

LA CRYPTOLOGIE

<u>INTRODUCTION</u>	2
<u>1. LE DROIT POSITIF FRANÇAIS</u>	3
<u>1.1. LES DÉCRETS N° 99-199 ET 199-200 DU 17 MARS 1999</u>	3
<u>1.1.1 Dispense de toute formalité</u>	4
<u>1.1.2 L'exportation</u>	4
<u>1.1.3 Matériel sous séquestre</u>	4
<u>La procédure d'autorisation :</u>	5
<u>La procédure de déclaration :</u>	5
<u>Tableau récapitulatif</u>	5
<u>1.2 LA CRYPTOLOGIE DANS LE PROJET DE LOI SUR LA SOCIÉTÉ DE L'INFORMATION</u>	6
<u>1.2.1 Utilisation, fourniture, transfert, importation et exportation de moyens de cryptologie</u>	6
<u>1.2.2 Fourniture de prestations de cryptologie</u>	9
<u>1.2.3 Sanctions administratives</u>	11
<u>1.2.4 Obligations et sanctions pénales</u>	12
<u>1.2.4.1 Quelles sont les obligations et les sanctions ?</u>	12
<u>1.2.4.2 Le recours à la cryptologie comme moyen l'infraction : une circonstance aggravante</u>	15
<u>Tableau récapitulatif des sanctions en matière de cryptologie :</u>	16
<u>Tableau de l'aggravation des sanctions – article 45 du PLSI - :</u>	17
<u>1.2.5 Les agents autorisés</u>	18
<u>1.2.5.1 Qui sont-ils ?</u>	18
<u>1.2.5.2 Quels seront leurs pouvoirs ?</u>	19
<u>2. DROIT POSITIF AMÉRICAIN</u>	20
<u>3. LES PROCÉDÉS DE CRYPTAGE</u>	21
<u>3.1 LE CRYPTAGE PAR BLOCS</u>	21
<u>Schéma : Le cryptage symétrique</u>	22
<u>3.2 LE CRYPTAGE ASYMÉTRIQUE</u>	22
<u>Schéma : Le cryptage asymétrique</u>	22

Introduction

La définition classique de la cryptologie est donnée par l'Encyclopédie Littré¹ : « Art d'écrire en caractères secrets, qui sont de convention ou le résultat d'une transposition des lettres de l'alphabet. La cryptologie est la même chose que l'écriture en chiffres... ». La cryptologie n'est pas nouvelle, cependant, le problème de son évolution se pose chaque jour avec plus d'acuité. Si la cryptologie permet de répondre aux attentes de sécurité des internautes et du commerce électronique, son utilisation peut, également, favoriser la réalisation d'infractions. Les enjeux en présence ont rendus nécessaire des adaptations ponctuelle de la réglementation. Le droit positif actuel se trouve dans les décrets n° 99-199 et 199-2000 du 17 mars 1999. Cependant, le projet de loi sur la société de l'information (PLSI)² comprend dans son titre V « De la sécurité de la société de l'information » un chapitre II intitulé « liberté d'utilisation des moyens et des prestations de cryptologie. »³ Le droit positif est donc appelé à être modifié par la loi nouvelle. Il importe donc d'exposer, non seulement, le droit applicable mais aussi le droit futur. A cet égard, il faut remarquer que le projet de loi sera débattu et amendé lors de la procédure parlementaire et que les décrets d'applications n'interviendront pas avant l'année 2003.

L'article 36 du projet de loi sur la société de l'information donne une **définition légale** de la cryptologie :

« 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 sécuriser le stockage ou la transmission de données, en permettant, en particulier, d'assurer la confidentialité des données ou, par exemple à des fins de signature électronique, leur authentification ou le contrôle de leur intégrité. »

et distingue les moyens de cryptologie, de **la prestation de cryptologie** :

« On entend par prestation de cryptologie toute opération visant à la mise en oeuvre de moyens de cryptologie, effectuée pour le compte d'autrui, y compris la gestion des conventions secrètes

¹ Edition de 1875 p. 922.

² Consultable en ligne : <http://www.assemblee-nationale.fr/projets/pl3143.asp>.

ou des conventions publiques permettant d'assurer des fonctions de confidentialité ou, par exemple à des fins de signature électronique, d'authentification ou de contrôle d'intégrité.»

1. Le droit positif français

L'adaptation des législations au nouvel équilibre de la transparence et de la confidentialité est désormais urgente. Pourtant, la menace terroriste donne une nouvelle actualité aux restrictions concernant la fourniture de moyens de chiffrement fiables. Il s'agit donc d'arbitrer des intérêts contraires, d'une part la sécurité nationale et d'autre part la sécurité des transactions via les réseaux.

1.1. Les décrets n° 99-199 et 199-200 du 17 mars 1999

En France, la libéralisation de la cryptologie tant à l'usage qu'à la fourniture s'est réalisée en trois étapes législatives :

1. Par la **loi n° 90-1170 du 20 décembre 1990 modifiée par la loi 91-648 du 11 juillet 1991** l'Etat voulait assurer le maintien des intérêts en présence.
2. Une nouvelle étape fut franchie avec la **loi 96-659 du 26 juillet 1996** qui se voulait plus « libérale ».
3. Enfin les **décrets 99-199 et 99-200 du 17 mars 1999** sont les seuls à avoir réalisé une libéralisation effective quoique minimum, les lois précédentes ne permettant notamment pas d'assurer le secret des affaires.

Dans ce contexte **les décrets n° 99-199 et 199-200 du 17 mars 1999⁴** font figure de pionniers et sont de nature à lever le doute planant sur l'efficacité du chiffrement dans le cadre légal. S'ils abrogent les décrets 98-206 et 98-207 du 23 mars 1998, ils **laissent subsister les décrets 101 et 102 relatifs à l'institution de tiers agréé et au régime d'autorisation du Premier ministre**. Les opérations dispensées d'autorisations préalables sont donc distinguées des opérations qui y sont soumises. **Le recours au tiers agréé permet d'utiliser des cryptages dits « forts ».**

Le décret 99-199 définit les catégories de moyens et de prestations de cryptologie pour lesquels la **procédure de déclaration préalable est substituée à**

³ Article 36 à 49 du PLSI.

⁴ JORF du 19 mars 1999.

l'autorisation. Le décret 99-200 précise les moyens et prestations **dispensés de toutes formalités préalables.**

1.1.1 Dispense de toute formalité

Aux termes du décret n°99-200 l'utilisation et l'importation **des algorithmes de chiffrement dont la longueur de clé est comprise entre 40 et 128 bits, sont dispensées de toute formalité.** Leur fourniture est soumise à simple déclaration auprès du SCSSI⁵, soit que les dits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par le producteur, soit qu'ils soient destinés uniquement à l'usage privé d'une personne physique.

1.1.2 L'exportation

L'exportation des logiciels et matériels dont l'algorithme présente une longueur de clé inférieur ou égale à 56 bits est libre ; de même celle des produits présentant une clé d'une longueur inférieure à 64 bits qui remplissent les conditions posées par la décision 94/942/PESC modifiée⁶.

L'exportation des moyens et prestations présentant une clé supérieure à 64 bits est libre en transfert intra communautaire, si les conditions fixées par le point 5 de la décision PESC sont remplies.

Il reste néanmoins des opérations soumises à **autorisation préalable.** L'utilisation, La fourniture et l'importation en provenance de l'union Européenne d'un matériel ou logiciel dont l'algorithme présente une **clé supérieure à 128 bits demeure soumise à l'autorisation préalable du SCSSI.**

1.1.3 Matériel sous séquestre

⁵ Service Central de la Sécurité des Systèmes d'Information appelé à devenir la Direction Centrale des Systèmes d'Information.

⁶ Par la décision PESC 2000/402 ; consultable sur le site: <http://europa.eu.int/eur-lex/fr/>.

L'utilisation des matériels ou des logiciels séquestrés dont l'algorithme est supérieure à 128 bits est libre.

Réserve faite des exceptions visées ci-dessus, **l'exportation des matériels et logiciels dont la clé présente un algorithme supérieur 56 bits est soumise à autorisation.**

Le droit français a donc entamé un mouvement de libéralisation de l'usage et de la fourniture de moyens de cryptologie. En dépit de la fixation par les Etats-Unis du standard de 56 bits, tant critiqué, il ne faut pas oublier que l'usage du chiffrement est libre sur leur territoire. L'influence des techniques juridiques américaines s'est fait sentir jusqu'en France, qui a, depuis, adopté une réglementation moins abstraite et plus détaillée afin de mieux coller aux attentes des acteurs du marché.

La procédure d'autorisation :

1. Dépôt : formulaire + dossier technique + exemplaires du produit ;
2. Droit de refus de l'Administration ;
3. Délai maximum de décision : 4 mois (à partir du dossier complet) ;
4. S'applique au chiffrement > 128 bits de clé secrète.

La procédure de déclaration :

1. Dépôt : formulaire + dossier technique + exemplaires du produit ;
2. Simple vérification par l'Administration (sans droit de refus) ;
3. Délai avant vente-utilisation : 1 mois (à partir du dossier complet) ;
4. S'applique au chiffrement < = 128 bits de clé secrète ;

Tableau récapitulatif

(Source : « Journées sécurité multimédia, UJF Grenoble, 18 avril 2001, B. Warrusfel)

La réglementation de la cryptologie en France (depuis 1999)

Finalités	Fonctions assurées				
	Authentification Signature Intégrité	Confidentialité			
		<= 40 bits	40 bits <=128 bits	>128 bits	
				Avec séquestre (sans application particulière)	Sans séquestre
Utilisation	LIBRE	LIBRE	Soumise à déclaration	LIBRE	Soumise à autorisation
Fourniture	Soumise à déclaration simplifiée	Soumise à déclaration	Soumise à déclaration	Soumise à autorisation	Soumise à autorisation
Importation	LIBRE	LIBRE	Soumise à déclaration	Soumise à autorisation	Soumise à autorisation
Exportation	LIBRE	(non contrôlée)	Soumise à autorisation (si > 56 bits)	Soumise à autorisation	Soumise à autorisation

© B. Warusfel, 2001 Journées Sécurité du Multimedia
(UJF Grenoble, 18 avril 2001) 11

1.2 La cryptologie dans le projet de loi sur la société de l'information

1.2.1 Utilisation, fourniture, transfert, importation et exportation de moyens de cryptologie

L'article 37 du PLSI⁷ dispose en son premier alinéa que : « l'utilisation des moyens de cryptologie est libre. »

Le projet de loi distingue différentes situations :

1. Les pays en cause sont-ils membres de la communauté ?
2. Les moyens de cryptologie sont-ils exclusivement dédiés à l'authentification ou au contrôle de l'intégrité, notamment à des fins de signature électronique ?

Article 37 du PLSI - II - :

⁷ Projet de loi sur la société de l'information (précité).

« 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. »

Il faut noter que le projet de loi ne donne aucune indication sur ce que peut être un « *moyen de cryptologie dont la seule fonction cryptologique est une fonction d'authentification ou de contrôle d'intégrité* ». Si le maintien de la confidentialité n'est pas abordé pour des raisons compréhensibles⁸ ; il sera, en pratique, difficile de distinguer les produits entre eux. En effet, un produit assurant des fonctions d'authentification et de maintien de l'intégrité comporte usuellement une fonction de garantie de la confidentialité, celle-ci étant souvent liée au maintien de l'intégrité. Cependant, il ne faut pas douter que les développeurs de solutions techniques intégreront la législation nouvelle dans la conception de leurs produits de cryptologie.

Pour les situations mettant en scène des acteurs ressortissants de pays de l'Union, l'article 37 alinéa III du PLSI dispose

« 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 libres, dès lors que le fournisseur ou la personne procédant au transfert ou à l'importation les déclarent au préalable auprès du Premier ministre et tiennent ensuite à la disposition de celui-ci une description des caractéristiques techniques du moyen en question. Sont fixées par décret :

⁸ Le but de la réglementation étant de réserver des moyens de levée de la confidentialité pour des raisons intéressant la sécurité de l'Etat. Cet objectif a connu un nouveau souffle avec les attentas du 11 septembre 2001.

a) **Les conditions** dans lesquelles sont souscrites ces **déclarations et 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 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.»

Certains moyens de cryptologie permettant le maintien de la confidentialité bénéficieront du régime libéraire s'ils correspondent aux catégories définies par décret. Cependant, la loi sur la société de l'information n'étant pas encore votée, les décrets d'applications ne devraient pas voir le jour avant 2003.

Le quatrième alinéa de l'article 37 concerne les **moyens de cryptologie n'étant pas exclusivement dédiés au maintien de l'intégrité ainsi qu'à l'authentification** quand ils ne remplissent pas les conditions du troisième alinéa :

«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. **Sont fixées par décret :**

a) **Les conditions dans lesquelles est accordée cette autorisation, et notamment les délais de réponse aux demandes d'autorisation ;**

b) **Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard de intérêts de la défense nationale et**

de la sécurité intérieure de l'Etat, leur transfert vers un Etat membre de la Communauté européenne ou leur exportation peuvent être, soit seulement soumises au régime déclaratif et aux obligations d'information prévus au III ci-dessus, soit dispensées de toute formalité préalable »

Une fois encore, il faudra attendre le vote de la loi puis l'adoption des décrets d'application pour connaître le régime exact qui sera, alors, applicable.

1.2.2 Fourniture de prestations de cryptologie

Il s'agit d'une activité réglementée⁹ soumise à déclaration auprès des services du premier ministre. Cependant, le texte prévoit que des exceptions puissent être instituées par décret. Naturellement, la loi n'étant pas votée il est impossible de connaître les conditions juridiques de la non déclaration. Cependant, le texte précise qu'elles seront appréciées au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat.

Article 38 du PLSI :

*« I.- **L'activité de 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 physiques ou morales exerçant cette activité peuvent faire l'objet d'une accréditation volontaire dans des conditions fixées par décret au

⁹ Pour une liste indicative des prestataires de cryptologie : http://directory.google.com/Top/Computers/Security/Products_and_Tools/Cryptography/File_Encryption/ .

Conseil d'Etat. Elles sont assujetties au secret professionnel, sous réserve des dispositions des articles 230-1 à 230-5 du code de procédure pénale et de l'article 434-15-2 du code pénal.»

En application de l'**article 39 du PLSI**, les fournisseurs de prestations de cryptologie engageront, à ce titre, leur **responsabilité professionnelle**, qui **est présumée** et dont ils ne pourront se dégager contractuellement :

*« **Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence**, les personnes physiques ou morales 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.»*

Les autorités de certification qui, par nature, ont recours aux solutions de cryptologie sont tenues comme responsables de la qualité des certificats qu'elles délivrent :

Article 40 du PLSI :

*« **Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence**, les personnes physiques ou morales **prestataires de services de certification électronique** ou fournissant **d'autres services liés aux signatures électroniques** sont **présumées responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats qu'elles délivrent.***

*Elles 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. **Elles doivent justifier d'une garantie financière suffisante**, spécialement affectée au paiement des sommes qu'elles pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qu'elles délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.»*

1.2.3 Sanctions administratives

Les prestataires de services de cryptologie qui ne respecteraient pas leurs obligations légales sont susceptibles de voir interdire la mise en circulation de leurs produits sur le fondement de **l'article 41 alinéa 1^{er} du projet de loi** :

*« Lorsqu'un fournisseur de moyens de cryptologie, à titre payant ou gratuit, ne respecte pas les obligations auxquelles il est assujéti en application du III de l'article 37, 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'alinéa second de l'article 41 précise les modalités de l'interdiction de circulation prononcée par le premier Ministre. Tout d'abord, elle définit le champs d'application territorial de la mesure en précisant que l'interdiction est applicable sur l'ensemble du territoire national. Avant de préciser que, de cette sanction, découle

l'obligation pour le prestataire de retirer tout exemplaire ayant été communiqué au public.

« 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. »

Une fois encore, il faut signaler que les dispositions du projet de loi sur la société de l'information ont vocation à être remaniées au cours du débat parlementaire et qu'il importera de se tenir informé des évolutions tant législatives que réglementaires susceptibles d'intervenir dans les mois et les années à venir.

1.2.4 Obligations et sanctions pénales

1.2.4.1 Quelles sont les obligations et les sanctions ?

La section quatrième du projet de loi sur la société de l'information s'intitule : « Dispositions de droit pénal ». **L'article 42 du PLSI** se propose d'introduire dans **la loi 91-646 du 10 juillet 1991** un **article 11-1** qui se décompose en trois alinéas. Le premier pose l'obligation, le second la sanction et le troisième prévoit une intervention réglementaire.

L'obligation figurant au premier alinéa consiste, pour les fournisseurs de moyens de cryptologie visant à garantir la confidentialité des échanges, à conserver et à rendre accessible aux agents autorisés les conventions permettant le déchiffrement. Cette exigence trouve son fondement dans le nécessaire arbitrage qui doit être effectué entre le droit au respect de la vie privée et la sécurité de l'Etat.

« Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues, lorsque leur prestation inclut la gestion de

*conventions secrètes, 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 second alinéa pose les sanctions pénales consécutives au non-respect de l'obligation consacrée à l'alinéa premier :

*« 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 € d'amende**. »*

L'article 43 du PLSI sanctionne :

- La **non déclaration** de fourniture de moyens de cryptologie lorsque celle-ci est requise sur le fondement de l'article 37 du PLSI, par une **amende de 15.000 € et une peine d'emprisonnement pouvant aller jusqu'à un an**.
- L'**exportation** de moyens de cryptologie **sans les autorisations** nécessaires par une **amende de 30.000 € et une peine d'emprisonnement pouvant aller jusqu'à deux ans**.
- La **vente ou la location d'un moyen** de cryptologie ayant fait l'**objet d'une interdiction administrative** par une **amende de 30.000 € et une peine d'emprisonnement pouvant aller jusqu'à deux ans**.
- La **non déclaration d'un moyen de cryptologie visant à assurer la confidentialité**, lorsque celle-ci est requise sur le fondement de l'article 38 par une **amende de 30.000 € et une peine d'emprisonnement pouvant aller jusqu'à deux ans**.

Article 43 du PLSI, alinéas I à III:

«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 37 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 € d'amende ;

b) Le fait d'exporter un moyen de cryptologie sans avoir préalablement obtenu l'autorisation mentionnée à l'article 37 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 € 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 41 est puni de deux ans d'emprisonnement et de 30 000 € 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 38 est puni de deux ans d'emprisonnement et de 30 000 € d'amende ».

Les alinéas IV et V traitent des spécificités propres aux personnes physique et morales :

*« IV. - **Les personnes physiques** coupables des infractions prévues au présent article encourent les peines complémentaires prévues aux articles 131-19, 131-21 et 131-27 du code pénal et, à titre définitif ou pour une durée de cinq ans au plus, les peines prévues aux articles 131-33 et 131-34 du code pénal.*

*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 :*

1° 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.»

1.2.4.2 Le recours à la cryptologie comme moyen l'infraction : une circonstance aggravante

L'article 45 du PLSI énumère précisément quelle sera le barème d'une majoration de la peine encourue lorsque l'infraction aura été commise par le recours à des moyens de chiffrement.

« Il est inséré, après l'article 132-75 du code pénal, un article 132-76 ainsi rédigé :

" Art. 132-76. - Lorsqu'un moyen de cryptologie au sens de l'article 36 de la loi n° du sur la société de l'information 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." »

L'article 46 du PLSI participe de la même idée de dissuasion des malfaiteurs et leurs complices de recourir à la cryptologie pour mener leurs opérations :

*« Est puni de **trois ans d'emprisonnement et de 45 000 € d'amende** le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie, au sens de l'article 36 de la loi n°X du X.X.X sur la société de l'information, 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 œuvre, 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 œuvre 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 € d'amende.**»*

Tableau récapitulatif des sanctions en matière de cryptologie :

INFRACTION	SANCTION
Non déclaration (article 37 du PLSI)	Sanction administrative : interdiction de fournir des moyens de cryptologie. (Art 41 du PLSI)

	Sanction pénale : Un an d'emprisonnement Amende : 15.000 € (Art 43 du PLSI)
Non déclaration d'un moyen de cryptologie visant à assurer la confidentialité, lorsque celle-ci est requise sur le fondement de l'article 38	Deux ans d'emprisonnement et 30.000 € d'amende (Art 43 du PLSI)
L'exportation de moyens de cryptologie sans les autorisations	Deux ans d'emprisonnement et 30.000 € d'amende (Art 43 du PLSI)
Refus de communication de la convention de déchiffrement	Deux ans d'emprisonnement et 30.000 € d'amende (Art 43 du PLSI)
Refus de communication de la convention de déchiffrement sur le fondement de l'article 46 (il y a eut crime ou délit)	Trois ans d'emprisonnement et 45.000 € d'amende
Refus de communication de la convention de déchiffrement et la communication de la convention aurait pu prévenir le crime ou le délit	Cinq ans d'emprisonnement et 75.000 € d'amende
Vente ou la location d'un moyen de cryptologie ayant fait l'objet d'une interdiction administrative	Deux ans d'emprisonnement et 30.000 € d'amende (Art 43 du PLSI)

Tableau de l'aggravation des sanctions – article 45 du PLSI - :

PEINE ENCOURUE	PEINE AGGRAVEE
Trente ans de réclusion criminelle	Réclusion criminelle à perpétuité
Vingt ans de réclusion criminelle	Trente ans de réclusion criminelle

Quinze ans de réclusion criminelle	Vingt ans de réclusion criminelle
Dix ans d'emprisonnement	Quinze ans de réclusion criminelle
Sept ans d'emprisonnement	Dix ans d'emprisonnement
Cinq ans d'emprisonnement	Sept ans d'emprisonnement
Trois ans d'emprisonnement au plus	Peine portée au double

1.2.5 Les agents autorisés

1.2.5.1 Qui sont-ils ?

Il s'agit :

1. Des officiers de police judiciaire ;
2. Des agents des douanes ;
3. Des agents habilités à cet effet par le premier ministre dans les conditions fixées par décret en Conseil d'Etat :

Article 44 du PLSI alinéa 1^{er} :

« 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 37, 38, 41 et 43 de la présente loi et des textes pris pour leur application. »

1.2.5.2 Quels seront leurs pouvoirs ?

La mission de chacun des acteurs est de rechercher, constater et dresser procès verbal des infractions à la législation sur le chiffrement.

Concernant les agents de police judiciaire et des douanes, leurs pouvoirs s'exercent dans la limite de leur compétence et de la conformité au code de procédure pénale pour les uns et au code des douanes pour les autres.

Le projet de loi propose d'introduire un nouveau représentant de l'autorité définit à l'alinéa 1^{er} de **l'article 44** comme étant un agent habilité par le premier ministre pour contrôler le respect des dispositions relatives à la cryptologie. Le texte détermine les pouvoirs de ces nouveaux agents :

1. Ils peuvent accéder aux locaux, terrains ou moyens de transport à usage professionnel en vue de rechercher et de constater les infractions.
2. Ils peuvent, demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications.
3. 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 pour partie de domicile aux intéressés.
4. Ils doivent informer le procureur de la république de leurs opérations et lui transmettre la copie des procès verbaux qu'ils auront dressés.
5. Ils peuvent procéder à une saisie sur autorisation judiciaire après avoir obtenu une ordonnance du président du tribunal de grande instance.

Une obstruction à l'exercice de leur pouvoir par les agents autorisés pourra être sanctionné sur le fondement de l'article 44 du PLSi d'une peine d'**emprisonnement** pouvant aller jusqu'à **six mois** et d'une **peine d'amende** pouvant atteindre **7500 €**

2. Droit positif américain

Jusqu'en 1999 l'exportation de programmes de chiffrement nécessitait une autorisation pour chacun des clients, processus complexe qui obligeait les fabricants à se soumettre aux critères rigides de la très puissante NSA (national security agency). Les industriels se plaignaient depuis des années que leur compétitivité souffrait de cette procédure car ils devaient le plus souvent concevoir deux versions du programme, celle qui était destinée à l'exportation étant bridée.

Un mouvement de libéralisation des contrôles à l'exportation des produits de chiffrement est entamé aux Etats-Unis. En effet **le 8 mai 1999 la Cour d'appel du neuvième circuit (San Fransisco), dont les décisions s'appliquent dans neuf Etats de l'ouest américain, a estimé que le contrôle à l'exportation appliqué par le gouvernement américain aux procédés cryptographiques est contraire à la liberté d'expression garantie par le premier amendement de la Constitution.** Cette décision infirme un jugement de 1996 qui avait interdit à un professeur de mathématique de l'Illinois, Daniel Bernstein, de publier sur Internet un procédé cryptographique développé par ses soins.

« Pour exprimer leurs idées, les cryptographes échangent leurs codes source de la même manière que des mathématiciens échangent des équations ou les économistes des graphiques » écrit le juge Betty Fletcher qui estime « que les codes cryptographiques véhiculent des formules et des idées dont le gouvernement ne peut empêcher indéfiniment la circulation ».

L'assouplissement des règles relatives à l'exportation des programmes de chiffrement a été poursuivie par l'administration américaine. Les ministères de la justice, du commerce et de la défense ont pris conjointement la décision de **simplifier la procédure d'exportation le 15 décembre 1999. Désormais il faudra déposer une demande d'exportation mais en un seul exemplaire et non plus une par client et remettre à la NSA une « revue technique ».** En outre, le demandeur aurait dû s'engager à donner aux autorités une liste de ses clients. Ce dernier point fut mis en échec par le Congrès, cependant, le contexte de la

menace terroriste lui donne une nouvelle actualité. L'interdiction d'exportation découlant des accords de « Wassenaar » vers les sept pays « ennemis » subsiste.

Enfin depuis le **14 janvier 2000**, l'administration a parachevé la libéralisation de l'exportation de matériels et produits de chiffrement **malgré l'opposition du FBI et des services de renseignements, principaux adversaires de la libéralisation**. Toutefois, à l'image de la France, **le gouvernement peut encore refuser la diffusion d'informations relatives au chiffrement**. Si certaines associations regrettent la complexité et les limites de ces nouvelles dispositions qui sont assez similaires à la réglementation française, la plupart des acteurs du commerce électronique étaient plutôt satisfaits de cette évolution. Ainsi pour Eric Schmidt président de la société Novell «cette annonce prépare clairement la prochaine grande phase de développement de l'internet ». Quant à l'Americans for computer privacy qui réunit les principaux leaders du commerce électronique, elle s'est réjouie de cette « bonne nouvelle pour les Etats-Unis ». Il faut cependant compter avec l'impact des attentas du 11 septembre 2001 sur la politique de sécurité des Etats-Unis qui laisse présager un retour aux restrictions concernant les moyens de cryptologie.

3. Les procédés de cryptage¹⁰

Les procédés de cryptage se divisent en deux grandes catégories selon leurs principes mais aussi selon leur usage. On a d'un côté les algorithmes de cryptage par blocs, d'un autre les algorithmes asymétriques.

3.1 Le cryptage par blocs

- **Le cryptage par blocs** (block cipher) est un algorithme qui transforme un bloc de données de taille fixe (en général 64 bits) en un bloc de même longueur. Cette propriété est essentielle pour des applications demandant une bande passante de garantie. Les algorithmes de cryptage par bloc sont le plus souvent des algorithmes symétriques, ce qui signifie que le cryptage et le décryptage s'effectuent par la même fonction ce qui rend ces procédés assez rapides. Les

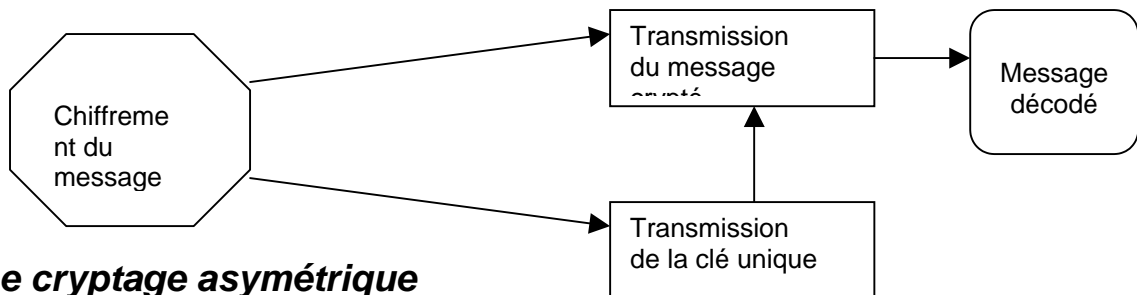
¹⁰ Cette partie est à mettre en relation avec celle sur la certification incluse dans le chapitre sur l'adaptation du droit de la preuve à l'environnement des réseaux.

algorithmes de ce type qui sont les plus connus sont DES, triple DES, RC4, IDEA, SAFER, skipjack, Blowfish.

Les procédés du type DES sont également appelés **procédés « à clé privée »** car la confidentialité des informations est conditionnée au secret qui entoure la clé de cryptage.

L'inconvénient du procédé symétrique est que la clé doit être communiquée à son interlocuteur dès que l'on souhaite transmettre un message crypté. Il faut donc disposer d'un canal très sûr pour la transmission de la clé. De plus, il faut changer de clé à chaque nouvel échange.

Schéma : Le cryptage symétrique



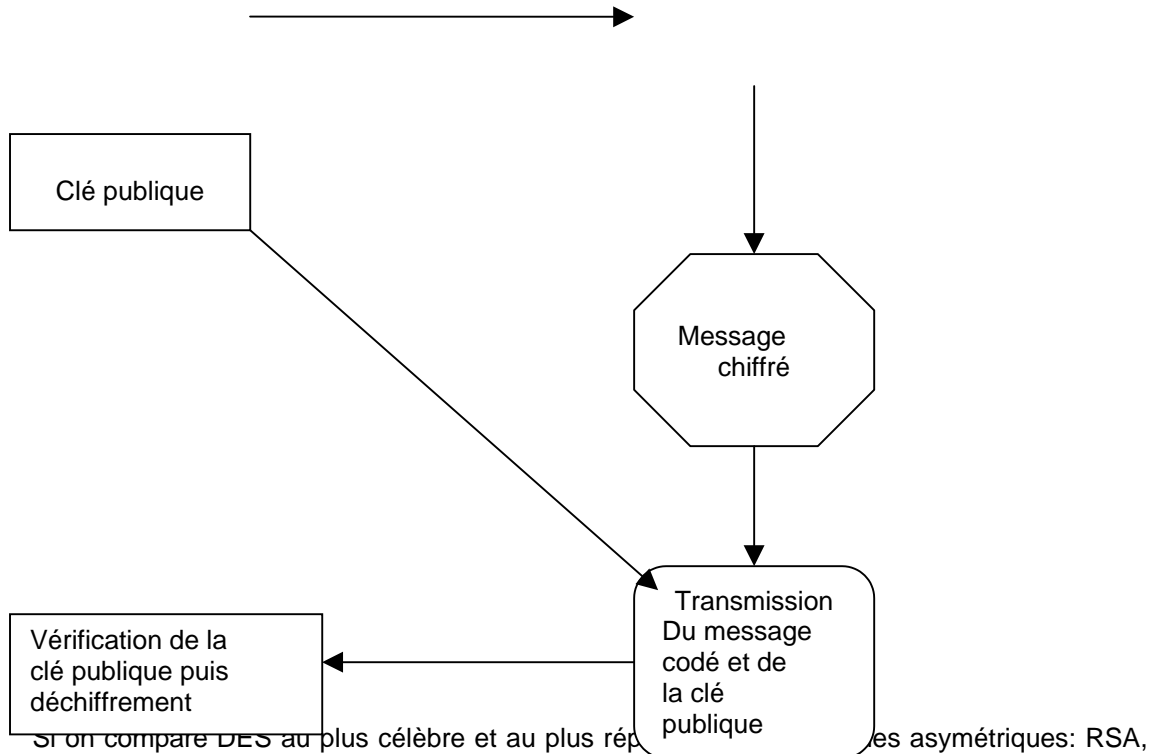
3.2 Le cryptage asymétrique

- **Le cryptage asymétrique est un algorithme pour lequel cryptage et décryptage sont des fonctions différentes.** Le plus souvent il s'agit de la même opération qui fait intervenir deux clés différentes. Les procédés asymétriques sont par opposition appelés « à clé publique » car ils sont conçus pour que l'une des deux clés, la clé publique, puisse être révélée sans compromettre l'autre, la clé privée.

C'est à dire que l'on code avec la clé privée et on décode avec la clé publique. La clé privée n'a donc jamais besoin d'être communiquée par son détenteur. La même clé peut par conséquent être employée pendant longtemps, il est cependant conseillé d'en changer tous les deux ans.

Schéma : Le cryptage asymétrique





Si on compare DES au plus célèbre et au plus répandu des algorithmes asymétriques: RSA, le premier est cent fois plus rapide en logiciel et en implantation matérielle : il est de 1000 à 10.000 fois plus rapide.

Les procédés à clé publique sont néanmoins appelés à se développer et prendre le pas sur les procédés à clé privée qui sont dans la pratique très lourds à gérer et moins sûrs . Des solutions techniques commencent à apparaître telle que « Phase forward » qui autorise la saisie des données depuis un navigateur Internet, en les cryptant à 128 bits et en ne les stockant pas en local, le tout étant protégé derrière des « firewalls.»

Le recours à l'un ou l'autre des procédés de cryptage¹¹ est suffisant pour être en mesure d'assurer l'obligation de confidentialité. En effet, bien que la confidentialité absolue n'existe pas, l'interception de données cryptées est l'apanage de quelques services de renseignement ainsi que de quelques milliers de pirates, ce qui constitue un taux de fraude marginal. Toutefois, les responsables du traitement devront être vigilants sur l'état de la technique afin de maintenir leurs algorithmes de cryptage à jour. A défaut leur responsabilité civile et pénale pourrait être recherchée.

Une attention particulière devra être portée aux informations couvertes par le secret bancaire dans la mesure où elles constituent une cible privilégiée. Si actuellement le protocole SSL est le plus répandu, il est acquis qu'il n'offre pas un degré de sécurité satisfaisant. Dès lors, les responsables devront s'informer sur le développement de nouvelles solutions (SET, C-SET ou autres) afin de garantir de manière optimale la confidentialité des informations bancaires.

¹¹ Pour plus d'informations techniques sur les procédés de chiffrement : <http://www.securiteinfo.com/>