Le droit actuel de la cryptologie est-il adapté aux utilisateurs d'Internet ?

Claudine Guerrier (*)

Le droit de la cryptologie était une réponse aux exigences de la sécurité des Etats. Il est interpellé par les acteurs économiques et est sommé de se plier à leurs exigences, au niveau international, européen, français... Trois axes : tiers de confiance, exportation, écriture numérique cryptée.

La cryptologie fut longtemps considérée comme un instrument de sécurité et de protection pour les Etats-Nations. Elle devient un instrument des échanges dans le monde des affaires globalisé, un enjeu pour le développement du commerce électronique. 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 E.U.A., où les exportations étaient sévèrement limitées. 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. Au Japon, où le taux de criminalité informatique est faible, les ministères japonais de l'Industrie et du Commerce, des Communications, se sont associés pour sécuriser les réseaux. 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, les décrets et les arrêtés de 1998 (1), le chiffrement est libre en France pour l'utilisation des clefs d'une longueur inférieure ou égale à 40 bits. Une mission étudie les conditions du passage à 56 bits. Un régime de déclaration ou d'autorisation s'applique dans la plupart des cas.

Dans le contexte d'Internet, le droit de la cryptologie est appelé à évoluer (2). Les acteurs concernés sont tous d'accord : il est urgent de ne plus attendre. Nos axes privilégiés de réflexion sont les tiers de confiance, l'exportation, l'authentification et la signature.

1- La notion de tiers de confiance, après avoir induit des débats, débouche sur des projets, semble reculer. Le tiers de confiance aurait pour mission de récupérer, de protéger, de gérer les clefs de chiffrement.

L'initiative traduit une convergence d'idées entre plusieurs pays souvent sécuritaires. Les Etats concepteurs sont les E.U.A., le Japon, le Royaume-Uni, l'Allemagne, la France. L'administration Clinton s'est prononcée en 1996 en faveur des tiers de confiance. Le Royaume-Uni a initialisé un travail important au DTI (Department of Trade and Industry). Le projet se base non seulement sur les considérations de protection, mais aussi sur le souci de maintenir la Grande – Bretagne parmi les premières puissances dans le domaine du multimédia. La France a élaboré ses textes dans la discrétion (3).

L'opération de lobbyng en faveur du tiers de confiance a été menée avec une apparente efficacité au sein du G4 et de l'Union Européenne. Le G4 (Allemagne, Grande-Bretagne, France, Pays-Bas) a proposé quatorze conditions auxquelles devaient se soumettre les tiers de confiance pour être agréés. Il s'appuie sur le protocole Royal Holloway de gestion des clefs de chiffrement présenté par le Communications Etectronics Security Group britannique. Son relais au sein de

l'Union Européenne est le Senior Officiers Group for Information Systems Security (SOG-IS), créé en 1993 dans le cadre du programme INFOSEC, présidé par le Britannique David Herson, rattaché à la DG13 (Télécommunications). Il a permis l'introduction du concept de tiers de confiance dans la Communication de la Commission du 8 octobre 1997 (4).

Le tiers de confiance est devenu une néo-réalité au Royaume-Uni et en France. Au Royaume-Uni, le choix du tiers de confiance (TTP : Tierces parties de confiance) est libre et non obligatoire. L'agrément est accordé pour une durée de cinq ans minimum. Les tiers étrangers peuvent demander un agrément s'ils disposent d'un représentant enregistré et les utilisateurs britanniques peuvent recourir à un tiers de confiance étranger. L'accès de la police et des services de renseignements aux clefs ne sera possible que sur présentation d'un mandat. Les tiers de confiance envisagés sont tous des personnes privées, détentrices d'une compétence qui en ferait un interlocuteur privilégié pour l'utilisateur d'Internet. En France, le choix du tiers de confiance est libre, mais obligatoire. L'organisme qui souhaite devenir tiers de confiance adresse une demande auprès du Service central de la sécurité des systèmes d'information. L'agrément est accordé intuitu personae par le Premier Ministre ou son représentant, pour une durée de quatre ans, avec possibilité de renouvellement ; il s'accompagne d'un cahier des charges. Les relations entre le tiers de confiance et l'utilisateur reposent sur la pratique contractuelle. L'accès de la police est réglementé : au stade d'une enquête préliminaire, s'il n'y a pas flagrance, la perquisition ne peut avoir lieu sans l'accord du tiers de confiance qui ferait l'objet de la perquisition. Les tiers de confiance seraient privés ou publics. Le GIE carte bancaire, le notariat sont pressentis (5).

Le rapport de force international semble moins favorable aux tiers de confiance. 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 clefs " par un tiers de confiance sont plus chères et moins efficaces que les produits sans séquestre. Le SOG-IS n'est plus un intermédiaire aussi utile au sein de l'Union Européenne : son mandat n'est pas renouvelé, même si David Herson a annoncé, en 1997, le démarrage de huit projets expérimentaux de tiers de confiance.

Les adversaires des tiers de confiance ont développé une thématique fédératrice. En 1997, l'OCDE évite de se prononcer sur les tiers de confiance dans ses lignes directrices, ou recommandations, qui n'ont pas d'ailleurs valeur contraignante. La Commission européenne finalise en 1998 un projet de directive sur les signatures digitales et la sécurité des communications électroniques. Elle exclut le recours aux tiers de confiance, ainsi qu'au séquestre ou à la récupération des clefs de chiffrement. La Commission est persuadée que le système des tiers de confiance n'est pas fiable. Le Royaume-Uni, alors président de l'Union Européenne, organise un débat public en avril 1998 sur ce projet de directive, avec la participation des six pays candidats à l'Union Européenne, les E.U.A., la Russie, l'OCDE, l'UNCITRAL. La Commission prévoit que les fournisseurs de services de certification seront en mesure de s'installer sans autorisation préalable. L'Autorité de certification peut être perçue comme une solution alternative au tiers de confiance ; cet aspect apparaissait déjà dans la Communication du 8 octobre 1997 (6). Le Royaume-Uni et la France, si le projet de directive est adopté, seront obligés de modifier leur législation. Des réserves se font jour chez les éventuels utilisateurs français. Le droit français considère l'exercice illégal d'une activité de tiers de confiance comme un délit ; or, le délit est difficile à cerner : il n'est pas nécessaire de recourir à un tiers pour établir une communication inviolable. Le tiers de confiance serait une notion politique (intérêt de la cité), non technique. La loi du 26 juillet 1996 précise que les organismes agrées exercent leurs activités sur le territoire national. Des entreprises font remarquer qu'elles pâtiraient de la concurrence étrangère…si les autres pays ne s'imposaient pas de conditions de contrôle analogues. Enfin, des utilisateurs redoutent que les tiers de confiance ne refusent les perquisitions en cas d'enquête préliminaire, par crainte d'un non-renouvellement de l'agrément. Le dossier du tiers de confiance est engagé avec difficultés.

2- L'exportation des moyens et des prestations de cryptologie cristallise les conflits d'intérêts, notamment entre lobbie militaire et utilisateurs d'Internet. Le marché est favorable à la libéralisation de l'exportation de la cryptologie mais n'a pas encore gagné la bataille juridique.

Les références sont internationales, américaines, européennes, françaises.

Les textes internationaux étaient protectionnistes, dans un contexte de guerre froide. Le COCOM (Coordination Committe for Multilateral Export Controls) était spécialisé dans le contrôle de l'exportation des produits et de la technologie à finalité stratégique. Il entretenait des liens étroits avec l'OTAN et fut dissous après l'effondrement du bloc soviétique. Le labeur entrepris au sein du COCOM pour parvenir à un contrôle utile en matière d'exportation cryptographique fut poursuivi. L'arrangement de Wassenaar (publié le 15 janvier 1998 sur le territoire américain) met en place un contrôle des exportations des technologies à double usage. Il s'agit moins de multiplier les contrôles que de concentrer les investigations sur les prestations les plus sensibles.

Pendant des décennies, les E.U.A., s'ils n'imposaient aucune limitation en matière d'importation, ont soumis l'exportation des moyens et des prestations de cryptologie à un régime sévère. Les tenants de la liberté arguent que le contrôle ne se justifie que si la sécurité des E.U.A. est menacée.

La jurisprudence a été partagée, notamment dans les affaires Philip Karn et Daniel Bernstein (7). Au Congrès, des projets d'inspiration libérale ont été présentés. En février 1998, une loi, soutenue officiellement par le FBI, entre en vigueur : elle impose de nouvelles contraintes à l'exportation de super-ordinateurs. L'exécutif souhaite cependant donner des gages aux industriels, qui redoutent de perdre la bataille des logiciels de cryptage sur Internet (8). Au niveau de l'Union Européenne, le Règlement du 19 décembre 1994, connu sous son intitulé : " Règlement Double usage ", instituait un régime de contrôle des exportations des biens à double usage (dont la cryptographie). La Communication du 8 octobre 1997 recommande que le règlement soit révisé en permettant une libéralisation sélective des contrôles actuels.

En Europe, certains pays sont libéraux dans le secteur de l'exportation. La France est au contraire rigoriste. La loi, les décrets, les arrêtés exigent une déclaration ou une autorisation en cas de fourniture, d'importation, d'exportation de moyens et de prestations de cryptologie assurant une fonction de confidentialité hors Union Européenne et hors Espace Economique Européen. Le dossier de demande d'autorisation est envoyé au service central de la sécurité des systèmes d'information. Il comporte une partie administrative et une partie technique. La Commission des lois a souligné que l'Union Européenne constituait un champ d'action privilégié pour les " hackers ". Les industriels français émettent à l'égard de ce contrôle à l'exportation les mêmes réserves que les industriels américains (9).

Une libéralisation des exportations américaines aurait des effets généralisés. Dans le cas contraire, des contrôles seraient maintenus à l'exportation dans les domaines les plus sensibles.

3- Le droit de la cryptologie enregistre les progrès du marché dans un projet de signature électronique, certifiée, chiffrée, authentifiée. Tous les rapports sur le commerce électronique demandent l'intronisation de cette mesure (10).

Le droit américain proclame le droit des citoyens à utiliser la cryptologie sans restrictions sur le territoire des E.U.A. Néanmoins, le gouvernement exige des utilisateurs le recours à des normes connues, tout en favorisant l'essor de la cryptologie dans le commerce électronique. Le Japon est convaincu que l'authentification par la cryptologie est un instrument de la compétition. L'OCDE, dans le cadre de ses lignes directrices de mars 1997 sur la cryptologie, s'est prononcée en faveur d'une signature cryptée et authentifiée. L'Union Européenne a trouvé un thème porteur dans la signature cryptée. L'expansion d'Internet, le décollage du commerce électronique rendent indispensable une signature numérique, avec deux clefs, la clef-signature, privée, et la clef-vérification de signature, publiée. Le message émis peut alors être chiffré, ce qui assure une garantie supplémentaire. Les autorités de certification authentifieraient le propriétaire. La globalisation des échanges implique la reconnaissance mutuelle des certificats alloués par des autorités de certification

étrangères. L'Union Européenne (cf : la Communication du 8 octobre 1997 et le projet de directive d'avril 1998) est favorable à ces mesures.

L'adoption d'une signature numérique cryptée obligerait certains Etats à modifier leur droit des contrats et leur droit de la preuve. Actuellement, dans de nombreux pays, les signatures autorisées sont manuscrites. En effet, une signature numérique donne la possibilité à une tierce personne de signer un document si elle possède la clef privée. En outre, il n'y a pas équivalence (cf : Belgique, France, Grèce) dans les modes de preuve entre documents électroniques et documents écrits. La forme écrite remplit de plus une fonction d'authenticité.

La France souhaite que des solutions soient trouvées. Elle élabore des propositions dans le mémorandum présenté aux Etats-Membres de l'Union Européenne lors des Conseils du 26 février 1998 (Télécommunications) et du 9 mars 1998 (Ecofin) : " Créer un environnement communautaire et international pour développer le commerce électronique ". Elle prône la comptabilité des infrastructures de clés publiques, appelle de ses vœux une directive sur la reconnaissance mutuelle des autorités de certification. Le Code Civil français serait modifié (11).

S'il n'y a pas unanimité sur les sujets des tiers de confiance et de l'exportation, un consensus se dessine en faveur d'une signature numérique, cryptée, authentifiée.

Conclusion

Le droit de la cryptologie évolue en fonction de l'apparition et de la convergence technologiques (12), des exigences habituelles de la sécurité, et surtout des nouveaux besoins des acteurs économiques.

Pour les utilisateurs d'Internet, la vison apocalyptique d'une dilution de leur patrimoine par des " hackers " de plus en plus efficients ne disparaît pas même si elle est de moins en moins plausible ; par contre, il est probable que les négociations OMC sur le commerce électronique valoriseraient la cryptologie (signature, authentification). Un protocole sera vraisemblablement ratifié à échéance de l'an 2 000. Aussi les utilisateurs d'Internet auront-ils servi une nouvelle association entre un droit de la cryptologie traditionnel et le droit de la concurrence sur les marchés transfrontaliers et régionaux. L'édifice commence à s'édifier.

Sommaire vol 4, numéro 1 (hiver 1998)

Notes

(*) Maître de conférences

INT (Institut National des Télécommunications)
Rue Charles Fourier – 91011 Evry, France
Maître de conférences, spécialisée dans le droit des TIC
Tél. : 01 60 76 46 83

Fax : 01 60 76 43 83
E mail : claudine.guerrier@int-evry.fr

1 : La loi n° 96.659 du 26 juillet 1996 porte sur la nouvelle réglementation des télécommunications, qui applique les directives communautaires. Elle inclut les dispositions dans le secteur de la cryptologie, en reprenant et modifiant des dispositions de l'ancienne LRT (loi de réglementation des télécommunications) du 29 décembre 1990.

Les décrets sont les suivants :

- Le décret n° 98.101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie.

- Le décret n° 98.102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi n° 90.1170 du 29 décembre 1990 sur la réglementation des télécommunications.

- Le décret n° 98.206 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.

- Le décret n° 98.207 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation

Les arrêtés sont les suivants :

- Arrêté du 13 mars 1998 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie.

- Arrêté du 13 mars 1998 définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie.

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

2. Lire notamment A. Bensoussan " Internet, aspects juridiques " Editions Hermès – 1996 ; O. Iteanu " Internet et le droit " Editions Eyrolles – 1996 ; Thierry Piette-Condol et André Bertand " Internet et la loi " Editions Dalloz-Sirey – 1996 ; Olivier Hance " Business et droit d'Internet ", Best of édition – 1996 ; Jérôme Huet " Le droit du multimédia, de la télématique à Internet ", dans le Rapport A.F.T.E.L, Les Editions du téléphone – 1996 ; A.F.D.I.T (Association Française de Droit de l'Informatique et de la Télécommunication) " Internet saisi par le droit " Editions des Parques, 119 rue de Flandre, 75019 Paris – 1997.

3. C'est le Premier Ministre qui, en France, délivre les autorisations dans le domaine de la sécurité (ex : écoutes de sécurité).

4. COM (97) 503 – 8 octobre 1997.

Il est indiqué " La Commission envisage de soumettre une proposition de Décision du Conseil et du Parlement pour un programme INFOSEC II. Le programme pourrait viser à développer des stratégies d'ensemble pour la sécurité des communications électroniques " COM (97) 503 p 21 (I) Programme de soutien.

Une annexe III définit les systèmes de clé sous seing privé, de recouvrement de clé, et le tiers de confiance qui bénéficie de " la confiance des deux parties, l'utilisateur et l'organisme d'Etat ". COM (97) 503 p 33 Annexe III.

5. Le notariat, inconnu aux E.U.A., semble particulièrement apte en France à remplir avec efficience le rôle de tiers de confiance. Un comité " Ialta " envisage d'organiser en France la profession de tiers de confiance. Un code de déontologie a été étudié par les pouvoirs publics et les utilisateurs. Il conviendrait de respecter la confidentialité, d'éviter les conflits d'intérêts. L'administration, des personnes morales et physiques privées seraient associées à l'élaboration de ce code de déontologie.

6. Les personnes ne désirant pas communiquer leur nom, peuvent choisir un pseudonyme leur permettant de sauvegarder leur anonymat dans les transactions et communications. Celle possibilité est également mentionnée dans la Directive 95/46/CE du 24.10.1995, 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.

7. Dans l'affaire Philip Karn la Cour du district de Washington soutient que les restrictions à l'exportation ne constituent pas une violation du premier amendement de la Constitution (Décision du 22 mars 1996).

Dans l'affaire Daniel Bernstein, en Californie du Nord, le juge considère que la régulation en matière d'exportation est une limitation à la liberté d'expression. (Décision du 18 décembre 1996).

8. Le 15 avril 1998, devant des entrepreneurs spécialisés dans les hautes technologies, le secrétaire d'Etat du Commerce Daley déclare " Notre politique de cryptage, comble de l'ironie, encourage la croissance des fabricants étrangers mais, parallèlement, retarde notre croissance ". Daley mentionne que fin 1997, 29 pays en dehors des E.U.A. produisaient 656 modèles de cryptage : " Il y a de grands producteurs en Allemagne, au Canada, en Irlande, en Israël et en Grande-Bretagne ; et la plupart d'entre eux n'ont pas besoin de licences d'exportation pour envoyer leurs logiciels à l'étranger ". Cf Analyse de Sylvie Kauffmann dans " L'Administration américaine est de plus en plus divisée sur le cryptage pour Internet " " Le Monde " Paris, 25 avril 1998.

Voir aussi " The Emerging Digital Economy " Rapport officiel présenté par M. Daley.

9. Dès 1996, Bull s'était joint à d'autres entreprises, surtout américaines, pour présenter des doléances.

10. En outre, en matière d'importation, l'utilisateur français craint d'être sanctionné sévèrement en téléchargeant un serveur hors Union Européenne ; il pourrait procéder à une importation illégale. Lire, surtout, en France le rapport du groupe de travail sur le commerce électronique présidé par François Lorentz (1998).

11. Voir, en particulier, dans le Code Civil français, l'article 1341.

" 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, et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse de somme ou d'une valeur moindre.

Le tout sans préjudice de ce qui est prescrit dans les lois relatives au commerce ".

12. Se reporter notamment au " Livre vert sur la convergence des secteurs des télécommunications, des médias et des technologies de l'information et les implications pour la réglementation ".

COM (97) 623. Bruxelles, 3 décembre 1997.
