Sécurité technique et cryptologie dans le commerce électronique en droit français

Eric A. CAPRIOLI (*)

NTRODUCTION

Le projet de loi sur les télécommunications, suite à l'amendement Fillon déposé au Sénat, prévoyait que la régulation et le contrôle du contenu des informations diffusées sur Internet devaient être assurés par le Conseil Supérieur de la Télématique, organisme rattaché au Conseil Supérieur de l'Audiovisuel. Sous réserve de proposer à leurs clients des moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, les fournisseurs d'accès étaient exonérés de leur responsabilité pénale. L'article 15 de la nouvelle loi de règlementation des télécoms du 26 juillet 1996[1] intégrait trois articles numérotés 43-1, 43-2 et 43-3 dans la loi du 30 septembre 1986 relative à la liberté de communication. Cependant, par sa décision ndeg.96-378 en date du 23 juillet 1996, le Conseil Constitutionnel a déclaré inconstitutionnel les articles 43-2 et 43-3 du projet de loi [2]. Le législateur a méconnu la compétence qu'il tient de l'article 34 de la Constitution en ne définissant pas les principes que doit respecter le Conseil supérieur de la télématique lors de ses recommandations et avis. Entre autres choses, la loi réservait à un organe administratif le pouvoir de censurer ou non un serveur ; il appartient, en effet, selon le Conseil constitutionnel

<< au législateur d'assurer la sauvegarde des droits et des libertés constitutionnellement garantis ; que s'il peut déléguer la mise en oeuvre de cette sauvegarde au pouvoir réglementaire, il doit toutefois déterminer lui-même la nature des garanties nécessaires, ..., il a confié au Conseil supérieur de la télématique le soin d'élaborer et de proposer à l'adoption du Conseil supérieur de l'audiovisuel, auprès duquel il est placé, des recommandations propres à assurer le respect par certains services de communication de règles déontologiques, sans fixer à la détermination de ces recommandations, au regard desquelles dse avis susceptibles d'avoir des incidences pénales pourront être émis, d'autres limites que celles, de caractère très général, résultant de l'article 1er de la loi du 30 septembre 1986 >>.

La tentative de réguler Internet a échoué. Cependant, l'adoption de l'article 15 de la loi intègre un nouvel article 43-1 dans la loi du 30 septembre 1986 relative à la liberté de communication [3]. Ainsi, cette loi s'applique à tous les réseaux, y compris Internet et le Conseil supérieur de l'audiovisuel est compétent en matière de communications audiovisuelles diffusées sur ceux-ci. Renonçant à une régulation législative, le Gouvernement français s'oriente aujourd'hui vers une solution de régulation plus souple avec l'adoption d'un *<< Code de bonne conduite pour l'autorégulation de l'internet par les professionnels >>*. Pour cela, le Ministre, délégué à la Poste, aux Télécommunications et à l'Espace (M. F. Fillon) a annoncé la création d'un groupe de travail le 24 octobre 1996. Cette mission à un groupe de travail présidé par M. Beaussant (président du Groupement des Editeurs de Services Télématiques[4]). Des propositions sont attendus pour le premier

trimestre 1997. Par ailleurs M. François Fillon a proposé l'adoption d'une Chatre de coopération internationale sur Internet à l'OCDE[5].

La sécurité technique se situe au coeur du commerce électronique ; sans sécurité ni confidentialité point de salut. Par delà le simple rappel des principaux risques techniques liés aux communications de messages électroniques (I), nous examinerons les solutions envisageables au travers des obligations légales françaises en matière de cryptologie (II).

I) Sécurité et risques techniques

Le développement du commerce électronique suppose que les informations soient transmises en parfaite sécurité, c'est à dire dans des conditions techniques permettant d'assurer la confidentialité, l'authentification et l'intégrité des messages échangés. Il ne sera pas question ici d'aborder la question de la confidentialité sous l'angle des données personnelles eu égard à la loi Informatique et liberté ndeg.78-17 du 6 janvier 1978 [6].

Le niveau de sécurité adopté doit correspondre au niveau des risques acceptables d'un point de vue commercial par l'entreprise, d'autant que les procédures de sécurité varient considérablement selon la valeur accordée au message et son type. Sil'on prend l'hypothèse d'un paiement sur Internet basé sur la carte bancaire, la transmission du code confidentiel personnel, du numéro de la carte, de sa date d'expiration et du nom du titulaire, impliquent des procédures de sécurité comme le cryptage des données transmises.

Concernant les techniques de sécurité, il conviendra de se référer aux travaux du Club de la sécurité informatique français (CLUSIF) qui a mis au point une méthode d'analyse des risques permettant de mettre en place les solutions techniques de prévention et de protection. La méthode développée par cet organisme s'intitule Messedi. Nous rappellerons que les pertes dues à des sinistres informatiques ont été évaluées par le CLUSIF à 11,56 milliards de francs en 1995 contre 11,2 en 1994 [7].

Par exemple en matière d'EDI, une bonne protection technique suppose que les parties à l'échange utilisent les technologies les plus avancées ainsi que les réseaux (RVA et numériques). Cela est également vrai pour les paiements sur l'Internet ; en effet, certains systèmes adoptent déjà une approche de tiers certificateur ou tiers de confiance dont le métier sera de garantir la sécurité et la confidentialité des transactions commerciales et financières. D'autres solutions peuvent cependant être envisagées [8].

Sur le plan technique, il existe actuellement une importante palette de moyens de protection mis à la disposition des entreprises. Une étude réalisée par KPMG en 1992 pour le programme TEDIS [9] a inventorié les mécanismes et procédures de sécurité suivants : chiffrement, signatures numériques, gestion des clés, bourrage du trafic, contrôle de l'acheminement, notaire électronique, certification. Ces techniques incluent les différents audits des systèmes et des réseaux de transmission, ainsi que les tests opérés sur les logiciels de communication et sur les réseaux utilisés ; la mise en place d'accusés de réception des messages ; les cartes à puce ; la cryptologie ; la conservation des données ; les "process" de traduction des messages en langage clair ; les procédures de "back up". Par ailleurs, le livre blanc sur la sécurité des systèmes d'information des établissements de crédit comporte des recommandations pour les banques et fournit de précieuses indications méthodologiques à respecter [10].

Outre les pare-feux nécessaires à la sécurité des systèmes d'information pour éviter les intrusions non autorisées, il nous semble indispensable de lister les différents items relatifs à la sécurité juridique et technique des échanges de messages de données.

a) Identification de l'émetteur. L'hypothèse concerne le cas de la fraude à l'expédition de message. Cela recouvre partiellement la question de l'authentification du message. Un dispositif de cryptage permet la mise en oeuvre des procédures de codes d'accès.

b) Principe de non-répudiation des messages. Le destinataire d'un message ne doit en aucun cas être en mesure, après la réception du message, d'affirmer ne pas avoir eu connaissance du message ou de son contenu. A fortiori, cela s'impose en matière de paiement.

c) Intégrité des messages. Il est impératif que le message reçu soit totalement identique à celui qui a été envoyé. Pendant la durée de la transmission aucune modification du message, ni même d'une partie du message, ne peut être tolérée. Cette opération fait partie du dispositif de cryptage. Elle s'effectue au moyen de l'émission d'une information codée qui permet de vérifier que le message transmis ne comporte aucune modification.

d) Retards afférents aux messages. Tous les retards relatifs à la délivrance des messages peuvent être dommageables, surtout lorsque le paiement éteint une obligation (de payer), par exemple les pénalités de retard, le coût des délais de dédouanement pour des marchandises, ...

e) Acheminement erroné des messages. La défaillance du réseau peut entraîner un acheminement accidentel d'un message vers une personne qui n'en est pas le destinataire ou vers une partie du réseau où il n'est pas traité.

f) Perte temporaire ou permanente du service. Toute interruption du système d'information, même limitée à quelques heures, peut causer un préjudice (coupure d'électricité, ...).

g) Conservation des données échangées. Hormis les obligations légales de conservation, variables selon leur modalité et leur durée [11], la mise en place d'un système de conservation de données sur support numérique implique que l'on prenne en compte les éléments suivants : le volume des données à conserver, le support et le format utilisés, la durée de conservation, et enfin le degré de sécurité des données.

h) Divulgation de données confidentielles. L'assurance que les données échangées ne seront pas divulguées ou captées durant le transit constitue une donnée essentielle notamment lorsque l'envoi de données commerciales comporte des informations confidentielles ou personnelles. Le cryptage des données confidentielles pallie le risque en matière de communication de messages ; le dispositif de cryptage a pour but de rendre indéchiffable l'intégralité du message à toutes personnes non autorisées.

II) Obligations légales en matière de cryptologie

Au cours des années passées, les échanges électroniques à caractère commercial s'effectuaient par l'entremise du kiosque télématique de France Télécom, le Minitel. La sécurité des échanges ne posait pas de problème majeur, le système étant fermé. Avec Internet aujourd'hui, comme demain avec les autoroutes de l'information, le réseau est ouvert. Par nature, la sécurité n'est pas l'apanacée des réseaux ouverts. Ainsi, une personne mal intentionnée peut intercepter des messages et avoir accès à des informations relevant du secret

des affaires. L'identité de l'expéditeur, la réception par le destinataire, l'intégrité du message et son interception, (...), constituent des aspects fondamentaux à prendre en considération. La cryptologie est au coeur des questions que l'on se pose au sujet de la confidentialité des transactions et de la sécurité du paiement sur Internet car les procédés techniques mis en oeuvre permettent de prévenir la plupart des risques inhérents à la transmission de messages électroniques. En effet, il est classique de définir la cryptologie comme étant une opération destinée à rendre inintelligibles pour des tiers, par un procédé de chiffrement, les informations communiquées ou conservées sous forme de messages. Internet soulève également du point de vue de la cryptologie des questions relatives aux libertés fondamentales et aux droits de l'homme, mais qui ne seront pas étudiées [12].

En général, on distingue la cryptogie symétrique où une clé identique est utilisée pour crypter et décrypter le (ou les) message(s) envoyé(s) et la cryptologie asymétrique qui utilise deux clés différentes. L'utilisateur distribue sa clé publique et il garde sa clé privée. Seules les personnes autorisées ont accès aux données transmises. Vis-à-vis de l'intégrité des données sur le message, c'est l'association d'une formule mathématique au message qui permet d'en garantir la teneur. La cryptologie permet de prévenir également contre le risque de répudiation des messages. Le plus célèbre système de cryptage, le logiciel "Pretty Good Privacy" (PGP) [13], était pour l'instant interdit d'utilisation en France !

A) Bref historique de la règlementation sur la cryptologie

Depuis le Décret du 18 avril 1939, l'Etat français soumet la cryptologie au régime du matériel de guerre de deuxième catégorie [14]. Le premier assouplissement notable en la matière provient du Décret ndeg.86-250 du 18 février 1986[15]. Aux termes de l'article 28 de la loi ndeg.90-1170 du 29 décembre 1990, inspiré directement du Décret de 1986, "*on entend par prestations de cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en information ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet.*[16] La loi française soumettait les logiciels de cryptographie à déclaration ou à autorisation préalables pour des raisons qui relèvent de la défense nationale et de la sécurité intérieure et extérieure de l'Etat (article 28 al. 2 de la loi) [17]. Le système reposait sur un double mécanisme : déclaration préalable "*lorsque ce moyen ou cette prestation ne peut avoir d'autre objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis*" et demande d'autorisation préalable dans les autres cas ; l'ensemble s'effectuant auprès des services du Premier Ministre (SCSSI). Les sanctions étaient les suivantes (article 28 II de la loi du 29 décembre 1990) : "*Sans préjudice de l'application du code des douanes, sera puni d'une amende de 6.000 F à 500.000 F et d'un emprisonnement d'un mois à trois mois, ou l'une de ces deux peines, seulement quiconque aura soit exporté un moyen de cryptologie, soit fourni ou fait fournir une prestation de cryptologie sans l'autorisation mentionnée au SS 1 du présent article. Le tribunal pourra, en outre, interdire à l'intéressé de solliciter cette autorisation pendant une durée de deux ans au plus, portée à cinq ans en cas de récidive .*>>

Plus concrètement, on peut affirmer que les utilisations des procédés de chiffrement des messages étaient étroitement contrôlées par l'administration. Qu 'en est-il depuis l'adoption de la loi ndeg.96-659 du 26 juillet 1996 de réglementation des télécommunications ? [18]

B) La nouvelle réglementation : Article 17 de la loi du 26 juillet 1996

Après de nombreuses critiques, parfaitement justifiées à notre sens [19], certes si nous pouvons estimer que la législation française s'est assouplie, il n'en demeure pas moins que la liberté accordée reste étroitement contrôlée par les pouvoirs publics. En simplifiant le débat, on peut dire que la position française était difficile à soutenir dans le concert international, surtout à l'heure où l'on entre dans la société de l'information [20]. Il en allait de la compétitivité des entreprises françaises utilisatrices de pouvoir communiquer par des moyens électroniques, en parfaite sécurité, avec leurs partenaires économiques, ainsi que de celle des entreprises qui développent des produits informatiques concurrentiels pour le commerce électronique. En matière de paiement, les établissements bancaires doivent pouvoir créer de nouveaux services adaptés aux besoins de leurs clients et tout spécialement sur Internet, où le problème de base c'est la sécurité.

L'article 28-I définissant la cryptologie, modifié par l'article 17 de la loi, est complété comme suit : << *On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié dans le même objectif.* >> Par l'adjonction de cette phrase, alors que la loi de 1990 ne les définissaient pas, le texte couvre désormais l'ensemble des équipements techniques : équipements de chiffrement d'une communication, codeurs, décodeurs de programmes de télévision, ou de logiciels de chiffrement [21].

Concernant le régime juridique du cryptage, essentiel en matière de commerce électronique, la volonté du législateur consiste à concilier les intérêts de sécurité intérieure et extérieure de l'Etat tout en << *permettant la protection des informations et le développement des communications et des transactions sécurisées.* >> Pour se faire, la loi prévoit différents régimes : de liberté, d'autorisation et de déclaration préalable.

L'utilisation d'un moyen ou d'une prestation de cryptologie ne sera << **libre** >> que dans deux hypothèses :

soit << *elle ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis.* >> Cette disposition vise en principe les systèmes d'identification utilisés par les cartes bancaires et les logiciels de signature électronique. L'objectif consiste à promouvoir le commerce électronique et le courrier électronique [22].

soit elle << *assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par un organisme agréés dans les conditions définies au II.* >> Les conditions d'agrément et de garantie de ces << tiers de confiance >> ou << tiers certificateur >> seront fixées par un décret en Conseil d'Etat. Le rapporteur à l'Assemblée Nationale nous éclaire quelque peu sur l'orientation adoptée << *la procédure (...) est suffisamment contraignante sans qu'il soit nécessaire de surajouter une autorisation.* >>[23]

Dans les autres cas, l'utilisation d'un moyen ou d'une prestation de cryptologie est soumise à **autorisation** du Premier ministre. Par exemple lorsque le moyen ou la prestation assure des fonctions de confidentialité sans passer par un tiers de confiance agréé.

En outre, seront soumis à une autorisation préalable du premier ministre les opérations de fourniture, importation et exportation de moyen ou de prestation de cryptologie de pays n'appartenant pas à l'Union européenne, dès lors qu'ils assurent des fonctions de confidentialité. Un mécanisme de **déclaration préalable** auprès du Premier ministre est prévu dans les autres cas (fonctions d'authentification et d'intégrité). Un décret précisera les modalités d'application du texte.

La loi prévoit également l'instauration d'un système simplifié de déclaration et d'autorisation. <<*Une telle disposition devrait s'appliquer par exemple aux logiciels de cryptologie de faible puissance et concerner des prestations touchant le grand public ou certaines professions. Les << bouquets de services >> commerciaux*

fournis sur abonnement ou les décodeurs de programmes audiovisuels devraient entrer dans cette catégorie. >> [24]

Concernant les sanctions, la loi les renforce. Le nouveau dispositif législatif définit trois infractions en son SS III :

- défaut d'autorisation préalable lors de la fourniture, l'importation de pays non membres de l'Union européenne ou l'exportation de moyens ou prestations de cryptologie : six mois d'emprisonnement et 200.000 francs d'amende ;

- défaut d'agrément du tiers : deux ans d'emprisonnement et 300.000 francs d'amende ;

- fourniture ou utilisation de moyens ou prestations de cryptographie ayant permis un crime ou délit : cinq ans d'emprisonnement et 500.000 francs d'amende).

Ainsi, la liberté n'est pas totale, elle est encadrée par un dispositif législatif et règlementaire rigoureux pour tout ce qui touche à la confidentialité. Seules les fonctions d'authentification et d'intégrité des messages incarnent le principe de liberté.

A titre d'exemple, les banques, notamment avec le GIE Cartes bancaires, disposent d'un organisme doté de la confiance et de l'expérience en la matière. D'autres banques ou filiales de banques sont également sur les rangs [25]. Assujetti au secret professionnel, l'organisme agréé, le tiers de confiance, aurait pour mission de recevoir le dépôt des conventions secrètes, de les conserver et de les gèrer pour le compte de l'utilisateur. En fonction de la procédure ouverte, ce tiers devrait par ailleurs remettre les clés de chiffrement aux autorités judiciaires ou ou celles spécialement habilitées à cette fin. Cette dernière mesure sauvegarde les intérêts stratégiques de l'Etat qui peut accéder à l'information, voire l'intercepter. On regrettera cependant que les modalités d'agrément ont été réservées au seul pouvoir réglementaire et qu'elles échappent ainsi au pouvoir législatif. Les tiers devront certainement fournir au SCSSI des garanties techniques, financières, d'indépendance et de bonne moralité (non condamnation pénale), pour obtenir l'agrément. Il semble que l'on s'oriente vers une forme juridique variable (statut privé, public, mixte, ...), mais en tout état de cause, le tiers devra être de nationalité française. Dès lors, les professionnels concernés et les utilisateurs attendent l'adoption des deux décrets d'application qui, en principe, sont prévus pour le début de l'année 1997[26]. De ces textes dépendent les conditions d'agrément des tiers de confiance ainsi que la sécurité dans le commerce électronique.

Notes

(*) Docteur en Droit
Avocat au Barreau de Nice Professeur Associé à l'Université de Nice - Sophia Antipolis.
Expert consultant aux Nations Unies sur le droit du commerce électronique

[1]Lucien Rapp, *Le nouveau droit français des télécommunications : présentation commentée de la loi sur la règlementation des télécommunications*, Cahiers du droit de l'informatique, ndeg.83, Juillet 1996, Fasc. D, p.1-9 et Lionel Costes, *1996 : l'année des profonds changements pour les télécommunications françaises*, Lamy droit de l'informatique, Bull. d'actualité ndeg.83, Juillet 1996.

[2] J.O. du 27 juillet 1996, p.11400 s. et Petites affiches, 26 juillet 1996, p.4.

[3] Article 43-1 : << *Toute personne dont l'activité est d'offrir un service de connexion à un ou plusieurs services de communication audiovisuelle mentionnés au 1deg. de l'article 43 est tenue de proposer à ses clients un moyen technique leur permettant de restreindre l'accès à certains services ou de les sélectionner.* >>, J.O. du 27 juillet 1996, p.11395.

[4] Sur ce projet, consulter : http://www.telecom.gouv.fr.

[5] Ce projet a été présenté le 23 octobre 1996, il comprend trois volets dont le texte intégral peut être consulté à l'adresse électronique suivante : http ://www.telecom.gouv.fr ; v. également : Gaz. Pal. des 11 et 12 décembre 1996, Au fil du net, p.9-10.

[6] La loi informatique et liberté s'applique sur Internet dans la mesure où l'on réalise un traitement automatisé des données personnelles collectées. V. spéc. Herbert Maisl, *La protection des données et des systèmes, in Le droit du multimédia, De la télématique à Internet,* Paris, éd. du Téléphone, Rapport AFTEL, 1996, p.167 s., v. égal. d'un point de vue plus général : Jean Frayssinet, *Informatique fichiers et libertés*, Paris, Litec, 1992, Préface de Jacques Fauvet.

[7] Lamy Droit de l'informatique, Bull. d'actualité ndeg.81, Mai 1996, B, v. les tableaux p.17-18.

[8] Conseil national du Crédit (Rapporteur M. J.-Y. Gresser), *EDI financier & paiements, Vers de nouveaux services bancaires aux entreprises*, Paris, éd. AFNOR, Septembre 1995.

[9] Commission des Communautés européennes, *EDI et sécurité : comment gérer le problème ?*, Luxembourg, 1992, v. p.24 s.

[10] Commission bancaire, *Livre blanc sur la sécurité des systèmes d'information*, Paris, Janvier 1995. Pierre-Yves Thoraval, *Informatique bancaire : le livre blanc sécurité*, Banque, Février 1995, p. 68 s.

[11] V. Isabelle de Lamberterie, *La valeur probatoire des documents informatiques dans les pays de la C.E.E.*, R.I.D.C. 1992, ndeg.3, spéc. p. 641 s. et Eric A. Caprioli, *Contribution au régime juridique de la conservation des documents : du papier au message électronique*, Droit de l'informatique et des télécoms 1993/3, p. 5 s.

[12] Nancy Risacher, *Internet et la protection des droits fondamentaux de la personne humaine*, Lamy droit de l'informatique, Bull. d'actualité ndeg.82, Juin 1996, p.1-4.

[13] Planète Internet, Avril 1996, *Le croisé de l'intimité numérique*, p. 41 s.

[14] Assemblée nationale, Rapport de M. Claude Gaillard, ndeg.2750 du 30 avril 1996, v. p.215.

[15] L'article 223 du traité de Rome autorise exceptionnellement les Etats membres de la communauté à s'opposer au principe de libre circulation des marchandises et dès lors << *à prendre les mesures qu'ils estiment nécessaires à la protection des intérêts de leur sécurité et qui se rapportent à la production et au commerce d'armes, de munitions et de matériels de guerre.* >> En ce sens, v. le Rapport de M. Claude Gaillard, ndeg.2750, préc. note ndeg.12, p.216.

[16] J.O. du 30 décembre 1990 ; J.C.P. 1991, éd. G, III, 64426. V. également le Décret d'application du 28 décembre 1992

[17] Herbert Maisl, *La protection des données et des systèmes, in Le droit du multimédia, De la télématique à Internet, op. cit.*, p.177-180.

[18]J.O. du 27 juillet 1996, p.11384 s. V. égal. : Frédérique Olivier et Eric Barbry, *Aperçu rapide sur la loi du 26 juillet 1996 de réglementation des télécommunications*, J.C.P. 1996, éd. G, Actualité du 18 septembre 1996.

[19] En ce sens, la prise de position de la Chambre de commerce internationale sur une politique internationale du chiffrement; D.I.T. 1994/2, p.70. << *A l'exception de celles spécialement élaborées à des fins militaires ou diplomatique les conventions de chiffrement ne devraient pas faire l'objet de contrôle à l'exportation ou à l'importation, de restrictions à l'utilisation, d'accords de licences restrictifs, ou de toute autre restriction.* >> En conséquence, selon la C.C.I. les utilisateurs << *devraient être libres d'utiliser et d'appliquer le cadre existant des méthodes de chiffrement généralement disponibles et généralement acceptées et de choisir sans restriction les clés et la gestion des clés.* >> En outre, l'O.C.D.E. a décidé de publier au début de 1997 une série de recommandations sur l'utilisation du chiffrement sur le réseau, v. Le Monde du 29-30 septembre 1996, Cahier Télévision, Radio, Multimédia, p.28.

[20] Commission européenne, *La préparation des Européens à la société de l'information*, Edité par Alain Dumont et Werner Hermann, 1996, EUR 16606 FR/EN.

[21] Sénat, Rapport de M. Gérard Larcher, ndeg.389 du 29 mai 1996, (2 tomes) v. p.215 (tome 1).

[22] Rapport Gaillard, *préc. note ndeg.12*, v. p. 217.

[23] Rapport Gaillard, *préc. note ndeg.12*, v. p. 217.

[24] Rapport Gaillard, *préc. note ndeg.12*, v. p. 220.

[25] V. en ce sens, Rapport Larcher, préc. note ndeg. 19, v. tome 1, p. 217 : << *Il est permis de penser que les banques, certains établissements financiers, les sociétés de services informatiques seront amenés à jouer ce rôle de << tiers de confiance >>.* >>

[26] Pour les premières indiscrétions sur les projets de décrets, v.. Planète internet, Janvier 1997, p.21 et le site http://www.planete-internet.com/crypto/décret.htm