Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Décret nº 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie

NOR : *PRMD0751412D*

Le Premier ministre,

Vu le règlement (CE) nº 1334/2000 du Conseil du 22 juin 2000 modifié instituant un régime communautaire de contrôles des exportations de biens et technologies à double usage ;

Vu la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 modifiée prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la défense ;

Vu le code pénal, notamment ses articles L. 131-21, L. 226-13 et R. 610-1 ;

Vu la loi nº 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique, notamment ses articles 30, 31, 36 et 40 ;

Vu le décret nº 95-589 du 6 mai 1995 modifié relatif à l'application du décret-loi du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions ;

Vu le décret nº 96-67 du 29 janvier 1996 modifié relatif aux compétences du secrétaire général de la défense nationale dans le domaine de la sécurité des systèmes d'information ;

Vu le décret nº 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Vu le décret nº 2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information ;

Vu le décret nº 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage ;

Vu la notification à la Commission européenne nº 2006/0253/F du 29 mai 2006 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

CHAPITRE Ier

Régime de dispense de toute formalité préalable

Art. 1er. – Sont dispensées des formalités préalables prévues aux chapitres II et III du présent décret les opérations de fourniture, de transfert, d'importation ou d'exportation des moyens et prestations de cryptologie mentionnées à l'annexe 1 du présent décret.

Art. 2. – Sont dispensées des mêmes formalités les opérations de transfert, d'importation et d'exportation des moyens de cryptologie qui ont fait l'objet d'une autorisation d'importation ou d'exportation en application des dispositions des articles L. 2335-1 à L. 2335-3 du code de la défense.

CHAPITRE II

Régime de déclaration

Art. 3. – Sont soumises à déclaration préalable, dans les conditions fixées au présent chapitre :

1º Les opérations, non mentionnées au chapitre Ier du présent décret, de fourniture, de transfert depuis un Etat membre de la Communauté européenne et d'importation de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité ;

2° Les opérations de transfert ou d'exportation de moyens de cryptologie mentionnées à l'annexe 2 du présent décret ;

3° La fourniture de prestations de cryptologie non mentionnées à l'annexe 1 du présent décret.

Art. 4. – Un mois au moins avant l'opération mentionnée à l'article 3, le dossier de déclaration est adressé par envoi recommandé avec demande d'avis de réception ou déposé contre accusé de dépôt à la direction centrale de la sécurité des systèmes d'information au secrétariat général de la défense nationale. Cette direction en délivre récépissé revêtu du numéro d'enregistrement du dossier.

La forme et le contenu du dossier de déclaration sont définis par un arrêté du Premier ministre. Ce dossier comporte une partie technique et une partie administrative.

Art. 5. – Dans le délai d'un mois à compter de la réception du dossier de déclaration, si le dossier est incomplet, la direction centrale de la sécurité des systèmes d'information invite le déclarant, par lettre recommandée avec demande d'avis de réception, à fournir les pièces complémentaires. Dans ce cas, le délai d'un mois prévu au premier alinéa de l'article 4 court à compter de la réception des pièces complémentaires.

Si le moyen de cryptologie déclaré relève du régime de l'autorisation, la direction centrale de la sécurité des systèmes d'information, dans le délai d'un mois à compter de la date à laquelle le dossier a été reçu ou, le cas échéant, complété, invite le déclarant, par lettre recommandée avec demande d'avis de réception, à procéder à l'application des dispositions du chapitre III.

A l'expiration du délai d'un mois, en cas de silence de la direction centrale de la sécurité des systèmes d'information, le déclarant peut procéder librement aux opérations faisant l'objet de la déclaration. La direction centrale de la sécurité des systèmes d'information peut, le cas échéant, avant l'expiration de ce délai, délivrer au déclarant une attestation confirmant que celui-ci s'est acquitté de son obligation déclarative.

Art. 6. – La déclaration de fourniture d'un moyen de cryptologie effectuée conformément aux dispositions du présent chapitre vaut, dans les mêmes conditions, déclaration pour les intermédiaires qui assurent, le cas échéant, la diffusion du moyen de cryptologie fourni par le déclarant.

Art. 7. – Pour les opérations mentionnées au 1° et au 2° de l'article 3, le Premier ministre peut demander au déclarant, par lettre recommandée avec demande d'avis de réception, dans un délai d'un an à compter de la date de réception du dossier complet de déclaration prévu à l'article 4 :

1° De lui communiquer, dans un délai de deux mois, les caractéristiques techniques et le code source du moyen de cryptologie qui a fait l'objet de la déclaration ;

2° De mettre à la disposition de la direction centrale de la sécurité des systèmes d'information deux exemplaires du moyen de cryptologie pour une durée qui ne peut excéder six mois.

Lorsque les éléments fournis par le déclarant sont incomplets, le Premier ministre dispose d'un délai de deux mois à compter de leur réception pour demander au déclarant, par lettre recommandée avec demande d'avis de réception, de lui communiquer des éléments complémentaires dans un délai de deux mois.

Un arrêté du Premier ministre précise la nature des caractéristiques techniques mentionnées au 1°, qui portent sur la description complète de la mise en œuvre du moyen de cryptologie ainsi que sur ses fonctions ou procédés de cryptologie.

Art. 8. – Les délais d'un mois prévus aux articles 4 et 5 sont portés à deux mois lorsque la déclaration concerne la fourniture de prestations de cryptologie.

Ces délais sont également portés à deux mois lorsque la déclaration concerne l'exportation de moyens de cryptologie vers des Etats non membres de la Communauté européenne. Dans ce cas, le délai d'un an prévu au premier alinéa de l'article 7 est réduit à deux mois.

CHAPITRE III

Régime d'autorisation

Art. 9. – Le dossier de demande d'autorisation est adressé par envoi recommandé avec demande d'avis de réception ou déposé contre accusé de dépôt à la direction centrale de la sécurité des systèmes d'information. Cette dernière en délivre récépissé revêtu du numéro d'enregistrement du dossier.

La forme et le contenu du dossier de demande d'autorisation sont définis par un arrêté du Premier ministre. Ce dossier comporte une partie technique et une partie administrative.

Art. 10. – Si le dossier est complet, le Premier ministre notifie sa décision, par lettre recommandée avec demande d'avis de réception, dans un délai de quatre mois à compter de la délivrance de l'avis de réception ou de l'accusé de dépôt de la demande. Un défaut de notification dans ce délai vaut autorisation pour une durée d'un an.

Le dossier est réputé complet si, dans le délai de deux mois suivant la réception de la demande, la direction centrale de la sécurité des systèmes d'information n'a pas invité, par lettre recommandée avec demande d'avis de réception, le demandeur à fournir des pièces complémentaires. Dans ce dernier cas, le délai de quatre mois fixé à l'alinéa précédent court à compter de la réception des pièces complétant le dossier.

Le Premier ministre peut également requérir le demandeur, dans le délai de deux mois mentionné à l'alinéa précédent, de mettre à la disposition de la direction centrale de la sécurité des systèmes d'information le code source et, pour une durée qui ne peut excéder six mois, deux exemplaires du moyen de cryptologie.

Art. 11. – L'autorisation peut être assortie de conditions visant à assurer la protection des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat.

Elle est délivrée pour une durée qui ne peut excéder cinq années. Elle peut être renouvelée dans les mêmes conditions que la demande initiale.

Art. 12. – L'autorisation peut être retirée par le Premier ministre :

1° En cas de fausse déclaration ou de faux renseignement ;

2° Lorsque son maintien risque de porter atteinte à la défense nationale ou à la sécurité intérieure ou extérieure de l'Etat ;

3 En cas de non-respect des prescriptions dont est, le cas échéant, assortie l'autorisation ;

4° Lorsque le titulaire de l'autorisation cesse l'exercice de l'activité pour laquelle a été délivrée l'autorisation ;

5° Lorsque les conditions auxquelles est subordonnée la délivrance de l'autorisation ne sont plus réunies.

Le retrait ne peut intervenir qu'après que le titulaire de l'autorisation a été mis à même de faire valoir ses observations dans un délai de huit jours.

En cas d'urgence, l'autorisation peut être suspendue immédiatement.

CHAPITRE IV

Dispositions pénales

Art. 13. – Le fait de fournir des prestations de cryptologie ne visant pas à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue aux articles 3 et 4 est puni des peines prévues pour les contraventions de la 5e classe.

Les personnes coupables de l'infraction prévue à l'alinéa précédent encourent également la peine complémentaire de confiscation, suivant les modalités prévues par l'article L. 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.

CHAPITRE V

Dispositions diverses et transitoires

Art. 14. – L'habilitation prévue au premier alinéa de l'article 36 de la loi du 21 juin 2004 susvisée est accordée par arrêté du Premier ministre à des agents en fonction à la direction centrale de la sécurité des systèmes d'information.

Cette habilitation peut être retirée à tout moment par décision du Premier ministre.

Les agents habilités prêtent devant le tribunal de grande instance dans le ressort duquel se trouve leur résidence administrative le serment suivant : « Je jure et promets de bien et loyalement remplir mes fonctions et d'observer, en tout, les devoirs qu'elles m'imposent. Je jure également de ne rien révéler ou utiliser de ce qui sera porté à ma connaissance à l'occasion de l'exercice de mes fonctions. » La prestation de serment est enregistrée sans frais au greffe du tribunal, l'acte de ce serment est dispensé du timbre et d'enregistrement, il est transcrit gratuitement sur les commissions d'emploi visées à l'alinéa suivant.

Dans l'exercice de leurs fonctions, ces agents doivent être munis de leur commission d'emploi faisant mention de leur habilitation et de leur prestation de serment. Ils sont tenus de la présenter à la première réquisition.

Art. 15. – Les agents de l'Etat veillent à la protection des informations à caractère secret qui sont recueillies dans le cadre des procédures prévues par le présent décret et dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal.

Art. 16. – L'accomplissement des formalités prévues par le présent décret ne dispense pas les intéressés de souscrire, s'il y a lieu, les autres déclarations prévues par la réglementation ni de solliciter les autres autorisations requises par les textes en vigueur, notamment en application des dispositions de l'article L. 2332-1 du code de la défense et du décret du 13 décembre 2001 susvisé pris pour l'application du règlement (CE) n° 1334/2000 susvisé.

Art. 17. – Les dispositions du présent décret s'appliquent aux demandes d'autorisation déposées avant sa date d'entrée en vigueur et pour lesquelles aucune décision, tacite ou expresse, n'est intervenue avant cette date. Les délais prévus par le présent décret commencent, en ce cas, à courir à compter de sa date d'entrée en vigueur.

Les titulaires d'autorisations d'importation ou de fourniture de moyens ou de prestations de cryptologie en cours de validité à la date d'entrée en vigueur du présent décret sont réputés avoir satisfait à l'obligation de déclaration prévue au chapitre II du présent décret lorsque celle-ci est requise pour l'opération concernée.

Art. 18. – A l'article 2 du décret du 6 mai 1995 susvisé, le *d* du paragraphe 4 de la deuxième catégorie du A est remplacé par les dispositions suivantes :

« *d)* Moyens de cryptologie : matériels ou logiciels permettant la transformation à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers ou réalisant l'opération inverse lorsqu'ils sont spécialement conçus ou modifiés pour porter, utiliser ou mettre en œuvre les armes, soutenir ou mettre en œuvre les forces armées, ainsi que ceux spécialement conçus ou modifiés pour le compte du ministère de la défense en vue de protéger les secrets de la défense nationale. »

Art. 19. – Au I de l'article 9 du décret du 30 mars 2001 susvisé, les mots : « l'article 28 de la loi du 29 décembre 1990 susvisée » sont remplacés par les mots : « l'article 31 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ».

Art. 20. – Dans tous les textes réglementaires, notamment à l'article 3 du décret du 31 juillet 2001 susvisé, la référence au décret nº 98-101 du 24 février 1998 est remplacée par la référence au présent décret et la référence au décret nº 98-102 du 24 février 1998 est supprimée.

Art. 21. – Les dispositions du présent décret sont applicables en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna, à Mayotte et dans les Terres australes et antarctiques françaises.

Art. 22. – Les décrets nº 98-101 du 24 février 1998, nº 98-102 du 24 février 1998, nº 99-199 du 17 mars 1999 et nº 99-200 du 17 mars 1999 sont abrogés.

Toutefois, les déclarations souscrites avant la date d'entrée en vigueur du présent décret demeurent régies par les dispositions du décret nº 98-101 du 24 février 1998.

Art. 23. – Le garde des sceaux, ministre de la justice, et le ministre de l'outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 2 mai 2007.

DOMINIQUE DE VILLEPIN

Par le Premier ministre :

Le garde des sceaux, ministre de la justice,
PASCAL CLÉMENT

Le ministre de l'outre-mer,
HERVÉ MARITON

ANNEXE 1

OPÉRATIONS DE FOURNITURE, DE TRANSFERT DEPUIS OU VERS UN ÉTAT MEMBRE DE LA COMMUNAUTÉ EUROPÉENNE, D'IMPORTATION OU D'EXPORTATION DISPENSÉES DE FORMALITÉ PRÉALABLE

CATÉGORIES	OPÉRATIONS
	A. – La fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation ou l'exportation des catégories de moyens de cryptologie suivantes :
1	Cartes à microprocesseur personnalisées destinées à des applications pour le grand public : *a)* lorsque la capacité cryptographique est conçue et limitée pour servir uniquement avec les équipements relevant des catégories 2, 3, 4 et 5 de la présente annexe, ou *b)* lorsque la capacité cryptographique n'est pas accessible à l'utilisateur et qu'elle est spécialement conçue et limitée pour permettre la protection des données qui y sont stockées.
2	Equipements de réception de radiodiffusion ou de télévision, à destination du grand public, dont la capacité de chiffrement est limitée à la facturation, la gestion ou la programmation, et où le déchiffrement est limité aux fonctions vidéo, audio ou de gestion technique.
3	Equipements spécialement conçus et limités pour servir dans des opérations bancaires ou financières, à destination du grand public, et dont la capacité cryptographique n'est pas accessible à l'utilisateur.
4	Equipements de radiocommunication mobiles, destinés au grand public, dont les seules capacités de chiffrement sont celles mises en œuvre par l'opérateur du réseau pour la protection du canal radio, et qui ne sont pas en mesure de procéder au chiffrement direct entre radioéquipements.
5	Equipements téléphoniques sans fil, destinés au grand public, qui ne sont pas capables de procéder au chiffrement direct de téléphone à téléphone et lorsque la portée entre le téléphone et sa station de base n'excède pas 400 mètres conformément aux spécifications du fabricant.
6	Equipements spécialement conçus et limités pour assurer la protection de logiciels ou de données informatiques contre la copie ou l'utilisation illicite et dont la capacité cryptographique n'est pas accessible à l'utilisateur.
7	Equipements autonomes spécialement conçus et limités pour assurer la lecture de données audio-vidéo, sans capacité de chiffrement, et où le déchiffrement est limité aux informations audio, vidéo et de gestion technique.
	B. – Le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation ou l'exportation de la catégorie de moyens de cryptologie suivante :
8	Equipements, dotés de moyens de cryptologie, transportés par : *a)* une personnalité étrangère sur invitation officielle de l'Etat, ou *b)* une personne physique et lorsque l'équipement est destiné exclusivement à l'usage de cette personne.

CATÉGORIES	OPÉRATIONS
	C. – La fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne ou l'importation des catégories de moyens de cryptologie suivantes :
9	Stations de base de radiocommunications cellulaires commerciales civiles, conçues pour assurer le raccordement d'équipements mobiles destinés au grand public, et qui ne permettent pas d'appliquer des capacités de chiffrement direct au trafic de données entre ces équipements mobiles.
10	Equipements, destinés au grand public, permettant d'échanger entre eux des données par radiocommunications, et lorsque les seules capacités cryptographiques de l'équipement sont conçues conformément aux normes de l'Institute of Electrical and Electronics Engineers suivantes : IEEE 802.15.1, IEEE 802.15.3, IEEE 802.15.4, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.
	D. – La fourniture, le transfert depuis un Etat membre de la Communauté européenne ou l'importation de la catégorie de moyens de cryptologie suivante :
11	Moyens de cryptologie spécialement conçus et limités pour administrer, gérer, configurer un système d'information sous réserve qu'ils ne permettent de chiffrer que les seules données nécessaires à l'administration, la gestion ou la configuration du système à l'exclusion de toutes autres données.
	E. – Le transfert depuis un Etat membre de la Communauté européenne ou l'importation de la catégorie de moyens de cryptologie suivante :
12	Moyens de cryptologie destinés exclusivement : *a)* à l'usage de la personne physique qui procède à son importation ou à son transfert, y compris par voie électronique, ou *b)* à des fins de développement, de validation ou de démonstration par la personne qui procède à son importation ou à son transfert, y compris par voie électronique.
	F. – Le transfert vers un Etat membre de la Communauté européenne ou l'exportation des catégories de moyens de cryptologie suivantes :
13	Moyens de cryptologie ne mettant en œuvre aucun algorithme cryptographique présentant l'une des caractéristiques suivantes : *a)* un algorithme cryptographique symétrique employant une clé de longueur supérieure à 56 bits ; *b)* un algorithme cryptographique asymétrique fondé soit sur la factorisation d'entiers de taille supérieure à 512 bits, soit sur le calcul de logarithme discret dans un groupe multiplicatif d'un corps fini de taille supérieure à 512 bits ou dans un autre type de groupe de taille supérieure à 112 bits.
14	Moyens de cryptologie permettant de générer un code de découpage en canaux, un code de brouillage, ou un code d'identification de réseau, pour des systèmes de modulation ultra-large bande et ne présentant aucune des caractéristiques suivantes : *a)* une bande passante supérieure à 500 MHz ; *b)* une bande passante fractionnelle, définie comme la bande passante pour laquelle la puissance demeure constante à 3 dB, divisée par la fréquence centrale et exprimée en pourcentage, de 20 % ou plus.
	G. – La fourniture de la catégorie de prestations de cryptologie suivante :
15	Prestations de cryptologie visant à la mise en œuvre des moyens de cryptologie relevant des catégories 1, 2, 3, 4 et 5 de la présente annexe, sous réserve que la prestation ne consiste pas à délivrer des certificats électroniques ou fournir d'autres services en matière de signature électronique au sens de l'article 1er du décret du 30 mars 2001 susvisé.

ANNEXE 2

OPÉRATIONS DE TRANSFERT VERS UN ÉTAT MEMBRE DE LA COMMUNAUTÉ EUROPÉENNE OU D'EXPORTATION SOUMISES À DÉCLARATION

CATÉGORIES	OPÉRATIONS
	A. – Le transfert vers un Etat membre de la Communauté européenne ou l'exportation vers l'Australie, le Canada, les Etats-Unis d'Amérique, le Japon, la Nouvelle-Zélande, la Norvège ou la Suisse des catégories de moyens de cryptologie suivantes :
1	Moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité et mettant en œuvre : *a)* soit un algorithme cryptographique symétrique employant une clé de longueur supérieure à 56 bits ; *b)* soit un algorithme cryptographique asymétrique fondé soit sur la factorisation d'entiers de taille supérieure à 512 bits, soit sur le calcul de logarithme discret dans un groupe multiplicatif d'un corps fini de taille supérieure à 512 bits ou dans un autre type de groupe de taille supérieure à 112 bits.
2	Moyens de cryptologie permettant de générer un code d'étalement de fréquences y compris un code de saut de fréquences ou permettant de générer un code de découpage en canaux, un code de brouillage, ou un code d'identification de réseau, pour des systèmes de modulation ultra-large bande et présentant l'une des caractéristiques suivantes : *a)* une bande passante supérieure à 500 MHz ; *b)* une bande passante fractionnelle, définie comme la bande passante pour laquelle la puissance demeure constante à 3 dB, divisée par la fréquence centrale et exprimée en pourcentage, de 20 % ou plus.
	B. – L'exportation vers un Etat autre que ceux mentionnés au A ci-dessus de la catégorie de moyens de cryptologie suivante :

CATÉGORIES	OPÉRATIONS
3	Moyens de cryptologie relevant des catégories 1 ou 2 de la présente annexe et pour lesquels toutes les conditions ci-après sont remplies : *a)* sont couramment à la disposition du public en étant vendus directement sur stock, sans restriction, à des points de vente au détail, que cette vente soit effectuée en magasin, par correspondance, par transaction électronique ou par téléphone ; *b)* la fonctionnalité cryptographique ne peut pas être modifiée facilement par l'utilisateur ; *c)* sont conçus pour être installés par l'utilisateur sans assistance ultérieure importante de la part du fournisseur.