imposées aux tiers de confiance (personnel habilité « secret-défense », cahier des charges contraignant, politique de sécurité d'ordre quasi-militaire, mesures de contrôles par le SCSSI, notification des mesures prises pour préserver la sécurité).

[174] Le premier tiers de confiance agréé en France fut « Trithème », une filiale de Thomson-CSF, Revue Expertises, novembre 1998, p.323.

[175] Ibidem

Donc, sauf à diminuer la sécurité, des conditions administratives et techniques strictes sont imposées aux tiers de confiance, ce qui va se traduire en terme de coûts. En effet, Ces contraintes, qui se justifient du point de vue de la sécurité, vont nécessiter une organisation rigoureuse et vont avoir des répercussions directes sur les coûts des produits proposés.

Les auteurs du rapport *The Risks of key recovery, key escrow and trusted party Encryption*[176] indiquent que le déploiement d'infrastructures de tiers de confiance va avoir pour résultat des sacrifices en terme de sécurité et à un coût accru pour l'utilisateur final. Construire un tel environnement pourrait s'avérer d'une énorme complexité et nécessiter un haut degré de confiance dans les personnes chargées de gérer le système.

Un autre problème évoqué par les experts est celui de l'évaluation de la sécurité du produit offert par le tiers de confiance. Le tiers de confiance est le garant de la fiabilité des moyens de cryptographie utilisés.

Or, les procédures et algorithmes utilisés seront propriétaires, et par conséquent, ils ne seront connus que du tiers de confiance (et du SCSSI). Et donc, ici aussi il ne sera pas possible d'apprécier le degré de fiabilité du logiciel de cryptage, ni le risque qu'il soit cassé par un professionnel du chiffre (à titre de comparaison, les sources de PGP sont publiques). Sous la réglementation française, ce point est laissé à l'appréciation du SCSSI, qui indique cependant avoir mis au point des procédés d'évaluation et de certification des produits sécurisés.

L'apparition de la cryptographie en dehors du milieu militaire redéfinis le rôle de l'État. Celui-ci voit ses possibilités de contrôle restreinte mais en parallèle une nouvelle responsabilité apparaît. Cette dernière ne s'arrête pas à garantir des moyens fiable de cryptage mais elle s'étend aussi au niveau international.

[176] op. cit.

B- Vers une coordination mondiale

La France a adopté une nouvelle loi de télécommunications, l'Allemagne une loi sur les signatures numériques[177] et l'Italie une loi sur l'usage des documents et des contrats électroniques[178]. Le gouvernement britannique a lancé une consultation publique sur la réglementation des tiers de confiance. Le gouvernement néerlandais a crée un groupe de travail (task force) interministériel[179]. Le Danemark et la Belgique[180] préparent également des propositions de législation sur les signatures numériques. Quant au gouvernement suédois, il a organisé une audition publique en juin 1997.

Si nous pouvons qu'encourager ces évolutions vers un cadre juridique clair, la diversité des approches suivies ou l'absence de tout cadre réglementaire dans d'autres États membres, pourrait constituer une barrière sérieuse au commerce et à la communication électronique au sein de l'Union européenne. Ceci empêcherait la libre circulation de la cryptologie, des produits et services qui y sont liés dans le Marché intérieur, ainsi que le développement de nouvelles activités économiques liées au commerce électronique. Un cadre communautaire est donc requis d'urgence afin de stimuler le commerce électronique et la compétitivité de l'industrie européenne, ainsi que pour abolir les obstacles à la libre circulation et pour faciliter l'usage trans-frontalier des signatures numériques.

Mais, la communication électronique ne se limite pas au territoire de l'Union européenne. Un cadre doit donc être développé, dans les domaines appropriés, au niveau international, une fois qu'une position communautaire aura été arrêtée. Cela nécessite la participation de l'Europe (tant au niveau communautaire qu'au niveau des États membres) à des initiatives ou des instances internationales.

[177] Gesetz zur digitalen Signatur (SigG), 1.8.97; http://www.iid.de/rahmen/iukdgbt.htm#a3

[178] Schema di Regolamento "Atti, documenti e contratti in forma elettronica," appouvé apr la Conseil des ministres italien le 5.8.97

[179] Staatscourant nr. 54, 18.3.97

[180] Voir http://www.agoraproject.org/

Beaucoup de ces initiatives internationales ont été lancées à des niveaux différents. Des discussions bilatérales (*UE/USA, UE/Japon*) et multilatérales (par exemple l'*UNCITRAL*[181]) ont démarré. L'*UNCITRAL* a achevé son travail sur un modèle de loi pour le commerce électronique[182] et a récemment lancé un travail subséquent visant à la préparation de règles uniformes sur les signatures numériques et les services (trans-frontaliers) (Autorité de Certification) qui y sont liés. Les travaux sur les Directives en matière de politique cryptographique se poursuivent dans le cadre de l'OCDE. D'autres organisations internationales, telle que l'OMC (Organisation Mondiale du Commerce), pourraient être impliquées pour éviter de nouveaux obstacles au commerce, pour d'autres aspects liés à leurs domaines de compétence ainsi que dans le cadre d'expertises spécifiques.

Aux États-Unis[183], pratiquement tous les États ont soit commencé à élaborer, soit ont déjà une législation sur les signatures numériques. Des agences, telles que la *Federal Food and Drug Administration*, ont promulgué des réglementations spécifiques à leur domaine de responsabilité[184]. Au niveau fédéral, le Congrès examine plusieurs initiatives législatives. Au Japon, certaines activités techniques et réglementaires dans les domaines de l'authentification et des transactions électroniques ont été lancées.

Au niveau commercial, *l'American Bar Association* a élaboré des Directives pour les signatures numériques[185] (*Digital Signature Guidelines*) et le *Internet Law and Policy Forum* (ILPF) travaille sur le rôle des Autorités de certification dans les transactions impliquant les consommateurs[186].

Aussi, au vue de ces activités la communauté européenne doit prendre des initiatives afin de faire tomber les barrières existantes et créer un cadre international compatible pour le

[181] United Nations Commission on International Trade Law

[182] http://www.un.or.at/uncitral/index.html

[183] Une mise à jour du statut de la législation des USA peut être trouvée à http://www.mbc.com/ds_sum.html

[184] http://www.fda.gov/cder/esig/part11.htm

[185] http://www.abanet.org/scitech/ec/isc/dsg_tutorial.htm

[186] http://www.ilpf.org/work/ca/draft/htm

commerce électronique, en particulier pour établir des normes techniques et juridiques communes. Si des restrictions nationales sont établies, elles doivent rester compatibles avec la législation communautaire. D'ailleurs la commission au parlement européen a considéré que les divergences dans les approches légales et techniques en matière de cryptographie constituent un obstacle au marché unique et un obstacle au développement de nouvelles activités économiques liées au commerce électronique[187].

Ainsi la France, qui est un des rares pays dans lequel le libre usage de la cryptographie forte est interdit, se trouve dans une position de plus en plus difficilement compatible avec son appartenance à l'Union européenne et son statut international. D'ailleurs, le Conseil d'État a proposé de développer la coopération entre États pour faire respecter le droit sur les réseaux numériques ainsi que de définir des orientations stratégiques communes afin d'assurer la cohérence des positions françaises dans les diverses négociations internationales concernant Internet et les réseaux numériques[188].

Donc, compte tenu de la nature universelle de la communication et du commerce électronique, une fois qu'un système harmonisé aura été mis en place, des accords internationaux pourraient s'avérer nécessaires entre la Communauté et d'autres pays. Le but de ces accords devrait être de lever les obstacles existants de manière à créer un cadre international compatible pour le commerce électronique, en particulier pour l'établissement de normes techniques.

D'ailleurs, L'OCDE recommande aux pays membres de répondre au besoin de solutions pratiques et opérationnelles dans le domaine de la politique internationale de cryptographie. De plus, elle demande :

[187] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, COM (97) 503 en date du 8 octobre 1997, « Assurer la sécurité et la confiance dans la communication électronique » disponible à http://www2.echo.lu/legal/fr/internet/actplan.html.

[188] Conseil d'État, Section du rapport et des études, Internet et les réseaux numériques, *Étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998*

> « de veiller à la levée ou d'éviter de créer au nom de la politique de cryptographie, des obstacles injustifiés au commerce international et au développement des réseaux d'information et de communication. »[189]

Ainsi, si les pays partent de situations différentes (absence de réglementation pour l'Allemagne, réglementation très restrictive à l'origine pour la France), il y a un consensus au niveau international sur la nécessité de trouver un équilibre entre les contraintes industrielles commerciales et de vie privée, et celles liées à l'ordre public et à la sécurité des États[190].

Malgré ce consensus, un reproche peut tout de même être fait à l'ensemble de ces réglementations ou propositions (qu'elles soient nationales, communautaires ou internationales): c'est la « myopie » des projets. En effet, la vision restrictives des approches actuelles montrent que les États n'ont pas encore pris conscience que les dispositions relatives à l'usage des cryptotechnologies, aux écoutes, aux tiers de confiance, à l'interopérabilité internationale et à la valeur des documents électroniques forment un tout indissociable. Ainsi, à quoi sert de définir la signature électronique si ce n'est pas pour donner une valeur à celle-ci ? A quoi sert de permettre le scellement d'un document électronique si ce n'est pour lui donner une valeur de preuve convenable ? Ainsi, seule l'Allemagne semble par plusieurs textes sur les tiers de confiance, la protection des données nominatives et la signature électronique, avoir pris une mesure relative du caractère inséparable de ces composantes.

Les administrations européennes ne semblent pas apprécier à leurs justes valeurs le poids de leurs décisions de repousser des textes, même imparfaits. En effet, une année sur Internet représente sept ans dans le reste des activités[191]. Aussi, pour chaque décision retardée, se sont des projets qui ne voient pas le jour, des chiffres d'affaire qui s'installent ailleurs…. Donc, il est urgent que les institutions organisent une réunion afin que les États acceptent de mettre en place des expérimentations globales et programment l'élaboration d'un traité commun.

---

[189] Recommandation du conseil de l'OCDE du 27 mars 1997 relative aux lignes directrices régissant la politique de cryptographie

[190] Rép. Min. n°13318, JOANQ 29 juin 1998, p.3614.

[191] ROS de LOCHOUNOFF Nicolas, « chiffrement, tiers de confiance, signature électronique et interceptions : les gouvernements et les internautes sont-ils myopes. », *revue expertises* n°211, janvier 1998, p.417.

Chapitre II : La protection des informations face à la *raison commerciale*

En 1994 un avocat de San Francisco spécialisé en droit de l'informatique voyait la communauté électronique dans un dilemme classique :

> « the tug-of-war between the desire for a free flow of information, and need for privacy. The problem can be recast as the pull between freedom of access on the one hand, and, on the other, what might be thought of as the right of self-determination and control over the dissemination of information »[192]

Nous traiterons d'abord d'une période où les Autoroutes de l'information commençaient à devenir une réalité. À une période où *l'Electronic Frontier Foundation* et les autres groupes de pression n'existaient pas encore pour réveiller les consciences sur les dangers que peuvent supposer un libre flux d'information sans contrôle. Cela dit, nous verrons dans cet partie l'aspect commercial de la cryptologie et nous traiterons, tout aussi chronologiquement le passage d'un aspect confidentiel (section I) à celui comme solution à un besoin nouveau (section II) et, même, comme une solution nécessaire (section III)♦.

Section I : Avant l'émergence d'un besoin : une cryptographie à usage confidentiel

Le commerce est depuis des siècles une activité humaine universelle. Son exercice ne posait que peu de difficultés tant que les relations commerciales nécessitaient un contact physique. En effet, les informations échangées, au cours de ces contacts commerciaux, n'impliquaient que peu de moyens techniques afin de conserver leurs confidentialité. Avec l'apparition du commerce électronique les données du problème ont été accentuées (I). De plus, une approche classique du commerce ne soulève pas les même difficultés, en matière de preuves, que lors d'échanges commerciaux dématérialisés (II).

[192] KARNOW, Curtis E.A., « The encrypted self : fleshing out the rights of electronic personalities », *The John Marshall journal of computer and information law*, Vol. XIII, n°1, october 1994

I- Le secret à l'épreuve d'une informatique émergente

L'utilisation de la cryptographie est nécessaire au développement du commerce et à la circulation des informations sur le réseau. En effet, sans protection, les informations circulant électroniquement seraient trop vulnérables. Or, pour cela, la commercialisation des moyens ou prestations de cryptologie est une condition première à leurs utilisations(A). Enfin, la notion de preuve, comme nous la percevons actuellement, n'est peut être plus adaptée au commerce électronique (B).

A- La circulation du cryptographe :

La circulation des moyens de cryptologie doit s'inscrire dans une optique de liberté de commerce et d'industrie. En effet, si la protection des informations passe par des moyens de cryptologie, il faut que ceux-ci puissent être développés et distribués sans entraves.
L'étude de la liberté du commerce et de l'industrie doit être analysée en fonction du principe de liberté mais aussi de ses limitations.

Le principe de la liberté du commerce et de l'industrie trouve sa première expression, en France, dans le décret d'Allarde des 2 et 17 mars 1791. Aujourd'hui, toutes ses dispositions ont été abrogées à l'exception de son article 7 au terme duquel :

> *« Il sera libre à toutes personnes de faire tel négoce ou d'exercer telle profession, art ou métier qu'elle trouve bon ».*

Ces fondements juridiques sont parfois considérés comme dépassés en raison de la réaffirmation du principe en droit interne mais aussi communautaire[193].

Plusieurs textes ont réformulé le principe de manière directe[194]. D'ailleurs, le Conseil d'État reconnaît aussi cette liberté du commerce et de l'industrie comme une liberté publique[195],

---

♦ Ce paragraphe a été modifié par rapport à la version originale du présent mémoire étant donné que l'annonce du plan a été malencontreusement oubliée…

[193] AZEMA J., *Droit de la concurrence*, PUF, Thémis, p.27

[194] Loi Royer du 27 décembre 1973, article 1er : « *la liberté et la volonté d'entreprendre sont les fondements des activités commerciales et artisanales* », M.GUIBAL, *REP. com. Dalloz V° Commerce et industrie*, 1994,n°55.

ainsi que le Conseil constitutionnel. En effet celui-ci estime que la liberté du commerce et de l'industrie fait partie des libertés :

> *« Qui ne peuvent s'exercer que dans le cadre d'une réglementation instituée par la loi »*[196]

De plus il a récemment conféré une valeur constitutionnelle à cette liberté en soulignant que :

> *« La liberté qui aux termes de l'article 4 de la Déclaration (des droits de l'homme et du citoyen), qui consiste à pouvoir faire tout ce qui ne nuit pas à autrui, ne saurait elle-même être préservée si des restrictions arbitraires ou abusives étaient apportées à la liberté d'entreprendre »*[197]

Le droit communautaire a également reconnu ce principe de liberté du commerce et de l'industrie. Ce principe découle directement de la conception libérale de l'activité économique qui imprègne l'ensemble des dispositifs européens: Traité de Rome, Acte unique européen, Traité de Maastricht.

Ainsi, au sein de ces documents se trouvent affirmées la liberté de circulation des marchandises[198], des personnes[199], des services[200], ainsi que la liberté d'établissement et d'activités non salariées[201]. En effet, au niveau intra-communautaire, le principe est celui de la libre circulation des marchandises, c'est à dire, les transferts effectués d'un État membre à un autre (ne sont pas considérés comme transferts, les envois de marchandises ayant déjà fait l'objet de formalités d'exportation vers les pays tiers dans un État membre et empruntant le territoire d'un autre pour sortir de la Communauté).

---

[195] CE, 28 octobre 1960, de LABOULAYE, AJDA 1961, 20 ; CE 9 janvier 1981, Sté Claude publicité, D. 1981, IR 113, obs. DELVOLE ; CE 22 mars 1991, AJDA 1991, 650

[196] Décision du 27 juillet 1982, *Rev. Dr. Pub.* 1983, 333, obs. L. FAVOREU.

[197] Décision du 16 janvier 1982, D. 1983, 169, note L. HANON .

[198] Traité de Rome, art. 30

[199] Traité de Rome, art. 48

[200] Traité de Rome, art 59 et 60.

[201] Traité de Rome, art. 52.

Ces normes européennes sont d'application directe, comme l'a souligné la Cour de justice des Communautés européennes à l'occasion d'espèces concernant, de manière générale, la liberté d'établissement à laquelle on peut rattacher la liberté du commerce et de l'industrie[202].

En conséquence, ces libertés ont plein effet sur le territoire français et le principe de droit communautaire prévaut sur notre droit interne. Cette solution a été affirmée, par la cour de Cassation dans l'arrêt *Jacques Vabre* du 24 mai 1975[203], la Cour de justices des Communautés européennes le 9 mars 1978[204] et par le conseil d'État dans l'arrêt *Nicolo* du 20 octobre 1989[205].

Cette liberté du commerce et de l'industrie comprend la liberté d'entreprendre et d'exploiter, qui en sont le prolongement économique. Ainsi, toute personne physique ou morale peut s'installer en créant ou en acquérant une entreprise et exercer l'activité de son choix. En effet, en France, il n'existe pas de déterminations limitatives des types ou modes d'activités commerciales ou industrielles autorisées. Donc, cette liberté d'exploiter emporte la possibilité pour toute personne de gérer son entreprise à sa guise, c'est à dire la possibilité de choisir ses partenaires, ses fournisseurs, ses clients…

La liberté du commerce et de l'industrie est issue des premiers pas de la Révolution française. Mais, elle a été vite contredite par des mesures restrictives comme la loi sur la taxation du pain et de la viande[206].

Il est vrai qu'une liberté, quel que soit son objet, ne saurait être absolu et doit trouver sa limite dans le respect de la liberté des autres ou de l'intérêt général. Ainsi, après avoir affirmé que toutes personnes bénéficiaient du régime de la liberté du commerce et de l'industrie, l'article 7 du décret d'Allarde ajoutait :

---

[202] Arrêt REYNES, CJCE 21 juin 1974, REC. 631, *RTD europ*. 1975, p.561, application de l'article 52 analysé cependant comme un prolongement de l'article 7 du Traité de Rome qui pose le principe de non-discrimination en fonction de la nationalité.

[203] D.1990, 497, concl. A. TOUFFAIT.

[204] Arrêt Simmenthal, Rec.269

[205] D. 1990, 57, note R. KOVAR.

[206] Loi 19-22 juillet 1791

« Mais elle sera tenue de… se conformer aux règlements de police qui pourront être faits»

D'ailleurs, le Conseil constitutionnel a jugé que la liberté du commerce et de l'industrie relève de ces libertés qui :

« *Ne sont ni générales, ni absolues* » et qui « *ne peuvent s'exercer que dans le cadre d'une réglementation instituée par la loi.»*[207]

Mais, si la liberté du commerce et de l'industrie ne saurait s'imposer de manière absolue au législateur, ce dernier ne pourra, toutefois, la restreindre de manière abusive ou arbitraire. Il devra invoquer des impératifs de sécurité, moralité publique, des exigences d'ordre public ou de protection.

Or, à l'origine la cryptologie a été classifiée comme une arme de guerre. En France, par exemple, la cryptologie était considérée comme du matériel de guerre de deuxième catégorie (décret du 18 avril 1939)[208]. Plus tard, la lutte contre la criminalité et la nécessité de pouvoir intercepter des messages chiffrés ont justifié une politique restrictive en matière de cryptologie. En fait, sous des couverts de sécurité nationale ou de protection de l'ordre public, l'État a toujours eu une bonne raison pour restreindre la libre commercialisation et l'utilisation de moyens ou de prestations de cryptographies.

Mais, actuellement ces considérations ne sauraient être privilégiées face à la liberté du commerce est de l'industrie. En effet, sous la pression d'une économie libérale, cette liberté est de plus en plus souvent invoquée et protégée notamment contre l'interventionnisme des autorités publiques internes et communautaires.

[207] Cons. Const. 27 juillet 1982, *Rev. Dr.pub.* 1983, 333, obs. L. FAVOREU.

[208] MEILLAN Eric, « Le contrôle juridique de la cryptographie », *droit de l'informatique & des Télécoms, 1993/1, p.78 et s.*

B- La circulation des informations

La circulation des informations est aussi une circulation ayant un potentiel économique important. Par exemple, dans une situation d'achat de marchandises, des échanges financiers interviennent de façon massive à tel point que certaine cargaisons peuvent changer plusieurs fois de propriétaire entre le départ et l'arrivé d'une marchandise. Ces échanges immatériels constituent un important transfert financier qui semble faire la joie des spéculateurs au dépend des producteurs. En dehors de toute polémique, et dans la situation qui prévalait avant l'utilisation des outils cryptographique et des échanges électronique, une protection se révèle nécessaire , cette protection était relativement assurée .

Une protection nécessaire et légalement reconnue

Comme tout bien, les informations obéissent aux règles commerciales notamment pour ce qui à trait à la liberté du commerce et de l'industrie. Ceci dit, le Conseil constitutionnel à jugé que cette liberté n'est « ni générale, ni absolue [ne pouvant s'exercer] que dans le cadre d'une réglementation instituée par la loi »[209]. Le refus de la France d'adhérer à l'AMI (Accord Multilatéral d'Investissement) rejoint cette position qui préserve les biens culturels d'une *normalisation* qui, sans cela aurait été inévitable et dommageable dans ce domaine. La loi anti-trust aux États-Unis veille également à éviter certaines de ces situations en effet, trop de liberté économique nuisent à l'économie, ainsi la liberté de constituer un monopole empêcherait la concurrence et freinerait ainsi la libre entreprise.

La liberté de la concurrence revient au droit pour l'entrepreneur d'user de moyens loyaux pour exercer son activité et rechercher une clientèle. Le parasitisme est ainsi une pratique condamnée[210].

Cela étant, le secret est un moyen de conserver une certaine avance dans certains domaines amenés à devenir économiques et de prévenir ainsi tout recours en cas de

[209] Cons. Const. 27 juillet 1982, Rev. Dr. Pub., 1983, 333, obs L. Favoreux

[210] VIVANT, Michel, et Christian LE STANC, *Lamy droit de l'informatique et des résaux*, Paris, Ed. Lamy, 1998, n°276

parasitisme. La recherche et développement occupe ainsi une par importante des investissements de certaines entreprises et, pour reprendre Michel Vivant,

> « adopter la voie du secret, c'est faire un choix dans une stratégie d'entreprise, largement tributaire de données telles que le secteur d'activité, le caractère obsolescent ou non des produits, l'état de la concurrence, la taille de l'entreprise…
> À titre d'exemple, le brevet supposant une divulgation, il peut être préférable pour une entreprise qui estime n'avoir pas la surface financière nécessaire pour le défendre et donc ne saurait en tirer profit, d'opter pour le secret. Ce peut être la voie raisonnable »[211]

Mais le secret vise à garantir d'autres objectifs comme vis-à-vis de la clientèle, pour la conserver et pour la protéger le cas échéant. La *Loi relative à l'informatique, aux fichiers et aux libertés*[212] vise indirectement et directement à régler ces questions en France.

Le secret est donc un élément important dans toute stratégie d'entreprise, il importe de voir à présent que cette protection est, au stade d'émergence de l'informatique, relativement bien assurée.

Une protection satisfaisante ?

Le secret se gère en premier lieux par des moyens physiques qui continuent à être un minimum essentiel et qui assure une protection efficace : une protection qui , selon les moyens mis en œuvre, reste inviolable. Le problème réside au moment où l'information sors des coffres.

Avec l'informatique le problème de sécurité des informations est plus complexe. D'une part, les informations sont faciles à recopier, d'autre part les réseaux internes sont fragiles et peuvent être la proie des intrusions. Le principal facteur de risque ne tient d'ailleurs pas à l'informatique mais le plus souvent aux utilisateurs : les mots de passes sont notés ou prêtés, les système de pare-feu (*firewalls*) sont mal configurés ou inexistant et permettent ainsi les intrusions externes… Autant de problèmes que l'informatique ne pourra pas régler. Le secret

[211] ib. p. 17

[212] Loi n° 78-17 du 6 janvier 1978

est avant tout une question de responsabilité et, de la même manière, l'utilisation des outils cryptographiques est une question qui ne pourra être éludée par les entreprises sérieuses.

Concernant les données personnelles, un avocat de San Francisco spécialisé en droit de l'informatique voyait en 1994 la communauté électronique dans un dilemme classique :

> « the tug-of-war between the desire for a free flow of information, and need for privacy. The problem can be recast as the pull between freedom of access on the one hand, and, on the other, what might be thought of as the right of self-determination and control over the dissemination of information »[213]

La science du secret appliquée à l'informatique entre donc tout naturellement dans un débat sur la protection des informations

II La preuve confrontée à une informatique émergente

La promotion du commerce électronique est devenue l'un des enjeux économiques majeurs du XXI^{ème} siècle. Encore faut-il lui assurer un cadre juridique adéquat. Valérie Sédaillan exprime cette idée dans la formule suivante :

> *« Dans le contexte d'une société ou les échanges d'informations numériques se développent, il est indispensable de pouvoir bénéficier de systèmes sécurisés pour protéger les données à caractère personnel confidentiel, assurer la sécurité des transactions financières et commerciales, passer des contrats en l'absence de support papier »*[214]

Le développement d'un véritable marché électronique répond essentiellement à des exigences de sécurité (juridique) et d'authentification. Les acteurs du commerce électronique souffrent constamment des incertitudes liées à la dématérialisation des échanges de données. L'écrit n'existe plus et les moyens de preuves actuels ne sont peut être plus adaptés à ce monde électronique. Le Code civil français détermine cinq modes de preuve[215] et il fixe leur

[213] Op. cit. note 192

[214] SEDAILLAN, Valérie, « Les enjeux et l'état de la législation française », *la lettre de l'Internet*, 31 juillet 1997, http://www.argia.fr/lij/Étatcrypto.html

[215] L'écrit, les témoins, les présomptions de fait, l'aveu et le serment.

admissibilité en fonction de l'objet de cette preuve. En matière commerciale, la preuve peut varier selon les personnes concernées (B). En général elle passera par un contrat (A).

A- Un contrat papier privilégié

La numérisation des informations ou la signature numérique entraînent des conséquences juridiques importantes[216]. En effet, habituellement les contrats passés en matière commerciale sont surtout des actes sous seing privé (c'est à dire sous signature privée).

Pour cela, une seule condition indispensable de forme est prescrite : la signature manuscrite.
Donc cela ne fait pas de doute, la signature est intimement liée à l'écrit. De nombreux textes prescrivent d'établir certains actes juridiques par écrit ou par un écrit signé[217]. Pour D. PONSOT, la signature se définis comme :

> *« étant une inscription (ou un graphisme) originale, personnelle, habituelle et notoire, par laquelle un individu manifeste son consentement au contenu d'un écrit »*

Comme la loi ne définie pas ce qu'il faut entendre par le terme « signature », la jurisprudence et la doctrine ont établi son régime juridique. Pourtant, le code civil mentionne à plusieurs reprises l'obligation d'une signature. Ainsi, l'article 1322 du code civil sur les actes sous seing privé prescrit une signature manuscrite[218]. A côté de la signature manuscrite, en pratique, il peut être utilisé le sceau, la griffe[219], voire des moyens électroniques à l'instar des cartes bancaires.

En matière probatoire, si l'article 1341 du code civil consacre la prééminence de l'écrit, ses dispositions ne sont pas d'ordre public et les parties ont le droit d'y renoncer[220]. En

---

[216] D.SYX, « Vers de nouvelles formes de signature. Le problème de la signature dans les rapports électroniques », *DIT* 1986/3, p.133 s.

[217] D.PONSOT, « La signature en droit privé » : *Dr. Informatique et télécoms* 1996/4, p14 s.

[218] « Une simple croix n'est pas suffisante », Cass. 1er civ, 15 juillet 1957, *Bull civ. I, n°331*. « L'engagement du représentant légal d'une société anonyme par une signature ou un paraphe ne permettant pas de l'identifier », *Petite affiche*, 22 août 1997, p.10

[219] Cour d'appel de Paris, 19 décembre 1958, *JCP G*, 1960, I, 1579

[220] Cass. 3ème civ, 16 novembre 1977, *Bull civ*, III, n°393.

conséquence la solution consisterait à élaborer un véritable formulaire électronique sur le plan contractuel. De cette façon, les parties peuvent écarter les exigences de l'article 1341 et décider que la preuve des contrats conclus s'effectuera par d'autres moyens que l'écrit et ceci au moyen d'une convention de preuve.

La jurisprudence a reconnu la validité de telle convention portant sur la signature informatique en matière de paiement par cartes bancaires (arrêts Crédicas[221]). La Cour de cassation a jugé que le litige portait sur :

> *« des droits dont les parties ont la libre dispositions"* et que *"ces conventions relatives à la preuve sont licites»*

Selon la Cour de cassation, les parties peuvent par contrat accorder une valeur probante à un document dépourvu de signature, au sens classique du terme. C'est à dire manuscrite.

Dans son rapport annuel pour 1989, la Cour de cassation a estimé que :

> *« ce procédé moderne présente les mêmes garanties que la signature manuscrite, laquelle peut être imitée tandis que le code secret n'est connu que du seul titulaire de la carte»*[222]

Toutefois, sauf à faire intervenir un tiers certificateur qui apporte toutes les garanties de sécurité et de confiance dans le système, on peut s'interroger sur la validité de la signature numérique réalisée en dehors de toute convention sur la preuve[223].

Une remarque doit être formulée quant à l'admission de la validité de la signature numérique. Le système d'information utilisé doit être fiable et son efficacité informative

---

[221] Cass. 1er civ., 8 novembre 1989, Bull. civ. I, n°342. Dalloz 1990, p.369, note C.Gavalda

[222] Paris, la documentation française, 1990, p.32.

[223] « Plaidoyer pour un droit conventionnel de la preuve en matière informatique », Expertises, juillet- août 1987, p.260 s.

crédible. Donc, si comme le dit M. CABRILLAC : la sécurité du télexe « *milite également en faveur de l'intégration de la clé informatique dans le formalisme cambiaire fût ce avec quelques précautions ou précisions* »[224], la cryptographie en apportant la sécurité nécessaire à la signature peut militer en faveur d'une valeur probante de la signature numérique.

Si la signature est la condition indispensable du contrat papier, son obstacle pourrait être franchi par le truchement de la cryptographie. En revanche, des conditions supplémentaires de formes peuvent devenir plus difficiles à contourner.

Un contrat commercial (par exemple un contrat de vente) est souvent un contrat de type synallagmatique. Or, l'article 1325 du Code civil édicte la formalité du double :

« … autant d'originaux qu'il y a de parties ayant un intérêt distinct.»

Sinon, l'acte juridique n'est pas nul, mais il ne peut servir de preuve. Il pourra toutefois servir de commencement de preuve. Or, les contrats commerciaux passés sur le réseau regroupent bien deux cocontractants. Chacun possède un intérêt distinct (chacun attend la prestation de l'autre). Donc, la formalité du double (original) devrait être effectuée sous peine de n'avoir qu'un commencement de preuve. Mais, sur le réseau les cocontractants ne se rencontrent pas. Donc, le seul exemplaire papier du contrat qu'ils peuvent obtenir, est celui qui apparaîtra sur leurs imprimantes. Peut-on considérer ce papier comme un original ?

En fait, la problématique est autre. La véritable difficulté réside dans ce que l'on peut considérer comme «l'original» dans ce genre de transaction ? En effet, le seul contrat original qui est passé entre deux internautes, est celui qui apparaît sur l'écran. Mais, ce contrat là n'est pas papier. Donc, devons-nous considérer que toutes les impressions du contrat passé sur un écran sont des originaux ?

Nous pouvons considérer que, soit l'original se situe uniquement au sein de l'unité centrale de l'ordinateur, et dans ce cas, il n'y a pas de preuve écrite, soit nous pouvons

[224] M.CABRILLAC, « Chron. De législation et de jurisprudence française » : *RTD com*. 1997, p. 120

considérer que seules certaines impressions sont originales. Dans ce dernier cas, il paraît insurmontables de déterminer quels sont les « véritables » originaux .

Heureusement, il existe des tempéraments à cette formalité du double :

- L'écrit devient inopposable en tant que preuve pour celui qui a exécuté la convention.
- La formalité est réputée accomplie si un seul exemplaire est rédigé mais déposé entre les mains d'un tiers. Cette solution pourrait voir une adaptation au travers des tiers de confiance.
- La règle est inapplicable aux actes commerciaux. Mais, il ne faut pas oublier que si le contrat est conclu entre un commerçant et un non commerçant, l'acte n'est pas considéré comme commercial pour celui qui n'est pas commerçant.

Aussi, même si dans un certains nombres de cas le problème de la valeur probante du document ne se posera pas, la preuve du contrat, sous sa forme actuelle, ne semble pas totalement adaptée au commerce électronique. En fait, tout dépendra du type de preuve qui sera appliqué : la preuve civile ou la preuve commerciale.

B- La preuve (civile et commerciale)

Comme nous l'avons vu précédemment, l'admissibilité de la preuve de l'acte passé peut dépendre selon que nous nous situons dans un acte commercial, civil ou mixte. Deux régimes sont concevables : soit le régime de liberté de la preuve, soit celui de sa légalité.

Dans le premier cas, tous les modes de preuves sont admis et le juge appréciera librement leurs valeurs pour former sa conviction.

Dans le second cas, c'est la loi qui déterminera les modes de preuves recevables et qui fixera leur force probante.

En droit civil, pour les actes juridiques, le principe est celui de la légalité de la preuve (contrairement au droit pénal ou administratif). En effet, le législateur a estimé qu'il était possible de se préconstituer une preuve. Donc, il existe une supériorité de l'écrit en matière

contractuelle. En effet, cet écrit semble plus objectif et plus durable que les autres modes de preuves.

Selon l'article 1341 du Code civil, la preuve par écrit est obligatoire :

> « *Il doit être passé acte devant notaire ou sous signatures privées de toutes choses excédant une somme ou une valeur fixée par décret même pour dépôts volontaires, (…) le tout sans préjudice de ce qui est prescrit dans la loi relative au commerce* »

La somme visée par cet article a été fixée par décret à 5000 FF[225]. Pour tout contrat dont la somme dépasse 5000FF, la preuve par écrit est nécessaire. Mais l'article 1341 du Code civil n'impose pas la preuve écrite systématiquement.

Tout d'abord, en matière commerciale, pour des motifs de rapidité des transactions commerciales, il est possible de prouver par tous moyens. Ainsi, l'article 109 du code de commerce dispose :

> *« A l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi.»*

Cette règle s'applique même si la somme en question dépasse le seuil des 5000 FF. Mais, il existe des limites à cette liberté de la preuve. Si le contrat est purement commercial (c'est à dire entre deux commerçants), cette liberté s'applique pleinement. En revanche, dans le cas d'un contrat mixte (c'est à dire entre un commerçant et un non commerçant), la liberté de la preuve n'est possible qu'à l'encontre de la partie commerçante. A l'encontre de la partie non commerçante, c'est la légalité de la preuve qui devra être mise en œuvre. Cette obligation de se prémunir d'une preuve écrite à l'encontre de la partie non commerçante, peut engendrer une insécurité juridique pour le commerçant. En effet, comme nous l'avons vu précédemment, en matière de commerce électronique, la constitution de cette preuve écrite soulève des difficultés.

[225] Décret n°80-533 du 15 juillet 1980

Ensuite, en matière civile, l'article 1341 du code civil fixe une limite de 5000 FF pour la nécessité de se prémunir d'un écrit. Donc, a contrario, si la somme dont il est question est inférieure à ce seuil, l'obligation de procurer une preuve écrite n'existe pas. Dans ce cas, la liberté de la preuve jouera pleinement son rôle et il sera possible de prouver les obligations prisent par tous moyens.

Enfin, toujours en matière civile, l'article 1341 du code civil n'est pas d'ordre public. En effet, c'est une règle protectrice des simples intérêts privés. Donc, les parties à un acte juridique peuvent renoncer à l'exigence de la preuve écrite, soit au moment de la conclusion de l'acte, soit au cours du procès.

Une autre possibilité peut également être prise en compte. Dans le cas du commerce électronique, ne pouvons nous pas considérer que nous nous trouvons devant un cas d'impossibilité de se préconstituer ou de produire une preuve écrite. En effet, l'article 1348 du code civil dispose :

> *« Les règles ci-dessus* (dont l'article 1341 du code civil) *reçoivent exception lorsque (…) l'une des parties, soit n'a pas eu la possibilité matérielle ou morale de se procurer une preuve littérale de l'acte juridique, (…)*
> *Elles reçoivent aussi exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support.»*

Dans le cas de la préconstitution, elle pourrait découler des usages appliqués dans le cadre du commerce électronique. La distance entre les deux cocontractants pourrait créer une nouvelle forme d'usage, propre à ce type de commerce, empêchant la préconstitution d'un original du contrat.

Ensuite, dans le cas de la production de la preuve écrite, si nous supposons que l'original du contrat n'est autre que ce qui apparaît sur l'écran, le fait d'imprimer cet écran constitue une reproduction durable est fidèle du titre original.

Malgré tout, il apparaît que le régime actuel de la preuve est adapté à un monde physique. Cela soulève des difficultés d'application lorsque nous passons dans un monde dématérialisé. Pour répondre au nouveau besoin que crée le développement du commerce électronique, la cryptographie peut être un outil très utile.

Section II : La cryptographie, un outil nécessaire au développement d'un besoin nouveau : le commerce électronique

Étant donné qu'un nombre croissant de transactions se font non plus sur un réseau fermé mais sur un réseau ouvert[226], la cryptographie devient indispensable au commerce électronique. Par le passé, le commerce électronique, comme l'échange de données informatisées (EDI) ou le transfert électronique de fonds, s'effectuait en grande partie sur des réseaux fermés. Dans le contexte commercial mondial, on ne pourra tirer pleinement parti du commerce électronique que si l'on passe par des réseaux ouverts.

Toutefois, ces réseaux posent divers problèmes, en ce qui concerne l'authentification des parties communiquant, l'intégralité des documents, la confidentialité des renseignements et l'assurance que les transactions ont été autorisées par les utilisateurs légitimes.

Sans la cryptologie pour assurer cette fiabilité, nous risquons de ne pas pouvoir régler ces problèmes.

Avec le développement croissant de l'informatique, à tous les échelons de notre société, la protection des informations communiquées fait l'objet de nouveaux défis (I). De même, la notion de preuve nécessite une remise en question (II).

I- Le secret à l'épreuve d'une informatique installée

La circulation d'informations sur un réseau ouvert soulève des questions quant à leurs niveaux de confidentialité. Même si des textes français prennent déjà en compte ce paramètre, leurs confrontations avec les normes européennes peuvent voir surgir des oppositions (A). Mais, en dehors de cet aspect de confidentialité, le commerce électronique réclame toujours une certaine sécurité juridique quant aux transactions passées sur le réseau (B).

[226] Le réseau fermé, relie des utilisateurs entretenant déjà une relation contractuelle et se font mutuellement confiance. Par comparaison, Internet constitue l'exemple le plus connu de réseau ouvert. Il s'agit d'un vaste réseau interconnecté composé de milliers de réseaux.

A- Lois françaises face aux normes européennes

Au niveau européen, un règlement communautaire du 19 décembre 1994[227] institue un régime de contrôle des exportations de biens à double usage (en revanche, il ne prévoit pas de restrictions dans le domaine de l'utilisation ou de l'importation des produits de cryptographie). Mais la politique générale tend vers un certain assouplissement des contrôles à l'exportation des produits dits « sensibles». Cet assouplissement est justifié par les progrès de la technologie et par la forte pression des industries exportatrices européennes et des pays tiers.

Ce régime, applicable depuis le 1er juillet 1995, est marqué par les principes directeurs du marché commun, notamment celui de libre circulation des biens à l'intérieur du marché commun ainsi que celui de reconnaissance mutuelle des licences d'exportation entre les États membres.

Néanmoins, des restrictions temporaires aux transferts intra-communautaires subsistent pour certains biens considérés comme particulièrement sensibles, parmi lesquels figurent les produits et logiciels de cryptographie. Ainsi, sont visés les télécommunications, logiciels et matériels informatiques de haute technologie et la sécurité de l'information.[228]

Au niveau intra-communautaire, le principe de la libre circulation des marchandises persiste[229]. En revanche, pour les pays tiers, les équipements de sécurité de l'information et les logiciels de chiffrement ne peuvent pas être exportés hors de la communauté sans licence [230].

---

[227] Règlement (CE), n°3381/94 du Conseil, du 19.12.1994, instituant un régime communautaire de contrôle des exportations de biens à double usage, JOCE, n°L367/1, du 31.12.1994 ; modifié par le règlement Conseil CE n°837/95 du 10.04.1995, JOCE du 21.04.1995,n°L90 ; décision du Conseil du 16.02.1996,JOCE du 1.03.1996,n°L52 ; décision du Conseil du 22.10.1996,JOCE 30.10.1996,n°L278 ; JOCE du 28.02.1997,n°C64 p.1; décision du Conseil du 20.01.1997,JOCE 4.02.1997, n°L34.

[228] La catégorie 5 « *télécommunications* » de l'annexe I comprend une partie 2 sécurité de l'information définie comme : « *tous les moyens et toutes les fonctions réglant l'accessibilité ou assurant la confidentialité ou l'intégrité de l'information ou des télécommunications, à l'exclusion des moyens et des fonctions prévues pour la protection contre les défaillances* » ; . Par conséquent, sont compris la « cryptologie », la « cryptanalyse », la protection contre les émanations compromettantes et la sécurité des ordinateurs.

[229] L'article 9 du Traité Rome dispose que « *La Communauté est fondée sur une union douanière qui s'étend à l'ensemble des échanges de marchandise, et qui comporte l'interdiction, entre les États membres, des droits de douanes à l'importation et à l'exportation (…)* ».

La compatibilité de la loi française avec la législation communautaire est abordée dans la communication de la Commission européenne sur la sécurité et la confiance dans la communication électronique[231]. Pour elle :

> *« Une réglementation limitant l'usage de produits et de services de chiffrement dans le marché intérieur constitue un obstacle à la libre circulation des informations personnelles et à la fourniture de biens et de services qui y sont liés, et sa justification doit être examinée à la lumière du Traité (de Rome) et de la directive communautaire sur la protection des données personnelles.*
> ……
> *Indépendamment de la compatibilité de restrictions avec les dispositions du Traité en matière de libre circulation des biens et des services, des contrôles nationaux spécifiques pourraient également avoir des effets secondaires sur la libre circulation des personnes similaires à ceux identifiés par le Comité Veil.*»

L'article 9 du Traité de Rome a institué le principe de libre circulation des marchandises. L'article 30 interdit également les mesures dites d'effet équivalent. Donc, en principe, une marchandise légalement produite dans un État membre doit pouvoir être produite et commercialisée sur le marché des autres États membres.

Le droit communautaire garantit également la liberté d'établissement, la libre circulation des personnes et des services (articles 52 et 59 du Traité de Rome). Une discrimination contre un prestataire de service qui serait fondée sur sa nationalité ou sur la circonstance qu'il réside dans un État membre autre que celui où la prestation doit être fournie, est interdite.

L'article 36 prévoit qu'il peut être fait exception à ces principes notamment pour des raisons d'ordre public et de sécurité publique.

---

[230] L'exportation est définie par le règlement comme « *le régime permettant la sortie temporaire ou définitive de marchandises communautaires du territoire douanier de la communauté conformément à l'article 161 du Code des douanes communautaires ; ce régime inclut la réexportation, c'est-à-dire l'opération au sens de l'article 182 dudit code consistant en la sortie du territoire douanier de la Communauté de marchandises non communautaires.*»

[231] Voir Communication de la Commission européenne, « Assurer la sécurité et la confiance dans la communication électronique », COM (97) 503.

Cependant, l'article 36 est d'interprétation stricte et la restriction invoquée doit respecter le principe de proportionnalité, c'est-à-dire que la mesure doit être appropriée, efficace, et ne pas aller au-delà de ce qui est strictement nécessaire pour atteindre l'objectif poursuivi.

La France est le seul pays de l'Union européenne à disposer d'une législation restreignant sur son sol le libre usage et la fourniture de la cryptographie. Cela engendre une impossibilité de fait, pour un ressortissant communautaire voyageant en France, d'utiliser des produits de chiffrement supérieur à 128 bits, autorisés dans son pays (il devrait déposer un dossier déclaration). Or, les moyens techniques devraient être en mesure de circuler avec les informations personnelles qu'ils protègent.

De plus, les organismes agréés doivent exercer leurs activités sur le territoire français, ce qui est un obstacle à la libre prestation de services et un obstacle à la libre circulation des marchandises.

En effet, un produit librement commercialisé dans un autre pays de l'Union est soumis à autorisation pour pouvoir être fourni en France. Donc, il y a entrave aux échanges de produits légalement fabriqués et commercialisés dans d'autres pays de l'Union européenne.

La Directive européenne sur les traitements de données à caractère personnel[232] requiert que les États membres protègent les droits et les libertés des personnes physiques à l'égard du traitement des données à caractère personnel, et notamment le droit au respect de leur vie privée, afin d'assurer la libre circulation des ces données dans la Communauté.

L'article 17 de cette directive indique que le responsable d'un traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction, la perte, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau. L'article précise que :

[232] Directive n°95/46 du 24 octobre 1995, JOCE 23/11/95 L 281/30.

« Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.»

Les régimes établis pour l'utilisation et la fourniture des moyens et de prestations de cryptographie pourraient affecter l'application de la directive, dans la mesure ou selon la Commission :

« les moyens appropriés nécessaires pour sécuriser les données personnelles ne seraient pas disponibles en France et/ou ne pourraient pas "voyager" avec les données qu'elles sécurisent provenant d'autres États membres. »

De même, les régimes d'autorisation et d'intervention de tiers de confiance risquent d'entraver l'utilisation et la libre circulation des moyens de chiffrement appropriés.

B- Les enjeux de la cryptographie en question ?

Le commerce électronique se caractérise par l'abolition des distances géographiques. C'est d'ailleurs cette même distance qui entraîne une perte de confiance entre les différents protagonistes de ces échanges. Il existe un impératif, qui est de connaître l'identification des individus ou organisations avec qui nous contractons.

L'essor du commerce électronique repose sur la confiance que les utilisateurs accorderont au système. En terme de sécurité, des incertitudes demeurent. Il faut en effet pouvoir transmettre des informations dans des conditions techniques qui garantissent l'identité et le consentement de l'émetteur, la teneur des messages et leurs réceptions. Or, par nature, la sécurité constitue le point faible des réseaux ouverts.

Il est possible d'imaginer qu'un cocontractant refuse d'honorer ses engagements, voire même qu'une personne mal intentionnée intercepte le message, ce qui lui donnerait accès à des informations relevant du secret des affaires ou de la vie privée. Cette personne aurait même la possibilité de modifier ces informations.

De même, il faut pouvoir s'assurer que l'information concernant l'identification tirée des transactions réalisées, ne soit pas ambiguë, erronée ou incorrecte. Cela pourrait également amener la connaissance d'un « identifiant » par un tiers, comme par exemple, un numéro de carte de crédit. Une méthode d'identification qui suscite un bon degré de confiance est donc essentielle[233]. Aussi, comment se prémunir contre de tels risques ?

Cette question de la sécurité transactionnelle et de l'identification individuelle peut être un frein au commerce électronique. Dans le cadre de transactions, les usagers sont appelés à fournir des renseignements personnels comme le numéro de carte de crédit ou leur identification. Ici, la question posée est de savoir par quels mécanismes il est possible de garantir que les renseignements personnels ne seront pas interceptés ?

La confidentialité des échanges ne concerne pas uniquement des intérêts individuels. Un des intérêts à protéger, de manière générale, est tout ce qui relève du secret commercial. Il est aisé de comprendre que parmi les messages échangés, certains peuvent avoir une importance capitale pour les entreprises de telle sorte que leurs détournements, ou pis encore leurs diffusions, pourraient avoir des conséquences extrêmement fâcheuses. Sur ce point, le fait que l'échange de données se fasse de manière électronique ne change pas les principes mêmes de la protection de ce type de secret. Le problème tient de la vulnérabilité des transmissions par voie de télécommunications, qui sont une proie facile pour l'espionnage. Il en résulte un besoin de recourir à des règles de protection pour assurer la confidentialité des échanges.

Ainsi, quatres catégories de risques peuvent être liées à l'échange de documents et à la signature:

- La première catégorie est **la non-identification de l'expéditeur**. L'usurpation d'identité, représente un risque important dans toutes transactions. Elle résulte de l'appropriation non

[233] R. CLARKE et autres, « The Scope for Transaction Annymity and Pseudnymity », présenté dans le cadre du *Fifth Conference on Computers, Freedom, and Privacy, Conférence* organisée par le Board of Trustees de l'Université Leland Stanford, juin-juillet 1994, p.108 ; http://www-techlaw.stanford.edu/CFP95.Program.html.

autorisée d'un identifiant ou de simulation d'un identifiant appartenant à autrui. Ce type de risque est proportionnel à l'accessibilité du réseau[234].

Les conséquences de cette usurpation doivent être considérées comme non négligeables. Ainsi, en absence d'une identification formelle :

> *« un concurrent pourrait utiliser l'EDI pour obtenir, par exemple, une liste de prix ou d'informations confidentielles concernant les plans de productions. Une banque pourrait agir sur la base d'instruction qui semblent provenir d'un client, mais qui, en réalité, sont émises par un pirate.»*[235]

- La catégorie suivante est **l'altération des données**. L'intégrité des données représente l'une de préoccupations principales quant à la sécurité de l'information. Les données d'un message peuvent être modifiées, supprimées ou insérées, lors de transmission, de façon accidentelle ou du fait de la malveillance de personnes non habilitées.

Les conséquences découlant de l'altération des données qui composent un message peuvent être importantes, particulièrement lorsque le message comporte une autorisation ou est accompagné d'une signature. Dans le cas de la signature, toute modification non autorisée du contenu du message qui survient après la signature aurait pour effet de vicié l'objet du contrat.

- Ensuite, il existe le risque de **divulgation non autorisée des données**. La confidentialité peut s'avérer très importante lors de transit de données à caractère personnel ou comportant une valeur économique. Pour être efficace, la confidentialité de données doit être préservée à toutes les étapes. C'est à dire tant à la transmission, qu'à la réception. De plus, pour éviter tous risques d'observation pendant le flux des données, la confidentialité de toute la transmission doit être également effectuée. Ainsi :

---

[234] PARISIEN, Serge et Pierre TRUDEL, « l'identification et la certification dans le commerce électronique », *Rapport final,* Montréal, Centre de recherche en droit public, avril 1996, p.84

[235] Commission des communautés européennes, « EDI et sécurité : Comment gérer le problème ?» , *rapport préparé par KPMG dans le cadre du programme TEDIS,* 1992, p.10.

« le niveau d'activité économique d'une entreprise peut être déterminé en comptant le nombre de messages envoyés et reçus, même si la teneur des messages reste secrète. »[236]

Les atteintes à la confidentialité peuvent découler du dysfonctionnement du réseau de communication (entraînant l'acheminement erroné des données) ou d'actes de piratage.

- Enfin, la dernière catégorie de risque est **la répudiation**. Elle désigne la situation dans laquelle un émetteur nie, en tout ou partie, l'émission d'un message. La répudiation peut être la conséquence d'une erreur, d'un acte de piratage ou d'un refus de l'expéditeur d'endosser la paternité et la responsabilité d'un message. Cette répudiation peut être aussi le fait du destinataire. En effet, ce dernier peut nier la réception d'un message ou son contenu. Les conséquences de la répudiation ne sont pas négligeable. Ainsi, une entreprise qui réalise un produit sur demande devra, suite à la répudiation du message de commande, supporter les coûts de fabrication du produit tout en étant privée des revenus tirés de sa vente.

Ainsi, utiliser des réseaux ouverts suppose que l'on mesure les risques de façon à pouvoir y apporter une double sécurité technique et juridique[237]. Sous cet angle, il est classique d'associer les outils cryptographiques à la sécurité. L'utilisation de la cryptographie permet d'assurer des fonctions juridiques fondamentales :

- d'authentification, c'est à dire l'identification d'une tiers personne (en principe, le terme « authentification » employé par le législateur peut surprendre certains juristes. Il est classique de définir l'authentification, en droit civil, comme étant une opération réalisée par un officier public à des fins probatoires et qui consiste à conférer l'authenticité à un acte[238])
- d'intégrité

[236] Commission des communautés européennes, « EDI et sécurité : Comment gérer le problème ? » , *rapport préparé par KPMG dans le cadre du programme TEDIS*, 1992, p.11.

[237] V. I. De LAMBERTERIE, « la valeur probatoire des documents informatiques dans les pays de la CEE » : *RID comp*. 1992, n°3, spéc. P.64 et E-A. CAPRIOLI, « contribution à la définition d'un régime juridique de la conservation des documents : du papier au mesurage électronique » : *Dr. Informatique et Télécoms* 1993/3, p.5s.

[238] G.CORNU (SS dir. De), *Vocabulaire juridique*, Paris, *PUF*, 1987, V° authenticité et authentification. Une autre acceptation existe, mais elle a pour vacation de vérifier l'authenticité.

- de non-répudiation
- de confidentialité

En principe, ce sont des tiers prestataires de services (à valeur ajoutée), dits « autorité de certification », qui rempliront ces fonctions[239].

Par ailleurs, la confidentialité des données nominatives impose des obligations issues principalement de la Loi relative à l'informatique, aux fichiers et aux libertés[240] et de la directive européenne 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[241]. Mais, même si la directive a vocation à s'appliquer de façon plus étendue au niveau international (elle concerne tous les États membres de l'Europe à la différence de la loi française qui ne concerne que l'État français), le territoire d'application de ces deux textes est relativement restreint dans une optique de commerce à l'échelon mondial. Aussi, une garantie des individus dans le cadre de relations commerciales est nécessaire.

Dans cette optique, la France, dans un *Memorandum* présenté aux États membres de l'Union européenne, a dégagé un certain nombre d'orientation afin établir la confiance dans les instruments et les réseaux de commerce électronique[242].

En effet, les technologies sûres, telles que les signatures numériques et les moyens de paiement électronique protégés sont disponibles, pour la plupart, et de plus en plus utilisés commercialement. Cependant, le cadre indispensable à l'usage de ces technologies reste imprécis. Donc il est nécessaire d'adapter les règles commerciales à la réalité du commerce électronique.

---

[239] Voir *supra.*

[240] Loi n°78-17 du 6 janvier 1978, JO du 7 janvier 1978

[241] Directive 95/46/CE du parlement et du conseil, JOCE n°L281/31, 23 novembre 1995.

[242] *Memorandum* présenté par la France aux États-membres de l'Union européenne lors des Conseils du 26 février 1998 (Télécommunications) et du 9 mars (Ecofin), *Créer un environnement communautaire et international pour développer le commerce électronique.*

En effet, en ce qui concerne la protection des données personnelles et de la vie privée, des différences significatives en matière de protection des données entre les États pourraient entraver les échanges électroniques.

De plus, l'Union européenne a adopté une directive sur la protection des personnes physiques à l’égard du traitement des données à caractère personnel et de la libre circulation des données. Cette directive, dont la transposition dans le droit des États membres aurait du être achevée en octobre 1998, réglemente notamment les transferts de données à destination des États tiers. Donc, la prise en compte des effets de cette directive sur les échanges électroniques avec les États qui ne disposent pas de protection des personnes physiques aussi élaborée, doit être examinée à la lumière des développements récents du commerce électronique.

Ensuite, pour la France, afin d’encourager les possibilités de personnalisation de l'offre que permet le commerce électronique, il convient de favoriser les systèmes technologiques permettant de dissocier l'établissement du profil des consommateurs de, leur identification, qui elle, doit demeurer protégée.

Enfin, la sécurité des transactions devrait faire l'objet d'effort concerté au niveau communautaire afin d'aboutir à un compromis entre les besoins de protection demandés par les acteurs économiques et les nécessités de la sécurité publique. Cet effort est nécessaire pour fluidifier les échanges électroniques mondiaux. Un effort de concertation et d'échanges doit être mené au sein de l’Union européenne afin de permettre un minimum d'interopérabilité et de confiance mutuelle, dans une optique de respect des réglementations nationales.

Mais, une fois la confiance suscité au sein des utilisateurs du commerce électronique, un cadre juridique de la preuve doit être développé afin qu'il puisse s'adapter aux échanges électroniques.

II La preuve confrontée à une informatique installée

Force est de constater que nous sommes entré dans une société de l'information ou, plutôt, que cette situation s'est accélérée depuis le début des années 1990. Devant cet état de fait, les échanges de documents électroniques se sont accélérés et sont devenu le quotidien de nombreux services. La raison en est bien simple, l'EDI (l'échange de données ou d'information) est pratique, il allie souplesse et rapidité. Les applications sont ici nombreuses et, pour certaines, elles facilitent considérablement le travail de nombreux secteurs d'activité.

Cela étant, en matière contractuelle comme en matière factuelle, le document écrit, sur lequel est apposé une signature manuscrite possède une valeur de preuve qui demeure lorsque le document est sous forme numérique dans les échanges de type commerciaux (*supra*). La validité d'une inscription informatisée pour prouver un acte ou un fait juridique pose des problèmes. Pour cela, il est nécessaire de développer un système de preuve électronique (A) afin de susciter la confiance des utilisateurs (B).

A- La nécessité d'une preuve électronique

Les différentes initiatives en cours dans les États membres conduisent à une situation juridique très hétérogène. Bien que les États membres semblent se concentrer sur les mêmes questions (notamment les exigences imposées aux prestataires de services et aux produits, les critères qui détermineront l'effet juridique des signatures électroniques, et la structure des régimes d'accréditation), il est évident que la diversité des réglementations respectives ou leur inexistence sera telle, que le fonctionnement du marché intérieur dans le domaine des signatures électroniques s'en trouvera menacé.

Toute divergence dans les règles définissant l'effet juridique attribué aux signatures numériques est particulièrement préjudiciable au développement futur du commerce électronique.

Des incertitudes peuvent également résulter des régimes différents en matière de responsabilité et du risque d'incohérences de la jurisprudence en cette matière. De plus, il est probable que les critères techniques en fonction desquels les signatures électroniques seront considérées comme sûres varieront d'un État membre à l'autre.

Donc, l'hétérogénéité de la situation, en entravant l'utilisation et la fourniture de services liés aux signatures électroniques et en freinant le développement de nouvelles activités économiques en rapport avec le commerce électronique, risque de constituer un sérieux obstacle à la communication et aux affaires par réseaux ouverts dans l'Union européenne.
Aussi, un besoin d'harmonisation se fait ressentir au niveau européen. En effet, plusieurs États membres ont déjà pris des initiatives législatives détaillées en ce qui concerne les signatures électroniques[243].

Dans sa communication du 16 avril intitulée : «une initiative européenne dans le domaine du commerce électronique»[244] et adressée au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, la Commission reconnaissait que les signatures numériques constituaient un moyen essentiel d'assurer la sécurité et de développer la confiance sur les réseaux ouverts. Dans la *Déclaration ministérielle de Bonn*[245], les signatures numériques apparaissaient également comme une question prioritaire pour le commerce électronique.

Dans un premier temps, la Commission a présenté au Parlement européen, ainsi qu'au Conseil, au Comité économique et social et au Comité des régions, une communication intitulée «assurer la sécurité et la confiance dans la communication électronique : vers un cadre européen pour les signatures numériques et le chiffrement»[246]. Dans cette communication, elle soulignait la nécessité d'une approche cohérente dans le domaine de la signature numérique.

Ainsi, une proposition de directive instituant un cadre juridique pour l'utilisation des signatures électroniques a été présentée par la Commission européenne[247]. L'objectif de la proposition de directive vise à «permettre» l'usage des signatures électroniques dans un espace sans frontières

[243] Voir annexe n°4

[244] COM(97) 157 final du 16.4.1997.

[245] Conférence ministérielle européenne, *Global information networks : realising the potential*, Bonn 6-8.7.1997.

[246] COM(97) 503 final du 8.10.1997.

[247] Proposition de directive du parlement européen et du conseil « sur un cadre commun pour les signatures électronique », présentée par la Commission, Bruxelles, le 13.05.1998 COM(1998) 297 final, 98/0191 (COD).

en se concentrant sur les obligations essentielles pour les services de certification, et laisse les détails de la mise en œuvre à la discrétion des États membres.

En instituant des règles minimales en matière de sécurité et de responsabilité, cette proposition garantira la reconnaissance juridique des signatures électroniques dans toute l'Union européenne sur la base des principes de libre circulation des services et du contrôle par le pays d'origine régissant le marché unique. Elle créera un cadre pour des transactions en ligne sûres dans tout le marché unique et ainsi favorisera l'investissement dans les services de commerce électronique. Pour M. Bangemann :

> « *la sécurité des transactions est capitale si l'on veut que ce potentiel* (du commerce électronique) *puisse être exploité en Europe. Une fois adoptée, cette directive supprimera l'un des principaux obstacles qui continuent d'entraver un développement à grande échelle du commerce électronique*.»

Cette proposition arrive avant que les États membres mettent en place un cadre législatif régissant les signatures électroniques. Elle garantira donc, dès le début, un cadre juridique harmonieux pour le marché unique et évitera de devoir lutter contre des initiatives nationales n'allant pas forcément dans le même sens.

Cette proposition définie des exigences essentielles pour les certificats attestant la signature numérique et les services de certification, afin de garantir un niveau minimal de sécurité et permettre la libre circulation des certificats et des services dans le marché unique. Ces exigences porte notamment sur la fiabilité des prestataires et sur l'utilisation de systèmes dignes de confiance.

De plus, cette proposition fixe des règles minimales en matière de responsabilité des prestataires de services notamment en ce qui concerne la validité du contenu du certificat. Cette approche permettra de gagner la confiance des consommateurs, et encouragera les opérateurs à concevoir des systèmes et des signatures sûrs.

Aucune discrimination juridique ne devra s'exercer à l'encontre d'une signature électronique pour la seule raison qu'elle se présente sous une forme électronique, car il est

essentiel pour la mise en place d'un système ouvert et fiable de signatures électroniques que ces signatures aient des effets juridiques. Les signatures électroniques, doivent être considérées comme l'égale des signatures manuscrites. Ainsi, elles pourront être acceptées comme preuve dans une procédure judiciaire. Étant donné le rythme de l'innovation technologique, la reconnaissance juridique des signatures électroniques existera indépendamment de la technologie utilisée (par exemple les signatures numériques reposant sur la cryptographie asymétrique).

Mais cette proposition concerne uniquement la fourniture au public de certificats visant à identifier l'expéditeur d'un message électronique. En effet, elle n'a pas à s'appliquer aux groupes fermés d'utilisateurs, tels que les intranets ou les systèmes bancaires, dans lesquels une relation de confiance existe déjà. Par conséquent, il n'existe pas de besoin manifeste de réglementation dans ce domaine.

La proposition obligera donc les États membres à revoir leurs législations nationales pour en éliminer toute interdiction ou restriction pesant sur l'utilisation de moyens électroniques pour la conclusion de contrats. En effet, toute directive communautaire entraîne une obligation de mise en conformité du droit interne avec les dispositions européennes. Ce texte n'est pour l'instant qu'une proposition et le Parlement européen ou le Conseil peuvent toujours l'amender. Mais après son vote, la mise en conformité des législations nationales devra intervenir. Cette directive devrait occasionner, en France, des travaux législatifs en matière de signature.

La signature numérique, s'inscrit dans le cadre plus général de la signature électronique. Cette dernière comprend plusieurs technologies qui permettent de réaliser, dans un environnement électronique, les fonctions de la signature manuscrite (l'identification du signataire de l'acte ou du document et l'expression de la volonté d'adhérer au contenu de l'acte). Dans cette perspective d'approche fonctionnelle et de convention de preuve, l'article 7 de la loi-type de la commission des Nations Unies pour le droit commercial international (CNUDCI) sur le commerce électronique peut être une orientation :

> *« Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données :*

a) *Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données ;*

b) *Si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière (…). »*[248]

Ainsi, l'État français dispose déjà d'un texte qui suit l'approche de l'équivalence fonctionnelle de la signature[249], tout en étant acceptable par notre système juridique. Donc, pour la sécurité juridique des transactions et autres enregistrements électroniques, il semble important de modifier le Code civil français en introduisant expressément les notions de preuve informatique et de signature numérique[250]. Dans cette optique, l'exemple québécois ne semble pas dénué d'intérêt.

Le Code civil du Québec prévoit des dispositions générales sur la preuve électronique, et en plus, il introduit une définition de la signature qui « élargit ainsi les formes extérieures de la signature au- delà de la simple transcription du nom. »[251]

Le Code civil du Québec aborde en effet la notion de signature de façon originale. La jurisprudence et la doctrine ont traditionnellement adopté, vis-à-vis de cette notion, une approche dogmatique hostile à l'idée que de nouvelles formes de signature puissent constituer une alternative valable à la signature manuscrite[252].

---

[248] Rapp. Comm. Nations Unies pour le droit commercial international sur les travaux de sa 21ème session, 28 mai - 14 juin 1996, Assemblée générale, Documentation officiels, 51ème session, suppl. n°17 (A/51/17), V. p.77.

[249] L'équivalence avec l'écrit a déjà été consacrée par plusieurs textes législatifs français. Par exemple, l'article 47 de la loi de finance rectificative pour 1990 en matière de déductibilité de la TVA lorsqu'une facture numérisée est émise, « tenant lieu de facture d'origine »

[250] Groupe de travail « l'écrit et les nouveaux moyens technologique au regard du droit » de la mission de recherche droit et justice, V. l'interview du Pr A. LUCAS in *Expertises* 1997, p.222.

[251] Art 2827 C.c.Q ; Pierre TRUDEL, Guy LEFEBVRE et Serge PARISIEN, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Publication du Québec, 1993, p.65. cité dans Trudel, Pierre et autres, *Droit du cyberespace*, Montréal, *Éditions Thémis*, 1997.

[252] Dirk SYX, « Vers de nouvelles formes de signatures ? Le problème de la signature dans les rapports juridiques électroniques », *droit de l'informatique,* 133, 1986.

Les codificateurs québécois se sont tournés vers une approche plus pratique en élargissant la notion de signature au-delà de la simple transcription d'une marque personnelle utilisée de façon courante par une personne pour manifester son consentement :

> *« La signature consiste dans l'apposition qu'une personne fait sur un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement. »*[253]

Du fait de cette formulation large, rien ne s'oppose à l'utilisation de signatures électroniques. Il apparaît légitime de soutenir qu'une signature électronique constitue bel et bien une marque dont le caractère personnel se trouve par ailleurs assuré par le haut niveau de confidentialité qui entoure généralement les mécanismes de signature électronique. Par ailleurs, l'utilisation du terme « marque » apparaît significative. Rien ne suppose en effet qu'une marque soit numérique. Il apparaît évident que celle-ci ne peut exister que sous forme électronique dans le cadre d'un environnement informatisé.

La recevabilité de la signature électronique par le législateur québécois semble confirmée par le fait que le Code civil québécois reconnaît la validité du document informatisé comme moyen de preuve. De plus, lors de la réforme du Code civil du Québec, les codificateurs ont, estimés qu'il n'était pas nécessaire de définir la notion de signature sauf à l'élargir. En effet, l'absence de cette définition dans le Code civil du Bas-Canada, n'a donné lieu, après environ 125 ans d'expérience, à aucun contentieux. Donc, si le but est d'enfermer la notion de signature dans une signature manuscrite, il n'est pas nécessaire de la définir.

C'est en n'excluant pas les nouvelles formes de signature que le Code civil du Québec admet la signature électronique[254]. Tous les mécanismes de signature qui remplissent les deux fonctions de base de la signature (identification et manifestation de la volonté du signataire d'adhérer au contenu de l'acte ou du message signé) sont admis.

---

[253] Art 2827 C.c.Q

[254] La signature électronique est régie par l'article 1827 du C. c Q. portant sur la signature. Donc, la preuve de son authenticité doit se faire selon les règles générales de la preuve. Le fardeau de la preuve incombe à celui qui invoque l'acte signé (2829 C. c. Q).

L'exemple québécois semble une alternative qui peut être suivie par le législateur français. Mais la reconnaissance juridique de la signature numérique ne suffira pas, à elle seule, à susciter la confiance des utilisateurs.

B- Susciter la confiance des utilisateurs

La signature numérique ne suffit pas en tant que telle à certifier quelle personne se situe derrière cette signature. Pour cela, il est nécessaire de passer par un tiers. Ces tiers sont des autorités de certifications qui assurent plusieurs fonctions, dont une essentielle : formaliser le lien qui existe entre une personne physique ou morale et une paire de clés asymétriques. Une autorité de certification est donc :

> *« une autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat »*[255]

Certains ont rapproché les tiers certificateurs des notaires en les appelant les «cybernotaire». Mais, ces tiers se distinguent des notaires dans la mesure où ils n'ont pas pour mission d'établir, de dater et de conserver des actes juridiques conformément aux prescriptions légales[256].

Les autorités de certification doivent non seulement apporter aux utilisateurs toutes les garanties d'intégrités et de sécurité, mais aussi que ces qualités leurs soient reconnues. Il semble donc indispensable d'assurer une protection des utilisateurs. Or, la multiplication des tiers et une concurrence anarchique risquent de nuire au suivi de spécifications minimales communes, spécialement en matière d'intéropérabilité des autorisations et d'usage de profils de sécurité[257]. Il est impossible de douter que le niveau de confiance dépendra du niveau de sécurité.

---

[255] Recommandation n°509 de l'IUT-T, Annuaire, Cadre d'authentification, Fasc. VIII. 8, 1988, art. 10.1.1

[256] V. A. GOBIN, « pour une problématique notariale des autoroutes de l'information » : *JCP N* 1995, n° 50-51, p. 1749s.

[257] Cosiform, *Recommandation relative à l'utilisation de profils de protection dans les échanges informatisés entre l'administration et ses partenaires et usagers*, n°R 96.02, 19 juin 1996, http://www.cerf.gouv.fr

La fonction de l'autorité de certification qui consiste à remettre les certificats est fondamentale. Ce certificat est un message électronique délivré par un tiers de confiance qui a pour fonction d'établir un lien entre une personne physique ou morale dûment identifiée et une paire de clés (privée et publique). Il permet donc l'identification du titulaire de la clé privée correspondant à la clé publique mentionnée dans le certificat pour la signature.

En principe, le certificat contient une série d'informations relatives à l'utilisateur (nom, adresse,…), au nom du tiers certificateur, à la clé publique de l'utilisateur, au numéro de série, à ses dates de délivrance et d'expiration. Il est entendu que les données nominatives doivent être soumises aux prescriptions légales. De plus, les autorités certificatrices authentifient elles-mêmes les certificats en y apposant leur signature numérique.

Avec ce certificat, un destinataire qui se fie à une signature numérique créée par la personne nommée dans ledit certificat, peut utiliser la clé publique mentionnée dans celui-ci afin de vérifier que la signature numérique a bien été créée avec la clé privée correspondante. Si cette vérification est positive, le destinataire a la certitude que la signature numérique émane véritablement du titulaire de cette clé publique. De plus, il a la garantie que le message n'a pas été modifié depuis la création de la signature (grâce à la fonction de hachage).

Les autres activités de l'autorité de certification sont : les fonctions relatives à l'archivage, les informations relatives à la signature numérique, la création de clés asymétriques indispensables pour la signature, l'horodation des signatures, la vérification des signatures numériques et se prononcer sur leurs validités, l'intégrité et la non-répudiation du message par le biais de la «fonction contrôle ou hachage».

Pour remplir toutes ces fonctions, le système d'information utilisé par l'autorité de certification doit être fiable, c'est à dire que le matériel, les logiciels et les procédures doivent répondre à des critères stricts :

- Une sécurité suffisante contre toutes intrusions et mauvaises utilisations.
- Un niveau raisonnable de disponibilité, d'intégrité et de services.

- Être suivis pour exécuter les fonctions prévues.
- Adhérer à des principes de sécurité généralement accepter[258].

Ainsi, un système fiable poursuit des objectifs de confidentialité, d'intégrité, de disponibilité et d'utilisation légitime.

Le système de la signature numérique est basé sur la confiance envers les autorités certificatrices. Donc, en contrepartie, il doit exister des garanties juridiques pour les cas où les autorités certificatrices manqueraient à leurs obligations.

Les utilisateurs doivent pouvoir compter sur les compétences techniques de celui qui émet les clés et/ou les certificats. À cette fin, il convient d'examiner attentivement les contours des engagements souscrits par le tiers, notamment en ce qui concerne son obligation de sécurité du système mis en place et les certificats qu'il émet. Cela est particulièrement sensible lorsque la confidentialité des clés de certification est compromise ou bien lorsque le certificat est partiellement ou totalement erroné. La mise en jeu de la responsabilité aura également trait à la gestion des certificats émis, spécialement quand ils font l'objet de suspensions ou d'annulations (ou révocations).

Il faudra veiller à ce que le tiers soit responsable en cas de dommage découlant d'un manquement quelconque à ces obligations. Il peut même être envisager la constitution d'un fond de garantie collectif.

La responsabilité du tiers découle pour partie du contenu du certificat. Quant elles existent les procédures d'agrément ainsi que le cahier des charges à respecter constituent des instruments intéressant pour éviter tout débordement.

En ce qui concerne les infrastructures de certification et leurs contrôles, plusieurs options sont possibles. Ce peut être une implication forte de l'État (autorisation délivrée par l'État) ou une absence de ce dernier (le marché de la certification s'autorégule)[259]. Ainsi, la mise en œuvre

[258] Point 4 du guide de l'ABA
[259] PARISIEN, Serge, Pierre TRUDEL, Véronique WATTIEZ-LAROSE (Centre de Recherche en Droit Public de l'Université de Montréal), « Options relatives aux pratiques communes de certification au Québec », étude menée

juridique des tiers peut s'effectuer soit par voie législative ou réglementaire, soit par voie contractuelle. Pour la phase de développement du marché, un système de contrôle minimum émanant des pouvoirs publics semble plus adapté. En effet, ce système semble plus à même d'assurer la création et le respect des pratiques de certification. En définitif, la confiance des utilisateurs dépendra du niveau de fiabilité requis.

Le développement du commerce électronique passe par la confiance des utilisateurs potentiels. Cette confiance ne peut s'acquérir, uniquement si les utilisateurs se sentent en sécurité lors de l'utilisation de réseau ouvert pour leurs opérations d'achat-vente. Or, cette sécurité qui est réclamée passe aujourd'hui par l'utilisation de moyens de cryptographie.

Section III : Une liberté totale de la cryptographie : une solution adaptée au commerce électronique.

Le commerce électronique est devenu une réalité sur l'internet, les butineurs les plus populaires (Netscape et Internet explorer) intègrent d'ailleurs l'algorithme breveté[260] de RSA Data Security Inc. Pour information, ces butineurs sont donnés sous une version 40 bits et seuls les utilisateurs résidents des États-Unis ou du Canada peuvent utiliser la version 128 bits (après un questionnaire, et une vérification de la localisation du fournisseur d'accès du demandeur – l'adresse IP donnant ces informations- et, enfin télédéchargement du complément). Il y a alors un décalage dans le commerce électronique via l'internet : les européens n'ont pas accès à la même sécurité dans les transactions que les Nord américains du fait des restrictions apportés à l'exportation des outils cryptographiques dans ces pays (et à leur importation en France). Cela dit, nous sommes dans une hypothèse où ces moyens cryptographiques sont libres et puissant, au train où vont les choses, cette hypothèse reste hautement probable.

---

pour le compte du secrétariat du conseil du trésor du Québec, juin 1997, cité dans : Pierre Trudel : Trudel, Pierre et autres, *Droit du cyberespace*, Montréal, *Éditions Thémis*, 1997.

[260] On peut d'ailleurs s'interroger sur la brevetabilité d'un tel algorithme… Lamy Droit de l'informatique, op. cit. 104, arrêt Schlumberger canadien et français

I La liberté du commerce et de l'industrie reconquise.

La transmission de données sous forme numérique a de nombreux avantages comparée aux méthodes traditionnelles. Les documents peuvent être disponibles pratiquement instantanément, en n'importe quelle quantité, et constituent une matière sur laquelle le destinataire peut travailler directement. L'envoi est considérablement moins cher et plus rapide. Les documents peuvent être transmis en tout point du globe, en quelques secondes, sans délai. Toutefois, les services d'authentification et d'intégrité sont nécessaires à la sécurité et à la confiance dans la transmission de données sur les réseaux ouverts.

La vitesse du progrès technologique implique que beaucoup de nouveaux domaines d'application pour les services d'authentification et d'intégrité sont difficiles à déterminer. Ces nouveaux domaines d'application (par exemple: la protection des droits de propriété intellectuelle, les données stockées, la sécurité des réseaux ou la monnaie électronique) sont en développement continus. Les signatures numériques sont considérées comme jouant un rôle important, en particulier pour la communication électronique. Mais les cantonner uniquement au commerce électronique serait avoir une vision réductrice de leurs applications (B). Malheureusement, ces moyens de signature ne sont pas toujours disponible (A).

A- Les moyens de signature et la problématique de leurs diffusions.

Il existe différentes méthodes pour signer un document électroniquement. Les signatures numériques peuvent varier d'une méthode très simple (par exemple, l'insertion d'une image numérisée d'une signature faite à la main dans un document réalisé par traitement de texte), à des méthodes très avancées (par exemple la cryptographie). Les signatures numériques basées sur la « cryptographie à clé publique » sont appelées signatures numériques. Elles sont considérées comme cruciales pour diverses applications.

Techniquement, les signatures numériques sont créées et vérifiées par des techniques cryptographiques similaires à celles utilisées pour le chiffrement. Deux clés complémentaires sont générées et assignées à un utilisateur. L'une d'elles, la clé de signature, reste privée (« *clé privé »*), alors que l'autre, la clé de vérification de signature, est rendue publique Il est évidemment essentiel que la clé privée ne puisse être calculée à partir de la clé publique.

Différents mécanismes permettent l'identification des intervenants dans un environnement dématérialisé.

- La première technique est la signature fondée sur la cryptographie asymétrique (RSA). Cette cryptographie dite « à clé publique » ou encore « signature numérique » est couramment utilisée dans le cadre du commerce électronique. Elle présente, outre l'identification des parties, l'avantage d'assurer l'intégrité du message. Elle permet également au titre de la confidentialité, de garantir que seul le système informatique du destinataire est en mesure de lire le message transmis. Il s'agit d'avantages indéniables (inexistant dans un environnement papier), qui permettent de répondre aux plus hautes exigences en matière de sécurité.

Dans un système à clé publique, la réalisation des différentes fonctions d'identification suppose qu'une personne dispose de deux clés mathématiques complémentaires : une clé privée, dont le caractère secret est préservé, et une clé publique, qui peut être librement distribuée.

La clé privée permet de signer le message. L'opération de décodage s'effectue, quant à elle, selon le principe de la complémentarité des clés : un message encodé avec une clé privé ne peut être décodé qu'avec sa clé publique complémentaire.

Nous l'avons vu dans l'introduction, la principale application de signature à clé publique (numérique) est celle proposée par la firme *RSA*. Sa fiabilité et son haut degré de sécurité en font un standard en matière de commerce électronique[261]. Cette technologie, fait partie intégrante de différents standards officiels dans le monde. Par exemple, il figure dans la norme 9796 de l'ISO à titre d'algorithme compatible.

La technologie RSA est brevetée depuis 1983 par la firme « *Public Key Partners » (PKP)* de *Sunnyvale* en Californie[262]. Ce brevet expirera en l'an 2000. L'obtention d'une licence est

[261] RSA, *RSA's FAQ About Today's Cryptography*, http://www.rsa.com/rsalabs/faq/faq_rsa.html

[262] *Ibidem.*

donc nécessaire afin d'utiliser ou vendre *RSA*. Néanmoins PKP autorise de manière générale, l'utilisation non commerciale de sa technologie, à des fins personnelles, académiques ou intellectuelles[263]. Le gouvernement américain bénéficie d'un droit d'utilisation illimité et gratuit de RSA puisque la recherche qui a permis cette technologie a été partiellement financée par celui-ci.

- La seconde technique est l'algorithme de signature spécifié dans le « *DSS* qui est le *Digital Signature Algorythm » (DSA).* Il peut être utilisé pour les messageries électroniques, le transfert de fonds électronique, l'EDI (l'Echange de Données Informatisées), l'archivage ou plus généralement pour toute application nécessitant une assurance quant à l'intégrité et à l'origine des données transmises[264]. Cet algorithme est mis gratuitement à la disposition du public.

Le *DSA* utilise une clé privée dans le but de réaliser une signature et une clé publique complémentaire afin de la vérifier. Il est basé sur un cryptosystème proposé par *EL GAMAL*[265]. A la différence de la technologie *RSA*, le *DSA* n'est pas réversible et ne peut être utilisé afin de chiffrer un message. C'est l'une des raisons pour lesquelles le processus de sélection d'un algorithme de signature a été si dur.

Le *DSA* a reçu un accueil mitigé de la part du secteur privé. Beaucoup préfère le standard *RSA*, qui lui est réversible. D'autres critiques ont été adressées au *DSA*, entre autre, une relative à la signature. Bien que la réalisation de la fonction de signature soit plus rapide sous *DSA*, la vérification de la signature s'effectue quant à elle de façon plus rapide sous *RSA*. Il semble que cette dernière caractéristique soit plus recherchée par l'industrie que la capacité à signer un document[266].

---

[263]RSA, *Miscellaneous,* http://www.rsa.com/rsalabs/faq/faq_misc.html#misc.10

[264] United States Of Technology Assessment (OTA), *Information Security and Privacy in Network Environments,* Annexe C : *Evolution of digital signature standard, 15 septembre 1994,* http://otabbs.ota.gov/E511T93

[265] US Patent 5,231, 668. Voir T. EL GAMAL, «« A public-key cryptosystem and a signature scheme based on discrete logartithms », *IEEE transactions on Information Theory*, vol IT-31, 1985, p.469-472. Cité dans : E-A. Caprioli, « Commerce électronique : Sécurité et confiance dans le commerce électronique - Signature et autorité de certification », JCPG, 1 avril 1998, n°14, I, 123, p.583 s.

[266] RSA, *Capstone, Clipper and DSS,* http://www.rsa.com/asalabs/faq/faq_ccd.html#ccd.3.

Mais la critique la plus sérieuse à l'encontre du *DSA*, a trait à la sécurité. Le DSS autorise l'utilisation de clés algorithmiques pouvant aller jusqu'à 1024 bits[267]. Selon l'avis d'experts en cryptographie, la création du *DSA* demeure trop récente et n'a pas fait l'objet d'un nombre suffisant d'études pour que les utilisateurs puissent s'y fier[268]. En règle générale, un cryptosystème doit être disponible sur le marché durant plusieurs années avant que les inévitables erreurs de conception puissent être identifiées et adéquatement corrigées. Dans ce sens et comme pour le DES, des chercheurs ont mis en garde les utilisateurs du *DSA* contre l'existence de « portes cachées » permettant de percer les défenses de ce dernier plus aisément[269].

Contrairement à la cryptographie utilisée à des fins de confidentialité, les signatures numériques sont annexées aux données et laissent le contenu (par exemple du document signé électroniquement ou de la transaction électronique) intact. Evidemment, le message peut en plus être chiffré. C'est cette double capacité qui crée un obstacle à la diffusion des moyens de cryptographie à des fins de signatures.

À nouveau, une réglementation restrictive concernant la circulation des produits cryptographiques, limite la diffusion des produits de signature numérique[270]. En effet, la conception par des industriels de ces systèmes de signature électronique, n'est faite que dans un but lucratif. Or, les restrictions posées par l'Arrangement de Wassenaar et le règlement communautaire du 19 décembre 1994[271], limitent les possibilités de diffusion des outils cryptographiques et portent un frein au commerce de ces produits. Donc, il existe un réel risque de ralentir leurs diffusions et par conséquent leurs utilisations. De plus, la perspective d'un

---

[267] United States Office Of Technology Assesment (OTA), « Information Security and Privacy in Network Environments », Annexe C : *Evolution of Digital Signature*, 15 septembre 1994, http://otabbs.oat.gov/E511T93

[268] M.E SMID et D.K BRANSTAD, « Respons to comments on the NIST proposed Digital Signature Standard », *Advances Cryotlogy* - Crypto'92, Network, Springer_Verlag, 1993, cité dans E-A. Caprioli, « Commerce électronique : Sécurité et confiance dans le commerce électronique - Signature et autorité de certification », JCPG, 1 avril 1998, n°14, I, 123, p.583 s.

[269] *Ibidem.*

[270] Voir *supra.*

[271] Op. cit.

marché restreint, n'encourage pas les initiatives industrielles permettant de développer de nouveaux systèmes.

Mais, l'utilisation de ces technologies cryptographiques n'est pas cantonnée qu'au commerce électronique.

B- Une solution à d'autres problèmes juridiques

Que l'internet ne soit plus un lieu d'échange d'idées mais devienne de plus en plus une place commerciale n'est plus à démontrer. Mais les systèmes de cryptographie et de signature ne sont pas l'apanage du commerce électronique mais s'adaptent également à la protection des œuvres. De manière plus générale, les systèmes technologiques (tatouage, etc.) permettent de contrôler l'accès et l'utilisation d'informations enfermées dans des banques de données mieux que des coffres-forts.

Le terrain d'entente du cryptage et du droit d'auteur réside dans le monde numérique. Le milieu numérique nivelle tout élément communicable, qu'il soit texte, image ou son. La numérisation contracte le temps et l'espace. L'informatique, l'audiovisuel et les télécommunications se confondent[272]. L'œuvre ne peut échapper à cette dynamique.

La capacité technique permet donc de numériser indifféremment des œuvres de toute nature. Textes, sons, et images protégés sont convertibles en langage binaire. La numérisation conduit le professeur André LUCAS à constater qu'elle aboutit à une dématérialisation qui :

> *« ne peut que brouiller les concepts juridiques sur lesquels s'est édifié le droit de la propriété littéraire et artistique. »*[273]

[272] Il y a donc un mariage entre les différents médiums qui fait place à une véritable « polygamie technique». Il n'existe actuellement qu'un régime de cohabitation qui repose sur la distinction entre régime des télécommunications et celui de la communication audiovisuelle (distinction instaurée par la loi n°90_1170 du 29 décembre 1990, JCP 191, éd. G, III, 64426). Cette cohabitation semble devoir se légaliser dans un avenir proche par l'avènement d'une législation portant déréglementation. Voir F. OLIVIER et E.BARBY, « Des réseaux aux autoroutes de l'information : Révolution technique ? Révolution juridique? 1- de l'utilisation des réseaux », *JCPG 1996*, I, 3926.

[273] A.LUCAS, « Nouvelles technologies et modes de gestion », *L'avenir de la propriété intellectuelle*, IRPI n°11, Le droit des affaires, Propriété intellectuelle, p.26 , cité dans : Romain Leymonerie, « cryptage et droit d'auteur », *Les cahiers de propriété intellectuelle*, janvier 1998, volume 10 n°2, p.417 à 460, édition Yvon Blais inc., Canada

Le droit d'auteur c'est bâti sur un monde analogique et le phénomène numérique a une influence sur celui-ci.

Le droit d'auteur est :

> *« une institution juridique complexe qui peut être appréhendée comme l'ensemble des prérogatives, d'ordres morales et d'ordre patrimonial, reconnues aux auteurs d'œuvres de l'esprit.»*[274]

Le cryptage permet la protection et une meilleure exploitation des œuvres, ainsi qu'un meilleur respect de l'étendue de l'autorisation donnée par l'auteur pour exploiter ses œuvres. Le cryptage permet aussi, le tatouage, marquage ou la signature numérique. Il permet l'identification de l'œuvre et de l'utilisateur, l'intégrité de l'œuvre et le suivi à la trace[275] des trafics illicites. Avant il y avait le sigle physique visible sur les supports de l'œuvre, désormais il peut y avoir une signature électronique ou un nombre qui garantit l'authenticité de l'œuvre. Seul l'auteur est capable de calculer ce nombre mais tout le monde peut vérifier l'authenticité. Ce sceau électronique est diffusé en parallèle avec l'œuvre et non par-dessus, la non-séparabilité étant obtenue par une technique mathématique et non physique[276].

Comme le souligne le professeur A.LUCAS :

---

[274] A.LUCAS et H.J.LUCAS, «Traité de propriété littéraire et artistique », *Litec 1994*, p.1.

[275] dit aussi le « tracking ».

[276] La classification des techniques de marquage se fait au moyen de plusieurs critères :
- la dépendance par rapport à un code secret du signataire.
- La nécessité de la comparaison de l'image initiale vierge avec celle signée
- La tolérance vis-à-vis des manipulations de l'image et la survivabilité du code enfoui.

L.LABORELLI, «tatouage des images et des sons : techniques cryptographiques d'authentification et contrôle du copyright », *Expertise des systèmes d'information*, décembre 1995, p.428 et s.

« les auteurs seront prêts à jouer le jeu du développement des réseaux que si la règle inclut des parades techniques propres à conjurer le risque d'une évaporation de leurs investissements.»[277]

Face à cette inquiétude des auteurs, la technique du cryptage intervient. Une des atteintes majeures portée au droit d'auteur, concerne la diffusion des œuvres sur les réseaux du type Internet.

La technique du cryptage permet d'interdire l'accès à l'œuvre. Par le jeu du marquage, les œuvres peuvent porter en leur sein les moyens de se défendre. Avec un code caché et indélébile, qu'elles contiendront, elles pourront se voir facilement tracées et transmettre leurs informations propres. Elles pourront même commander l'interdiction de leur reproduction, voire limiter le nombre de ses représentations en agissant directement sur le matériel de lecture.

Le cryptage semble donc constituer une arme particulièrement adaptée au contexte actuel d'utilisation massive de l'œuvre, dont doit pouvoir jouir l'auteur. Le double but du cryptage est de limiter l'accès à l'œuvre et contrôler son utilisation.

Le cryptage constitue un outil technique au service de la prérogative majeure du droit d'auteur qu'est le monopole de l'auteur. Dans sa fonction d'interdiction d'accès, le cryptage peut s'appliquer à tout type de forme de l'œuvre, dès lors qu'elle est diffusée par le biais d'un moyen technique. Il ne peut s'appliquer que lors de la diffusion de cette œuvre et/ou lors de sa réception par le biais de moyens techniques tel qu'un terminal informatique ou un écran de télévision. Il convient dans ce cas de parler de « télédiffusion ».

En effet, l'article L.122-2 du CPI dispose que la représentation consiste :

« dans la communication de l'œuvre au public par un procédé quelconque et notamment (…) par télédiffusion. »

[277] A.LUCAS, « protéger l'information : de la cryptologie à la stéganographie », *les dossiers de la semaine juridique,* n° hors série, février 1996.

Dans son alinéa 2, l'article L.122-2 du CPI donne comme définition de la télédiffusion :

> *« 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. »*

Ainsi, sont visés les procédés de télécommunication par voie hertzienne, le câble, le satellite et la télématique[278] (donc, les réseaux du type Internet). Le cryptage dans cette fonction spécifique, est donc cantonné aux transmissions et retransmissions de l'œuvre. La consultation directe et physique lui échappe.

Le cryptage, dans sa fonction tatouage de l'œuvre, ne peut s'appliquer que sur une œuvre numérisée. Toutefois, cette limite n'en est plus vraiment une, le « tout numérique » étant une réalité palpable.

Le marché des appareils et des supports de reproduction possède une fonction permettant de violer le monopole de l'œuvre. La numérisation permet facilement les copies serviles, véritables clones de l'œuvre qui peuvent être à l'origine d'un véritable marché pirate.

Contre cela, le cryptage et les techniques de cryptographie sont à la base des systèmes de protection allant de l'identification de l'œuvre, du contrôle et du maintien de son intégrité, à l'interdiction d'y accéder, en passant par la faculté d'interdire certaines utilisations de l'œuvre.

- Les outils d'identifications de l'œuvre comportent des éléments pour identifier la localisation de l'enregistrement, sa date de fixation et le nom de l'artiste (de nombreux projets sont à l'étude[279]). En matière de logiciel, l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) étudie avec l'Agence pour la Protection des Programmes (APP) un système d'identification internationale. Ce code identifiera l'œuvre et donnera aux utilisateurs des informations sur les utilisations autorisées. Ces techniques d'identification permettent un

[278] J.HUET, « droit de l'informatique; le régime juridique de la télématique interactive », *JCP 1984*, I, 3147, cité dans : Romain Leymonerie, « cryptage et droit d'auteur », *Les cahiers de propriété intellectuelle*, janvier 1998, volume 10 n°2, édition Yvon Blais inc., Cowansville (Québec), p.417 à 460

traçage de l'œuvre et couplées avec un système de repérage, elles laissent espérer une meilleure gestion des droits afférents à son utilisation.

- Les outils protégeant l'intégrité de l'œuvre sont composés d'un système de clé ou de signature numérique qui garantie la conservation de l'œuvre. Dès qu'une modification intervient au sein du support numérique de l'œuvre, la vérification échoue et avertit de cette modification.

- Les outils de protection contre les copies illicites sont des systèmes de prévention intégrés dans le matériel de lecture de l'œuvre. Ils n'autorisent qu'une seule copie numérique.

- Les outils d'interdiction d'accès à l'œuvre utilisent, soit un brouillage des impulsions dit de synchronisation qui empêchent toute lecture compréhensible du son et de l'image, soit la méthode de la « rotation active des lignes » ou de mélange des lignes. Dans ce dernier cas, les lignes restent à leur place sur l'écran de réception, mais elles sont coupées au hasard et les parties finales sont interverties (par exemple, les systèmes *Video Crypt, Syster, Eurocrypt*). Actuellement il existe, en matière de logiciel, des systèmes qui proposent l'œuvre à l'utilisateur sous forme cryptée (par exemple : *Software Envelop System*). Dès son adhésion aux conditions d'utilisation et au prix, un programme de décryptage lui est transmis.

Le cryptage est une des voies techniques, parmi les plus efficaces qui permet de renforcer le monopole de l'auteur.

Mais, la volonté des auteurs n'est pas de freiner le processus de diffusion de leurs œuvres. Le but serait plutôt de maîtriser et de percevoir une juste rémunération en contre partie de leurs investissements. Dans ce sens, le cryptage participe de la nature même du monopole de l'auteur. Ainsi, le cryptage constitue le mode de protection actif du monopole et la contrefaçon est le mode réactif de sa protection.

[279] Par exemple, le « MPPBD » pour *Music Program Production Block*

Le cryptage est donc le relais technique aux dispositions légales de protection du monopole du droit d'auteur. Des outils juridiques préexistent, mais au lieu de rechercher la punition et le contentieux, le cryptage apporte une protection préventive.

Le droit moral de l'auteur sur son œuvre permet de le protéger au travers d'une œuvre déterminée, indépendamment de tout acte d'exploitation. Le droit moral contient quatre attributs[280]: Le droit de divulgation, le droit à la paternité, le droit à l'intégrité et le droit de repentir ou de retrait.

En ce qui concerne le droit à la paternité, par les procédés de cryptographie de tatouages, le nom de l'auteur sera indissociable de l'œuvre numérisée, d'où une garantie d'effectivité de ce droit.

Le cryptage, par le biais de la signature électronique, offre une garantie sur l'authenticité et l'intégrité de l'œuvre. De plus, il est possible de verrouiller l'œuvre contre toute tentative de modification.

Ces techniques renforcent le droit moral mais ne le remplacent pas. Elles prolongent l'effectivité du droit. Ces techniques dépassent les frontières. Elles peuvent contrer les atteintes au droit moral dans une sphère privée, ce qui était impossible avant car ce droit se heurtait, dans la pratique, à la barrière de l'intimité et du respect de la vie privée de l'utilisateur. Ainsi, le cryptage remet en cause la liberté d'agir de l'utilisateur comme il l'entend au sein même de son intimité. En effet, il peut limiter les possibilités d'effectuer des copies privées. De même, le droit à la courte citation[281] peut se voir restreint par un accès limiter dû au cryptage. Mais au contraire, par sa fonction d'authentification, le cryptage peut, surtout faciliter le droit de courte citation. En effet, il permet de résoudre le problème d'identification de la source. L'article L122-5-3 du CPI exige que la citation indique clairement le nom de l'auteur et la source. Par l'intermédiaire du cryptage, le plagiat sera plus facile à déceler de façon électronique. Il sera possible de vérifier l'existence dans l'œuvre contestée de séquences extraites de l'œuvre originale.

[280] Articles L.121-1 et L. 121-2 du CPI et l'article 6 bis de la Convention de Berne.
[281] Article L. 122-5-3 CPI autorise un droit limité de courte citation dans un but éducatif, scientifique ou à titre d'information.

Finalement, le cryptage offre une effectivité réelle au monopole de l'auteur sur son œuvre et il encourage un plus grand respect de ses droits moraux.

II Des outils probatoires pertinents

Nous sommes conscient que l'un des atouts du commerce électronique réside dans sa facilité d'utilisation : acheter des livres[282], des logiciels ou faire son épicerie[283] est désormais à la porté de tout internaute. De par sa souplesse, l'achat en ligne permet au même instant au commerçant d'avoir, en plus d'une clientèle, une étude sur la façon de consommer pour un individu ou un autre. Les tris et croisements de fichiers ne peuvent que s'accélérer au détriment de l'individu. La CNIL, telle qu'elle fonctionne actuellement, ou tout autre organisme national n'y changeront rien, et nous renvoyons ici aux problèmes d'applicabilité des lois dans une situation transnationale où il est évident que les États-Unis ont une certaine avance. Cela étant, la CNIL jouît d'un prestige et pour le Conseil d'État, dans le rapport sur *l'internet et les réseaux numériques*,

> *« la dimension internationale de l'internet et l'extrême variété des pratiques des acteurs nécessitent un changement profond des modes de régulation. L'approche réglementaire doit se combiner avec les diverses pratiques d'autorégulation des acteurs et la Commission nationale de l'informatique et des libertés (CNIL) doit avoir pour nouvelle mission d'assurer le suivi de celles-ci : information et conseil sur les dispositifs techniques,* ***labellisation des codes*** *de déontologie et de conduite, des contrats...* ***C'est ce partage des missions d'encadrement entre acteurs publics et privés qui garantira une protection efficace et légitime. »***

La raison commerciale est aussi une raison et il est évident que les pressions contre les *Big Brother* étatiques s'appliquent avec la même force contre les pouvoirs économiques et obligent ces derniers à réagir : la *privacy* est devenu un argument commercial affiché sur les pages de la Toile marchande les plus populaires. L'argument tient de l'axiome mais, il semble bien que si en 1995 les revendications des internautes se portaient principalement pour la

---

[282] par exemple : http://www.amazon.com

[283] par exemple http://www.iga.net

liberté d'expression[284], il est certain que le même type de réactions s'applique désormais pour le respect de la vie privée.

L'autorégulation semble bien être la seule solution envisageable aux problèmes tenant à la sécurité des informations mais, dans le cadre du cryptage, cela suppose tout de même une autorité de certification (A), ici nous n'aborderont pas l'aspect technique de la certification et des tiers de confiance mais plutôt des considérations que doivent appréhender les personnes désirant avoir recours à la preuve électronique. En effet, il n'existe pas en une seule mais plusieurs procédures de certification. Il s'agira alors aux partenaires ou cocontractant de choisir entre ces procédures. Enfin nous prendrons le partis que cette autorité veille à un commerce à la fois sécurisé et, si tel est la volonté du cocontractant, anonyme (B).

A- L'autorité de certification

La certification est l'élément essentiel à toute approche juridique de la cryptologie. Nous l'avons vu, elle consiste à l'intervention d'un tiers (on parle le plus souvent de *tiers de confiance* ou, pour l'instant en France de *tiers de séquestre* puisque la fonction est plus large) pour garantir en son nom (nom personnel ou nom d'un organisme) la conformité avec les exigences attendues par les parties demandant un certain service. En clair, le rôle du tiers est de garantir la sécurité des échanges informatisé grâce au système des clés publiques. Cette sécurité étant modulable selon les attentes des intervenants.

En Illinois, il existe 3 méthodes pour établir des procédures de certifications appropriées :

«
- authorised by this Act, or
- **previously agreed to by the parties**, or
- certified by the secretary as being capable of creating an electronic signature that :
  - is unique to the signer within the context in which it is used
  - can be used to promply and objectively identify the person signing the electronic record
  - was reliably created by such identified person, such as because somme aspect of the procedure involves the use of a means or method that is under the sole control of such person, and
  - is created, and is linked to the electronic record to witch it relates, in a manner such that if the record or the signature is changed after signing the electronic signature is invalidated »[285]

[284] voir le ruban bleu de l'EFF

De la même façon, qu'en France, les parties peuvent faire des conventions de preuve[286], une autorité de certification pourrait être librement choisis. Il est peut être utile de rappeler que le logiciel PGP permet une certification par réputation, soit une auto régulation au sens le plus large du terme et sans autorité officielle.

Par ailleurs, la loi de l'Illinois sur la sécurité et le commerce électronique, comme celle de Californie[287] et d'autres aux États-Unis[288], décrit les exigences à attendre de la preuve électronique. C'est à l'autorité de certification de vérifier que les conditions de validité de la signature électronique sont réalisés.

B- Pour un commerce sécurisé et anonyme

Nous l'avons vu, la cryptographie est la solution idéale pour assurer une certain anonymat et la confidentialité. Cette possibilité est la solution aux différentes craintes concernant la *privacy* ou l'atteinte à la vie privée puisque le fichage des goût et habitudes des utilisateurs deviendrait, sans anonymat, une réalité facile à exploiter. Ici réside un des éléments qui doivent entrer dans toute approche préalable au recours à une autorité de certification.

Mais l'anonymat peut supposer également certaines dérives qui reviendrait à permettre des pratiques financières douteuses. Ici la raison économique se joint à la raison d'État. et la possibilité de *désanonymisation* par le tiers est avancé par certains.

Pierre Trudel décrit le procédé de la signature aveugle qui permet de réaliser des paiements anonymes :

---

[285] *Illinois Electronic Commerce and Security Act*, H.R. 3180, 90th Leg., 1997-98 Reg. Sess. § 302 (b)

[286] Cass. civ. 1re, *Sté Crédicas* 8 nov. 1989

[287] *California Government Code* § 16.5 (1995)

[288] l'Utah fut le premier État américain à légiférer exclusivement sur la signature numérique avec l'*Utah Digital Signature Act*, en vigueur depuis le 1er mai 1995.

« La signature aveugle représente une variante de la signature électronique à clé publique, et à été créée spécifiquement afin d'assurer l'anonymat et le respect de la vie privée des utilisateurs de mécanismes de paiement électronique. Ainsi, avant de transmettre une unité à la banque pour que celle ci la signe, le logiciel du consommateur multiplie le numéro de série auquel elle est associée par un nombre choisi au hasard. Lorsque la banque signe l'unité, elle ne connaît pas le numéro de série mais reste tout de même assurée de l'identité de l'utilisateur grâce à la signature électronique. De cette manière, il est impossible d'identifier l'utilisateur et la transaction. »[289]

Cela dit, dans le cas du commerce en ligne, excepté dans le cas de télédéchargement de produits immatériels, l'anonymat n'a pas de sens sauf à imaginer, pour les plus paranoïaques, une centrale de redistribution. L'anonymat est toutefois utile dans les cas de transferts financiers. Cet anonymat existe déjà puisqu' « à l'heure actuelle 90 % des transactions à travers le monde sont faites en argent contant, et sont donc largement non « auditable » »[290]. De fait, l'argent électronique peut permettre un anonymat pour le seul expéditeur de l'ordre, il est évident que celui qui reçois de l'argent laisse des traces, le simple dépôt en banque par exemple.

Tous ces procédés suppose un dépôt des clés à un organisme de certification. Le principal problème réside alors sur la fiabilité de ces organismes. On parle souvent de tiers de confiance au sujet des tiers certificateurs.

Un avis intéressant est celui de Bruce Schneier sur le dépôt des clés contre lequel il s'oppose farouchement :

« Le dépôt de clef a de considérables désavantages. L'utilisateur dot faire confiance à l'agent de sécurité des dépôts, ainsi qu'à l'intégrité des personnes impliquées dans la procédure. Il doit croire que les agents de dépôts ne changeront pas leur politique, que le gouvernement ne changera pas ses lois et que ceux qui ont toute autorité pour obtenir ses clef le fasse dans le cadre de la loi »[291]

Enfin, nous avons vu que le principal danger en matière de secrets réside le plus souvent dans les utilisateurs des systèmes. Il y a des garanties de sécurité à apporter mais le risque d'un oublis ou n'importe quel événement faible en probabilité est susceptible d'intervenir. Aussi, que ce soit en matière commerciale ou non, le dépôt de clés revient à ajouter un risque dans le

[289] Trudel, Pierre et autres, Droit du cyberespace, Montréal, Éditions Thémis, 1997, chap. 19, page 37
[290] ib. page 36

[291] SCHNEIER, Bruce, op. cit. p 105

caractère confidentiel des informations cryptées échangées. Dès lors un ensemble de questions restent en suspend: la responsabilité du tiers de confiance peut certes être engagée mais les dommages peuvent être irréparables ou le tiers insolvable, à ce sujet, sans fond de garantie, le tiers de séquestre ne pourra jamais être un particulier ou un *cyber-notaire*.

Conclusion : vers une cryptologie citoyenne?

Nous avons essayé d'exposer ici un ensemble exhaustif du droit de la cryptographie. En effet, nous avons bien établis que la cryptologie est un sujet intéressant les États et le monde des affaires et, aux travers eux, les individus confrontés à la société de l'information.

Il ne faut toutefois pas oublier que les questions entre la liberté individuelle et la cryptographie ne sont pertinentes que pour les pays développés, et pour être plus précis, pour les personnes disposant des moyens d'utiliser une technologie dont le développement accéléré laisse de côté, pour une durée de plus en plus longue, une tranche de plus en plus importante de la population mondiale. La liberté d'expression, chère aux ayatollah de PGP, n'a pas vraiment été appliquée dans les récentes manifestations étudiantes en Iran alors que la Guerre du Kosovo à vu un développement important de l'opposition aux dirigeants serbes grâce à l'internet; la Chine a également été témoins de faits similaires contre les répressions de son gouvernement. Il ne s'agit pas d'une critique : nous avons dans ce mémoire pris position pour l'utilisation libre de ces outils cryptographique. Il s'agit juste de relativiser : comme l'internet, la question de la cryptographie domestique est une question qui intéresse ceux que l'on peut appeler les *inforiches*, ayant accès à l'alphabétisation, au téléphone et à l'électricité.

Pour retourner à notre sujet, nous développerons ici en guise de conclusion une application de la cryptologie qui, à notre avis, deviendra l'objet de débats multiples que notre exposé à pourtant tenté de régler.

En plus d'être un outils pour le secret, la cryptographie permet d'obtenir en de nombreux points des applications plus satisfaisantes que le simple envoie de documents manuscrits. Nous avons ainsi vu que si une signature peut être contrefaite et un dossier modifié par l'ajout de lignes, la cryptographie, par le hachage permet d'assurer une parfaite intégrité d'un documents et, par la certification une certitude quant à la personne qui l'a réalisé.

De plus, la cryptographie à usage domestique à permis de développer de nouvelles garanties pour les individus, des garanties tenant à des valeurs constitutionnelles comme le

respect de la vie privée ou de la *privacy*. Ces garanties ne sont d'ailleurs pas applicable par les individus contre les seuls gouvernement mais également contre toute forme de pouvoirs, comme celui, par exemple, des sociétés à tendance monopolistiques et les multinationales. En effet, la cryptographie libre est un des moyen de la personne pour se prémunir de l'espionnage aux fins de fichage, il est aussi un moyen pour l'individu de se préserver un certain espace de liberté dans le monde du travail. Possédant les moyens de cryptage des États les plus puissant, l'individu est désormais à l'abris d'un certain paternalisme : maître de ses secrets, il s'émancipe un peu plus des différentes formes de pouvoirs.

Il est une question encore hypothétique qui ne manquera pas d'impliquer la cryptologie: le vote électronique. Pour ce qui est des élections, Bruce Schneier parle de protocoles ésotériques[292], mais il n'en demeure pas moins que permettre le vote électronique est un défi que de nombreux cryptanalystes[293] ont relevé. Pour réaliser des élections sûres, il s'agit d'éviter la tricherie et de garantir la confidentialité. Pour Schneier, le protocole idéal à

> « au minimum les 6 caractéristiques suivantes :
>
> 1- seules les personnes autorisées à voter peuvent voter.
> 2- Personne ne peut voter plus d'une fois.
> 3- Personne ne peut déterminer pour qui quelqu'un d'autre à voté.
> 4- Personne ne peut dupliquer le vote de quelqu'un d'autre. (il s'avère que cette exigence est la plus difficile à remplir).
> 5- Personne ne peut modifier le vote de quelqu'un d'autre sans être découvert
> 6- Tous les votants peuvent vérifier que leur vote à bien été pris en compte dans le décompte final. »

Nous manquons bien sûr d'éléments et de compétences en cryptanalyste pour offrir dans cette conclusion des réponse concrètes. Il n'en demeure pas moins que le vote électronique deviendra sans doute une des applications les plus courantes de la cryptographie. Le seul problème réside dans l'application de cette faculté à grande échelle. À petite échelle (vote d'actionnaires ou conseil d'administration dans le cadre d'une visio-conférence), le vote électronique deviendrait un instrument pratique qui susciterait moins de craintes qu'un vote politique, qui utiliserait pourtant les mêmes outils avec les mêmes garanties.

[292] op. cit., p135 et s.

Avec des applications aussi diverses et des perspective d'application aussi proche des citoyens, avec une popularité grandissante auprès du grand public, la cryptographie est désormais entrée à l'âge de la maturité. Ce mémoire à eu notamment pour objectif d'en persuader le lecteur.

[293] ib.

Annexes

ANNEXE 1 : décret n°99-199

MOYENS OU PRESTATIONS	OPÉRATIONS pour lesquelles la déclaration se substitue à l'autorisation
1. Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur inférieure ou égale à 40 bits.	F
2. Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur supérieure à 40 bits et inférieure ou égale à 128 bits.	F, U, 1 (1)
3. Equipements conçus ou modifiés pour utiliser la cryptologie faisant appel à des techniques analogiques tels que : a) Equipements utilisant des techniques de mélange de bandes " fixes " ne dépassant pas 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ; b) Equipements utilisant des techniques de mélange de bandes " fixes " dépassant 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les dix secondes ; c) Equipements utilisant l'inversion à fréquence "fixe " et où les changements de transposition ne s'effectuent pas plus	F

d'une fois toutes les secondes ; d) Equipements de fac-similé, e) Equipements de radiodiffusion pour audience restreinte f) Equipements de télévision civile.	
(1) L'utilisation et l'importation ne sont soumises à déclaration que si elles concernent un matériel ou un logiciel qui n'a pas fait l'objet préalablement d'une déclaration par leur producteur, un fournisseur ou un importateur, et si ledit matériel ou ledit logiciel n'est pas exclusivement destiné à l'usage privé d'une personne physique.	
(*) F : fourniture ; U : utilisation ; E : exportation ; 1 : importation.	

ANNEXE 2 : décret n°99-200

MOYENS OU PRESTATIONS	OPÉRATIONS (*) dispensées de toutes formalités préalables
1. Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur inférieure ou égale à 40 bits.	U, I
2. Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur supérieure à 40 bits et inférieure ou égale à 128 bits, à condition, soit que lesdits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par leur producteur, un fournisseur ou un importateur, soit que lesdits matériels ou logiciels soient exclusivement destinés à l'usage privé d'une personne physique.	U, I
3. Equipements conçus ou modifiés pour utiliser la cryptologie faisant appel à des techniques analogiques tels que : a) Equipements utilisant des techniques de mélange de bandes " fixes " ne dépassant pas 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ; b) Equipements utilisant des techniques de mélange de bandes " fixes " dépassant 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les dix secondes; c) Equipements utilisant l'inversion à fréquence , "fixe" et où les changements de transposition ne s'effectuent pas plus d'une	U, E, I

fois toutes les secondes; d) Equipements de fac-similé; e) Equipements de radiodiffusion pour audience restreinte; f) Equipements de télévision civile.	
4. Cartes à microprocesseur personnalisées ou leurs composants spécialement conçus, incapables de chiffrer le trafic de messages ou les données fournies par l'utilisateur ou leur prestation de gestion de clef associée.	F, U, E, I
5. Equipements de réception de télévision de type grand public, sans capacité de chiffrement numérique et où le déchiffrement numérique est limité aux fonctions vidéo, audio ou de gestion.	F, U, E, I
6. Radiotéléphones portatifs ou mobiles destinés à l'usage civil qui ne sont pas en mesure de procéder au chiffrement de bout en bout.	F, U, E, I
7. Equipements autonomes de lecture de disques vidéo numériques, de type grand public, sans capacité de chiffrement, où le déchiffrement est limité aux informations vidéo, audio, informatiques et de gestion.	F, U, E, I
8. 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	F, U, E, I

pas accessibles à l'utilisateur.	
9. Equipements de contrôle d'accès, tels que machines automatiques de distribution de billets, imprimantes libre-service de relevés de compte ou terminaux de points de vente, protégeant les mots de passe, numéros d'identification personnels ou autres données similaires empêchant l'accès non autorise a des installations, mais ne permettant pas le chiffrement des fichiers ou des textes, sauf lorsqu'il est directement lie à la protection des mots de passe ou des numéros d'identification personnels.	F, U, E, I
10. 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 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.	U, E, I
11. 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.	U, E, I

12. Systèmes de gestion de facturation inclus dans les dispositifs de relevés de compteurs dont les fonctions de chiffrement sont directement liées au comptage.	F, U, E, I
13. Equipements dotés de moyens de cryptologie lorsqu'ils accompagnent les personnalités étrangères sur invitation officielle de l'État	U, E, I
14 Stations de base de radiocommunications cellulaires commerciales civiles présentant toutes les caractéristiques suivantes: a) Limitées au raccordement de radiotéléphones qui ne permettent pas d'appliquer des techniques cryptographiques au trafic de messages entre terminaux mobiles, sauf sur les liens directs entre radiotéléphones et stations de bases (connues sous le nom d'interface radio) ; b) Et ne permettant pas d'appliquer des techniques cryptographiques au trafic de messages sauf sur l'interface radio.	F, U, I
(*) F : fourniture ; U, : utilisation ; E, : exportation ; 1 : importation.	

ANNEXE 3 :

PREMIER MINISTRE
SERVICE CENTRAL DE LA SECURITE
DES SYSTEMES D'INFORMATION
18, rue du Docteur-Zamenhof, 92131 Issy-les-Moulineaux Cedex
(téléphone : 01-41-46-37-00, Fax : 01-41-46-37-01)
Numéro de dossier (*) : .....
Déclaration/Demande d'autorisation
concernant un moyen ou une prestation de cryptologie
PARTIE ADMINISTRATIVE
Cocher la ou les cases correspondantes :
Déclaration
simplifiée
de fourniture
en vue de l'utilisation générale
en vue de l'exportation
d'importation en provenance de : .....
d'utilisation personnelle
Demande d'autorisation
de fourniture pour une durée de : ..... (cinq ans maximum)
d'un moyen ou d'une prestation qui n'utilise que des conventions secrètes gérées par un organisme agréé
de fourniture pour une durée de : ..... (cinq ans maximum)
en vue de l'utilisation générale
en vue de l'utilisation collective
d'exportation pour une durée de : ..... (cinq ans maximum)
d'importation en provenance de : .....
d'utilisation personnelle pour une durée de : .....
(dix ans maximum)
(*) Réservé à l'administration.
A. - Déclarant ou demandeur d'autorisation
A.1. Société
Nom : .....

Raison sociale : .....

Nationalité : .....

Numéro SIRET : .....

Adresse : .....

.....

Numéro de téléphone : .....

Numéro de télécopie : .....

Adresse du courrier électronique : .....

Personne chargée du dossier administratif

Nom et prénoms : .....

Adresse : .....

.....

Numéro de téléphone : .....

Numéro de télécopie : .....

Adresse du courrier électronique : .....

A.2. Particulier

Nom et prénoms : .....

Nationalité : .....

Adresse : .....

.....

Numéro de téléphone : .....

Adresse du courrier électronique : .....

B. - A renseigner selon les cas suivants

B.1. Demande d'autorisation de fourniture d'un moyen ou d'une prestation qui utilise des conventions secrètes gérées par un organisme agréé

Référence de(s) organisme(s) agréé(s) : .....

.....

.....

B.2. Demande d'autorisation de fourniture

en vue de l'utilisation collective

Catégories éventuelles d'utilisateurs auxquels le moyen ou la prestation est destiné :

Administrations (à préciser) : .....

Grandes entreprises (préciser secteur d'activités) : .....

Etablissements de crédit : .....

PME (préciser secteur d'activités) : .....

Autres (à préciser avec secteur d'activités) : .....

B.3. Demande d'autorisation d'utilisation personnelle

Besoins justifiant la demande : .....

.....

.....

.....

Lieux d'utilisation du moyen de cryptologie : .....

.....

.....

.....

Le cas échéant, réseaux de télécommunications employés : .....

.....

.....

.....

C. - Moyen ou prestation auquel s'applique
la déclaration ou la demande d'autorisation

C.1. Moyen ou prestation de cryptologie

Référence commerciale : .....

Référence constructeur : .....

Version : .....

Description succincte : .....

.....

.....

.....

.....

Référence de l'agrément du moyen s'il a été soumis au ministère chargé des télécommunications : .....

C.2. Fabricant du moyen ou fournisseur de la prestation

Nom : .....

Raison sociale : .....

Adresse : .....

.....

Numéro de téléphone : .....

Numéro de télécopie : .....

Adresse du courrier électronique : .....

C.3. Personne chargée du dossier technique

Nom et prénoms : .....

Adresse : .....

.....

Numéro de téléphone : .....

Numéro de télécopie : .....

Adresse du courrier électronique : .....

C.4. Divers

Si le moyen ou la prestation utilise des moyens ou prestations préalablement déclarés ou autorisés, préciser, pour chacun d'eux, leur identification, référence et date de notification de déclaration ou d'autorisation : .....

.....

C.5. Services de cryptologie fournis

Authentification (*) : .....

Contrôle d'accès (*) : .....

Signature (*) : .....

Intégrité (*) : .....

Confidentialité (*) : .....

téléphone

télécopie

messagerie

transmissions

de données (préciser le(s) type(s) de données chiffrées, par exemple données à caractère financier, médical, de gestion,...) : .....

autre(s) (à préciser) : .....

Autre(s) (à préciser) (*) : .....

C.6. Installation des algorithmes

Logiciel.

Matériel (à préciser) : .....

(*) Préciser le(s) nom(s) de(s) algorithme(s) utilisé(s).

D. - Attestation

Je soussigné (nom, prénoms).....

agissant en qualité de.....

représentant le fournisseur - exportateur - importateur - utilisateur (*) certifie que les renseignements figurant sur cette déclaration - demande d'autorisation (*) sont exacts et ont été établis de bonne foi, toute fausse déclaration ou tout manquement aux engagements souscrits m'exposant aux sanctions prévues par l'article 28 de la loi no 90-1170 du 29 décembre 1990 modifiée et par le décret no 98-101 du 24 février 1998.

Date :.....

Signature :

(*) Rayer les mentions inutiles.

PARTIE TECHNIQUE

A joindre au dossier de déclaration ou de demande d'autorisation concernant les moyens et prestations de cryptologie (1)

La partie technique comporte les informations suivantes :

La référence commerciale du produit :

- nom ;
- numéro de la version ;

La description générale du produit, le manuel utilisateur ;

La description des services offerts par le produit ;

La description des fonctions de cryptologie offertes par le produit (chiffrement, signature, gestion de clés) ;

Soit la description complète des procédés de cryptologie employés, sous la forme d'une description mathématique et d'une simulation dans un langage de haut niveau, type C ou pascal, soit la référence à un dossier préalablement déposé pour un produit usant du même procédé de cryptologie, soit la référence à un standard reconnu, non équivoque, et dont les détails techniques sont accessibles aisément et sans condition ;

La description de la gestion des clés mises en œuvre par le moyen, incluant au moins :

- le mode de distribution ;
- le procédé de génération des clés ;
- le format de conservation des clés s'il y a lieu ;
- le format de transmission des clés s'il y a lieu ;

La description des mesures techniques mises en œuvre pour empêcher l'altération du procédé de chiffrement ou de la gestion de clés associée (2) ;

La description des prétraitements subis par les données claires avant leur chiffrement (compression, formatage, ajout d'un en-tête, etc.) ;

La description des post-traitements des données chiffrées, après leur chiffrement (ajout d'un en-tête, formatage, mise en paquet, etc.).

(1) Conformément au troisième alinéa de l'article 1er de l'arrêté ci-dessus, la partie technique doit être accompagnée de deux exemplaires du matériel concerné ou bien d'un exemplaire du logiciel concerné.

(2) A fournir dans le cas d'une demande d'autorisation seulement.

ANNEXE 4 :

État membre	État d'avancement du processus législatif
Allemagne	• Loi et décret sur les signatures numériques adoptés : conditions dans lesquelles les signatures numériques sont jugées sûres; accréditation volontaire des prestataires de services; • Etablissement du catalogue des mesures de sécurité adaptées ; • Consultation publique en cours sur les aspects juridiques des signatures numériques et des documents électroniques signés numériquement.
Autriche	Travaux préparatoires.
Belgique	• Loi sur les télécommunications : régime volontaire de déclaration préalable pour les prestataires de services ; • Projet de loi sur les services de certification relatifs aux signatures numériques ; • Projet de loi modifiant le Code civil en ce qui concerne les preuves électroniques. • Elaboration d'une loi sur l'usage des signatures numériques pour la sécurité sociale et la santé publique.
Danemark	Projet de loi sur l'utilisation sûre et efficace des communications numériques.
Espagne	• Circulaires de la direction des Douanes sur l'utilisation des signatures électroniques ; • Résolution dans le domaine de la sécurité sociale régissant l'utilisation des moyens électroniques ; • Lois et circulaires dans le domaine des hypothèques, de la fiscalité, des services financiers et de l'enregistrement des entreprises autorisant l'utilisation de procédures électroniques ; • Loi de finances de 1998 mandatant le ministère de l'Intérieur à agir comme prestataire de service de certification.
Finlande	• Projet de loi sur l'échange électronique d'informations dans l'administration et les procédures judiciaires administratives ; • Projet de loi sur le statut du centre de recensement de la population en tant que prestataire de service de certification.

France	• Loi sur les télécommunications (décrets sur les autorisations et exemptions) : ⇒ fourniture de produits de signature électronique soumise à une procédure d'information ; ⇒ liberté d'utilisation, d'importation et d'exportation des produits et services de signature électronique. • Législation concernant l'utilisation des signatures numériques pour la sécurité sociale et la santé publique.
Italie	• Loi générale sur la réforme du service public et la simplification administrative adoptée : principe de la reconnaissance juridique des documents électroniques ; • Décret sur la création, l'archivage et la transmission des documents et contrats électroniques ; • Décret en préparation sur les exigences relatives aux produits et services ; • Décret en préparation sur les obligations fiscales découlant des documents électroniques.
Pays-Bas	• Régime volontaire d'accréditation en préparation pour les prestataires de services ; • Loi sur la fiscalité prévoyant la soumission des déclarations de revenus par voie électronique ; • Projet de loi modifiant le Code civil en préparation.
Royaume-Uni	Préparation d'une loi concernant l'accréditation volontaire des prestataires de services de certification et la reconnaissance juridique des signatures numériques.
Suède	Travaux préparatoires.

ANNEXE 5 :

R. c. Edwards

Calhoun Edwards, appelant;
c.
Sa Majesté la Reine, intimée.

[1996] 1 R.C.S. 128
[1996] A.C.S. no 11
No du greffe: 24297.

Cet arrêt est disponible à cette adresse :

http://www.droit.umontréal.ca/doc/csc-scc/fr/pub/1996/vol1/1996rcs1_0128.html

Bibliographie[1]

Documents Officiels :

- Loi n°78-17 du 6 janvier 1978 dit "fichier informatique et liberté", JO du 7 janvier 1978
- Loi sur la cryptographie,(Article 28 de la loi du 29 décembre 1990, modifié par la loi n° 91-648 du 11 juillet 1991 et la loi n° 96-659 du 26 juillet 1996)
  http://www.internet.gouv.fr
- loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications
  http://www.internet.gouv.fr/francais/textesref
- loi n°92-1477 du 31 décembre 1992 relative «*aux produits soumis à certaines restrictions de circulation et à la complémentarité entre les services de police, de gendarmerie, et de douane*», publiée au journal officiel le 05 janvier 1993
- Loi n° 96-659 du 26 juillet 1996, JO 27 juill. 1996.
- Décret français n°92-1358 du 28 décembre 1992, JO du 30 décembre 1990
- Décret 95-613 du 5 mai 1995 relatif au contrôle à l'exportation de biens à double usage, JO du 7 mai 1995
- Décret n° 98-101 du 24 février 1998
  http://www.internet.gouv.fr/francais/textesref/cryptodecret9801.htm
- Décret no 98-102 du 24 février 1998
  http://www.internet.gouv.fr/francais/textesref/cryptodecret98102.htm
- Décret n° 98-207 du 23 mars 1998
  http://www.internet.gouv.fr/francais/textesref/cryptodecret98207.htm
- Décret n° 98-206 du 23 mars 1998
  http://www.internet.gouv.fr/francais/textesref/cryptodecret98206.htm
- Décret n° 99-199 du 17 mars 1999
  http://www.internet.gouv.fr/francais/textesref/cryptodecret99199.htm
- Décret n° 99-200 du 17 mars 1999
  http://www.internet.gouv.fr/francais/textesref/cryptodecret99200.htm
- Arrêté du 5 mai 1995 relatif au contrôle à l'exportation vers les pays tiers et au transfert vers les Etats membres de la Communauté européenne de biens à double usage, Journal officiel du 7 mai 1995.
- Arrêté du 5 mai 1995 définissant la licence générale de G.502 d'exportation des moyens de cryptologie et fixant les modalités d'établissement et d'utilisation de cette licence, JO du 7 mai 1995.
- Arrêtés du 13 mars 1998
  http://www.internet.gouv.fr/francais/textesref/cryptarrete1.htm
- Arrêtés du 17 mars 1999
  http://www.internet.gouv.fr/francais/textesref/cryptarrete4.htm
- Nouveau Code pénal français (articles : 226-1, 226-15, 432-8, 432-9, 432-17)

[1] Les sites internet ont tous été consultés entre les mois de décembre 1998 et mai 1999. Une vérification de leur présence sur la Toile à été faite au début du mois de juillet 1999.

- Code de procédure pénale français (articles : 56 et s., 76 et s., 92 et s.)
- Article 9 du Code Civil français
- Code de la Propriété Intellectuelle (articles : L122-2, L121-1, L 121-2, L122-5-3)
- Loi n°91-646 du 10 juillet 1991, relative au secret de correspondances émises par voie de télécommunications, JO du 13 juillet 1991 ; Rect, JO 10 août.
- Rép. Min. n°13318, JOANQ 29 juin 1998, p.3614.
- Code civil du Québec (articles : 1827, 2827, 2829)
- la déclaration universelle des droits de l'homme, proclamé le 10 décembre 1948 par l'assemblée générale des nations unis.
- la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée le 4 novembre 1950, entrée en vigueur le 3 septembre 1953
- pacte international relatif aux droits civils et politiques, adopté le 16 décembre 1966 par l'assemblée générale des Nations Unis.
- "The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies".
  http://www.wassenaar.org
- « La politique de cryptographie : les lignes directrices et les questions actuelles » (les lignes directrices régissant la politique de cryptographie de l'OCDE Rapport sur la politique de cryptographie : contexte et questions actuelles), OCDE/GD (97) 204, le 27.03.1997
- Traité de Rome du 25 mars 1957 instituant la communauté économique européenne (articles : 9, 30, 48, 52, 59, 60)
- Décision n° 92/242/CEE en matière de sécurité des systèmes d'informations, JO L 123, 8 mai 1992
- Décision du conseil n°94/942/PESC du 19 décembre 1994, JO CE L 367 du 31 décembre 1994
- Règlement (CE), n°3381/94 du Conseil, du 19.12.1994, instituant un régime communautaire de contrôle des exportations de biens à double usage, JOCE, n°L367/1, du 31.12.1994.
- 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.
  http://www2.echo.lu/legal/fr/dataprot/directiv/direct.html
- Commission propose une directive sur les signatures electroniques DN: IP/98/423
  Date: 1998-05-13.
  http://europa.eu.int/comm/dg15 et http://www.ispo.cec.be/eil
- LES TECHNOLOGIES DE L'INFORMATION LA REGLEMENTATION FRANCAISE EN MATIERE DE CRYPTOLOGIE – Juin 1998 ,Annexe 8 : Modèle de cahier des charges des tiers de séquestre, Modèle de cahier des charges d'un organisme agréé à gérer des conventions secrètes pour le compte d'autrui.
- Proposition de DIRECTIVE DU PARLEMENT EUROPEEN ET DU CONSEIL, sur un cadre commun pour les signatures électroniques(présentée par la Commission), Bruxelles, le 13.05.1998, COM(1998) 297 final, 98/0191 (COD).
- Proposition de règlement du Conseil, 15 mai 1998, COM(98)257 final, instituant un régime communautaire de contrôle des exportations des biens à double usage, JOCE, 15.05.98, n°L257.

Ouvrages :

- AZEMA J., *Droit de la concurrence*, Paris, PUF, Thémis, 1998
- BENSOUSSAN, Alain, *Le commerce électronique : aspects juridiques*, *Edition Hermes* 1998.
- BERTOLUS, Jean-Jérome et Renaud de la BAUME, *Les nouveaux maîtres du monde*, Paris, *Edition Belfond*, 1995.
- BLANCHARD, Philippe, *Pirates de l'informatique enquêtes sur les Hackers français*, Paris, *Edition Addison – Wesley*, France, S.A 1995.
- CORNU, G (SS dir. De), *Vocabulaire juridique*, Paris, *PUF*, 1987.
- GUISNEL Jean, Guerres dans le cyberespace, Paris, Éditions la Découverte, 1998
- KATSH Ethan, *Law in a Digital World*, New York, Oxford University Press, 1995
- LUCAS André et H.J.LUCAS, *Traité de propriété littéraire et artistique*, Paris, *Litec 1994*, p.1.
- SCHNEIER, Bruce (VIENNOT, Laurent, (trad.)), *Cryptographie appliquée*, Paris, 2ème Éd., International Thomson Publishing France, 1997, 846 pages pour l'édition francophone
- STERN, Jacques, *La science du secret*, Paris, Éditions Odile Jacob, 1998.
- TRUDEL, Pierre et autres, *Droit du cyberespace*, Montréal, *Éditions Thémis*, 1997.
- VIVANT, Michel et Christian LE STANC, *Lamy, droit de l'informatique*, Paris, 1998
- STERN, Jacques, *La science du secret*, Paris, Éditions Odile Jacob, 1998
- KAHN, David, *La guerre des codes secrets*, Paris InterÉditions, 1980
- COURBE Patrick, "Introduction générale du droit", *mémentos DALLOZ série droit privé*, 2dition DALLOZ,4ème édition, 1995.
- DUPONT DELESTRAINT Pierre et COURBE Patrick, "droit civil, les personnes, la famille, les incapacités", *mémentos DALLOZ*, édition DALLOZ, 15ème édition, 1994.
- CABRILLAC Rémy, FRISON-ROCHE Marie-Anne, REVET Thierry, "Droits et libertés fondamentaux", *édition DALLOZ*, 3ème édition, 1996.

Revues :

- BREBAN, Yann et Isabelle POTTIER, « Les décrets et arrêtés cryptologie : la mise en œuvre effective de l'assouplissement des dispositions antérieures. », *Gazette du palais*, 19 au 21 avril 1998.
- CABRILLAC, M., « Chron. De législation et de jurisprudence française » : *RTD com.* 1997, p. 120
- GOLLIARD, François, « Télécommunication et réglementation française du cryptage », *Recueil Dalloz 1998*, 11 cahier, chronique.
- GUIBAL, M., REP. com. Dalloz V° Commerce et industrie, 1994,n°55.
- LEYMONERIE, Romain, « Cryptage et droit d'auteur », Cowansville, *Les cahiers de propriété intellectuelle*, janvier 1998, volume 10 n°2, Édition Yvon Blais inc., Canada. p.417 à 460,
- MASSE, David G. « Le cadre juridique en droit civil québécois des transactions sur l'inforoute », (1997) 42 R.D. McGill 403
- MASSEY, J.L., An introduction to contempory cryptology. Proceedings of the IEEE, vol. 76, n°5, mai 1988
- RIVEST, R.L., « The MD4 Message digest Algorithm. », *Advances in cryptology*, CRYPTO'90 Proceedings
- V. I. De LAMBERTERIE, « la valeur probatoire des documents informatiques dans les pays de la CEE », *RID comp*. 1992, n°3, spéc. P.64
- ***Juris Classeur Procédure Pénale Art. 100 à 100-7 n°122***

- ***Bulletin d'actualité Lamy droit de l'informatique et des réseaux :***

1. Juillet 1998, n°105, D.
2. Août-septembre 1998, n°106, E.
3. Octobre 1998, n°107,F.
4. Janvier 1999 ,n°110, I.

- ***JCP édition générale:***

1. LINDON Raymond, "protection de la vie privée : champ d'application ", 1971, 2, JCP.6734
2. GOBIN, V. A., « Pour une problématique notariale des autoroutes de l'information » : *JCP N* 1995, n°50-51, p. 1749s.
3. BARBRY, E. et F. OLIVIER, « Cryptologie des décrets tant attendus : quel droit pour la cryptologie », 1 avril 1998 n°14, I, 124.
4. CAPRIOLI, E-A., « Commerce électronique : Sécurité et confiance dans le commerce électronique – Signature et autorité de certification », 1 avril 1998, n°14, I, 123, p.583 s.
5. « Commerce électronique- Conditions de licéité de l'utilisation des moyens et prestations de cryptologie », actualité, 31 mars 1999 n°13, p609.
6. ESPAGNON, Michel, « Le paiement d'une somme d'argent sur internet : Evolution ou révolution du droit des moyens de paiements ? », 21 avril 1999, n°16-17, I, 131, p.787

- ***La revue expertise :***

1. Anonyme, « Plaidoyer pour un droit conventionnel de la preuve en matière informatique », juillet- août 1987, p.260
2. LABORELLI, L., « Tatouage des images et des sons : techniques cryptographiques d'authentification et contrôle du copyright », décembre 1995, p.428 et s
3. DEBOUZY, Olivier et Thaima SAMMAN, « L'exception française et la cryptologie : le chant du signe ? », mars 1997, p54.
4. Groupe de travail « l'écrit et les nouveaux moyens technologique au regard du droit » de la mission de recherche droit et justice, V. l'interview du P^{r} A. LUCAS 1997, p.222.
5. ROS de LCHOUNOFF Nicolas, « chiffrement, tiers de confiance, signature électronique et interceptions : les gouvernements et les internautes sont-ils myopes. », n°211, janvier 1998, p.417.
6. ROS de LOCHOUNOFF, Nicolas, « Cryptographie et droit », Janvier 1998, p417.
7. « L'utilisation des produits à 40 bits enfin libérée », Mai 1998, p129.
8. ROZENFIELD, Sylvie, « Quelle liberté pour le numérique ? », Juillet 1998, p206.
9. « le DES à 56 bits brisé en 56 heures », Octobre 1998, p286.
10. « le SCSSI agrée le premier tiersde confiance », Novembre 1998, p323.
11. SEDALLIAN, Valérie et Garance Mathias, « Les problèmes poses par la législation française en matière de chiffrement », octobre 1998.

- ***Droit de l'informatique et des télecoms :***

1. SYX, D : «Vers de nouvelles formes de signature ? le problème de la signature dans les rapports juridiques électroniques», 1986/3.
2. WARUSFEL Bertrand, «exportation de cryptologie : des régimes juridiques difficiles à concilier», 1993/1.
3. MEILLAN Eric, « Le contrôle juridique de la cryptographie », *1993/1, p.78 et s.*
4. WARUSFEL, Bertrand, «contrôle des exportations de technologie à double usage : le droit français réagit face au marché unique»,1993/2.
5. CAPRIOLI, E-A., « contribution à la définition d'un régime juridique de la conservation des documents : du papier au mesurage électronique », 1993/3, p.5s.
6. Prise de position de la CCI sur une politique internationale du chiffrement, 1994/2, p.70.
7. D.PONSOT, "la signature en droit privé", 1996/4, p14 s.

Articles de presse :

- ZIMMERMAN Philip, « Vie privée, vie cryptée », *Libération, cahier multimédia*, 23 février 1996.
- Vidonne, Paul, « Pour une vraie liberté de crypter », *Le Monde* du 15 mai 1996, p. 14.
- TORRÈS Astrad, « Faut-il brûler Internet », *Internet, l'extase et l'effroi*, Le Monde diplomatique, collection Manière de voir, HorsSérie, Octobre 1996
- THOUMYRE, Lionel, « La crypto encore au fond du trou », *Netsurf* n°34 de janvier 1999, p16.
- A.F, « 1335 minutes pour forcer une clé de 56 bit », *Le monde informatique*, n°795, janvier 1999, p.12.
- BARDY, Christophe, « Quand le 128 bit se réduit à 56 bit », *Le monde informatique*, n°795, janvier 1999, p.14.
- PARISOT, Thierry et Philippe ROSÉ, « Enfin les 128 bits ! », *Le monde informatique*, n°794,22 janvier 1999, p.4.
- DELBECQ, Denis, « Comment achetez les e-mails », *Le monde interactif*, mercredi 3 février 1999, p. VI.
- Pirate mag, hors série n°1, juillet 1999, p.17

Rapports, Avis et Communications :

- « The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption » Final Report -- 27 May 1997.
- CNIL, *17ème rapport d'activité 1996*, Documentation Française, ISBN : 2 11 003757-1.
- CNIL, 18ème rapport d'activité 1997, Documentation Française, ISBN : 2 11 004033-5.
- le rapport de Francis Lorentz.
  http://www.internet.finances.gouv
- CONSEIL D'ETAT ,Section du rapport et des études Internet et les réseaux numériques, Etude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998.
- The Green Book on the Security of Information Systems (18 octobre 1993) et, the Green Paper on Legal Protection for Encrypted Services in the Single Market, (le 6 mars 1996).
  http://info.risc.uni-linz.ac.at/1/misc-info/crypto/green-paper.txt .
- Avis de l'ART sur les projets de décrets, Avis no 97-313 du 8 octobre 1997 relatif au projet de décret définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie et au projet de décret définissant les conditions dans lesquelles sont agréés les organismes gérant, pour le compte d'autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité (J.O. du 27 février 1998).
- Commission des communautés européennes, « EDI et sécurité : Comment gérer le problème ? » , *rapport préparé par KPMG dans le cadre du programme TEDIS*, 1992, p.11.
- Recommandation relative à l'utilisation de profils de protection dans les échanges informatisés entre l'administration et ses partenaires et usagers, n°R 96.02, 19 juin 1996.
  http://www.cerf.gouv.fr

- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, COM (97) 503 en date du 8 octobre 1997, "Assurer la sécurité et la confiance dans la communication électronique" .
  http://www2.echo.lu/legal/fr/internet/actplan.html.

- Rapport final du comité consultatif sur l'autoroute de l'information, "Le défide l'autoroute de l'information", septembre 1995, *Ministre des approvisionnement et Services Canada*.

- Groupe de travail sur le commerce électronique Industrie Canada, *Politique cadre en matière de cryptographie aux fins du commerce électronique, Pour une économie et une société de l'information au Canada Politique cadre en matière de cryptographie aux fins du commerce électronique* Février 1998.
  http://strategis.ic.gc.ca/crypto.

- Rapp. Comm. Nations Unies pour le droit commercial international sur les travaux de sa 21ème session, 28 mai - 14 juin 1996, Assemblée générale, Documentation officiels, 51ème session, suppl. n°17 (A/51/17), V. p.77.

- Étude intérimaire STOA, Une évaluation des techniques de contrôle politique, résumé analytique disponible à cette adresse.
  http://www.europarl.eu.int/dg4/stoa.htm.

Jurisprudence :

- Arrêt de la 1er chambre civil du 20 octobre 1993, B.I, n°295, relatif à la publication de renseignements relatifs aux revenus.
- Arrêt du 13 avril 1988, B.I, n°98, relatif à l'impératrice d'Iran.
- CEDH24 avril 1990, Kruslin, série A, n°176 A ; D. 1990 p.353 note PRADEL, relatif à une affaire d'écoutes téléphoniques.
- CE, 28 octobre 1960, de LABOULAYE, AJDA 1961, 20.
- CE 9 janvier 1981, Sté Claude publicité, D. 1981, IR 113, obs. DELVOLE.
- CE 22 mars 1991, AJDA 1991, 650
- Décision du Conseil constitutionnel du 27 juillet 1982, *Rev. Dr. Pub.* 1983, 333, obs. L. FAVOREU.
- Décision du Conseil constitutionnel du 16 janvier 1982, D. 1983, 169, note L. HANON .
- Arrêt REYNES, CJCE 21 juin 1974, REC. 631, *RTD europ*. 1975, p.561
- Arrêt Simmenthal, CJCE le 9 mars 1978 Rec.269
- CE, arrêt "Nicolo" du 20 octobre 1989, D. 1990, 57, note R. KOVAR
- Cour de Cassation, arrêt "Jacques Vabre" du 24 mai 1975, D.1990, 497, concl. A. TOUFFAIT
- Conseil Constitutionnel, 27 juillet 1982, *Rev. Dr.pub.* 1983, 333, obs. L. FAVOREU.
- Cass. 1er civ, 15 juillet 1957, *Bull civ. I, n°331*
- Cour d'appel de Paris, 19 décembre 1958, *JCP G*, 1960, I, 1579
- Cass. 3ème civ, 16 novembre 1977, *Bull civ*, III, n°393.
- Cass. 1er civ., 8 novembre 1989, Bull. civ. I, n°342. Dalloz 1990, p.369, note C.Gavalda

Autres documents disponibles sur Internet :

- RSA, *RSA's FAQ About Today's Cryptography*, http://www.rsa.com/rsalabs/faq/faq_rsa.html

- Étude intérimaire STOA Résumé analytique du Parlement européen, Septembre 1998.
  http://PE166.499/int.st/Exec.sum/fr

- Programme d'action gouvernemental, Préparer l'entrée de la France dans la société de l'information,1998. Premier ministre - Service d'information du gouvernement (SIG) – France.
  http://www.internet.gouv.fr

- Conférence de presse de Monsieur Lionel JOSPIN, Premier ministre, à l'issue du Comité interministériel pour la société de l'information, Mardi 19 janvier 1999.
  http://www.internet.gouv.fr/francais/frame-actualité.htm

- Commerce électronique : la Commission propose un cadre Juridique , Date: 18 Novembre 1998. http://www.dg15.cec.be
- « Le secret médical à la merci du SCSSI », netizen - 22 nov 1995, ngroups : fr.network.divers, fr.comp.infosystemes ...

- BALTHAZAR, Géraldine, *Zivilrechtliche Probleme des Internet*, Wintersemester 1996-1997- Seminararbeit, Application et réglementation de la cryptographie en Belgique et en Francebei Dr. Jung, LL.M. http://www.fu-brlin.de/jura/netlaw/publits.atrionen/baitraege/w96-balthazar.html

- SEDALLIAN, Valérie, « Cryptographie : pourquoi faut-il libéraliser totalement la loi française?», octobre 1997. http://www.argia.fr/lij/etatcrypto.html

- SEDALLIAN, Valérie, « aspects internationaux du chiffrement des transmissions », texte rédigé à partir d'une intervention au séminaire du groupe réseaux de DECUS (association des utilisateurs de DIGITAL) du 12 décembre 1996. http://www.argia.fr/lij/etatcrypto.html

- SEDALLIAN, Valérie, « Cryptographie : les enjeux et l'état de la législation française. »,1997. http://www.argia.fr/lij/etatcrypto.html

- ANDERSON Ross J., Étude financée par Microsoft dans le but de pouvoir vérifier à distance la validité des licences des logiciels utilisés… http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf,

- DENNING, D.E . et W.E. Baugh JR, *Cases Involving encryption in crime and terrorism*, http://guru.cosc.georgetown.edu/~denning/crypto/cases.html,

- BONAVENTURE Olivier : « encryptage en Belgique : La loi ». http://pgp.netline.be/cryptage/loi.html .

- BORTMEYER Stéphane, «L'Utilisation du chiffrement en France». http://web.cnam.fr/Network/Crypto/

- MALHEY Bruno, «Législation sur la cryptographie». http://ns.urec.fr:70/00/Securite/Docs/Lois/chiffrement.txt

- ZIMMERMANN, Philip, « Pourquoi j'ai écrit PGP », Mode d'emploi de PGP freeware version. http://www.ifi.uio.no/pgp/

- la Fondation Omega de Manchester, "Une évaluation des techniques de contrôle politique", PE 166.499. http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm.

- MARIE, Fabrice, *Histoire de la cryptologie*, http://www.multimania.com/marief

Divers

- PARISIEN, Serge et Pierre TRUDEL, « L'identification et la certification dans le commerce électronique », *Rapport final*, Montréal, Centre de recherche en droit public, avril 1996, p.84
- *Memorandum* présenté par la France aux Etats membres de l'Union européenne lors des Conseils du 26 février 1998 (Télécommunications) et du 9 mars (Ecofin) , « Créer un environnement communautaire et international pour développer le commerce électronique ».
- GUERRIER, Claudine Maître de conférences, "Le droit actuel de la cryptologie est-il adapté aux utilisateurs d'Internet ? ", INT (Institut National des Télécommunications) Rue Charles Fourier – 91011 Evry, France Maître de conférences, spécialisée dans le droit des TIC.
- Les dix mesures pour le développement du commerce électronique présentées le 6 mai 1998 par Dominique Strauss-Kahn,ministre de l'Économie, des Finances et de l'Industrie, Ministère de l'Économie, des Finances et de l'Industrie 07/05/1998.