Projet ICare

Régime légal et réglementaire de la cryptologie

Référence : ICARE/CAB/TPC/DOC_25/v1
Type : Document
Diffusion : Membres du consortium

Date : 25/02/2003
Titre : **ICare – Régime légal et réglementaire de la cryptologie**

Sous-Projet :
Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Cette note expose le régime juridique de la cryptologie qui s'applique à la signature électronique, compte tenu de l'utilisation du bi-clé cryptographique et des traitements y afférants.

TABLE DES MATIERES

1 Introduction

La signature électronique basée sur une PKI emploie un bi-clé cryptographique. Ce bi-clé comme toutes les mesures et moyens de cryptologie entre dans un cadre fixé par la loi et précisé par la réglementation.

Cette note a pour but de présenter le régime juridique actuel de la cryptologie.

Marqué à l'origine par un monopole militaire et une interdiction aux activités civiles, le régime juridique de la cryptologie s'oriente cependant vers une libéralisation de plus en plus importante. La libéralisation pourrait devenir totale avec l'adoption du projet de Loi sur la Confiance dans l'Economie Numérique (LEN) qui sera présenté au parlement début mars.

2 Historique et bilan actuel du cadre juridique de la cryptologie

2.1 Une libéralisation par étapes

La cryptologie reposait autrefois sur un décret-loi du 18 avril 1939 complété par le décret du 12 mars 1973 qui classait "les équipements de cryptophonie ou de cryptographie" comme matériels de guerre de deuxième catégorie (décret n°73-364 du 12 mars 1973 relatif à l'application du décret-loi du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, JO du 30 mars 1973). Cette réglementation fit l'objet de nombreuses précisions sur la définition des procédés techniques de cryptologie concernés (décret du 18 février 1986, décret n°86-250 du 18 février 1986), ainsi que sur les conditions de fabrication, de commerce, d'acquisition, de détention et d'utilisation de moyens de cryptologie destinés à des fins professionnelles ou privées sur le territoire national (arrêté du 2 juillet 1990).

Le régime juridique de la cryptographie a été revu par la Loi de Réforme des Télécommunications (LRT), Loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, JO du 30 décembre 1990. Pour la première fois, le législateur reconnaissait que la cryptographie pouvait efficacement contribuer à la sécurisation des télécommunications. La loi créait le distinguo entre la cryptographie utilisée pour garantir d'authentification et d'intégrité et pour garantir la confidentialité. La loi stipulait que pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, la fourniture, l'exportation ou l'utilisation de moyens ou de prestations de cryptologie étaient soumises :

- à déclaration préalable lorsque ce moyen ou cette prestation ne pouvait avoir d'autre objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis ;
- à autorisation préalable du Premier ministre dans les autres cas.

2.2 Le régime actuel

Un nouveau pas vers la libéralisation des Télécommunications a été franchi avec la Loi n°96-659 du 26 juillet 1996 qui, en particulier, est revenu sur le régime de la cryptographie pour le simplifier. Cependant le début de l'année 1998 voit la parution de près d'une dizaine de textes réglementaires, décrets et arrêtés, qui rendent le respect de la réglementation très difficile.

De nombreuses voix s'étant élevées devant la complexité de la réglementation dont celle du Conseil d'Etat, le Premier Ministre annonce dans sa conférence de presse sur le Plan d'Action Gouvernemental pour la Société de l'Information (PAGSI), que le régime réglementaire de la cryptographie datant de février/mars 1998 est retouché avec une élévation du seuil critique des mesures cryptographiques de 40 à 128 bits.

Trois textes ont été publiés au JO du 19 mars 1999 et modifient les textes correspondants antérieurs :

- un 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 (abroge 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, JO du 25 mars 1998) ;

- un décret 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable (abroge le décret n°98-206 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie dispensées de toutes formalités préalables, JO du 25 mars 1998);
- un arrêté du 17 mars 99 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation (abroge l'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, JO du 15 mars 1998).

Suite à la parution des textes 128 bits, l'ensemble des textes régissant la cryptographie se présente de la façon suivante :

1) Article 28 de la Loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, modifié par l'article 17 de la Loi n°96-659 du 26 juillet 1996 de réglementation des télécommunications.
2) Décret no 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, JO du 25 février 1998,
3) Décret no 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 no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, JO du 25 février 1998,
4) Arrêté du 7 mars 99 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation,
5) 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, JO du 15 mars 1998.
6) Arrêté du 13 mars 1998 définissant le modèle de notification préalable par le fournisseur de l'identité des intermédiaires utilisés pour la fourniture d'un moyen ou d'une prestation de cryptologie soumis à autorisation, JO du 15 mars 1998.
7) Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes, JO du 15 mars 1998.
8) Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes, JO du 15 mars 1998.
9) Arrêté du 13 mars 1998 fixant le tarif forfaitaire pour la mise en oeuvre des conventions secrètes au profit des autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi n°90-1170 sur la réglementation des télécommunications, JO du 15 mars 1998
10) Décret 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable,
11) Décret n°99-199 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation,
12) Décret no 2002-997 du 16 juillet 2002 relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi no 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

L'article 28 de la Loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, modifié par l'article 17 de la Loi n°96-659 du 26 juillet 1996 de réglementation des télécommunications, se présente désormais de la façon suivante, le III de l'article 28 qui traite des sanctions pénales aux violations de la législation n'étant pas reproduit :

***Art. 28. - I**. - On entend par prestations de cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet. On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié dans le même objectif.*
Pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, tout en permettant la protection des informations et le développement des communications et des transactions sécurisées :

1°) L'utilisation d'un moyen ou d'une prestation de cryptologie est :

a) Libre :

- si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis,

- ou si le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par un organisme agréés dans les conditions définies au II ;

b) Soumise à autorisation du Premier ministre dans les autres cas ;

2°) La fourniture, l'importation de pays n'appartenant pas à la Communauté européenne et l'exportation tant d'un moyen que d'une prestation de cryptologie :

a) sont soumises à autorisation préalable du Premier ministre lorsqu'ils assurent des fonctions de confidentialité ; l'autorisation peut être subordonnée à l'obligation pour le fournisseur de communiquer l'identité de l'acquéreur ;

b) Sont soumises à la déclaration auprès du Premier ministre dans les autres cas ;

3°) Un décret fixe les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations. Ce décret prévoit :

a) Un régime simplifié de déclaration ou d'autorisation pour certains types de moyens ou de prestations ou pour certaines catégories d'utilisateurs ;

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 susmentionnés, 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.

d) Les délais de réponse aux demandes d'autorisation.

***II. -** Les organismes chargés de gérer pour le compte d'autrui les conventions secrètes de moyens ou prestations de cryptologie permettant d'assurer des fonctions de confidentialité doivent être préalablement agréés par le Premier ministre.*
Ils sont assujettis au secret professionnel dans l'exercice de leurs activités agréées.
L'agrément précise les moyens ou prestations qu'ils peuvent utiliser ou fournir.
Ils sont tenus de conserver les conventions secrètes qu'ils gèrent. Dans le cadre de l'application de la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ainsi que dans le cadre des enquêtes menées au titre des chapitres premier et II du titre II du livre premier du code de procédure pénale, ils doivent les remettre aux autorités judiciaires ou aux autorités habilitées, ou les mettre en œuvre selon leur demande.
Lorsque ces organismes remettent les conventions secrètes qu'ils gèrent dans le cadre des enquêtes menées au titre des chapitres premier et II du titre II du livre premier du code de procédure pénale, suite aux réquisitions du procureur de la République, ils informent les utilisateurs de cette remise.
Ils doivent exercer leurs activités agréées sur le territoire national.
Un décret en Conseil d'Etat fixe les conditions dans lesquelles ces organismes sont agréés ainsi que les garanties auxquelles est subordonné l'agrément ; il précise les procédures et les dispositions techniques permettant la mise en œuvre des obligations indiquées ci-dessus.
III. ...

3 Panorama de la réglementation

La base légale reste et demeure l'article 28 de loi de réglementation des télécommunications. La législation définit 4 *finalités* pour les moyens cryptographiques : la fourniture, l'utilisation, l'importation et l'exportation. Le décret n°99-200 liste une série de matériels et équipements et définissant par finalités s'il y a lieu de procéder à des formalités. Certains éléments de cette liste sont nouveaux et traduisent les intentions de réaménagement du Gouvernement. Compte tenu de l'élévation du seuil de 40 à 128 bits, le décret n°99-199 indique les mesures cryptographiques qui dépendront désormais d'une déclaration au lieu d'un régime d'autorisation. Quant à l'arrêté, il met à jour le formulaire à remettre au SCSSI pour les déclarations / autorisations et pose un nouveau principe qui pourrait poser quelques difficultés à l'usage puisqu'il s'agit du dépôt en deux exemplaires des matériels ou logiciels mettant en œuvre les prestations cryptographiques

A partir de ces 3 nouveaux textes, le dispositif se présente désormais ainsi qu'il suit :

- En ce qui concerne la signature électronique et les notions proches :

Pour les moyens et prestations concernant …
- la protection des mots de passe, des codes d'identification personnels ou des données d'authentification similaires,
- l'utilisation pour contrôler l'accès à des données, à des ressources, à des services ou à des locaux,
- l'élaboration ou la protection d'une procédure de signature, une valeur de contrôle cryptographique, un code d'authentification de message ou une information similaire,
- la vérification de la source des données,
- la preuve de la remise des données au destinataire,
- la détection des altérations ou de modifications susceptibles de porter atteinte à l'intégrité des données,

⇨ seuls les fournisseurs sont assujettis aux formalités. Les utilisateurs, importateurs et exportateurs sont exonérés.

Limitation : comme auparavant, ces moyens et prestations ne doivent pas permettre le chiffrement des données.

- En ce qui concerne la confidentialité :

⇨ Pour les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme à clé d'une longueur inférieure ou égale à 40 bits, l'utilisation est libre ainsi que l'importation / exportation. Seul le fournisseur se voit imposer une formalité de déclaration (autorisation dans le régime antérieur).

⇨ Pour les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme à clé d'une longueur comprise entre 40 et 128 bits, les utilisateurs et les importateurs sont dispensés de formalités qui incombent aux fournisseurs (et exportateurs), à la condition d'un usage privé par une personne physique ou à condition d'une déclaration par le fournisseur (ou importateur),

⇨ Pour les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme à clé d'une longueur comprise entre 40 et 128 bits, dans les autres conditions, les fournisseurs, les utilisateurs et les importateurs souscriront une déclaration (au lieu d'une autorisation). L'exportation suppose une autorisation.

⇨ Pour les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme à clé d'une longueur de plus de 128 bits, toutes les finalités supposent une autorisation.

4 Les organismes agréés

Les "organismes agréés" correspondent à ce qu'on appelle dans un monde non juridique les "Tiers de confiance" (TC). Ces Tiers interviennent dans la mise en oeuvre de mesures ou de moyens cryptographiques qui permettent aux utilisateurs finaux d'assurer la confidentialité de leurs échanges électroniques. La Loi française encadre étroitement l'utilisation de la cryptographie. Utilisée afin de garantir la confidentialité des échanges électroniques, la cryptographie nécessite des formalités administratives préalables complexes. Les formalités pèsent sur l'utilisateur, sauf s'il recourt aux services d'un Tiers de Confiance. Ce dernier devra assurer des formalités qui deviendront ainsi transparentes pour l'utilisateur. Le régime juridique applicable aux organismes agréés / tiers de confiance se distingue fondamentalement du régime des "Tiers certificateurs" qui participent à la mise en oeuvre de la signature électronique et dont la création et la pratique professionnelle restent libres.

Les textes réglementaires utilisent des termes et concepts dont la définition et le contenu demandent parfois à être précisés. On peut les trouver ci-dessous avec le sens que leur donnent les textes :

- "autorités habilitées" : autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi du 29 décembre 1990 ;
- "certification de conventions secrètes" : l'opération qui consiste à calculer une signature numérique ou un code d'authentification assurant la faculté d'emploi des conventions secrètes;
- "client" ou "utilisateur" : personne morale ou physique ayant passé un contrat avec le gestionnaire ;
- "conventions secrètes" : des clés non publiées nécessaires à la mise en oeuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;
- "gestion de conventions secrètes" : prestation consistant en la détention, la certification, la distribution ainsi que, éventuellement, la génération des clés dans les conditions définies au cahier des charges ;
- "gestionnaire" : l'organisme agréé auquel est confiée la gestion, pour le compte d'autrui, des conventions secrètes de cryptologie permettant d'assurer des fonctions de confidentialité, au sens du II de l'article 28 ;
- "mise en oeuvre des conventions secrètes" : opération de restitution des données claires d'un utilisateur, effectuée à la demande d'une autorité habilitée après fourniture par cette autorité des données chiffrées.
- "remise des conventions secrètes" : opération de délivrance des conventions secrètes d'un utilisateur à une autorité habilitée qui le requiert.

4.1 La procédure d'agrément

La composition du dossier de demande d'agrément est présentée, puis la procédure est décrite.

4.1.1. La constitution du dossier d'agrément

Le dossier d'agrément doit comprendre un certain nombre de pièces énumérées par l'arrêté correspondant du 13 mars 1998. Selon l'article 1 de l'arrêté, il s'agit de :

- l'ensemble des pièces établissant l'identification du demandeur : l'identité et structure juridique,
- un document décrivant la politique de sécurité de l'organisme,
- le contrat de service ou l'abonnement que l'organisme propose à ses clients,
- un exemplaire signé du cahier des charges proposé par le demandeur.

Identification de l'entreprise : Pour les entreprises qui se porteraient candidates, les pièces attestant de l'identité et de la structure juridique de l'organisme demandeur sont les suivantes :

- nom, raison sociale,
- adresse du siège social et numéro de téléphone,
- numéro SIRET,
- extrait du registre du commerce et des sociétés.

Les sociétés de capitaux devront indiquer la répartition du capital de la société. Les sociétés de personnes fourniront un extrait du registre du commerce et des sociétés, la fiche individuelle d'état civil et de nationalité de chaque associé et une répartition des parts sociales de la société.

Le cahier des charges : Le cahier des charges est l'élément central du dossier d'agrément. Ce cahier des charges n'est pas donné au candidat en même temps qu'il reçoit l'agrément. Il doit être rédigé, accepté (signé) préalablement par le candidat et joint au dossier de demande. Il s'agit d'un véritable engagement contractuel unilatéral. Selon le Décret, le cahier des charges comprend les éléments suivants:

- L'énumération des moyens ou des prestations de cryptologie dont l'organisme agréé est autorisé à gérer les conventions secrètes ;
- L'énumération des moyens ou des prestations de cryptologie que l'organisme agréé peut utiliser ou fournir ;
- Les conditions techniques ou administratives garantissant le respect des obligations imposées à l'organisme agréé ;
- Le nombre de personnes "habilitées" ;
- Les conditions dans lesquelles sont remises à un autre organisme agréé les conventions secrètes en cas de cessation d'activité ou à la demande de l'utilisateur ;
- Les dispositions techniques prises lors de la mise en service des conventions secrètes afin de permettre, pour chaque message ou communication protégé à l'aide de ces conventions, d'identifier l'organisme agréé les gérant ainsi que les utilisateurs concernés; - Les conditions techniques d'utilisation des conventions secrètes, des moyens ou des prestations et les mesures nécessaires pour assurer leur intégrité et leur sécurité ;
- Le format électronique standardisé dans lequel doivent être transcrites les conventions secrètes en cas de cessation d'activité ou de retrait d'agrément.

Le cahier des charges doit comporter également une annexe classifiée précisant les modalités pratiques de remise des conventions secrètes au SCSSI. Sous le terme de "remise" est visée la démarche des pouvoirs publics ordonnant au Tiers de Confiance la fourniture des éléments cryptologiques du client nécessaires au déchiffrement de ses échanges électroniques. Ce point particulièrement crucial est la cause centrale de tout le dispositif légal : le déchiffrement des messages et fichiers électroniques de l'utilisateur par le SCSSI pour pouvoir les lire. C'est à cette occasion que le Tiers trahit la confiance que lui accorde son client par ordre de la loi. Toute remise devra pouvoir être "traçée". Ainsi deux registres spéciaux seront créés : l'un pour les demandes effectuées par les autorités judiciaires, l'autre pour les demandes effectuées dans le cadre du titre II de la loi du 10 juillet 1991 (questions relatives aux interceptions de sécurité par l'administration).

Le régime du registre des autorités administratives est le suivant : le registre est enfermé dans une armoire forte placée dans la zone à accès contrôlé. Il se présente sous forme de cahiers reliés, aux pages numérotées par imprimerie dont aucune page ne doit être supprimée. Ce registre est classifié secret défense. Son accès est limité au Premier ministre et à la Commission nationale de contrôle des interceptions de sécurité ainsi qu'aux agents spécialement désignés par l'une ou l'autre de ces autorités. Les informations suivantes devront y être consignées, exclusivement :
- la date et l'heure de la demande,
- la durée de l'autorisation,
- la référence de l'ordre de communication des conventions secrètes.

Le régime du registre des autorités judiciaires est le suivant : Il est également enfermé dans une armoire forte placée dans la zone à accès contrôlé et se présente comme le registre précédent. Les informations suivantes y seront portées :
- la date et l'heure de la demande,
- l'identité des personnels ayant reçu la demande,
- les références de la commission rogatoire ou de la réquisition judiciaire,
- la durée de l'autorisation avec éventuellement la prolongation afférente.

A l'exception de cette annexe classifiée, le contenu de ce cahier des charges peut être communiqué, sur leur demande, aux clients. Pour aider le candidat dans sa rédaction, un modèle de cahier des charges est annexé à l'arrêté du 13 mars 1998 (fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes).

Le document "Politique de sécurité" : Le dossier doit comprendre un document relatant la Politique de sécurité du demandeur. Cette Politique s'envisage sous les 4 axes suivants : sécurité appliquée aux prestations, aux personnels, aux locaux et aux systèmes informatiques. La Politique de Sécurité est définie par un document spécifique mis en œuvre et dont l'application est contrôlée par le responsable de la sécurité. Ce document doit être porté à la connaissance de tous les employés du TC ayant une responsabilité en ce domaine. Il est approuvé personnellement par le plus haut responsable du TC. La loi fait obligation au TC d'intégrer dans sa Politique de Sécurité au minimum les éléments suivants :
- la définition des objectifs de sécurité du gestionnaire, en particulier ceux concernant son activité principale et la gestion des conventions secrètes ;
- les règles de sécurité et le rappel des sanctions disciplinaires et pénales applicables en cas de manquement à ces règles ;

- la présentation de l'organisation de sécurité interne, en particulier les procédures d'information et de responsabilisation du personnel, de contrôle de l'application des règles de signalement et de traitement des incidents.

Les personnels doivent s'engager personnellement à respecter le contexte sécuritaire. Ils doivent d'ailleurs présenter une compétence certaine dans ce domaine et un certain nombre d'entre eux doivent être habilités "défense".

Les opérations techniques et traitements centraux concernant la cryptologie, les clés et les certificats électroniques doivent se dérouler dans une enceinte spéciale, tout particulièrement sécurisée : la "zone d'accès contrôlée". Le TC devra communiquer au SCSSI la localisation de la zone, la description des dispositifs de sécurité mis en place et la liste des personnels autorisés. Toute intrusion ou toute tentative d'intrusion visant à pénétrer dans cette zone donne lieu au dépôt d'une plainte dans les vingt-quatre heures suivant sa découverte. De plus, le gestionnaire devra restaurer les dispositifs de sécurité dans les meilleurs délais.

Le contrat de service ou l'abonnement : Les relations juridiques du Tiers de Confiance avec son client sont organisées dans le cadre traditionnel d'un "contrat de service". La loi lui donne cependant un aspect formaliste puisque ce contrat est obligatoirement écrit et qu'elle énumère des clauses obligatoire. Le contrat devra mentionner les conditions légales et réglementaires s'appliquant au service, en particulier :

- les règles d'emploi des moyens et des conventions secrètes distribuées ;
- Un engagement de l'organisme agréé relatif à la sécurité des conventions secrètes qu'il gère pour le compte de l'utilisateur ;
- les sanctions encourues par le client en cas de mauvais usage ou de détournement du moyen dont le gestionnaire gère les conventions secrètes ;
- les sanctions encourues par le gestionnaire en cas de perte, vol ou altération des conventions secrètes d'un client ;
- La référence de l'agrément, la durée et la date d'expiration prévues par cet agrément, ainsi que tout élément d'information que le cahier des charges imposerait de communiquer aux utilisateurs ;
- Les modalités selon lesquelles l'utilisateur, ou toute autre personne éventuellement mandatée par celui-ci, pourra, à sa demande, se faire délivrer copie de ses conventions secrètes durant son contrat avec l'organisme agréé ou après son terme ;
- la remise au client d'une liste d'organismes agréés offrant les mêmes services en cas de cessation d'activité ou de retrait d'agrément du TC.

Un exemplaire du contrat de service entre le TC et ses clients devra être fourni.

4.1.2. La procédure d'agrément

Le premier agrément : Un dossier dont les éléments sont décrits ci-dessus doit être déposé auprès du SCSSI en envoi recommandé avec AR ou par dépôt direct. Le dossier fera ensuite l'objet d'un contrôle formel. Le dossier est réputé complet si, dans le délai d'un mois, le SCSSI n'a pas invité le demandeur, par lettre recommandée avec AR à fournir les pièces complémentaires nécessaires. Au cours de l'instruction du dossier qui suit, contrôles et avis seront formulés par les services des ministres de la défense, de l'intérieur, de l'industrie et du ministre chargé des télécommunications. Si l'instruction est favorable, l'agrément pourra être délivré. L'agrément peut cependant être refusé pour des motifs liés aux intérêts de la défense nationale ou de la sécurité intérieure ou extérieure de l'Etat. L'agrément, qui est donné pour 4 ans et renouvelable, est ou tacite ou express :

- le Premier ministre notifie sa décision expressément par lettre recommandée avec AR dans un délai de 4 mois à compter du dépôt de la demande ;
- l'agrément est tacite passé un délai de 4 mois sans réponse. Le défaut de notification dans ce délai vaut agrément.

Le renouvellement d'agrément : La demande de renouvellement doit être déposée au moins 2 mois avant la date d'expiration de l'agrément auprès du SCSSI par lettre recommandée avec demande d'avis de réception. L'absence de réponse de l'administration dans les deux mois vaut renouvellement tacite de l'agrément.

Les modifications de l'agrément : D'une part, toute proposition de modification du contenu du cahier des charges à une demande d'agrément complémentaire. D'autre part, certains changements doivent être notifiés sans délai au SCSSI :

- la nature juridique de l'organisme agréé,
- la nature ou l'objet de ses activités,
- la localisation de son établissement ;
- l'identité ou les qualités juridiques de ses dirigeants,
- toutes cessions d'actions ou de parts sociales susceptibles d'entraîner un changement du contrôle de l'organisme agréé,

- la cessation totale ou partielle de l'activité agréée.

Le retrait de l'agrément : En cas de violation de la législation, de non-respect de ses obligations, notamment issues du cahier des charges, le TC peut se voir retirer son agrément par une décision du Premier Ministre. Ce sera encore le cas si le maintien de celui-ci risque de mettre en péril les intérêts de la défense nationale ou de la sécurité intérieure ou extérieure de l'Etat. En cas d'urgence l'agrément peut être suspendu immédiatement.

Compte tenu de l'activité, des effets particuliers doivent être signalés. Ces effets jouent aussi, en cas de cessation d'activité par le TC. Ce sont les effets suivants :
- le TC concerné doit communiquer à ses utilisateurs la liste des organismes agréés offrant les mêmes services ;
- le TC en cessation d'activité confie les conventions secrètes à un autre organisme agréé selon le choix de chaque utilisateur. En cas de silence de l'utilisateur, l'arrêté du 13 mars 1998 désigne le SCSSI pour recevoir dépôt des conventions secrètes en cas de cessation d'activité d'un organisme agréé ou de retrait d'agrément prononcé à son encontre (article 2 de l'arrêté). Les conventions secrètes devront être transmises au SCSSI en notation ASN 1 sous une forme décrite dans l'article 10 de l'Arrêté.

4.2 Les obligations postérieures à l'agrément

4.2.1. Les exigences concernant les personnels

La composition du personnel : La composition du personnel reste naturellement libre de façon globale, sous la responsabilité du chef d'entreprise. Cependant quelques emplois doivent être obligatoire prévus. Ainsi parmi les personnels techniques, on distingue : l'ingénieur système, l'administrateur de sécurité et l'opérateur. L'ingénieur système est chargé de la mise en route et de la maintenance technique du système. L'administrateur est chargé de la gestion de sa sécurité et l'opérateur de son exploitation. Il n'est pas souhaitable que l'administrateur et l'ingénieur système soient une seule et même personne.

Il faudra aussi prévoir un "responsable sécurité" : il est chargé de l'application pratique de la politique de sécurité, particulièrement :
- l'élaboration d'un guide pratique de sécurité à l'intention du personnel,
- le contrôle de son application,
- l'organisation d'audits internes,
- le traitement des incidents signalés.

Le profil des personnels : Les personnels du TC doivent posséder une bonne compétence technique dans le domaine de la sécurité des systèmes d'information. Quant à ceux qui sont appelés à remettre ou à mettre en oeuvre des conventions secrètes, ils doivent posséder une habilitation de type "secret défense" (Décret n°81-514 du 12 mai 1981 relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'Etat). Le chef d'entreprise fera signer à tous les membres concernés de son personnel un document (à considérer par exemple, l'intégration dans le contrat) où ils reconnaîtront avoir pris connaissance de la Politique de Sécurité, des guides et manuels de sécurité et de leurs responsabilités en cas de manquement à leurs obligations. La dimension pénale leur sera exposée.

La communication de la liste du personnel : Le TC devra fournir à son interlocuteur administratif, le service central de la sécurité des systèmes d'information (SCSSI), la liste des personnels qu'il emploie dans le cadre de l'activité agréée. La liste contient les informations suivantes :
- nom, prénom,
- adresse,
- nationalité,
- type de contrat de travail et poste occupé.

La mise à jour de cette liste est permanente : elle est modifiée lors du changement des éléments d'information. Les nouvelles versions sont communiquées au SCSSI.

Le répertoire des clients : La communication d'informations au SCSSI s'étend au répertoire des utilisateurs de moyens cryptographiques mis à disposition par le TC. Le répertoire comporte pour chaque client les éléments suivants :
- le nom, le prénom ou la dénomination sociale,
- l'adresse,
- le moyen dont les conventions secrètes sont gérées,

- la valeur des identifiants électroniques.

Le répertoire sera transmis au minimum une fois par semestre, au mieux, à chaque changement dans les éléments d'information.

Comme le répertoire prendra vraisemblablement la forme d'un fichier informatique faisant l'objet d'un "traitement automatisé de données" selon les termes de la loi du 6 janvier 1978 (Informatique et Libertés), le Tiers devra prévoir l'accomplissement des formalités de déclaration auprès de la CNIL. Ces formalités sont également préalables à tout traitement technique.

4.2.2. Les exigences techniques

Le système technique doit présenter certaines fonctions de sécurité.

Garantie d'identification/authentification : Les moyens de sécurité doivent permettent d'identifier, puis d'authentifier les personnels. Le mécanisme d'authentification nécessite la présentation d'un support matériel associé à un code personnel. Le système reconnaît, sur la base de cette Identification/Authentification, les trois rôles suivants: ingénieur système, administrateur de sécurité, opérateur.

Manipulation des clés : Nul ne doit avoir directement accès à la clé permettant de certifier les conventions secrètes des clients. L'utilisation d'un processeur de sécurité interfacé avec le système est indispensable. Pendant toute la durée de leur détention, les conventions secrètes sont chiffrées. Lorsqu'il n'est plus utilisé, le dispositif contenant la clé de certification est détruit et sa destruction fait l'objet d'un compte rendu. Les dispositifs servant à déchiffrer les conventions secrètes sont conservés dans une armoire forte.

Traçage des traitements : Un enregistrement est généré pour toute opération permettant l'accès aux conventions secrètes ou autres ressources de sécurité du système. Tous les enregistrements sont retracés dans un fichier d'audit. Celui-ci n'est consultable que par l'administrateur. Une sauvegarde régulière en est faite et archivée. Cet enregistrement comporte les informations suivantes :

- le nom de l'opérateur,
- l'opération effectuée,
- la date et l'heure de l'opération.

L'archivage des conventions secrètes : La loi impose au TC une obligation d'archivage des conventions secrètes pendant une durée de 4 ans. Au-delà de cette période, l'arrêté du 13 mars 1998 ("fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes"), le SCSSI peut être désigné pour un dépôt de longue durée (article 1er de l'arrêté).

5 Annexes

5.1 Décret no 2002-997 du 16 juillet 2002

REMARQUE : Nous reproduisons ci-dessous le dernier texte publié en matière de cryptologie.

Décret n°2002-997 du 16 juillet 2002 relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi no 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

Art. 1er.

L'obligation mise à la charge des fournisseurs de prestations de cryptologie par l'article 11-1 de la loi du 10 juillet 1991 susvisée résulte d'une décision écrite et motivée, émanant du Premier ministre, ou de l'une des deux personnes spécialement déléguées par lui en application des dispositions de l'article 4 de la même loi. La décision qui suspend cette obligation est prise dans les mêmes formes.

Art. 2.

Les décisions prises en application de l'article 1er sont notifiées au fournisseur de prestations de cryptologie et communiquées sans délai au président de la Commission nationale de contrôle des interceptions de sécurité.

Art. 3.

Les conventions mentionnées dans le présent décret permettant le déchiffrement des données s'entendent des clés cryptographiques ainsi que de tout moyen logiciel ou de toute autre information permettant la mise au clair de ces données.

Art. 4.

La décision mentionnée au premier alinéa de l'article 1er : a) Indique la qualité des agents habilités à demander au fournisseur de prestations de cryptologie la mise en oeuvre ou la remise des conventions, ainsi que les modalités selon lesquelles les données à déchiffrer lui sont, le cas échéant, transmises ; b) Fixe le délai dans lequel les opérations doivent être réalisées, les modalités selon lesquelles, dès leur achèvement, le fournisseur remet aux agents visés au a du présent article les résultats obtenus ainsi que les pièces qui lui ont été éventuellement transmises ; c) Prévoit, dès qu'il apparaît que les opérations sont techniquement impossibles, que le fournisseur remet aux agents visés au a les pièces qui lui ont été éventuellement transmises.

Art. 5.

Les fournisseurs prennent toutes dispositions, notamment d'ordre contractuel, afin que soit respectée la confidentialité des informations dont ils ont connaissance relativement à la mise en oeuvre ou à la remise de ces conventions.

Art. 6.

L'intégralité des frais liés à la mise en oeuvre de l'obligation prévue par l'article 11-1 de la loi du 10 juillet 1991 susvisée est prise en charge, sur la base des frais réellement exposés par le fournisseur et dûment justifiés par celui-ci, par le budget des services du Premier ministre.

Art. 7.

Le présent décret est applicable en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

Art. 8.

Le ministre de l'intérieur, de la sécurité intérieure et des libertés locales, la ministre de la défense, le ministre de l'économie, des finances et de l'industrie, la ministre de l'outre-mer et le ministre délégué au budget et à la réforme budgétaire sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

5.2 Extrait du projet de LEN relatif à la cryptologie

REMARQUE : Comme dit dans notre introduction, la LEN devrait modifier profondément la réglementation de la cryptologie dans le sens de la libéralisation. Nous publions ci-dessous les dispositions s'appliquant aux PSCE (AC) de la signature électronique, ainsi qu'aux autres prestataires.

PROJET DE LOI POUR LA CONFIANCE DANS L'ECONOMIE NUMERIQUE

TITRE III - DE LA SECURITE DANS L'ECONOMIE NUMERIQUE

CHAPITRE I ER - MOYENS ET PRESTATIONS DE CRYPTOLOGIE

Article 17
On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.
On entend par prestation de cryptologie toute opération visant à la mise en oeuvre, pour le compte d'autrui, de moyens de cryptologie.

SECTION 1 - UTILISATION, FOURNITURE, TRANSFERT, IMPORTATION ET EXPORTATION DE MOYENS DE CRYPTOLOGIE

Article 18
I. – L'utilisation des moyens de cryptologie est libre.
II. – La fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation et l'exportation des moyens de cryptologie dont la seule fonction cryptologique est une fonction d'authentification ou de contrôle d'intégrité, notamment à des fins de signature électronique, sont libres.
III. - La fourniture, le transfert depuis un Etat membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Premier ministre, sauf dans les cas prévus au *b)* ci-dessous. Le fournisseur ou la personne procédant au transfert ou à l'importation tiennent à la disposition du Premier ministre une description des caractéristiques techniques de ce moyen de cryptologie. Un décret en Conseil d'Etat fixe :
a) Les conditions dans lesquelles sont souscrites ces déclarations, les conditions et les délais dans lesquels le Premier ministre peut demander communication des caractéristiques du moyen, ainsi que la nature de ces caractéristiques ;
b) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, leur transfert depuis un Etat membre de la Communauté européenne ou leur importation peuvent être dispensées de toute formalité préalable.
IV. - Le transfert vers un Etat membre de la Communauté européenne et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation du Premier ministre, sauf dans les cas prévus au *b)* ci-dessous. Un décret en Conseil d'Etat fixe :
a) Les délais dans lesquels le Premier ministre statue sur les demandes d'autorisation;
b) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur transfert vers un Etat membre de la Communauté européenne ou leur exportation peuvent être, soit soumis au régime déclaratif et aux obligations d'information prévus au I ci-dessus, soit dispensés de toute formalité préalable.

SECTION 2 - FOURNITURE DE PRESTATIONS DE CRYPTOLOGIE

Article 19
I. - La fourniture de prestations de cryptologie doit être déclarée auprès du Premier ministre, dans des conditions définies par décret. Ce décret peut prévoir des exceptions à l'obligation de déclaration pour les prestations dont les caractéristiques techniques ou les conditions de fourniture sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, cette fourniture peut être dispensée de toute formalité préalable.
II. - Les personnes exerçant cette activité sont assujetties au secret professionnel, dans les conditions prévues aux articles 226-13 et 226-14 du code pénal.

Article 20
Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie à des fins de confidentialité sont présumées responsables, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.

Article 21
Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont présumés responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés, dans des conditions fixées par décret en Conseil d'Etat lorsque :
1° Les informations contenues dans le certificat qualifié, à la date de sa délivrance, étaient inexactes ou lorsque les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;
2° Les prestataires n'ont pas procédé à la vérification de :
a) La détention par le signataire, au moment de la délivrance du certificat qualifié, des données relatives à la création de signature correspondant aux données fournies ou identifiées dans le certificat et permettant la vérification de la signature ;
b) La possibilité d'utiliser de façon complémentaire les données relatives à la création et à la vérification de signature, dans le cas où le prestataire de services de certification électronique peut être à l'origine de ces deux types de données ;
3° Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat qualifié et tenu cette information à la disposition des tiers.
Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites aient été clairement portées à la connaissance des utilisateurs dans le certificat.
Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

SECTION 3 - SANCTIONS ADMINISTRATIVES

Article 22
Lorsqu'un fournisseur de moyens de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujetti en application du I de l'article 18, le Premier ministre peut, après avoir mis l'intéressé à même de présenter ses observations, prononcer l'interdiction de mise en circulation du moyen de cryptologie concerné.
L'interdiction de mise en circulation est applicable sur l'ensemble du territoire national. Elle emporte obligation de procéder au retrait des moyens de cryptologie qui ont été mis en vente, offerts à la location ou fournis à titre gratuit, directement ou par l'intermédiaire de diffuseurs commerciaux, antérieurement à la décision du Premier ministre.

SECTION 4 - DISPOSITIONS DE DROIT PENAL

Article 23
I. - Sans préjudice de l'application du code des douanes :
a) Le fait de ne pas satisfaire à l'obligation de déclaration prévue à l'article 18 en cas de fourniture, de transfert, d'importation ou d'exportation d'un moyen de cryptologie ou de refus de satisfaire à l'obligation de communication à l'autorité administrative prévue par ce même article, est puni d'un an d'emprisonnement et de 15 000 euros d'amende ;

b) Le fait d'exporter un moyen de cryptologie ou de procéder à son transfert vers un Etat membre de la Communauté européenne sans avoir préalablement obtenu l'autorisation mentionnée à l'article 18 ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
II. - Le fait de vendre ou de louer un moyen de cryptologie ayant fait l'objet d'une interdiction administrative de mise en circulation en application de l'article 22 est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
III. - Le fait de fournir des prestations de cryptologie visant à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue à l'article 19 est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
IV. - Les personnes physiques coupables de l'une des infractions prévues au présent article encourent également les peines complémentaires suivante :
1° L'interdiction, suivant les modalités prévues par l'article 131-19 du code pénal et pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
2° La confiscation, suivant les modalités prévues par l'article 131-21 du code pénal, de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit à l'exception des objets susceptibles de restitution ;
3° L'interdiction, suivant les modalités prévues par l'article 131-27 du code pénal et pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ;
4° La fermeture, dans les conditions prévues par l'article 131-33 du code pénal et pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion, dans les conditions prévues par l'article 131-34 du code pénal et pour une durée de cinq ans au plus, des marchés publics.
V. - Les personnes morales sont responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions prévues au présent article. Les peines encourues par les personnes morales sont :
l° L'amende, suivant les modalités prévues par l'article 131-38 du code pénal ;
2° Les peines mentionnées à l'article 131-39 du code pénal.

Article 24
Outre les officiers et agents de police judiciaire agissant conformément aux dispositions du code de procédure pénale et, dans leur domaine de compétence, les agents des douanes agissant conformément aux dispositions du code des douanes, les agents habilités à cet effet par le Premier ministre et assermentés dans des conditions fixées par décret en Conseil d'Etat peuvent rechercher et constater par procès-verbal les infractions aux dispositions des articles 18, 19, 22 et 23 de la présente loi et des textes pris pour leur application.
Les agents habilités par le Premier ministre mentionnés à l'alinéa précédent peuvent accéder aux locaux, terrains ou moyens de transport à usage professionnel en vue de rechercher et de constater les infractions, demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications. Les agents ne peuvent accéder à ces locaux que pendant leurs heures d'ouverture lorsqu'ils sont ouverts au public et, dans les autres cas, qu'entre 8 heures et 20 heures. Ils ne peuvent accéder aux locaux qui servent de domicile aux intéressés.
Le procureur de la République est préalablement informé des opérations envisagées en vue de la recherche des infractions. Il peut s'opposer à ces opérations. Les procès-verbaux lui sont transmis dans les cinq jours suivant leur établissement. Une copie en est également remise à l'intéressé.
Les agents habilités peuvent, dans les mêmes lieux et les mêmes conditions de temps, procéder à la saisie des moyens de cryptologie mentionnés à l'article 17 sur autorisation judiciaire donnée par ordonnance du président du tribunal de grande instance dans le ressort duquel sont situés ces matériels et logiciels, ou du juge des libertés et de la détention. La demande doit comporter tous les éléments d'information de nature à justifier la saisie. Celle-ci s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée.
Les matériels et logiciels saisis sont immédiatement inventoriés. L'inventaire est annexé au procès-verbal dressé sur les lieux. Les originaux du procès-verbal et de l'inventaire sont transmis, dans les cinq jours suivant leur établissement, au juge qui a ordonné la saisie.
Le président du tribunal de grande instance ou le juge des libertés et de la détention peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner mainlevée de la saisie.
Est puni de six mois d'emprisonnement et de 7 500 euros d'amende le fait de refuser de fournir les informations ou documents ou de faire obstacle au déroulement des enquêtes mentionnées au présent article.

Article 25

Il est inséré, après l'article 132-75 du code pénal, un article 132-76 ainsi rédigé :
« *Art. 132-7*6. - Lorsqu'un moyen de cryptologie au sens de l'article 17 de la loi n°……. du……..…… relative à la communication électronique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :
« 1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle ;
« 2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle ;
« 3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle ;
« 4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d'emprisonnement ;
« 5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d'emprisonnement ;
« 6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement ;
« 7° Il est porté au double lorsque l'infraction est punie de trois ans d'emprisonnement au plus.
« Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement. »

Article 26
I. - L'article 31 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne est abrogé.
II. - Après l'article 11 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, il est inséré un article 11-1 ainsi rédigé :
« *Art. 11*-1. - Les personnes qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en oeuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.
Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
Un décret en Conseil d'Etat précise les procédures suivant lesquelles cette obligation est mise en oeuvre ainsi que les conditions dans lesquelles la prise en charge financière de cette mise en oeuvre est assurée par l'Etat. »
III. - Après l'article 434-15-1 du code pénal, il est inséré un article 434-15-2 ainsi rédigé :
« *Art. 434-15*-2. - Est puni de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.
Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende. »

SECTION 5 - SAISINE DES MOYENS DE L'ETAT POUR LA MISE AU CLAIR DE DONNEES CHIFFREES

Article 27
I. - L'article 30 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne est abrogé.
II. - Après l'article 230 du code de procédure pénale, il est inséré un titre IV ainsi rédigé :
« TITRE IV
DISPOSITIONS COMMUNES
CHAPITRE UNIQUE
De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité
Art. 230-1. - Sans préjudice des dispositions des articles 60, 77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation

empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire.
Si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au présent chapitre.
Art. 230-2. - Lorsque le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire décident d'avoir recours, pour les opérations mentionnées à l'article 230-1, aux moyens de l'Etat couverts par le secret de la défense nationale, la réquisition écrite doit être adressée au service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information, avec le support physique contenant les données à mettre au clair ou une copie de celui-ci. Cette réquisition fixe le délai dans lequel les opérations de mise au clair doivent être réalisées. Le délai peut être prorogé dans les mêmes conditions de forme. A tout moment, l'autorité judiciaire requérante peut ordonner l'interruption des opérations prescrites.
Le service de police judiciaire auquel la réquisition a été adressée transmet sans délai cette dernière ainsi que, le cas échéant, les ordres d'interruption, à un organisme technique soumis au secret de la défense nationale, et désigné par décret. Les données protégées au titre du secret de la défense nationale ne peuvent être communiquées que dans les conditions prévues par la loi nº98-567 du 8 juillet 1998 instituant une commission consultative du secret de la défense nationale.
Art. 230-3. - Dès l'achèvement des opérations ou dès qu'il apparaît que ces opérations sont techniquement impossibles ou à l'expiration du délai prescrit ou à la réception de l'ordre d'interruption émanant de l'autorité judiciaire, les résultats obtenus et les pièces reçues sont retournés par le responsable de l'organisme technique au service de police judiciaire qui lui a transmis la réquisition. Sous réserve des obligations découlant du secret de la défense nationale, les résultats sont accompagnés des indications techniques utiles à la compréhension et à leur exploitation ainsi que d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis.
Ces pièces sont immédiatement remises à l'autorité judiciaire par le service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information.
Les éléments ainsi obtenus font l'objet d'un procès-verbal de réception et sont versés au dossier de la procédure.
Art. 230-4. - Les décisions judiciaires prises en application du présent chapitre n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours.
Art. 230-5. - Sans préjudice des obligations découlant du secret de la défense nationale, les agents requis en application des dispositions du présent chapitre sont tenus d'apporter leur concours à la justice. »

SECTION 6 - DISPOSITIONS DIVERSES

Article 28
Les dispositions du présent chapitre ne font pas obstacle à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, à ceux des moyens de cryptologie qui sont spécialement conçus ou modifiés pour porter, utiliser ou mettre en oeuvre les armes, soutenir ou mettre en oeuvre les forces armées, ainsi qu'à ceux spécialement conçus ou modifiés pour le compte du ministère de la défense en vue de protéger les secrets de la défense nationale.

Article 29
I. - L'article 28 de la loi n° 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications est abrogé à compter de l'entrée en vigueur du présent chapitre.
II. - Les autorisations et déclarations de fourniture, d'importation et d'exportation de moyens de cryptologie, délivrées ou effectuées avant la date de publication de la présente loi, conservent leurs effets jusqu'à l'expiration du terme prévu par les dispositions antérieurement en vigueur. Les agréments délivrés aux organismes chargés de gérer pour le compte d'autrui des conventions secrètes de moyens de cryptologie permettant d'assurer des fonctions de confidentialité valent, pour ces moyens, déclaration au sens de l'article 19.