DIX ANS DE RÉGLEMENTATION DE LA CRYPTOLOGIE EN FRANCE : DU CONTRÔLE ÉTATIQUE À LA LIBERTÉ CONCÉDÉE

par

Bertrand Warusfel

Maître de conférences à la faculté de droit de Paris V,
Conseil en propriété industrielle

L'histoire du régime juridique de la cryptologie en France a été très mouvementée depuis dix ans. A l'origine (c'est-à-dire avant décembre 1990), les moyens de cryptologie (logiciels ou matériels) étaient considérés comme faisant partie des équipements assimilés aux matériels de guerre et soumis – comme tels – à un régime de prohibition, auquel il ne pouvait être dérogé qu'au cas pas cas sur décision gouvernementale. Un décret de 1986 avait, tout au plus, élargi les conditions dans lesquelles une dérogation pouvait être attribuée aux moyens de cryptologie à usage commercial [1].

1. De 1990 à 1996 : un régime dissuasif pour l'usage du chiffrement

A partir de l'entrée en vigueur de la loi de réglementation des télécommunications du 29 décembre 1990, la perspective fut renversée : d'une situation où la règle était l'application du régime des matériels de guerre et l'exception la "déclassification" de certains matériels commerciaux, on est passé à une situation dans laquelle les moyens de cryptologie ne sont plus des matériels de guerre, sauf dans le cas particulier de moyens de cryptologie *"qui sont spécialement conçus ou modifiés pour permettre ou faciliter l'utilisation ou la mise en oeuvre des armes."* [2]

Cette loi de 1990 a prévu dans son article 28 le principe de la distinction entre deux types de procédure (déclaration préalable ou autorisation préalable) suivant le type de moyen (c'est-à-dire d'équipement) ou de prestation concerné :

- un contrôle par voie de déclaration préalable pour les activités touchant les moyens ou prestations qui n'assurent que la fonction d'authentification ou de contrôle d'intégrité [3] sans permettre le chiffrement des données ;

- un contrôle par voie d'une demande d'autorisation préalable (et, donc beaucoup plus contraignant et restrictif) pour les activités qui assurent réellement une fonction de confidentialité (c'est-à-dire qui chiffre le contenu des messages ou des communications pour le rendre intelligible aux tiers).

Sur la base de cette distinction, les autorités françaises (et, en particulier, le Service Central de la Sécurité des Systèmes d'Information, SCSSI, dépendant du Premier ministre) menèrent jusqu'en 1995-1996 une politique destinée à dissuader les personnes privées d'utiliser des moyens de chiffrement (qui ont l'inconvénient de rendre beaucoup plus délicates les "interceptions" menées par les services de sécurité ou décidées par la justice) tout en leur facilitant l'accès aux technologies de signature (qui permettent de sécuriser l'accès aux réseaux informatiques ou le télépaiement).

Mais l'arrivée sur le marché de l'Internet et – avec lui – l'intégration dans la plupart des logiciels standards (notamment navigateurs Web ou logiciels de messagerie) de moyens de chiffrement (dont certains mettant en œuvre le logiciel PGP, *Pretty Good Privacy*, mis au point par l'informaticien américain Phil Zimmermann) obligèrent la France à assouplir sa position en matière de chiffrement.

---

[1] Décret n° 86-250 du 18 février 1986.

[2] Article 28.VI de la loi n° 90-1170 du 29 décembre 1990 modifiée. L'article 10 du décret du 28 décembre 1992 ne mentionnait, pour sa part, que les moyens *"conçus ou modifiés pour les besoins militaires"* (Décret n° 92-1358 du 28 décembre 1992 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, *J.O.R.F.*, 30 décembre 1992, p. 17915).

[3] C'est-à-dire s'assurer de l'identité de l'émetteur (authentification) ou du fait que le message n'a pas été altéré depuis son émission (contrôle d'intégrité), fonctions qui peuvent être mis en œuvre par le biais de ce que l'on appelle aujourd'hui les "signatures électroniques".

Publié in *Annuaire français de relations internationales*, n° 1, 2000, pp. 657-661

2. 1996 : la tentative d'une réforme de compromis

Sur le plan technologique, le SCSSI s'appuya d'abord sur le fait que la législation de contrôle des exportations fédérale américaine ne permettait alors d'exporter librement vers l'Europe que des produits dont le chiffrement ne mettait en œuvre que des clés d'une longueur maximale de 40 bits [4]. A partir de 1994-1995, le SCSSI commença à autoriser, au cas par cas, certains logiciels standards mettant en œuvre un chiffrement à 40 bits (en particulier, les premières versions des navigateurs Navigator de Netscape et Explorer de Microsoft, qui mettaient l'un et l'autre en œuvre le protocole de sécurité SSL dans une version export limitée à 40 bits).

Par ailleurs, le gouvernement français, conscient de ce qu'il serait rapidement nécessaire d'offrir aux entreprises françaises des solutions de chiffrement de plus haut niveau, afin qu'elles puissent se protéger contre la piraterie informatique, commença à étudier un concept apparu à l'origine aux Etats-Unis : le séquestre de clés, système dans lequel l'utilisateur met en œuvre un algorithme de chiffrement fort (ce qui accroit sa protection) en contrepartie du dépôt d'une clé de déchiffrement auprès d'un tiers (ce qui permet alors à l'Etat de procéder aux éventuelles déchiffrements dont il pourrait avoir besoin, en cas d'interception).

Ces orientations qui visaient à permettre une certaine libéralisation de l'usage de la cryptologie tout en maintenant un contrôle et en préservant les capacités d'interception étatiques, furent concrétisées dans la loi sur les télécommunications du 26 juillet 1996 qui modifia et compléta la loi précédente de 1990.

Cette loi conservait la distinction entre la procédure déclarative réservée aux produits de signature et la procédure d'autorisation pour les produits de chiffrement, mais elle y introduisait trois dérogations possibles :

1°) l'usage des moyens de signature devint automatiquement libre (dès lors que le fournisseur avait préalablement déclaré le produit) ;

2°) la loi de 1996 permit au gouvernement d'établir une liste de produits de chiffrement pour lesquels la procédure déclarative se substituerait à la procédure d'autorisation. Mais il fallut attendre jusqu'au début de 1998 pour les produits de chiffrement dont la clé ne dépassait 40 bits puissent – sous certaines conditions techniques – bénéficier de ce changement de régime [5] ;

3°) la loi décida que seraient totalement libres d'usage tous les systèmes de chiffrement (quel que soit leur niveau de sécurité et la taille de leurs clés) dès lors que ceux-ci mettraient en oeuvre un système de séquestre de clés de confidentialité auprès d'un tiers agréé par le Premier ministre [6].

Ce dernier volet de la réforme [7] était le plus original et avait été conçu pour avoir les conséquences les plus importantes. Le projet gouvernemental était d'offrir aux entreprises françaises l'accès au chiffrement fort tout en facilitant l'action de l'Etat et en créant sur le marché français une catégorie nouvelle d'intermédiaires de sécurité informatique, fortement contrôlés par l'Etat (puisqu'agréés par le Premier ministre). Et le SCSSI comptait sur cette alternative pour échapper au déferlement en France de logiciels sécurisés non contrôlables et dont l'interception serait très difficile (si ce n'est impossible).

---

[4] Depuis lors, ce niveau d'exportabilité a été porté à 56 bits, et pour certains produits, à 128 bits.

[5] Cf. le décret n° 98-206 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 (*J.O.R.F.*, 25 mars 1998, p. 4449).

[6] Article 28-I 1° a) et 28-II de la loi du 29 décembre 1990, tels que modifiés par l'article 17 de la loi du 26 juillet 1996.

[7] Que l'on appela souvent improprement, le système des "tiers de confiance", alors que le terme n'est pas mentionné dans la loi et qu'en toute logique ces tiers étaient tout au plus des "tiers de séquestre.

Publié in *Annuaire français de relations internationales*, n° 1, 2000, pp. 657-661

3. 1999 : la transition vers la libéralisation complète du chiffrement

Très discutée dès son annonce, cette réforme fut rapidement un échec. En effet, pour les mêmes raisons de délais administratifs (accrus, visiblement, par des querelles internes et des combats d'arrière-garde), le décret fixant le statut et les conditions d'exercice des tiers de séquestre ne parut qu'en février 1998 [8], ce qui repoussa l'agrément du premier tiers à la fin de cette même année. De plus, durant la même période, les industriels de l'informatique américains et européens s'étaient divisés sur la question des systèmes à séquestre de clés et, notamment, un groupe important d'entre eux (réunis autour d'IBM dans la "Key Recovery Alliance") avaient promu un système de récupération des clés qui s'avérait être une alternative technique au système prôné en France, sans qu'il soit sûr d'être juridiquement équivalent. Enfin – et surtout – l'essor irrésistible de l'Internet et des solutions de communication suscita un besoin croissant de confidentialité dans les échanges et l'émergence de nouveaux standards internationaux en matière de sécurité.

Le Premier ministre, Lionel Jospin tira les conséquences de l'incapacité de ses services à imposer un système de séquestre lors de son allocution du 19 janvier 1999 à Hourtin. Il annonça *"un changement fondamental d'orientation"*, reconnaissant que *"les dispositions issues de la loi de 1996 ne sont plus adaptées"* et proposa de *"rendre complètement libre l'usage de la cryptologie en France, tout en adaptant les moyens des pouvoirs publics pour garantir les libertés publiques dans ce nouvel environnement et pour lutter contre l'utilisation des moyens de chiffrement à des fins délictueuses."* [9] La nouvelle politique annoncée s'articulerait autour de deux axes : "*offrir une liberté complète dans l'utilisation des produits de cryptologie, sous la seule réserve du maintien des contrôles à l'exportation découlant des engagements internationaux de la France"* [10] et *"supprimer le caractère obligatoire du recours au tierces parties de confiance pour le dépôt des clefs de chiffrement."*

Cette nouvelle politique s'est traduite immédiatement par l'adoption de nouveaux textes réglementaires mettant en œuvre une étape supplémentaire de la libéralisation du commerce et de l'usage de la cryptologie [11] :

- s'agissant des produits de chiffrement dont la clé ne dépasse pas 40 bits, leur régime a été encore allégé, puisque désormais leur importation et leur utilisation sont totalement libres, seule leur fourniture demeurant soumise à déclaration ;

- la procédure déclarative fut élargie à tous les produits de chiffrement utilisant une clé comprise entre 40 et 128 bits (dont l'utilisation et l'importation peuvent même ne pas nécessiter de déclaration préalable dans certains cas particuliers [12]) ;

- enfin, la libéralisation de la fourniture des produits de signature fut poussée avec le passage sous un régime déclaratif simplifié [13].

---

[8] Décret n° 98-102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications (*J.O.R.F.*, 25 février 1998, pp. 2915-2916).

[9] Cf. la déclaration du Premier ministre reproduite in *Droit & Défense*, n° 98/4, p. 77.

[10] C'est-à-dire le maintien d'un contrôle des exportations de moyens de chiffrement utilisant des clés supérieures à 56 bits, conformément aux engagements pris au sein de l'Arrangement de Wassenaar et retranscrits dans la liste de contrôle des biens à double usage publiée par l'Union européenne.

[11] Décret n°99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation ; Décret n°99-200 du 17 mars 1999 les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable ; Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie (*J.O.R.F.* du 19 mars 1999, pp. 4050-4053).

[12] Notamment lorsque le produit est "*exclusivement destiné à l'usage privé d'une personne physique*" (ce qui est une notion difficile à apprécier, cf. Marie Pasquier "Une étape importante dans la libéralisation de la cryptologie", *Droit & Défense*, n° 99/1, pp. 72-73).

[13] C'est-à-dire, le dépôt d'un simple formulaire administratif sans fourniture d'un dossier technique détaillé.

Publié in *Annuaire français de relations internationales*, n° 1, 2000, pp. 657-661

Par ailleurs, une nouvelle loi – modifiant sensiblement les dispositions de 1996 – a été annoncée pour le courant 2000, qui devrait poursuivre vers la voie d'une libéralisation presque complète de l'usage de la cryptologie et revoir complètement le statut des tiers de séquestre. En contrepartie, ce nouveau texte devrait sans doute renforcer les pouvoirs de l'État en ce qui concerne la remise du contenu clairs des messages chiffrés interceptés ou découverts lors d'une perquisition [14].

Conclusion :

Un tel historique illustre quelques-uns des particularismes du modèle français en matière de technologies de l'information. On y voit bien ressortir quelques éléments dynamiques :

- la volonté française de maîtriser les évolutions technologiques et de prendre en compte leurs différentes dimensions (industrielles, économiques, mais aussi juridiques et en termes de sécurité publique ou de sécurité nationale) ;

- l'ambition des autorités françaises de faire jeu égal avec les États-Unis sur certains domaines sensibles en cherchant à la fois à les défier sur le fond (essayer d'éviter la domination de la cryptologie américaine) tout en les imitant sur la forme (la mise en œuvre d'une législation de contrôle nationale contraignante).

Mais les faiblesses sont encore plus frappantes :

- une gestion du temps administratif sans aucune mesure avec la rapidité de diffusion des technologies et de réaction des marchés ;

- un positionnement juridique intransigeant en complet décalage avec les "valeurs" du monde de l'Internet (individualisme, liberté de communication, globalisme) et celles du libéralisme économique dominant ;

- une mauvaise prise en compte de l'impact indirect (mais réel, dans ce dossier) du cadre européen et communautaire, y compris dans des domaines concernant la sécurité nationale ;

- une insuffisante pratique du compromis et de la négociation avec les acteurs privés en vue de faire accepter une solution de compromis originale (celles des tiers de séquestre) ;

- enfin – et surtout - l'incapacité de profiter de ces dix années de relatif protectionnisme pour faire émerger une technologie de sécurité d'origine française capable de concurrencer les standards de fait américains.

A travers cette question, c'est toute une partie de l'"exception française" qui dévoile ici ses limites et qui montre que si l'État colbertiste sait encore s'appuyer sur ses missions régaliennes de sécurité pour jouer un rôle actif sur certains segments du marché des technologies nouvelles, il n'est plus capable de tirer des avantages durables de cette posture.

Bertrand Warusfel

[14] La loi du 10 juillet 1991 qui organise et réglemente les interceptions de sécurité et les interceptions judiciaires ne prévoit pas, en effet, de pouvoirs spécifiques conférés à l'administration pour requérir – en cas de besoin – les informations techniques nécessaires (et, en particulier, la livraison des clé) au déchiffrement des messages ou des communications.

Publié in *Annuaire français de relations internationales*, n° 1, 2000, pp. 657-661