Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 30-Jun-1999
Dist. : 02-Jul-1999

Or. Ang.

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE ET DES COMMUNICATIONS

DSTI/ICCP/REG(98)4/FINAL
Non classifié

Groupe de travail sur la sécurité de l'information et la vie privée

INVENTAIRE DES MESURES DE CONTROLE APPLIQUEES AUX TECHNOLOGIES DE LA CRYPTOGRAPHIE

79739

Or. Ang.

CONTEXTE DE L'INVENTAIRE

Ce rapport a été préparé par le Groupe de travail sur la sécurité de l'information et la vie privée sur la base de recherches conduites par le Secrétariat[1] et de contributions fournies par les pays Membres de l'OCDE.

Il est important de noter que dans de nombreux pays Membres, ces mesures de contrôle sont en train d'être revues eu égard aux évolutions récentes intervenues au sein de la Communauté européenne, ainsi qu'aux négociations en cours à l'échelon international. Un certain nombre de changements sont notamment à attendre à brève échéance dans les politiques nationales du fait des négociations en cours sur la révision de certaines dispositions de l'Arrangement de Wassenaar relatif au contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage.

L'attention est attirée sur le fait que cet inventaire donne un "instantané" de la situation en ce qui concerne les mesures de contrôle appliquées à l'exportation, l'importation et l'utilisation au plan intérieur des technologies de cryptographie notifiées par les pays Membres jusqu'au mois de septembre 1998. Il devrait être reconnu que le résultat des négociations internationales en cours dans ce domaine pourraient donner un caractère dépassé à certains aspects de l'information consignée dans cet inventaire.

TABLE DES MATIÈRES

INVENTAIRE DES MESURES DE CONTROLE APPLIQUEES AUX TECHNOLOGIES DE CRYPTOGRAPHIE

GENERALITES

Travaux de l'OCDE dans le domaine de la politique de cryptographie

Le Comité de la Politique de l'information, de l'informatique et des communications (PIIC) de l'OCDE mène des travaux sur les technologies et politiques de cryptographie dans le cadre de ses activités sur la sécurité et la vie privée depuis 1989. Les travaux actuels dans ce secteur incombent à son Groupe de travail sur la sécurité de l'information et la vie privée (WPISP). L'expérience acquise par l'OCDE dans l'étude de domaines à l'intersection des aspects économiques, technologiques et juridiques et la somme des travaux réalisés par l'Organisation concernant la sécurité des systèmes d'information, la protection des données de caractère personnel et de la vie privée et les technologies de l'information, de l'informatique et des communications en font une enceinte privilégiée pour débattre des technologies de cryptographie et des questions de politique économique et de politique sociale liées à l'utilisation de la cryptographie. *Les Lignes directrices de l'OCDE de 1980 régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* comme ses *Lignes directrices de 1992 régissant la sécurité des systèmes d'information* ont mis en évidence le besoin de moyens technologiques pour assurer la protection des données de caractère personnel et de la vie privée ainsi que la sécurité des systèmes d'information. *Les Lignes directrices de l'OCDE de 1997 régissant la politique de cryptographie*[2], qui s'appuient sur ces instruments, proposent une approche d'ensemble de la politique internationale de cryptographie en identifiant les principes de base que les gouvernements devraient prendre en considération lorsqu'ils élaborent leurs politiques sur la cryptographie.

Ces dernières années, les pays Membres de l'OCDE ont entrepris de développer et de mettre en oeuvre des politiques et des lois régissant la cryptographie, et dans de nombreux pays, ce processus est encore en cours. Toutefois, les gouvernements des pays Membres ont reconnu le besoin d'une approche internationale coordonnée afin de faciliter le développement sans heurt d'une infrastructure de l'information efficace et sûre. A cet effet, le Groupe de travail a engagé un échange permanent d'informations dans le domaine de la politique de cryptographie pour promouvoir un débat plus approfondi sur les questions qui s'y rattachent. Dans le cadre des travaux que l'OCDE conduit en permanence dans ce domaine, cet Inventaire des mesures de contrôle appliquées aux technologies de cryptographie a été compilé par le Groupe de travail à partir de recherche conduites par le Secrétariat de l'OCDE et de contributions émanant des pays Membres.

L'objet de cet inventaire est de faciliter la coopération internationale en passant en revue les instruments internationaux et nationaux applicables aux mesures de contrôle visant l'exportation, l'importation et l'utilisation au plan intérieur des technologies de cryptographie dans les pays Membres de l'OCDE. Ce rapport vise à apporter des réponses aux deux questions suivantes :

- Dans quelle mesure les pays appliquent-ils des contrôles intérieurs sur le chiffrement, et quelles modifications éventuelles à la législation intérieure envisagent-ils ? et

– Dans quelle mesure les pays appliquent-ils un contrôle à l'importation ou à l'exportation sur le chiffrement, et quelles modifications éventuelles de cette législation de l'importation ou de l'exportation envisagent-ils ?

Cet inventaire exclut les lois sur l'utilisation de la cryptographie à des fins d'authentification et de certification, qui sont examinées dans un rapport distinct consacré spécifiquement à cette question et intitulé *Inventaire des approches en matière d'authentification et de certification dans une société mondiale de réseaux*[3].

Technologies de cryptographie

La cryptographie est un élément important dans la sécurité des systèmes d'information et de communication et une technologie essentielle pour le commerce électronique, et diverses applications ont été élaborées qui intègrent des méthodes cryptographiques destinées à assurer la sécurité des données. La cryptographie offre un moyen de réaliser deux aspects connexes mais distincts de la sécurité des données : permettre de vérifier l'intégrité des données et/ou d'authentifier l'expéditeur d'un message (au moyen d'une fonction de "signature électronique") et assurer la confidentialité des données (au moyen d'une fonction de "chiffrement"). Chacune de ces utilisations de la cryptographie offre certains avantages et pose des problèmes différents.

Les Gouvernements doivent d'apporter une réponse au fait qu'il est impératif d'encourager l'utilisation généralisée de la cryptographie, à la fois pour faciliter le commerce électronique et pour permettre aux utilisateurs de protéger leurs données en assurant la confidentialité de leurs communications pendant la transmission, en sécurisant leurs données mémorisées et en fournissant des assurances sur l'identité de l'auteur d'un message donné ou d'une signature sur un contrat électronique. Dans le même temps, les gouvernements sont préoccupés par les répercussions que l'utilisation généralisée de la cryptographie peut avoir sur le respect des lois, du fait qu'elle risque de limiter les possibilités dont disposent les autorités pour comprendre des données transmises ou stockées auxquelles elles ont eu légalement accès. Bien que les Lignes directrices de l'OCDE régissant la politique de cryptographie identifient les divers intérêts qui doivent être pris en compte dans le contexte de la politique internationale de cryptographie, elles ne règlent pas la question fondamentale de savoir comment les Gouvernements peuvent permettre aux utilisateurs légitimes de bénéficier des avantages de la cryptographie, sans donner des armes aux criminels pour qu'ils l'utilisent dans leurs activités illégales.

Mesures de contrôle sur les technologies de cryptographie dans les pays Membres de l'OCDE

Diverses approches ont été adoptées par les pays Membres de l'OCDE pour contrôler l'utilisation des technologies de cryptographie. Voulant séparer les questions en fonction des deux utilisations distinctes qui peuvent être faites de la cryptographie, la plupart des pays ont adopté une double approche pour réglementer cette pratique, à savoir que dans les lois et la politique poursuivie, la cryptographie à des fins de chiffrement n'est pas considérée de la même manière que la cryptographie utilisée pour les signatures numériques. Un moyen de contrôler l'utilisation de la cryptographie à des fins de chiffrement consiste à en rendre l'utilisation illégale s'il s'agit de dissimuler l'information à moins que les autorités n'aient accès aux clés de déchiffrement privées. Une autre approche consiste à autoriser l'utilisation de la cryptographie au plan intérieur, mais de limiter les exportations de produits cryptographiques. Pour prévenir les utilisations criminelles de la cryptographie visant à dissimuler l'information, il est possible d'avoir recours au système judiciaire pour obtenir auprès de la partie en cause les clés donnant accès aux données chiffrées.

Le principal instrument international visant les contrôles à l'exportation des technologies de cryptographie est l'Arrangement de Wassenaar relatif au contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage (juillet 1996). L'Arrangement de Wassenaar instaure une collaboration entre les pays participants et définit un ensemble de lignes directrices préliminaires couvrant le matériel militaire ainsi que les biens et technologies sensibles à double usage, dont la pleine mise en œuvre doit se faire au niveau national. Les participants se sont mis d'accord sur le fait de contrôler par l'intermédiaire de leurs législations, réglementations et politiques nationales les produits et technologies figurant sur une liste des biens et technologies à double usage - qui comprend les produits et technologies de cryptographie - et sur une liste distincte des munitions. Tous les pays Membres de l'OCDE sauf deux sont membres de l'Arrangement de Wassenaar. De plus, le Règlement et la Décision du Conseil de l'Union européenne du 19 décembre 1994 concernant le contrôle des exportations de biens à double usage s'appliquent à l'ensemble des 15 Etats membres de l'Union européenne, qui sont tous également Membres de l'OCDE. Pour s'acquitter des obligations qu'ils ont souscrites dans l'Arrangement de Wassenaar (et pour les Etats membres de l'Union européenne dans le Règlement de la CE), 27 des 29 pays Membres de l'OCDE appliquent des contrôles sur les exportations de technologies de cryptographie. Bien que la plupart de ces pays ait promulgué des législations ou des réglementations, et créé des autorités chargées de délivrer les licences, les détails de mise en oeuvre varient suivant les pays.

L'inventaire montre que l'une des façons dont diffèrent les mesures nationales de contrôle des exportations de produits cryptographiques concerne le traitement des logiciels de cryptographie qui sont "couramment à la disposition du public" ou appartiennent au "domaine public". L'Arrangement de Wassenaar comme le Règlement de la CE font l'objet d'une "Note générale relative aux logiciels", qui exempte ce type de logiciels des contrôles à l'exportation. Toutefois, d'après l'Inventaire, il ressort que la note générale relative aux logiciels n'est pas du tout appliquée dans certains pays et seulement partiellement dans d'autres. Il existe également des différences dans les approches nationales à l'égard des contrôles à l'exportation dans la façon dont est considéré le logiciel distribué sous une forme immatérielle sur des réseaux pour données comme Internet. Les pays Membres n'ont pas tous explicité ce point, mais parmi ceux qui l'ont fait, l'Inventaire montre que certains semblent établir une distinction entre transfert "matériel" et transfert "immatériel", alors que d'autres traitent les deux types de transferts de la même manière.

L'Inventaire a montré qu'il est possible d'utiliser sans restriction au plan intérieur des produits de cryptographie dans la majorité des pays Membres de l'OCDE. Toutefois, dans un petit nombre de pays Membres, il existe des lois générales régissant l'utilisation au plan intérieur des technologies de cryptographie ou des dispositions réglementaires visant certains secteurs. Des contrôles sur l'importation de technologies de cryptographie, tels que l'obligation de solliciter une licence, sont en vigueur dans quatre pays Membres de l'OCDE.

INSTRUMENTS INTERNATIONAUX

L'Arrangement de Wassenaar

Pendant plus de 40 ans, les contrôles à l'exportation sur la cryptographie ont été gouvernés par le Comité de coordination pour le contrôle multilatéral des exportations (COCOM)[4]. Le COCOM a été créé en 1950 pour répondre à la menace de la Guerre froide en empêchant la vente d'armes et en contrôlant l'exportation de produits et informations techniques stratégiques des pays Membres du COCOM vers les pays du Pacte de Varsovie. Sous le régime du COCOM, la cryptographie était considérée comme un bien stratégique ayant des applications militaires, dont le commerce international était ainsi soumis à des restrictions. En 1991, le COCOM a décidé de permettre l'exportation des tous les logiciels de grande diffusion (y compris des logiciels du domaine public) ; la plupart des pays Membres du COCOM ont incorporé ces changements à leur réglementation nationale.

La menace de la Guerre froide ayant diminué, et avec l'apparition de nouveaux risques pour la sécurité mondiale, le COCOM a été dissous en mars 1994 dans le cadre d'un plan de transition vers un type d'accord différent. Il s'agissait de passer d'un dispositif occidental de filtrage destiné à contrôler le transfert des technologies militaires à un mécanisme destiné à répondre aux risques pour la sécurité et la stabilité régionales liés à la prolifération des armements conventionnels et des biens et technologies à double usage. Les anciens pays du COCOM entreprirent des négociations pour élaborer un arrangement qui serait nettement différent aussi bien par ses objectifs que par ses procédures, en insistant sur la transparence des mécanismes. Pour la période transitoire, les anciens membres du COCOM se mirent d'accord sur le principe de continuer d'utiliser les listes de contrôle du COCOM comme base des contrôles des exportations internationales exercés à l'échelle nationale, en attendant que le nouvel arrangement puisse être mis en place, de sorte que la cryptographie resta sur les listes des contrôles à l'exportation.

Depuis 1996, le principal instrument international concernant les contrôles à l'exportation sur les technologies de cryptographie est l'Arrangement de Wassenaar sur le contrôle à l'exportation des armes conventionnelles et des biens et technologies à double usage. L'Arrangement de Wassenaar a été officiellement ratifié par 33 pays, dont 27 des 29 pays Membres de l'OCDE, en juillet 1996.[5] Avant son adoption finale, cet accord s'est provisoirement appelé le "Nouveau Forum". L'Arrangement de Wassenaar instaure une collaboration entre les pays participants et définit un ensemble de lignes directrices préliminaires couvrant le matériel militaire ainsi que les biens et technologies sensibles à double usage, dont la pleine mise en œuvre doit se faire au niveau national. Il vise à faire face aux menaces contre la paix et la sécurité internationales et régionales en assurant une plus grande transparence grâce à la mise en commun d'informations sur les transferts d'armes et de biens ou technologies à double usage dans le monde.

Essentiellement, l'Arrangement de Wassenaar offre un mécanisme mondial pour contrôler les transferts légitimes d'armements conventionnels et d'articles sensibles à double usage, et une enceinte où les gouvernements peuvent examiner collectivement les implications d'activités diverses sur la sécurité internationale et régionale. Les décisions se font par consensus, et l'adhésion est ouverte sur une base mondiale et non discriminatoire à tous les pays qui satisfont à des critères fixés. Lorsqu'il s'agit de décider si un Etat peut devenir partie à l'Arrangement, certains facteurs, notamment, sont pris en considération, comme indicateurs de la capacité du pays à contribuer aux objectifs de l'Arrangement. Il s'agit d'examiner si le pays est producteur ou exportateur d'armes ou d'équipements à double usage, quelle est sa politique en matière de non-prolifération et de s'assurer qu'il poursuit des politiques nationales responsables et notamment adhère aux principaux régimes de non-prolifération et au principe

de l'application de mesures de contrôle des exportations pleinement efficaces. L'accord définit un processus structuré pour assurer la transparence, la consultation et, le cas échéant, une retenue multilatérale.

Les participants conviennent de contrôler par leurs législations, réglementations et politiques nationales les articles et technologies énumérés dans une liste de biens et technologies à double usage et dans une liste de matériel militaire distincte. La mise en œuvre de ces listes au niveau national a débuté en novembre 1996. L'Arrangement a établi un Secrétariat à Vienne où les participants se rencontrent régulièrement. Le premier réexamen de l'Arrangement interviendra en 1999. Des données agrégées sur les transferts et refus sont échangées tous les six mois. Les refus de biens sensibles/très sensibles et les acceptations d'exportations auparavant refusées[6] doivent être notifiés dans les meilleurs délais[7].

L'Arrangement a quatre objectifs principaux. Il vise à contribuer à la sécurité régionale et nationale :

- En favorisant la transparence et une plus grande responsabilité en ce qui concerne les transferts d'armes conventionnelles et de biens et technologies à double usage, évitant ainsi des accumulations déstabilisantes.

- En visant, par le biais des politiques nationales, à faire en sorte que les transferts de ces articles ne contribuent pas à la création ou au renforcement de capacités militaires contraires à cette sécurité et ne soient pas détournés au profit de ces capacités.

- En complétant et en renforçant, sans double emploi, les régimes de contrôle existants visant les armes de destruction de masse et leurs vecteurs, ainsi que les autres mesures internationalement reconnues tendant à promouvoir la transparence et une plus grande responsabilité, en visant particulièrement les menaces contre la paix et la sécurité internationales et régionales qui peuvent résulter de transferts de matériel militaire et de biens et technologies sensibles à double usage là où les risques sont jugés les plus grands.

- En renforçant la coopération pour empêcher l'acquisition de matériel militaire et d'articles sensibles à double usage en vue d'utilisations finales militaires, si la situation d'une région ou le comportement d'un Etat est ou devient un motif sérieux de préoccupation pour les Etats participants.

Les "éléments initiaux" de l'Arrangement de Wassenaar comprennent deux listes de produits et technologies sur lesquelles les pays Membres se sont mis d'accord[8]: (1) une Liste des munitions, qui couvre les biens et technologies militaires, et (2) une Liste de biens et technologies à double usage, c'est-à-dire qui peuvent servir à des fins aussi bien civiles que militaires. Cette dernière liste comprend trois niveaux : le niveau 1 (liste de base), le niveau 2 (liste sensible[9]) et un sous-ensemble du niveau 2 (liste très sensible[10]). L'accord impose l'obligation de notifier le transfert ou le refus de transfert à un pays non-participant des biens ou technologies à double usage répertoriés. La liste de niveau 1 requiert une notification des refus, sur une base agrégée avec la périodicité habituelle de six mois. Toutefois, les biens et technologies sensibles du niveau 2 et de son sous-ensemble comportent l'exigence plus stricte d'une notification distincte pour chaque transfert ou refus de transfert à un Etat non-participant, dans les 60 jours qui suivent. Les transferts de ces biens sensibles sont également notifiés de façon agrégée, deux fois par an.

L'Arrangement stipule aussi que les pays participants s'informent mutuellement de l'approbation d'une licence pour une transaction avec un utilisateur final auquel un autre pays participant

a refusé au cours des trois années précédentes une licence portant sur une transaction essentiellement identique ("entorse" ou "under-cutting"). Les pays participants sont invités à être vigilants dans le contrôle des articles énumérés dans les listes, mais il n'y a pas d'obligation explicite de soumettre les transferts à la délivrance de licences individuelles ; ce point est laissé à l'appréciation de chaque pays.

Les produits et technologies de cryptographie figurent sur la Liste des biens et technologies à double usage dans la Catégorie 5, Partie 2, "Sécurité de l'information". La liste soumet au contrôle les technologies aussi bien matérielles que logicielles. On notera les exceptions aux dispositions couvrant les technologies de cryptographie :

Le chiffre 5A.2 ne vise pas ce qui suit :

a) Les cartes à microprocesseur personnalisées ou leurs composants spécialement conçus, présentant l'une des caractéristiques suivantes :

1. Incapables d'encrypter le trafic de messages ou les données fournies par l'utilisateur ou leurs fonctions de gestion de clef associée ; ou

2. Destinées à servir uniquement avec les équipements ou systèmes non visés aux points 1 à 6 de la note au chiffre 5A.2.a.3 ou aux points b à h de la présente note.

b.Les équipements employant des techniques de compression ou de codage de données fixes.

c. Equipements de réception pour la radiodiffusion, la télévision payante ou la télévision similaire réservée à un nombre limité de téléspectateurs du grand public, sans capacité de chiffrement numérique et où le déchiffrement numérique est limité aux fonctions vidéo, audio ou de gestion.

d. Radiotéléphones portatifs ou mobiles destinés a l'usage civil, (par exemple pour l'emploi avec les systèmes de radiocommunications cellulaires commerciaux civils) qui ne sont pas en mesure de procéder au chiffrement de bout en bout.

e. Fonctions de déchiffrement spécialement conçues pour permettre l'exécution de logiciels protégés, à condition que ces fonctions ne soit pas accessibles à l'utilisateur.

f. Equipements de contrôle d'accès, tels que machines automatiques de distribution de billets, imprimantes libre-service de relevés de comptes ou terminaux de points de vente, protégeant les mots de passe, numéros d'identification personnels ou autres données similaires empêchant l'accès non autorisé à des installations, mais ne permettant pas le chiffrement des fichiers ou des textes, sauf lorsqu'il est directement lié à la protection des mots de passe ou des numéros d'identification personnels.

g. Equipements d'authentification des données qui calculent un code d'authentification de message ou un résultat similaire afin d'assurer qu'aucune modification de texte n'a été effectuée ou d'authentifier les utilisateurs, mais qui ne permettent pas de chiffrer des données, textes ou autres supports, sauf pour ce qui est nécessaire à l'authentification.

h. Equipements cryptologiques spécialement conçus et limités pour servir dans des machines d'opération bancaires ou financières, telles que machines automatiques de distribution de billets, imprimantes libre-service de relevés de comptes ou terminaux de points de vente.

Aux termes de la "Note générale sur la technologie" de la liste des biens à double usage, les contrôles ne s'appliquent pas aux "technologies" "du domaine public", à la "recherche scientifique fondamentale", ni à l'information minimale nécessaire pour les demandes de brevet. De plus, la Note générale relative aux logiciels stipule que :

Les listes ne soumettent pas au contrôle les "logiciels" qui soit :

1. *Sont couramment à la disposition du public, du fait qu'ils sont :*

   a. *Vendus directement sur stock, sans restriction, à des points de vente au détail :*

      1.En magasin ;

      2. Par correspondance ; ou

      3. Sur appel téléphonique ; et

   b. *Conçus pour être installés par l'utilisateur sans assistance ultérieure importante de la part du fournisseur ; ou*

2. *Relèvent "du domaine public".*

Un certain nombre de changements sont notamment à attendre à brève échéance dans les politiques nationales du fait des négociations en cours sur la révision de certaines dispositions de l'Arrangement de Wassenaar relatif au contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage. L'issue de ces négociations va sans doute nécessiter une révision du présent inventaire.

Union européenne

Contrôles à l'exportation

Le Règlement et la Décision du Conseil de l'Union européenne du 19 décembre 1994 concernant le contrôle des exportations de biens à double usage[11] constituent la base du régime communautaire gouvernant les exportations de technologies cryptographiques. La liste des produits soumis à des contrôles est basée sur l'Arrangement de Wassenaar et d'autres régimes internationaux de non-prolifération.

Le Règlement du Conseil soumet à un régime d'autorisations l'exportation de certains produits cryptographiques en dehors de l'Union européenne. Pendant une période transitoire, le Règlement impose aussi une procédure d'autorisations pour les échanges intra-communautaires de certains produits de chiffrement particulièrement sensibles, ce qui équivaut à des mesures de contrôle intérieur dans l'Union européenne sur les produits expédiés entre les Etats membres. Toutefois, le Règlement ne stipule pas complètement le champ, le contenu ou les pratiques d'application des mesures de contrôle nationales. En conséquence, il existe une certaine divergence dans les pratiques nationales entre les Etats membres de l'Union européenne.

La Décision prise en application du Règlement énonce des exceptions particulières aux contrôles à l'exportation qui ont une incidence sur les exportations de cryptographie et que certains ont interprété comme indiquant que le Règlement ne s'applique pas à l'exportation de produits cryptographiques par le biais d'Internet. En particulier, la Décision stipule que le contrôle des transferts de technologie se limite

aux formes tangibles[12]. En outre, la "Note générale relative à la technologie" de la Décision déclare que le contrôle sur les transferts de technologie ne s'applique pas aux connaissances qui sont "du domaine public", et la "Note générale relative aux logiciels" (qui reprend le libellé de la Note générale relative aux logiciels de l'Arrangement de Wassenaar) indique que la liste des produits soumis au contrôle à l'exportation exclut les logiciels qui sont "du domaine public" ou "couramment à la disposition du public", c'est-à-dire qui sont à la fois (1) vendus directement sur stock, sans restriction, dans des points de vente au détail, que cette vente s'effectue en magasin, par correspondance ou par téléphone, et (2) conçus pour être installés par l'utilisateur sans assistance ultérieure importante de la part du fournisseur.

Autres mesures de contrôle

La législation de l'Union européenne n'impose pas de contrôles à l'importation sur les technologies de cryptographie.

Le Traité de Rome énonce le principe de la libre circulation des biens à l'intérieur de la Communauté, ce qui a des implications pour les politiques nationales des Etats membres en matière de cryptographie.

La Résolution du Conseil de l'Union européenne du 17 janvier 1995 relative à l'interception légale des télécommunications[13] stipule que les opérateurs de réseaux ou les fournisseurs de services, s'ils procèdent à un chiffrement, doivent fournir "en clair" aux organismes chargés de l'exécution des lois les communications interceptées, c'est-à-dire fournir le signal tel qu'ils le reçoivent.

Evolution de la politique

En octobre 1997, la Commission européenne a publié une Communication intitulée "Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et le chiffrement"[14] qui décrit d'une part les fonctions d'authentification et d'intégrité de la cryptographie et, d'autre part, ses fonctions de confidentialité. Concernant ce dernier aspect, la Communication traite de l'accès légal aux clés de chiffrement (dispositifs de récupération de clés ou mise en dépôt de clés), ces dispositifs pouvant s'interpréter comme des mesures de contrôle intérieur de la cryptographie. La Communication reconnaît l'existence d'un certain nombre d'applications commerciales du "chiffrement", comme la télévision à péage qui ne peut fonctionner commercialement que grâce au chiffrement et au déchiffrement en contrepartie d'un abonnement.

La Communication admet l'utilisation du chiffrement par les citoyens et entreprises respectueux des lois pour se protéger contre les attaques délictueuses, tout en notant que l'on ne peut totalement empêcher les criminels d'utiliser ces technologies pour leurs propres agissements. Elle déclare que "le public doit avoir accès à des outils techniques permettant une protection efficace de la confidentialité des données et des communications contre les intrusions arbitraires. Le chiffrement des données est très souvent le seul moyen efficace et d'un bon rapport coût-efficacité de répondre à ces exigences". La Communication poursuit en indiquant que la Commission va s'assurer que les restrictions nationales par les Etats membres dans le domaine de la sécurité nationale et de l'exécution des lois se justifient et obéissent aux dispositions communautaires en matière de libre circulation et à la Directive sur la protection des données. Concernant les réglementations de l'utilisation du chiffrement, elle note que "des divergences entre les schémas réglementaires pourraient créer des obstacles au fonctionnement du Marché intérieur".

La Communication note aussi que les Etats membres doivent communiquer à la Commission les mesures techniques qu'ils envisagent d'imposer pour la vente, l'usage, la production ou l'importation de produits cryptographiques[15].

La Communication avance l'idée qu'il conviendrait d'adapter le Règlement concernant les biens à double usage à la lumière des besoins du marché des produits cryptographiques. Elle déclare que l'Article 19 du Règlement contient une disposition qu'il faudrait réexaminer, en particulier pour :

- Démanteler progressivement les contrôles intra-communautaires sur les produits de chiffrement commerciaux (mais pas nécessairement sur ceux basés sur un chiffrement très évolué).

- Lancer une discussion sur la portée et l'interprétation de certaines dispositions telles que la "Note générale relative aux logiciels" (qui stipule que les logiciels dans le domaine public ne sont pas soumis à contrôle) ; et

- Traiter des problèmes tels que les moyens de transmission immatériels (par exemple par télécopie ou courrier électronique).

Enfin, la Communication préconise une coopération entre les forces de police au niveau européen et international, ainsi qu'une action internationale en vue de créer un cadre pour le commerce électronique comportant la reconnaissance mutuelle des certificats et l'établissement de normes techniques communes.

Le 15 mai 1998, la Commission a adopté une Proposition de Règlement du Conseil (CE) instituant un régime communautaire de contrôle des exportations de biens et technologies à double usage [COM(1998), 257 final, 98/0162 (ACC)], qui introduit une procédure de notification pour les expéditions intracommunautaires de produits cryptographiques, se substituant à un mécanisme d'autorisation.

Le 13 mai 1998, la Commission européenne a adopté une proposition de Directive du Parlement européen et du Conseil relative à un cadre commun pour les signatures électroniques (Commission européenne, COM(1998) 297 Final, 13.05.98)[16]. La proposition de Directive suit la Communication, en vue d'harmoniser les initiatives européennes sur les signatures électroniques et de promouvoir la reconnaissance juridique des signatures électroniques. La proposition comporte également des dispositions relatives à des mécanismes transfrontières visant à assurer l'interopérabilité au niveau mondial. Elle est actuellement examinée par le Parlement européen et le Conseil.

En 1997, la Commission a proposé une Directive du Parlement européen et du Conseil sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel. Cette proposition s'appuie sur une large consultation dans le contexte du Livre vert sur "la protection juridique des services cryptés dans le marché intérieur". Ce projet de Directive couvrirait tous les services dont le cryptage a pour but d'assurer le versement d'une rémunération, y compris les services de la société de l'information fournis à distance par voie électronique à la demande individuelle d'un destinataire de services, ainsi que les services de radiodiffusion.[17]

Autres enceintes européennes

Le 11 septembre 1995, le Conseil de l'Europe a adopté une Recommandation[18] concernant les problèmes de droit procédural pénal liés à la technologie de l'information. Ce document déclare que des

mesures devraient être envisagées pour réduire le plus possible les effets préjudiciables de l'utilisation de la cryptographie sur les enquêtes concernant des infractions pénales, sans affecter indûment les utilisations légitimes. Toutefois, cette Recommandation n'exige pas que les Etats membres mettent en œuvre une politique particulière concernant le chiffrement dans leur juridiction.

Une conférence ministérielle sur les "Réseaux globaux de l'information" s'est tenue à Bonn du 6 au 8 juillet 1997. Dans la Déclaration[19] publiée à la suite de cette conférence, les ministres européens reconnaissent l'importance d'une cryptographie forte, et se déclarent en faveur de la disponibilité internationale et du libre choix des technologies cryptographiques par les utilisateurs, sous réserve des dispositions légales applicables. Ils soulignent que les mesures visant à assurer l'accès légal devraient être proportionnées et efficaces.

PAYS MEMBRES DE l'OCDE

Australie

Contrôles à l'exportation

L'Australie[20] est membre de l'Arrangement de Wassenaar.

L'exportation de matériels et logiciels de cryptographie à partir de l'Australie est régie par le Règlement 13E du Code des douanes (Exportations interdites)[21] et la Liste des Biens militaires et stratégiques que gère le Ministère de la défense[22].

Une autorisation écrite du Ministère de la défense est requise pour l'exportation de "systèmes, équipements ou composants" conçus ou modifiés de manière à utiliser la cryptographie, à assurer la sécurité de l'information ou à accomplir des fonctions de cryptanalyse. Les demandes de licences d'exportation sont revues par la Direction des transmissions militaires (*Defence Signals Directorate*) du Ministère. Dans la pratique, l'autorisation est maintenant accordée sans difficulté pour les logiciels de chiffrement dont la longueur de clé est inférieure ou égale à 56 bits.

Dans le cadre de ses mesures de contrôle à l'exportation, l'Australie n'applique pas la "Note générale relative aux logiciels" aux logiciels intervenant dans la sécurité de l'information, y compris les logiciels cryptographiques. En d'autres termes, les contrôles à l'exportation s'appliquent aux logiciels cryptographiques, même s'ils sont "du domaine public" ou s'ils sont "couramment disponibles". Toutefois, la "technologie" qui est du domaine public en est exclue.[23]

Les restrictions australiennes sur les exportations comportent les mêmes exemptions que celles énoncées dans la Liste des biens et technologies à double usage de l'Arrangement de Wassenaar. Il existe aussi une exemption pour usage personnel concernant l'exportation temporaire de quantités limitées de matériels ou logiciels cryptographiques par des citoyens australiens ou résidents permanents légaux, conformément aux limitations suivantes :

a) Aucun transfert de matériel, logiciel ou technologie n'a lieu en conséquence de l'exportation des produits cryptographiques.

b) Les produits cryptographiques restent sous le contrôle et en la possession de l'exportateur.

c) Les produits cryptographiques ne sont pas reproduits ni copiés.

d) Les produits cryptographiques doivent être rapportés en Australie quand l'exportateur revient en Australie ; et

e) Les produits cryptographiques ne doivent pas servir à la démonstration, commercialisation ou vente de produits cryptographiques soumis au contrôle.

La quantité de produits matériels ou logiciels cryptographiques qui peut être exportée conformément à la présente autorisation se limite à une unité de chaque produit matériel et un seul exemplaire de chaque produit logiciel par exportateur et par voyage en dehors de l'Australie. L'exportateur doit conserver pendant une période de 3 ans à compter de la date de chaque exportation temporaire un relevé des exportations et réimportations effectuées en vertu de ladite autorisation.

La législation australienne actuelle sur les contrôles à l'exportation ne donne pas de définition de la transmission de logiciels sous forme "tangible" ou "intangible" et la situation concernant l'application des restrictions à l'exportation n'est pas claire.

Mesures de contrôle intérieur et réglementation des importations

En Australie, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

Le Gouvernement australien n'envisage pas de modifier sa politique actuelle consistant à ne pas imposer de contrôle sur l'importation ou l'utilisation de produits cryptographiques. La question des contrôles à l'exportation sera revue à l'issue de la dernière série de discussions sur Wassenaar.

Autriche

Contrôles à l'exportation

L'Autriche est membre de l'Arrangement de Wassenaar et de l'Union européenne.

Les exportations de produits cryptographiques sont régies par la section 8 de *l'Aussenhandelsgesetz* (BGBl. Nr. 172/1995), qui interdit l'exportation si celle-ci est susceptible d'être en contravention avec le Règlement 3381/94 de l'UE ou d'autres obligations internationales ou de menacer la paix mondiale, la sécurité internationale ou la sécurité de l'Autriche ou encore de nuire aux relations extérieures de l'Autriche. L'exportation vers les zones de guerre est également interdite.

L'autorité responsable de l'administration des contrôles à l'exportation est le Ministère fédéral des affaires économiques[24].

Comme la Note générale relative aux logiciels figure à titre de référence dans la législation autrichienne, les logiciels "couramment disponibles" et les logiciels et technologies "du domaine public" n'entrent pas dans le champ d'application des mesures de contrôle.

Actuellement, la législation autrichienne sur les contrôles à l'exportation ne s'applique qu'aux exportations de produits cryptographiques qui se présentent sous une forme tangible.

Mesures de contrôle intérieur et réglementation des importations

En Autriche, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Le *Betriebsfunkverordnung* interdit l'utilisation de la cryptographie pour les transmissions radio internes à une organisation.

Evolution de la politique

L'Autriche suit les évolutions en cours au sein de l'UE, et n'a aucun projet susceptible de s'en écarter.

Belgique

Contrôles à l'exportation

La Belgique est membre de l'Arrangement de Wassenaar et de l'Union européenne.

En matière d'exportation, les règles belges sont inscrites dans la Loi du 5 août 1991, le Décret ministériel du 19 mai 1995 (portant application du Règlement de la CE) et le Décret royal du 8 mars 1993 concernant l'importation, l'exportation et la transmission d'armes, de munitions et de matériels à usage militaire et technologies connexes. Les contrôles suivent la réglementation de l'Union européenne sur l'exportation des produits cryptographiques. Pour l'exportation de matériels ou logiciels de cryptographie en dehors des pays du Bénélux, une licence d'exportation est requise.

C'est l'A.R.E., de la 4ème division, qui est l'organisme chargé de délivrer des licences pour l'exportation et la transmission de matériels cryptographiques. Les demandes de licences, accompagnées de la documentation technique correspondante, sont évaluées par les ingénieurs de la Division qui décident des dispositions législatives dont relève le produit. Lorsque le produit ne relève pas des mesures de contrôle à l'exportation, il peut être librement exporté et une attestation est délivrée à cet effet.

La Belgique applique les dispositions contenues dans la "Note générale relative aux logiciels" et les logiciels "couramment disponibles" et les logiciels et technologies "du domaine public" ne sont pas soumis à contrôle.

Les contrôles à l'exportation ne concernent que les exportations de biens matériels. Actuellement, les biens immatériels ne sont pas soumis aux contrôles, bien que la Belgique participe aux discussions sur cette question à l'échelon européen.

Mesures de contrôle intérieur et réglementation des importations

En Belgique, il n'y a pas actuellement de restrictions à l'importation des technologies de cryptographie.

La loi belge du 19 décembre 1997, ajoute un Article 109 à la Loi du 21 mars 1991 stipulant que "le recours à la cryptographie ne fera l'objet d'aucune restriction". Le but de cet article était de définir le cadre juridique nécessaire pour les applications de plus en plus répandues de la cryptographie. Il autorise

la libre utilisation des techniques cryptographiques dans le domaine privé, par les entreprises privées et sur les réseaux privés. Il est possible de transmettre librement des messages chiffrés. La Loi stipule également que :

> *Le Roi définira les services cryptographiques accessibles au grand public et pour l'usage desquels notification préalable doit être faite auprès de l'Institut belge des services postaux et des télécommunications (IBPT). Cette notification doit se faire par l'envoi d'une lettre recommandée quatre semaines au moins avant le début du recours à ces services.*

Les procédures permettant de s'acquitter de cette obligation, et les personnes physiques ou morales auxquelles s'appliquerait cette obligation devaient être précisées dans un décret d'application. Ce décret n'a toutefois jamais été publié et la cryptographie reste donc libre de toute restriction administrative. Compte tenu des évolutions récentes en Belgique concernant les signatures numériques[25] et la criminalité informatique (voir plus loin), c'est par ce biais que les problèmes liés à la cryptographie seront réglés dans une large mesure.

Evolution de la politique

Dans le cadre de la lutte menée contre le crime et de la volonté de modifier le Code pénal pour prendre en compte les nouvelles formes de délits liés à l'utilisation de l'ordinateur, un projet de loi sur la criminalité informatique est actuellement devant le parlement belge. Ce projet de loi autorise le Procureur général, en cas de flagrant délit, ou le magistrat instructeur, dans le cadre de son enquête, à faire déchiffrer un message pour le lire. Le procureur public ou le magistrat instructeur peut solliciter l'aide de toute personne possédant une connaissance particulière du système informatique, autre que le suspect lui-même ou un membre de sa famille, pour avoir accès sous une forme intelligible aux données chiffrées qui ont été stockées sur ce système ou transmises par son intermédiaire.

Canada

Contrôles à l'exportation

Le Canada est membre de l'Arrangement de Wassenaar.

Les mesures de contrôle des exportations appliquées par le Canada reposent sur la *Loi sur les licences d'exportation et d'importation* qui est administrée par le Ministère des affaires étrangères et du commerce international. La Liste des marchandises d'exportation contrôlée, promulguée en vertu de la loi, couvre un large éventail de biens militaires et stratégiques, notamment les produits matériels et logiciels conçus ou modifiés pour utiliser la cryptographie. Il existe toutefois un certain nombre d'exceptions, qui coïncident avec les exclusions prévues dans la liste de Wassenaar.

Le Canada dispense de licence d'exportation les logiciels grand public et logiciels du "domaine public" conformément à la Note générale relative aux logiciels de l'Arrangement de Wassenaar. Il est vivement encouragé de faire procéder à un examen ponctuel et à une clarification du statut des différents produits, ce qui implique notamment une évaluation détaillée des mécanismes de distribution susceptible de faire classer le produit comme logiciel grand public ou logiciel du domaine public.

Pour les produits cryptographiques soumis à contrôle, une licence individuelle d'exportation est requise, sauf dans les cas où un résident canadien se rendant temporairement à l'étranger souhaite

emporter avec lui son ordinateur portable sur lequel un logiciel de cryptographie est installé. Pour ce genre de situation, il existe une licence générale d'exportation.

Tous les produits originaires des Etats-Unis sont également contrôlés en vertu des règles canadiennes et doivent faire l'objet d'une licence d'exportation soit individuelle soit générale. Tous les types de produits cryptographiques peuvent être exportés sans licence du Canada vers les Etats-Unis. Toutefois, les produits cryptographiques originaires des Etats-Unis qui ne figurent pas sur la Liste des marchandises d'exportation contrôlée (par exemple logiciels grand public et logiciels du domaine public) ne peuvent être exportés du Canada sans une licence d'exportation canadienne individuelle ou générale.

Les exportations de produits cryptographiques étant hautement sensibles, le Canada encourage le respect de règles identiques pour les exportations de logiciels, que le produit soit sous forme matérielle (par exemple disquette) ou immatérielle (par exemple fichier électronique distribué via Internet).

Les licences d'exportation de produits soumis à contrôle sont délivrées par la Direction générale des contrôles à l'exportation et à l'importation du Ministère des affaires étrangères et du commerce international, après consultation des autres branches intéressées du Gouvernement canadien. Dans la pratique, l'autorisation d'exportation est maintenant accordée sans difficulté pour les logiciels de chiffrement DES ou équivalent dont la longueur des clés est inférieure ou égale à 56 bits. L'obtention de la licence est également facilitée lorsque la demande émane d'utilisateurs de confiance, comme les sociétés canadiennes ou les établissements financiers agréés.

Mesures de contrôle intérieur et réglementation des importations

Au Canada, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

Le Gouvernement canadien considère que si les avantages de la cryptographie pour le commerce électronique, la protection de la vie privée et la prévention du crime sont clairs, il est tout aussi vrai que les technologies de cryptographie peuvent être utilisées pour dissimuler des activités criminelles et menacer la sécurité nationale. Les investigations et poursuites, de même que le contrôle du respect des lois et réglementations, seront entravés s'il n'existe pas d'accès légal au texte en clair.

La politique canadienne dans le domaine de la cryptographie est en cours d'examen pour s'assurer qu'elle contribue à la réalisation de l'objectif que s'est fixé le Canada d'être un pays pilote dans l'utilisation du commerce électronique, et concilie au mieux les impératifs des entreprises, des droits de l'homme et de la vie privée, de la sécurité du public, du respect des lois et de la sécurité nationale. L'un des éléments de cet examen consistera en une procédure de consultation publique articulée autour d'un document de discussion intitulé "Politique cadre en matière de cryptographie aux fins du commerce électronique - Pour une économie et une société de l'information au Canada"[26] (février 1998). Une nouvelle politique de cryptographie pour le Canada sera rendue publique à l'automne 1998.

On trouvera une description de l'infrastructure à clé publique du Gouvernement du Canada, et des services d'authentification électronique et de confidentialité qu'elle assurera pour la prestation électronique des services publics, tant au plan interne qu'avec les clients, sur le site Web du Centre de la

sécurité des télécommunications, dans le document “Infrastructure à clé publique du Canada - Livre blanc” (février 1998)[27].

République tchèque

Contrôles à l’exportation

La République tchèque est membre de l’Arrangement de Wassenaar.

La République tchèque a récemment promulgué une loi de “Contrôle des exportations et importations de biens et technologies soumis aux régimes de contrôle internationaux”[28]. Un décret d’application de cette loi contient les listes de l’Union européenne et de l’Arrangement de Wassenaar concernant les biens à double usage soumis à contrôle.

Le Ministère de l’Industrie et du Commerce examine les licences d’exportation pour les produits soumis à contrôle. Il existe deux types de licences pour l’exportation de produits cryptographiques : la “licence individuelle” et la “licence ouverte individuelle”. Les exportateurs reçoivent habituellement une licence individuelle sur déclaration écrite concernant la transaction. Une licence ouverte individuelle s’applique à des exportations de biens spécifiques soumis à contrôle, dont on prévoit la répétition, à l’intérieur d’une zone territoriale et pendant une période définie.

Les restrictions d’exportation de la République tchèque ne s’appliquent qu’aux technologies sous forme tangible. Elles exemptent les logiciels “couramment disponibles” et les logiciels et technologies du domaine public.

Mesures de contrôle intérieur et réglementations concernant l’importation

Le régime de contrôle à l’exportation de la République tchèque décrit ci-dessus s’applique aussi de manière générale à l’importation de ces biens soumis à contrôle.[29] Toutefois, le Ministère a accordé une licence générale pour l’importation des produits cryptographiques[30]. Ainsi, alors que le gouvernement conserve le pouvoir de contrôler les importations de biens de chiffrement, un importateur de produits comportant des moyens de cryptographie n’a actuellement besoin d’aucune autorisation spéciale pour ces importations.

En République tchèque, il n’y a pas actuellement de mesures de contrôle intérieur sur l’utilisation de la cryptographie.

Danemark

Contrôles à l’exportation

Le Danemark est membre de l’Arrangement de Wassenaar et de l’Union européenne.

Il applique des contrôles à l’exportation en vertu du Décret sur les exportations de biens, technologies et savoir-faire à double usage[31]. L’autorité chargée de la délivrance des licences est l’Agence danoise du Commerce et de l’Industrie.

Le Danemark applique aux produits cryptographiques la Note générale relative aux logiciels conformément au texte de Wassenaar. Un exportateur peut contacter l'autorité chargée du contrôle des exportations pour savoir si un produit cryptographique est dispensé des obligations habituelles en matière de licence.

La législation danoise sur les contrôles à l'exportation couvre les transferts de logiciels sous forme aussi bien tangible qu'immatérielle. Bien qu'il n'y ait pas de contrôle préalable véritable susceptible d'empêcher les transferts non autorisés de produits immatériels, des sanctions pénales peuvent être appliquées en cas de transferts non autorisés de produits qui sont soumis aux contrôles à l'exportation.

Mesures de contrôle intérieur et réglementation des importations

Le Danemark n'applique pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

Le Danemark tendra en général à équilibrer les besoins des autorités chargées de faire appliquer les lois pour l'accès légal aux données transmises ou stockées avec les demandes des entreprises commerciales et des citoyens pour une politique renforcée de la cryptographie. Un Comité d'experts sur la cryptographie, sous les auspices du Ministère de la Recherche et des Technologies de l'information et comprenant des représentants d'autres ministères danois, a publié un rapport en avril 1997[32]. Ce Comité a étudié les avantages et inconvénients de l'introduction d'une réglementation sur l'utilisation et la vente de produits cryptographiques. Le Comité a recommandé de n'introduire aucune réglementation mais a indiqué qu'il convenait d'envisager la politique danoise en matière de cryptographie à la lumière de l'évolution internationale. Une analyse des effets qu'aurait l'introduction de dispositifs incitatifs en vue d'encourager l'emploi de systèmes à récupération de clés a été achevée en mai 1998, et a débouché sur la conclusion qu'il n'était pas possible de recommander l'introduction de ce type de mécanismes compte tenu de la situation internationale actuelle.

Dans ce contexte, le Comité d'experts a présenté ses conclusions finales en juin 1998. Il a conclu qu'il ne fallait introduire au stade actuel ni réglementation ni mécanisme d'incitation, mais néanmoins suivre de très près les évolutions à l'échelon international et réexaminer la possibilité de réglementer la cryptographie, si l'approche internationale générale évoluait dans ce sens. Le Gouvernement danois envisage actuellement de formuler une politique danoise de la cryptographie sur le contenu de la recommandation du Comité d'experts.

Finlande

Contrôles à l'exportation

La Finlande est membre de l'Arrangement de Wassenaar et de l'Union européenne.

Les contrôles sur l'exportation des produits cryptographiques depuis la Finlande relèvent de la Loi sur le contrôle des exportations de biens à double usage (562/96), du Décret sur les exportations de biens à double usage (645/96) et de la Décision du ministère du Commerce et de l'Industrie sur les

licences d'exportation de produits à double usage (9 janvier 1997, 54/1997). Ces lois transposent les réglementations et décisions de la CE concernant l'exportation de biens à double usage.

Pour l'exportation de produits cryptographiques, une licence est requise, conformément à une loi de 1996. L'autorité chargée de la délivrance des licences est le ministère du Commerce et de l'Industrie.

La législation finlandaise reprend les dispositions des décisions et réglementations de la CE. La Finlande applique la Note générale relative au logiciels : aucune licence d'exportation n'est requise pour les logiciels "couramment disponibles" ou pour les logiciels et technologies du domaine public. Toutefois, la Finlande restreint l'exportation de "l'assistance technique" et autres "services".

Les contrôles à l'exportation appliqués par la Finlande couvrent les transferts de logiciels sous forme aussi matérielle qu'immatérielle.

Mesures de contrôle intérieur et réglementation des importations

En Finlande, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

La politique nationale de la Finlande à l'égard des questions de cryptographie est toujours en préparation. Le niveau de contrôle des exportations de biens à double usage a été, et continuera d'être, convenu avec les autres pays participants aux régimes internationaux de contrôle des exportations, comme l'Arrangement de Wassenaar.

France

Contrôles à l'exportation, mesures de contrôle intérieur ou réglementation des importations[33]

La France est membre de l'Arrangement de Wassenaar et de l'Union européenne.

L'organisme gouvernemental chargé de mettre en œuvre la législation concernant la cryptographie est le Service Central de la Sécurité des Systèmes d'Information (SCSSI)[34], placé sous l'autorité du Secrétaire général de la Défense nationale.

En France, les mesures de contrôle sur le chiffrement sont régies par :

- La loi 90-1170 du 29 décembre 1990 (Journal officiel du 30 décembre 1990), notamment son article 28, modifiée par la loi 91-648 du 11 juillet 1991 (Journal officiel du 13 juillet) et de nouveau modifiée par la loi 96-659 du 26 juillet 1996, notamment l'Article 17 sur les sanctions pénales (Journal officiel du 27 juillet 1996).

- Le décret 95-613 du 5 mai 1995 relatif au contrôle à l'exportation de biens à double usage (Journal officiel du 7 mai 1995, page 7547).

- L'arrêté du 5 mai 1995 relatif au contrôle à l'exportation vers les pays tiers et au transfert vers les Etats membres de la Communauté européenne de biens à double usage (Journal officiel du 7 mai 1995, page 7561).

- L'arrêté du 5 mai 1995 définissant la licence générale G.502 d'exportation des moyens de cryptologie et fixant les modalités d'établissement et d'utilisation de cette licence (Journal officiel du 7 mai 1995, page 7578).

- Le décret 96-67 du 29 janvier 1996 relatif aux compétences du secrétaire général de la défense nationale (SGDN) dans le domaine de la sécurité des systèmes informatiques (Journal officiel du 30 janvier 1996).

- Le décret 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 (Journal officiel du 25 février 1998, page 2911).

- Le décret 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 (Journal officiel du 25 février 1998, page 2915).

En résumé, l'Article 28 de la Loi du 29 décembre 1990 sur la réglementation des télécommunications stipule que pour l'utilisation, la fourniture et l'exportation de produits de cryptographie n'ayant d'autre objet que d'authentifier des données ou d'assurer l'intégrité de données, une déclaration préalable est requise. Une copie du récépissé de cette déclaration doit être présentée à la douane à chaque exportation. Pour les exportations temporaires, une déclaration de l'utilisateur sert de déclaration d'exportation dans le cas de produits de cryptographie exclusivement à l'usage personnel de cet utilisateur. Pour tout autre type de cryptographie, une autorisation préalable est requise.

La France a actualisé sa loi sur les télécommunications[35] en 1996 ("loi du 26 juillet"). L'Article 17 de cette nouvelle loi traite de la cryptographie. La fourniture, l'importation à partir de pays n'appartenant pas à l'Union européenne ou l'exportation d'un dispositif ou service de chiffrement sont soumis à autorisation s'ils assurent des fonctions de confidentialité.

La loi française ne reprend pas les dispositions de la Note générale relative aux logiciels visant l'exportation de produits de cryptographie depuis la France.

Les contrôles à l'exportation appliqués par la France ne font pas de distinction entre les logiciels qui font l'objet d'une exportation physique, sous forme matérielle, et ceux qui sont distribués sous forme immatérielle, par exemple via un réseau pour données comme Internet.

En ce qui concerne l'utilisation de produits de cryptographie en France, l'Article 17 de la loi du 26 juillet assouplit les restrictions sur l'utilisation des dispositifs d'authentification, en stipulant qu'aucune déclaration préalable ne sera requise "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" (c'est-à-dire un tiers de confiance agréé).

Conformément à la législation française, le tiers de confiance sera un organisme agréé par l'Etat, chargé de gérer les clés de chiffrement pour les utilisateurs. La licence stipulera que le tiers de confiance doit, en vertu de la loi, remettre les clés de chiffrement aux autorités habilitées de telle sorte que l'Etat puisse avoir accès, si besoin est, aux informations. La fourniture de produits cryptographiques reste soumise à autorisation même si on les utilise en recourant à un tiers de confiance.

Le gouvernement français décrit la fonction du tiers de confiance en ces termes :

> *"Le tiers de confiance est un organisme agréé qui gère des clés de chiffrement pour le compte de l'utilisateur. Ce dernier passe un contrat avec le tiers de confiance qui lui transmet régulièrement les clés à utiliser pour chiffrer son information. Dans la licence du tiers de confiance figure une clause par laquelle celui-ci doit, en vertu de la loi, remettre les clés de chiffrement aux autorités habilitées, sur présentation d'une Commission rogatoire ou d'un ordre du Premier ministre. Ainsi l'utilisateur peut-il s'appuyer sur un professionnel de la cryptologie qui lui garantit un service de haute qualité, tandis que l'Etat peut, en cas de besoin, accéder au contenu de l'information".*

Evolution de la politique

La loi du 26 juillet est en vigueur, et on prévoit que les premiers tiers de confiance se verront attribuer une licence vers la fin du mois de septembre 1998. Le Ministère de l'Industrie doit organiser au début de 1999 un Forum pour un débat sur la mise en oeuvre de la Loi et l'examen d'amendements aux réglementations.

Allemagne

Contrôles à l'exportation

L'Allemagne est membre de l'Arrangement de Wassenaar et de l'Union européenne.

L'exportation de produits cryptographiques est régie en conformité avec le Règlement de l'Union européenne sur les biens à double usage. L'autorité qui administre ces dispositions est le Ministère Fédéral de l'Economie (BMWi).

Les logiciels "couramment disponibles" et les logiciels et technologies "du domaine public" ne sont pas soumis à ces contrôles.

Mesures de contrôle intérieur et réglementation des importations

En Allemagne, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

De manière générale, "l'Initiative du gouvernement fédéral en matière de commerce électronique", du 29 octobre 1997, expose l'approche du Ministère de l'Economie à l'égard du commerce électronique[36]. Cette déclaration indique que "le gouvernement allemand n'a pas actuellement l'intention

de légiférer sur la commercialisation et l'utilisation des produits de chiffrement. Ainsi, en Allemagne, on peut librement choisir et utiliser les systèmes de chiffrement".

Le rapport intérimaire du Gouvernement sur le plan d'action allemand "Info 2000 - la voie allemande vers la société de l'information" (automne 1997) énonce les objectifs suivants qui doivent être poursuivis concernant les produits de cryptographie :

- Veiller à ce que l'Allemagne dispose en permanence de systèmes fiables et robustes.
- Protéger la sécurité du pays et défendre les intérêts des autorités chargés des poursuites criminelles.
- Renforcer la position sur le marché des producteurs allemands de systèmes de chiffrement.

Le Gouvernement fédéral allemand a accepté de se dispenser de toute réglementation juridique visant la libre circulation et l'utilisation des produits et procédés de chiffrement pendant la législature en cours, ce qui signifie que les utilisateurs allemands conservent l'entière liberté de choisir et d'utiliser les systèmes cryptographiques qu'ils préfèrent. Le Gouvernement fédéral continuera de suivre de près les évolutions dans le domaine des technologies de cryptographie, principalement dans le contexte de la coopération européenne et internationale, et il prendra de nouvelles mesures, si nécessaire, pour mettre en oeuvre les objectifs qu'il s'est fixés.

Grèce

Contrôles à l'exportation

La Grèce est membre de l'Arrangement de Wassenaar et de l'Union européenne.

Mesures de contrôle intérieur et réglementation des importations

En Grèce, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Hongrie

Contrôles à l'exportation

La Hongrie est membre de l'Arrangement de Wassenaar.

Elle applique des contrôles conformément à la liste des biens à double usage établie par cet accord. L'autorité chargée de la délivrance des licences est le Ministère des Affaires économiques.

Les exportations de logiciels "couramment disponibles" et de logiciels et technologies du domaine public en sont exemptées.

Mesures de contrôle intérieur et réglementation des importations

Il existe un contrôle à l'importation symétrique du contrôle à l'exportation : une licence d'importation est requise si une licence d'exportation est nécessaire en Hongrie pour le même produit. Il n'y a pas de législation régissant l'utilisation de la cryptographie sur le plan intérieur.

Islande

Contrôles à l'exportation, mesures de contrôle intérieur et réglementation des importations.

En Islande, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie, ni de restrictions à l'exportation ou à l'importation de technologies cryptographiques.

Irlande

Contrôles à l'exportation

L'Irlande est membre de l'Arrangement de Wassenaar et de l'Union européenne.

Les mesures de contrôle des exportations appliquées par l'Irlande relèvent de la Loi sur le contrôle des exportations de 1983 (N°35 de 1983), du Décret de 1996 sur le contrôle des exportations (SI N°363 de 1996), qui énumère les articles militaires et paramilitaires soumis à l'obligation d'une licence d'exportation, du Règlement de 1996 des Communautés européennes (contrôle des exportations de biens à double usage) (SI N°362 de 1996), qui fixe les sanctions en cas d'infraction au Règlement de l'UE et de la Loi sur les douanes de 1956 (N°7 de 1956).

L'autorité chargée de délivrer les licences pour l'exportation de produits cryptographiques en Irlande est l'Unité des licences d'exportation du Ministère des entreprises, du commerce et de l'emploi.

L'Irlande applique la Note générale relative aux logiciels conformément au libellé de l'Arrangement de Wassenaar.

Mesures de contrôle intérieur et réglementation des importations

En Irlande, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Italie

Contrôles à l'exportation

L'Italie est membre de l'Arrangement de Wassenaar et de l'Union européenne.

L'Italie applique le Règlement de l'Union européenne sur les biens à double usage concernant l'exportation de technologies de cryptographie. L'autorité responsable de la délivrance des licences d'exportation de produits cryptographiques (produits énumérés dans l'Annexe 1 de la Décision

96/613/CUSP du Conseil de l'UE) est le *Ministerio del commercio con l'estero* (Ministère du commerce extérieur). La délivrance des autorisations est régie par l'Article 2 de la Loi N°89, du 24 février 1997.

La Note générale relative aux logiciels est appliquée en Italie. Les logiciels couramment à la disposition du public ou appartenant au domaine public ne sont pas soumis à autorisation et peuvent être librement exportés.

La situation actuelle n'est pas claire concernant le fait de savoir si les contrôles à l'exportation appliqués en Italie couvrent à la fois les exportations de logiciels sous forme tangibles et celles de logiciels sous forme immatérielle.

Mesures de contrôle intérieur et réglementation des importations

Avant la Loi No. 59 du 15 mars 1997 et le Décret du Président de la République No. 513 du 10 novembre 1997, l'Italie n'appliquait aucune mesure particulière de contrôle intérieur de la cryptographie, à l'exception des dispositions des articles 12 et 24 de la Loi No. 801 du 24 octobre 1997, qui portent sur des aspects spécifiques de la protection des secrets d'Etat et de la diffusion d'informations dont la divulgation est interdite. D'autres dispositions figurent dans les diverses réglementations relatives au contrôle, à l'exportation, à l'importation et au transit des armements ainsi qu'à l'exportation et au transit de matériels présentant une importance stratégique particulière[37].

Les technologies de cryptographie dans l'administration publique ne sont que brièvement mentionnées dans certaines des décisions de l'autorité chargée de la technologie de l'information dans l'administration publique (AIPA)[38], par exemple dans la décision du 28 juillet 1994, article 1, No. 9. Il y est déclaré que les questions relatives à l'utilisation du chiffrement, de la protection et de la conservation des clés pertinentes et l'utilisation des systèmes de signature électronique seront réglementées par des dispositions législatives ultérieures.[39] Il est déclaré en outre que chaque dossier stocké sur disque optique devrait contenir des informations sur la cryptographie conformément à des règles qui seraient définies ultérieurement.

Pour ce qui est des problèmes de sécurité soulevés par les techniques spécifiques d'utilisation des dispositifs de stockage optique, il est mentionné dans les notes explicatives de la décision citée plus haut que : "pour des raisons de confidentialité, la cryptographie doit être autorisée pour le stockage d'informations sur disque mais que, en pareil cas, l'algorithme cryptographique doit être normalisé et que les procédures de formation et de conservation des mots clés isolés ainsi que les responsabilités pertinentes doivent être régies par des réglementations spécifiques."

La cryptographie est aussi mentionnée dans l'étude de faisabilité sur le Réseau unitaire de l'administration publique [40]. Cette étude de vaste portée prévoit que la sécurité du Réseau unitaire sera assurée par le biais de domaines. Afin de garantir l'origine, le contenu, le caractère privé et la non-répudiation des messages échangés par les domaines, on utilisera des logiciels d'application fondés sur une cryptographie symétrique et/ou à clé publique. Ces clés seront gérées par un organisme qui sera constitué par la Présidence du Conseil des Ministres, dont il relèvera directement, et qui comprendra les trois sections distinctes : (1) la création et la distribution des clés, dépendant du centre des services ; (2) la gestion des documents notariés, dépendant du centre d'exploitation et (3) la certification des clés, dépendant de l'Agence pour la technologie de l'information.

Le rapport général contient aussi des études sur l'utilisation des signatures électroniques (pouvant garantir l'intégrité des données et la sécurité de l'origine du message) et sur la cryptographie à clé publique (assurant le caractère privé des données).

A la fin de 1995, l'AIPA a examiné des projets de dispositions concernant les documents juridiques et autres présentés sous forme électronique conformément à l'Article 3 du Décret loi No. 39 du 3 février 1993. Etant donné que ce texte résultait des travaux d'un groupe d'étude, l'AIPA l'a publié sur Internet afin de connaître les réactions du public. L'étude traite également de questions relatives à la gestion et au stockage des clés de chiffrement.

En novembre 1996, l'AIPA a présenté un document sur le "Réseau des organes et services responsables des systèmes de traitement de l'information automatisés", où il est question des problèmes relatifs à la sécurité du réseau et à l'emploi de la cryptographie.

La Loi No. 52 du 15 mars 1997 reconnaît par ailleurs la validité juridique des documents informatiques. Elle charge le gouvernement de réglementer l'attribution des fonctions et des tâches aux régions et aux autorités locales dans une perspective de restructuration de l'administration publique et de simplification des procédures administratives. Plus précisément, elle stipule que "les actes, les données et les documents produits par l'administration publique ou par des particuliers par le biais de systèmes d'ordinateurs et de systèmes de télécommunications et d'information, sont juridiquement valides et produisent leurs effets à toutes fins juridiques."[41]

En application de la loi susmentionnée, le Décret du Président de la République No. 513, du 10 novembre 1997, a été publié pour définir les règles concernant les critères et les modalités de formulation, de stockage et de transmission de documents par les systèmes d'ordinateurs et les systèmes de télécommunications et d'information. Ce Décret contient des mesures concernant notamment les documents informatiques et leur valeur probante ainsi que les systèmes de signature et de validation numériques, et l'utilisation de la cryptographie (systèmes à clé de chiffrement asymétrique), aussi bien dans le secteur privé que dans le secteur public.

L'Article 15 de la Loi No. 657 du 31 décembre 1996 sur la protection des personnes physiques et le traitement des données à caractère personnel est consacré à la sécurité des données. Il stipule que les normes minimales de sécurité qui doivent être adoptées à titre préventif (y compris la cryptographie) seront définies dans le cadre d'un ensemble de règles qui sera promulgué sous forme d'un Décret du Président de la République, sur proposition du Ministre de la justice, après consultation de l'AIPA et de l'Office de protection des données.

Japon

Contrôles à l'exportation

Le Japon est membre de l'Arrangement de Wassenaar.

Il applique des restrictions à l'exportation des produits cryptographiques conformément à la liste des biens à double usage établie par cet accord. L'exportation depuis le Japon de produits cryptographiques est régie par la Loi sur les échanges et le commerce extérieur (Loi N°228, 1949), l'Arrêté sur les échanges (Arrêté ministériel N°260, 1980), l'Arrêté sur le contrôle du commerce à l'exportation (Arrêté ministériel N°63, de 1949) et la Notification du Bureau de l'administration du commerce international (N°492, de 1992).

Une licence d'exportation est requise pour tous les produits cryptographiques et le ministère du Commerce international et de l'Industrie (MITI), qui est l'autorité chargée de la délivrance des licences, prend en principe une décision sur chaque demande de licence individuellement. Des procédures simplifiées ont été introduites en février 1998 concernant des produits considérés comme moins sensibles, comme les dispositifs DVD, les récepteurs de télévision numérique à péage, etc.

Les contrôles à l'exportation appliqués par le Japon respectent les dispositions de la Note générale relative aux logiciels ; les logiciels couramment à la disposition du public ou du domaine public ne sont pas visés par les contrôles.

Les mesures de contrôles mises en oeuvre par le Japon s'appliquent aux exportations de logiciels sous forme aussi bien matérielle qu'immatérielle.

Mesures de contrôle intérieur et réglementation des importations

Au Japon, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

De manière générale, deux ministères élaborent la politique japonaise en matière de cryptographie : le Ministère des Postes et Télécommunications (MPT)[42] et le ministère du Commerce international et de l'Industrie (MITI)[43]. Récemment, l'Agence de police nationale et le Ministère de la Justice ont aussi joué un rôle dans ce domaine.

En mai 1997, le MITI a publié un document intitulé "*Towards the Age of the Digital Economy - For Rapid Progress in the Japanese Economy and World Economic Growth in the 21st Century*"[44] qui présente l'approche de ce ministère à l'égard du commerce électronique en général. Il considère la cryptographie comme un outil important pour assurer la sécurité de l'information dans le commerce électronique. Il faut promouvoir le développement de la cryptographie et les investigations dans ce domaine, et donner aux utilisateurs des réseaux beaucoup plus d'informations sur les diverses initiatives en cours.

Etant donné que la cryptographie, qui est un instrument important de lutte contre la délinquance informatique, peut aussi être employée pour commettre divers délits, l'Agence de police nationale envisage d'adopter une politique de cryptologie qui permettra à la fois de promouvoir ces technologies et d'en éviter les utilisations abusives. Elle a donc examiné la politique de cryptographie en coopération avec un organisme extérieur et celui-ci a publié un document en février 1998.

Le rapport d'orientation intitulé *"Vision 21 for info-Communications"*, qui a été soumis au MPT par le Conseil des télécommunications en juin 1997, a souligné qu'il était indispensable d'instituer des mesures de sécurité comme le chiffrement, afin de créer un environnement favorable au commerce électronique et aux règlements électroniques sur les réseaux, et qu'il convenait de faciliter aussi bien le développement des technologies cryptographiques et la définition d'une politique dans ce domaine que la coopération internationale.

Corée

Contrôles à l'exportation

La Corée est membre de l'Arrangement de Wassenaar.

Elle applique des contrôles sur les exportations de matériels et logiciels cryptographiques conformément à cet accord. Les réglementations relatives à l'exportation de produits cryptographiques sont issues de l'Avis public sur l'exportation et l'importation de biens stratégiques, qui a été publié en vertu de la Loi sur le commerce extérieur et de son décret d'application. L'autorité chargée de la délivrance des licences est le ministère du Commerce, de l'Industrie et de l'Energie.

La Corée a repris la Note générale relative aux logiciels dans son Avis public, dont les dispositions pertinentes suivent le texte de l'Arrangement de Wassenaar. Les contrôle à l'exportation appliqués par la Corée ne concernent pas les logiciels qui sont "du domaine public" ou "couramment à la disposition du public".

Mesures de contrôle intérieur et réglementation des importations

Il n'existe pas de restrictions à l'importation des technologies de cryptographie. Il n'y a pas de réglementation régissant spécifiquement l'utilisation de la cryptographie sur le plan intérieur.

Evolution de la politique

En 1998, le ministère du Commerce, de l'Industrie et de l'Energie et le Ministère de la Justice ont conjointement proposé un projet de loi sur les transactions électroniques qui définit l'utilisation des technologies de cryptographie pour le commerce électronique en vue de renforcer la confiance des utilisateurs et des consommateurs. Le projet de loi stipule également que le gouvernement pourrait envisager des mesures concernant l'accès légal, lorsqu'il le jugera nécessaire pour des raisons de sécurité nationale.

En mai 1998, le Ministère de l'Information et des communications (MIC) a organisé un groupe de travail composé d'experts provenant de l'industrie, des universités et d'instituts de recherche pour qu'il étudie l'utilisation au plan intérieur de la cryptographie en vue de mettre en oeuvre les Lignes directrices de l'OCDE régissant la politique de cryptographie. Le MIC travaille également sur des mesures visant à protéger les informations importantes conservées par les autorités publiques et privées grâce à l'utilisation de technologies de cryptographie et au renforcement de la coopération internationale pour la gestion des clés publiques.

Luxembourg

Contrôles à l'exportation

Le Luxembourg est membre de l'Arrangement de Wassenaar et de l'Union européenne.

Le Luxembourg applique des contrôles sur les matériels et logiciels cryptographiques conformément au Règlement de l'Union européenne concernant les biens à double usage.

Mesures de contrôle intérieur et réglementation des importations

Au Luxembourg, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Mexique

Contrôles à l'exportation, mesures de contrôle intérieur et réglementation des importations

Au Mexique, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie, ni de restrictions à l'exportation ou à l'importation de technologies de cryptographie.

Pays-Bas

Contrôles à l'exportation

Les Pays-Bas sont membres de l'Arrangement de Wassenaar et de l'Union européenne.

L'exportation de logiciels et de matériels de cryptographie est réglementée par la législation nationale, à savoir la Loi de 1962 sur l'importation et l'exportation (Recueil des lois néerlandaises 1962, 295) et la Décision ministérielle concomitante sur l'exportation de biens stratégiques (Recueil des lois néerlandaises 1963, 128).

Une licence est nécessaire pour toute exportation de logiciel ou matériel de cryptographie à partir des Pays-Bas. L'autorité qui administre ces dispositions est l'Agence centrale pour l'importation et l'exportation, qui relève du Ministère des Affaires Economiques. A la réception de la demande, un processus d'évaluation est mis en route qui conduit à la décision d'octroyer ou non une licence d'exportation. En pratique, les produits sont évalués au cas par cas.

Les Pays-Bas appliquent la Note générale relative aux logiciels : l'exportation de logiciels et de technologies de grande diffusion ou qui sont du domaine public, ne requiert pas de licence. Le texte de la note est repris dans les instruments juridiques régissant les contrôle à l'exportation aux Pays-Bas, et il est appliqué par les autorités chargées du contrôle des exportations. Les expressions "assistance importante" et "du domaine public" sont interprétés au sens strict par ces autorités. Il est arrivé que des exportateurs ayant effectué eux-mêmes une interprétation trop libérale de la Note soient rappelés à l'ordre.

Actuellement, la législation néerlandaise sur les contrôles à l'exportation ne vise que les biens matériels. Cela comprend les logiciels incorporés dans des produits ou stockés sur disque, mais les transmissions sous forme immatérielle ne sont pas considérées comme des exportations.

Mesures de contrôle intérieur et réglementation des importations

Les Pays-Bas n'imposent aucune restriction à l'importation de technologies cryptographiques.

S'agissant de la réglementation intérieure, la Loi sur les télécommunications en vigueur actuellement stipule que l'utilisation de la cryptographie dans des réseaux de radiocommunications terrestres fermés (par opposition aux réseaux mobiles publics) est soumise à des restrictions et suppose l'octroi d'une licence par les services de réglementation des télécommunications. Dans le projet de loi sur

les télécommunications (approuvé par la première session du Parlement le 7 avril 1998), cette restriction ne figure plus.

Conformément à la Résolution du Conseil européen qui définit les spécifications internationales pour l'interception légale des télécommunications, la Loi néerlandaise sur les télécommunications fait obligation aux opérateurs de réseaux et aux fournisseurs de services de transmettre le signal en clair lorsqu'un ordre légal d'interception est donné.

La Loi néerlandaise sur la délinquance informatique précise que, dans le cas de données stockées sous forme chiffrée, sous le couvert d'une autorisation légale, toute entité concernée (à l'exclusion du suspect) est tenue de coopérer avec les autorités chargées de faire appliquer la loi. Cela afin de leur permettre d'avoir accès légalement aux données en clair.

Nouvelle-Zélande

Contrôles à l'exportation

La Nouvelle-Zélande est membre de l'Arrangement de Wassenaar.

La Nouvelle-Zélande applique les contrôles établis par cet accord par le biais des dispositions de la Loi sur les douanes et droits d'accises de 1996 et du Règlement des interdictions d'exportation de 1996. L'exportation de produits cryptographiques nécessite une licence d'exportation de produit stratégique, délivrée par la Division de la sécurité internationale et du contrôle des armes du Ministère des Affaires étrangères (MFAT). Cet organisme examine chaque demande individuellement.

Les contrôles appliqués par la Nouvelle-Zélande ne couvrent pas la cryptographie "du domaine public" ou "couramment à la disposition du public".

Actuellement, la Loi sur les douanes ne s'applique qu'aux exportations de produits cryptographiques sous forme tangible, tels que livres, CD-ROM ou disques. Il n'existe techniquement pas de contrôle sur l'exportation de produits cryptographiques sous forme immatérielle (électronique). (Mais l'exportation serait expressément interdite si elle devait contribuer à un programme de production d'armes de destruction massive.) Cet aspect de la Loi sur les douanes est en cours de réexamen.

Mesures de contrôle intérieur et réglementation des importations

En Nouvelle-Zélande, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

Bien qu'il ne soit actuellement envisagé aucun amendement à la législation intérieure néo-zélandaise, ce domaine reste constamment à l'étude afin de permettre la prise en compte des évolutions technologiques ou autres.

Un Comité national pour la politique de cryptographie, présidé par un représentant du Cabinet du premier Ministre et auquel participent des membres de diverses instances, notamment du ministère du Commerce, du MFAT, du Ministère de la Justice, de la Police néo-zélandaise et du Service des douanes

néo-zélandais a été formé pour coordonner les attributions des différents organismes dans des domaines comme les contrôles à l'exportation visant les produits stratégiques et les signatures numériques. C'est le ministère du Commerce qui a la responsabilité principale des questions touchant le commerce électronique au sein du Gouvernement néo-zélandais.

Norvège

Contrôles à l'exportation

La Norvège est membre de l'Arrangement de Wassenaar.

L'exportation de produits cryptographiques depuis la Norvège est réglementée par la Loi N°93 du 18 décembre 1987, relative au contrôle à l'exportation des biens, services, technologies etc. stratégiques, le Règlement du 10 janvier 1989 mettant en oeuvre le contrôle à l'exportation des biens, services, technologies, etc. stratégiques et la Liste des biens et technologies à double usage. Les contrôles à l'exportation sont administrés par le Ministère des Affaires étrangères.

La législation norvégienne suit les dispenses prévues dans la Note générale relative aux logiciels de l'Arrangement de Wassenaar. De plus, le distribution via Internet est considérée comme une base suffisante pour l'application de la Note générale relative aux logiciels.

Mesures de contrôle intérieur et réglementation des importations

En Norvège, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

Le Parlement norvégien a adopté une Loi sur la protection de la sécurité nationale (*Lov om forebyggende sikkerhetstjenester mm (Sikkerhetsloven),* St.prp N°12 (1997-98). Cette Loi entrera en vigueur dès que les décrets d'application seront prêts, ce qui devrait intervenir au printemps de 1999. Le Service d'inspection des données (*Datattilsynet)* devrait imposer le chiffrement des données de caractère personnel sensibles dans le cas de transmissions extérieures.

Un rapport du Conseil de la sécurité des technologies de l'information de Norvège recommande l'amendement de la politique existante ou la mise en place d'une politique de cryptographie dans les domaines prioritaires suivants : Administration publique, sécurité nationale, secteur de la justice, santé, échanges entre le secteur privé et l'administration publique, respect de la vie privée et services de tiers de confiance.

Pologne

Contrôles à l'exportation

La Pologne est membre de l'Arrangement de Wassenaar et a l'intention de devenir membre de l'Union européenne.

Une licence est requise pour l'exportation de logiciels ou matériels cryptographiques, conformément au Règlement de l'Union européenne sur les biens à double usage.

Mesures de contrôle intérieur et réglementation des importations

En Pologne, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie.

L'importation de technologies de cryptographie nécessite soit une autorisation générale soit un certificat d'importation.

Portugal

Contrôles à l'exportation

Le Portugal est membre de l'Arrangement de Wassenaar et de l'Union européenne.

Il applique des contrôles conformément au Règlement de l'Union européenne sur les biens à double usage. L'autorité chargée de la délivrance des licences est la Direction générale du commerce.

Mesures de contrôle intérieur et réglementation des importations

Au Portugal, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Espagne

Contrôles à l'exportation

L'Espagne est membre de l'Arrangement de Wassenaar et de l'Union européenne.

L'exportation de produits cryptographiques est régie par le *Real Decreto 491/1998 de 27 de marzo,* portant approbation du *Reglamento del Comercio Exterior de Materia de Defensa y de Doble Uso (*Journal Officiel du 8 avril 1998). Ce décret transpose en droit national l'Arrangement de Wassenaar et le Règlement de l'Union européenne sur les biens à double usage. Les produits cryptographiques sont spécifiquement cités dans l'Annexe I.1 (11) et l'Annexe II (12). Ils le sont aussi implicitement dans l'Annexe I.1 (18), qui couvre les moyens (équipements et technologies) nécessaires à leur fabrication. L'application et l'administration du décret sont confiées à un Comité interministériel (*Junta Interministerial Reguladora del Comercio Exterior de Materia de Defensa y de Doble Uso),* présidé par le Secrétaire d'Etat au Commerce.

Le Décret comporte à la fois une Note générale sur la technologie (Annexe I.1 *Nota general de technología)* et une Note générale relative aux logiciels qui reprend le libellé de l'Arrangement de Wassenaar (Annexe I.2 (1) (d) *Nota general para el equipo lógico).*

Les contrôles à l'exportation appliqués par l'Espagne concernent les exportations de logiciels sous forme aussi bien matérielle qu'immatérielle.

Mesures de contrôle intérieur et réglementation des importations

En Espagne, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie. L'Article 52(1) de la Loi générale sur les télécommunications[45] établit la liberté d'utiliser n'importe quel programme ou produit cryptographique pour protéger les échanges de données sur les réseaux de télécommunications.

Il n'y a pas non plus de restrictions à l'importation des technologies de cryptographie à l'usage des entreprises privées. Les contrôles ne s'appliquent que si le produit ou système importé, qu'il soit autonome ou intégré, est destiné à un usage relevant de la sécurité nationale. Ces contrôles sont mis en oeuvre par le *Centro Criptológico Nacional*, CESID, du Ministère de la Défense.

Evolution de la politique

Bien que l'Article 52(2) de la Loi générale sur les télécommunications autorise la création de mesures de contrôle administratif par le biais de la promulgation de réglementations spécifiques supplémentaires, il n'y a pas actuellement de travaux dans ce domaine.

Suède

Contrôles à l'exportation

La Suède est membre de l'Arrangement de Wassenaar et de l'Union européenne.

La Suède a transposé les dispositions et décisions de l'UE dans sa Loi sur le produits stratégiques (1991:341) et l'Arrêté sur les produits stratégiques (1994:2060). L'autorité chargée de la délivrance des licences est l'Inspection des biens stratégiques.

La Suède applique les dispositions de la Note générale relative aux logiciels, telle qu'elle figure dans l'Arrangement de Wassenaar.

Mesures de contrôle intérieur et réglementation des importations

En Suède, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

Le gouvernement suédois étudie actuellement les questions touchant à la politique de cryptographie, et des lignes directrices sont en préparation.

En octobre 1997, le gouvernement suédois a publié un rapport intitulé *"Cryptography Policy: Possible Courses of Action for Sweden"* [Politique cryptographique : lignes d'action possibles pour la Suède]. Bien que ne comportant pas de suggestions formelles sur la façon de traiter l'utilisation et la réglementation de la cryptographie dans la société, il propose une ébauche des préalables et des raisons de l'ouverture d'un débat sur la cryptographie. Ces préalables sont les suivants :

- Toute personne a le droit d'utiliser la cryptographie pour protéger ses données stockées et ses communications.

- L'importation de produits cryptographiques en Suède restera libre.

- Les contrôles à l'exportation subsisteront.

- Pour faciliter le développement du commerce électronique, un ensemble initial de règles devrait être élaboré à la fois pour permettre l'utilisation des signatures numériques et réglementer les activités des institutions chargées de délivrer les certificats de clé de signature numérique.

- Un certain nombre de pays vont introduire des obligations de remise de clé et d'accès au texte en clair ou aux clés confidentielles sur autorisation des tribunaux en cas de soupçon d'activités criminelles, parmi les conditions des licences d'exportation de produits cryptographiques.

- Il faut créer les conditions nécessaires pour permettre aux Suédois d'utiliser des moyens nationaux pour la remise de clés. D'autres pays devraient exiger la remise des clés en cas de trafic international ou comme condition préalable en cas d'achat de produits soumis à des contrôles d'exportation.

- Pour permettre aux autorités de police et de justice de combattre le terrorisme et le trafic de drogue, par exemple, il faut des dispositions juridiques instaurant l'accès légal au texte en clair ou aux clés cryptographiques.

- La Suède établira les réglementations nécessaires dans le domaine de la cryptographie, en coopération avec les autres pays et en concordance avec l'évolution internationale.

Suisse

Contrôles à l'exportation

La Suisse est membre de l'Arrangement de Wassenaar.

L'exportation de matériels et logiciels de cryptographie est régie par la Loi fédérale sur le contrôle des biens utilisables à des fins civiles et militaires et des biens militaires spécifiques (13 décembre 1996) et l'Ordonnance concernant l'exportation, l'importation et le transit de biens à double usage et biens militaires spécifiques (25 juin 1997), qui sont l'une et l'autre entrée en vigueur le 1er octobre 1997. L'autorité chargée de la délivrance des licences est l'Office fédéral des affaires économiques extérieures.

La Note générale relative aux logiciels a été intégré par la Suisse dans son Ordonnance dans les mêmes termes que l'Arrangement de Wassenaar. La Suisse applique de façon stricte le paragraphe (1)(b) de la Note qui précise que les logiciels doivent être "conçus pour être installés par l'utilisateur sans autre assistance importante du fournisseur" pour qu'ils puissent être considérés comme "couramment à la disposition du public". En particulier, si le logiciel de cryptographie est exporté vers une société qui se propose de le mettre à la disposition de ses clients sans assistance importante, une licence d'exportation

est exigée pour la première partie de la transaction, même si la deuxième partie entre dans le champ de la Note générale relative aux logiciels.

Les mesures de contrôle des exportations appliquées couvrent les exportations de logiciels sous forme aussi bien matérielle qu'immatérielle.

Des licences générales peuvent être délivrées pour des exportations vers des destinations désignées.

Mesures de contrôle intérieur et réglementation des importations

En Suisse, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Turquie

Contrôles à l'exportation

La Turquie est membre de l'Arrangement de Wassenaar.

L'exportation de biens à double usage est soumise en Turquie à l'autorisation du Sous Secrétariat au commerce extérieur (UFT) par le biais de la procédure d'enregistrement prévue à l'Article 3.a du Décret N°95/7623 du 22 décembre 1995 relatif au régime d'exportation. Les biens sensibles et les technologies et produits à double usage, notamment les produits cryptographiques (qu'ils soient ou non utilisés à des fins militaires), doivent être enregistrés auprès de l'Association des exportateurs de métaux et de minerais d'Istanbul (IMMIB), qui confirme cet enregistrement sur la déclaration douanière. Les procédures d'enregistrement pour les biens visés par des mécanismes internationaux de non prolifération sont mises en oeuvre par l'IMMIB sous les auspices de l'UFT. De plus, l'exportation de produits cryptographiques utilisés à des fins militaires sont soumises à la délivrance d'une autorisation par le Ministère de la Défense nationale (MND) en vertu de la Loi N°3763 de 1940 relative au "contrôle des entreprises industrielles privées produisant des armes, véhicules, équipements et munitions de guerre".

La Turquie applique les dispositions de la Note générale relative aux logiciels, telle qu'elle figure dans l'Arrangement de Wassenaar.

La législation turque sur le contrôle des exportations ne s'applique qu'aux logiciels sous forme tangible (par exemple enregistrés sur disque ou support similaire), mais non sous forme immatérielle, comme dans le cas de transfert sur Internet ou autres réseaux pour données.

Mesures de contrôle intérieur et réglementation des importations

En Turquie, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Royaume-Uni

Contrôles à l'exportation

Le Royaume-Uni est membre de l'Arrangement de Wassenaar et de l'Union européenne.

L'exportation de technologies de cryptographie est soumise à un contrôle conformément au Règlement de l'Union européenne sur les biens à double usage, mis en œuvre par le Décret de 1994 sur le contrôle de l'exportation de biens, modifié par le Règlement de 1996 sur le contrôle de l'exportation de biens à double usage et biens connexes. L'autorité chargée de délivrer les licences est le Service du contrôle des exportations (*Export Control Department*) du Ministère du commerce et de l'industrie (DTI)[46].

Les mesures de contrôle applicables aux exportations respectent les dispositions de la Note générale relative aux logiciels ; ces contrôles ne s'appliquent pas aux logiciels "couramment disponibles" ni aux logiciels et technologies qui sont "du domaine public". Les exportateurs ont accès à une Note interprétative donnant des "Indications pour l'interprétation de la Note générale relative aux logiciels" et ils peuvent décider eux-mêmes si la dispense s'applique ou demander l'avis du Service de contrôle des exportations du DTI.

Les contrôles à l'exportation au Royaume-Uni visent uniquement les exportations de biens tangibles, et celles de biens immatériels en sont dispensées (par exemple distribution de logiciels par téléchargement sur Internet).

Les exportateurs doivent demander une licence d'exportation de deux ans pour tout produit utilisant la cryptographie. Dans certains cas, le DTI délivre une "licence d'exportation individuelle ouverte" à caractère plus général, d'une validité de trois ans, qui peut stipuler des conditions spécifiques. Tous les exportateurs doivent tenir un relevé détaillé des exportations autorisées par une licence.

Les demandes de "licence d'exportation individuelle ouverte" *(Open Individual Export Licences : OIEL*) soumises par les exportateurs pour les produits de chiffrement employant l'algorithme DES à 56 bits (ou des algorithmes de puissance équivalente) sont prises en considération. Ces OIEL, selon chaque cas particulier, peuvent être limitées en ce qui concerne les pays de destination autorisés, le type d'utilisateur final, l'utilisation indiquée pour les produits et, entre autres, en fonction des discussions internationales éventuelles sur les exportations de produits cryptographiques. En outre, conformément à la politique du gouvernement concernant les tiers de confiance, l'exportateur peut dans certains cas avoir à apporter la preuve que ses produits sont (ou seront) capables d'interfonctionner avec les tiers de confiance agréés.

Depuis le 28 janvier 1998, le DTI délivre une Licence d'exportation générale ouverte *(Open General Export Licence*). Ces nouvelles licences permettent, sans délivrance d'autorisation mais sous réserve de certaines conditions, l'exportation de biens qui n'ont pas la capacité de chiffrer ou déchiffrer la parole en ligne et qui sont conçus pour être utilisés avec des ordinateurs et pour l'usage personnel de l'utilisateur, lorsque celui-ci les emporte avec lui.

Mesures de contrôle intérieur et réglementation des importations

Au Royaume-Uni, il n'y a pas actuellement de mesures de contrôle intérieur sur l'utilisation de la cryptographie ni de restrictions à l'importation des technologies de cryptographie.

Evolution de la politique

Dans un document de juin 1996 concernant la fourniture de services de chiffrement sur les réseaux de télécommunications publiques, le DTI déclare que les contrôles à l'exportation sur les produits de chiffrement (matériels ou logiciels) comprenant des algorithmes de chiffrement numérique resteront en place, mais que le gouvernement, avec ses partenaires de l'Union européenne, s'efforcera de simplifier les contrôles à l'exportation pour les produits de chiffrement qu'utilisent les tiers de confiance agréés. D'après ce document, le gouvernement établirait une législation régissant l'agrément et le fonctionnement des tiers de confiance, avec l'objectif de préserver l'accès des autorités de police et de justice aux données chiffrées. Avant de légiférer, il mènerait un processus de consultation avec toutes les parties intéressées.

Ce processus de consultation a été lancé par un *"Consultation Paper on Licensing of Trusted Third Parties for the Provision of Encryption Services"*[47] [document de consultation sur l'agrément de tiers de confiance pour la fourniture de services de chiffrement] publié par le DTI le 19 mars 1997. Ce document de consultation couvre les aspects de la cryptographie concernant l'agrément des tiers de confiance, leur utilisation à des fins de confidentialité, l'accès légal en relation avec la confidentialité, la reconnaissance légale des signatures numériques et les aspects internationaux.

A l'issue de la consultation, le DTI a annoncé le 27 avril 1998 ses propositions pour un projet de loi sur le commerce électronique sécurisé (*Secure Electronic Commerce Bill*). Le Gouvernement se propose d'introduire une législation qui comprendrait des mesures pour promouvoir la reconnaissance juridique des signatures numériques dans le commerce électronique, l'introduction d'un régime de licence volontaire pour les tiers de confiance (terme générique utilisé pour désigner les organismes fournissant un (ou divers) service(s) de cryptographie à leurs clients), les Autorités de certification (organismes qui délivrent principalement des certificats pour les signatures électroniques et les Agents de recouvrements de clés (chargés de faciliter la "récupération" de données chiffrées) ainsi que des mesures destinées à permettre aux autorités chargées de l'application des lois d'obtenir un mandat pour avoir un accès légal aux informations nécessaires pour déchiffrer le contenu de communications ou de données chiffrées (ce qui inclurait les clés cryptographiques utilisées uniquement pour des signatures numériques).

Etats-Unis

Contrôles à l'exportation

Les Etats-Unis sont membre de l'Arrangement de Wassenaar.

L'exportation de matériels et logiciels cryptographiques non militaires est administrée aux Etats-Unis par le Bureau d'administration des exportations (*Bureau of Export Administration* ou *BXA*[48]), sous l'autorité du *Department of Commerce*. Les technologies de cryptographie sont couvertes par la Liste de contrôle du commerce (*Commerce Control List ou CCL*) qui fait partie du Règlement d'administration des exportations (*Export Administration Regulations* ou *EAR*).

Les contrôles actuels appliqués aux exportations par les Etats-Unis couvrent les politiques en matière de licence visant les différentes catégories de produits de chiffrement, de produits à remise de clé et de produits à récupération de clé (les changements récemment annoncés dans la politique américaine sont examinés ci-après.) En vertu des règles actuelles, certains logiciels de chiffrement grand public peuvent être dispensés de licence après un examen unique effectué par le BXA. De plus, des dispenses de licence peuvent être obtenues pour des exportations de produits à remise ou récupération de clé à destination de pays non soumis à embargo. Les fabricants qui soumettent un plan d'engagement de

récupération de clé peuvent également exporter sans licence des produits DES à 56 bits sans récupération de clé. Les autres produits de chiffrement peuvent être couverts par des mécanismes de licence ou examinés au cas par cas. La délivrance de licence pour les “technologies de chiffrement” est examinée au cas par cas.

Les Etats-Unis n’appliquent que la partie I de la Note générale relative aux logiciels de l’Arrangement de Wassenaar en ce qui concerne les logiciels “couramment accessibles au public” (c’est-à-dire destinés au marché de masse) lorsque le logiciel utilise des algorithmes spécifiés dont la clé est inférieure ou égale à 40 bits (ou algorithmes exclusifs équivalents) qui ont été approuvés dans le cadre d’un examen unique. Les Etats-Unis n’appliquent pas la partie 2 concernant les logiciels de cryptographie qui sont “du domaine public”. La Partie 734 de l’EAR réglemente l’exportation de code source et de code objet de logiciels de chiffrement, même s’ils appartiennent au domaine public. Cela est contraire à la pratique de certains autres membres de l’Arrangement de Wassenaar.

En ce qui concerne la mise en oeuvre de la partie I de la Note générale relative aux logiciels, un exportateur doit soumettre une demande de classification pour une évaluation initiale unique conformément aux dispositions du Supplément N°6 à la Partie 742 de l’EAR. Cette demande est examinée d’une part sur la base des paramètres techniques du produit et d’autre part pour s’assurer qu’elle correspond à la définition de la Note générale relative aux logiciels, sous réserve de la limite à 40 bits de la longueur de la clé. Le texte de la Partie I de la Note est repris dans l’EAR.

Outre l’exportation de logiciels sous forme tangible, les Etats-Unis contrôlent les exportations de logiciels de chiffrement sous forme immatérielle, par exemple distribution via Internet.

L’exportation temporaire de produits cryptographiques destinés à un usage personnel sont dispensés des contrôles à l’exportation si certaines conditions spécifiées dans l’EAR sont satisfaites[49].

Mesures de contrôle intérieur et réglementation des importations

Aux Etats-Unis, il n’y a pas actuellement de mesures de contrôle intérieur sur l’utilisation de la cryptographie ni de restrictions à l’importation des technologies de cryptographie.

Evolution de la politique

Après plusieurs mois de dialogue entre les autorités américaines, l’industrie, les services chargés de l’application des lois et les groupes de défense de la vie privée, le Gouvernement américain a annoncé le 16 septembre 1998 une série de mesures qu’il se propose d’adopter pour actualiser sa politique en matière de cryptographie[50]. Dans le cadre de cette initiative, le Gouvernement américain se propose d’encourager la mise en place d’un centre de soutien technique destiné à aider à renforcer les moyens techniques des autorités chargées de faire appliquer les lois aux niveaux fédéral, des Etats et local, de manière à leur permettre de suivre l’évolution des technologies de communications modernes. Le Gouvernement va également renforcer son soutien au commerce électronique, par un certain nombre de mesures, à savoir :

- L’exportation de produits DES 56 bits ou équivalents sera rationalisée (dans le cadre des dispositions de dispense de licence, sauf à destination de sept pays spécifiés), et suppression des contraintes concernant les plans de récupération de clés.

- Les exportations de produits de cryptographie de robustesse non limitée (avec ou sans récupération de clé) seront rationalisées (dans le cadre des dispositions de dispense de licence) pour certaines industries, y compris les filiales de sociétés américaines partout dans le monde (sauf dans sept pays spécifiés), de même que pour les compagnies d'assurance, les organisations médicales et sanitaires civiles et les commerçants en ligne et utilisateurs du commerce électronique dans les 45 pays pour lesquels a été récemment approuvée l'exportation de produits cryptographiques à l'usage des banques et institutions financières.

- Les produits à récupération de clé continueront d'être exportables dans le cadre des dispositions de dispense de licence (sauf dans sept pays spécifiés) et l'agrément des agents étrangers de récupération de clé est éliminé.

- Les exportations de produits "récupérables" seront autorisées à destination de la plupart des entreprises commerciales des 45 pays pour lesquels a été récemment approuvée l'exportation de produits cryptographiques à l'usage des banques et institutions financières, dans le cadre d'arrangement de licence de produits de chiffrement.

Les exportations concernant des utilisateurs ou des destinations qui ne sont pas couverts par cette politique continueront de faire l'objet d'un examen au cas par cas. Avant l'exportation, tous les produits sont soumis à un examen technique unique. Le Gouvernement des Etats-Unis se félicite du dialogue permanent qu'il entretient avec les industriels et il se propose de réexaminer sa politique dans un an pour voir si d'autres mesures d'actualisation seraient nécessaires pour maintenir l'équilibre de son approche visant à protéger la sécurité publique et la sécurité nationale, assurer le respect de la vie privée, permettre à l'industrie américaine de garder sa première place dans ce domaine technologique et promouvoir le commerce électronique.

Le "*Framework for Global Electronic Commerce*" (cadre pour le commerce électronique mondial) publié par l'Administration américaine en juillet 1997[51] déclare que "les gouvernements devraient encourager l'autodiscipline.... et soutenir les efforts du secteur privé visant à élaborer des mécanismes facilitant le bon fonctionnement de l'Internet". Ce document réaffirme l'approche (non contraignante) du gouvernement à l'égard de la récupération de clés. Des responsables gouvernementaux ont indiqué que les Etats-Unis ne préconisaient pas de produit, de technologie ou même d'approche spécifique, et qu'ils souhaitaient conserver le plus de souplesse possible, à condition cependant que les solutions et arrangements qui en résulteraient préservent la capacité des Etats-Unis à protéger la sécurité du public et la sécurité nationale[52].

Parmi les autres initiatives récentes des Etats-Unis en ce qui concerne la politique de cryptographie on peut citer :

- En mai 1997, le *National Institute of Standards and Technology* a entrepris l'élaboration d'une Norme fédérale pour le traitement de l'information (FIPS ou *Federal Information Processing Standard*) relative à l'acceptation et l'échange de clés cryptographiques basées sur la cryptographie à clé publique[53].

- Le *National Research Council* (NRC) a publié une étude sur le "Rôle de la cryptographie dans la sécurisation de la société de l'information" (juin 1996).

- L'*Office of Management and Budget* (OMB) a publié un livre blanc intitulé "Permettre le respect de la vie privée, le commerce, la sécurité nationale et la sécurité du public dans l'infrastructure mondiale de l'information" (mai 1996).

– En octobre 1996, une loi a été adoptée qui stipule que la *Sentencing Commission* des Etats-Unis doit produire un rapport annuel sur l'utilisation qui est faite du chiffrement informatique pour dissimuler les activités criminelles.

Il existe actuellement un certain nombre de propositions de loi à divers stades du processus législatif ; certaines visent à imposer des restrictions à l'utilisation des technologies de chiffrement sur le plan intérieur, d'autres à instaurer des dispositions gouvernementales obligatoires ou volontaires de récupération de clés ou dépôt de clés, et d'autres visent à assurer la liberté d'utilisation et d'exportation de la cryptographie et des produits cryptographiques :

– *Computer Security Enhancement Act* de 1997 (H.R.1903).

– *Promotion of Commerce On-Line in the Digital Era* (Pro-CODE) Act de 1997 (S.377).

– *Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-Privacy) Act* (S.2067).

– *Communications Privacy and Consumer Empowerment Act* (H.R.1964).

– *Encrypted Communications Privacy Act* de 1997 (S.376).

– *Secure Public Networks Act* (S.909).

– *Security and Freedom Through Encryption (SAFE) Act* (H.R.695).

Trois actions en justice différentes contestant la réglementation américaine des exportations ont été intentées, au motif qu'elle enfreint le Premier amendement de la Constitution des Etats-Unis qui protège la liberté d'expression.[54]

NOTES

1. Le Secrétariat a consulté diverses sources pour la préparation du texte préliminaire de l'Inventaire, qui a servi de base pour de nouvelles contributions des Gouvernements des pays Membres, notamment le *Crypto Law Survey* compilé par Bert-Jaap Koops (voir http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm) et le Site Web Cryptome de John Young (voir http://jya.com/crypto.htm) ainsi que les sites Web exploités par la *Global Internet Liberty Campaign* (Voir http://www.gilc.org/), l'*Electronic Privacy Information Center* (Voir http://www.epic.org/) et le *Center For Democracy and Technology* (Voir http://www.cdt.org/).

2. Recommandation du Conseil de l'OCDE sur les Lignes directrices régissant la politique de cryptographie, 27 mars 1997.

3. DSTI/ICCP/REG(98)3/FINAL.

4. Le COCOM comprenait les 17 membres suivants : Australie, Belgique, Canada, Danemark, France, Allemagne, Grèce, Italie, Japon, Luxembourg, Pays-Bas, Norvège, Portugal, Espagne, Turquie, Royaume-Uni et Etats-Unis. Les membres coopérants étaient l'Autriche, la Finlande, la Hongrie, l'Irlande, la Nouvelle-Zélande, la Pologne, Singapour, la République slovaque, la Corée, la Suède, la Suisse et Taïwan.

5. Les membres de l'Arrangement de Wassenaar sont les suivants : Argentine, Australie, Autriche, Belgique, Bulgarie, Canada, République tchèque, Danemark, Finlande, France, Allemagne, Grèce, Hongrie, Irlande, Italie, Japon, Luxembourg, Pays-Bas, Nouvelle-Zélande, Norvège, Pologne, Portugal, République de Corée, Roumanie, Fédération de Russie, République slovaque, Espagne, Suède, Suisse, Turquie, Ukraine, Royaume-Uni et Etats-Unis.

6. L'acceptation d'une licence qui a été refusée par un autre Etat participant pour une transaction essentiellement identique au cours des trois années précédentes doit être notifiée de préférence dans les 30 jours et sans dépasser un délai de 60 jours. Arrangement de Wassenaar, Eléments initiaux, Section II, paragraphe 4.

7. Les refus de biens sensibles/très sensibles doivent être notifiés de préférence sous 30 jours, mais dans un délai n'excédant pas 60 jours. Arrangement de Wassenaar, Eléments initiaux, Section H, paragraphe 3.

8. Voir l'Appendice 5 des "éléments initiaux" de l'Arrangement de Wassenaar.

9. Enumérés dans l'Annexe 1 des biens et technologies à double usage.

10. Enumérés dans l'Annexe 2 des biens et technologies à double usage.

11. Le Règlement CE 3381/94 (JOLJ L 367/1, 31.12.94) et la Décision 94/942/PESC (JOCE L 367/8, 31.12.94) du Conseil de l'Union européenne du 19 décembre 1994 exposent le régime de contrôle des exportations de biens à double usage et établissent la liste des biens à double usage soumis au Règlement.

12. Voir les notes à l'Annexe 1 de la Décision 94/942/PESC (Une version entièrement nouvelle du Règlement est en cours d'examen).

13. Résolution du Conseil 96/C329/01.

14. COM(97)503, voir http://www.ispo.cec.be/eif/policy/.

15. Voir la Directive du Conseil 83/189/CEE (JOCE L 109, 26.4.83*).*

16. Voir http://www.ispo.cec.be/policy.

17. (97/C314/07) (Texte intéressant également l'EEE) COM(97)356 Final.

18. Recommandation [R(95)13] du Conseil de l'Europe, voir http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.htm.

19. Voir la Déclaration de Bonn à http://www.2.echo.lu/bonn/finalfr.html.

20. L'adresse électronique du point de contact du Gouvernement australien en ce qui concerne les questions de cryptographie est crypto@ag.gov.au.

21. Voir le Code (*Regulations*) à l'adresse http://www.austlii.edu.au/au/legis/cth/consol_reg/cer439/s13e.html.

22. La cryptographie relève de la Partie 3, catégorie 5 "Sécurité des télécommunications et de l'information" de la Liste des biens militaires et stratégiques. Le Document est disponible à l'adresse : http://www.defence.gov.au/dao/exportcontrols/.

23. Pour plus d'informations pratiques concernant l'exportation de technologies de cryptographie, voir le guide intitulé *Australian Controls on the Export of Defence and Strategic Goods*, disponible à l'adresse http://www.defense.gov.au/dao/exportcontrols/greenbk/guidelin.htm.

24. *Bundesministerium für wirtschaftliche Angelegenheiten,* Gruppe II/A, Stubenring 1, 1011, Vienne, (Autriche).

25. La Belgique travaille sur un projet de loi relatif aux signatures numériques. Cette question est examinée dans l'Inventaire de l'OCDE des approches à l'égard de l'authentification et la certification dans une société mondiale de réseaux.

26. Document disponible sur le site Web d'Industrie Canada à l'adresse http://strategis.ic.gc.ca/crypto.

27. Document disponible à l'adresse http://www.cse-cst.gc.ca/cse.

28. Loi n° 21/1997, Décret n° 43/1997.

29. Voir la Loi n° 21/1997.

30. Conformément au Décret n° 44/1997 et au § 16 de la Loi n° 21/1997.

31. Décret N° 468 du 13 juin 1995.

32. Voir http://www.fsk.dk/fsk/publ/1997/crypt/.

33. Dans cette section de l'inventaire, les contrôles à l'exportation sont examinés en même temps que les mesures de contrôle intérieur et les réglementations importantes, dans la mesure où la législation française traite de ces questions ensemble.

34. Service central de la sécurité des systèmes d'information.

35. Loi n° 96-659 du 26 juillet 1996. Pour le texte de la loi, voir le site du gouvernement français : http://www.telecom.gouv.fr/francais/activ/telecom/nloi.htm. Pour d'autres informations du gouvernement français sur cette loi : http://www.telecom.gouv.fr/francais/activ/telecom/.

36. Voir http://www.bmwi.de.

37 . Loi No. 185 du 8 juillet 1990, Loi No. 222 du 27 février 1992 et décrets ministériels pertinents des .28 octobre 1993, 18 novembre 1993, 5 mai 1994 et 1er septembre 1995.

38. L'AIPA a été créée par le Décret législatif No. 39 du 12 février 1993.

39. Précisé dans l'article 9 notamment.

40. Créé par la Directive du Président du Conseil des Ministres du 5 septembre 1995, publiée au Journal Officiel no. 272 du 21 novembre 1995.

41. Article 15, paragraphe 2.

42. Voir http://www.mpt.go.jp.

43. Voir http://www.miti.go.jp.

44. Voir http://www.miti.go.jp/intro-e/a228101e.html.

45. Loi 11/98 du 24-04-1998, Journal officiel du 25 avril 1998.

46. Voir le site Web du DTI à l'adresse: http://www.dti.gov.uk.

47. Voir http://www.dtiinfo1.dti.gov.uk/pub.

48. Voir http://www.bxa.doc.gov/.

49. Voir l'EAR 15 CFR Partie 740, *Licence exemptions*, 740.9 TMP (*Temporary imports, exports and re-exports*) et 740.14 -BAG (*Baggage*).

50. Voir http://207.96.11.93/press/98/WHPress1.htm.

51. Voir http://www.whitehouse.gov.

52. Déposition de Robert S. Litt, Principal Associate Deputy Attorney General, devant la Sous-Commission sur la constitution, le fédéralisme et les droits de propriété de la Commission des affaires judiciaires, Etats-Unis, 17 mars 1998.

53. Voir http://csrc.nist.gov/.

54. Voir Karn à http://people.qualcomm.com/karn, Bernstein à www.eff.org et Junger à http://jya.pdj.com.

ANNEXES

ANNEXE I: TABLEAU RECAPITULATIF DES REPONSES NATIONALES

Légende :

Symbole	Signification
*	Oui
?	Information non communiquée par le pays Membre

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Australie	*		*	Reg 13E des *Customs (Prohibited Exports) Regulations*; et *Defence and Strategic Goods List*	*Defence Signals Directorate* du *Department of Defence*		Indéterminé		
Autriche	*	*	*	Section 8 de la *Außenhandels-gesetz* (BGBl. Nr. 172/1995)	Ministère fédéral des Affaires Economiques (*Bundesministerium für wirtschaftliche Angelegenheiten*)	* (intégrée par référence)	* (Pas de contrôle sur les exportations de produits immatériels)	*(transmis-sions radio internes)	
Belgique	*	*	*	Loi du 5 août 1991; Décret ministériel du 19 mai 1995; et Décret royal 8 mars 1993	A.R.E., 4ème Division	?	* (Pas de contrôle sur les exportations de produits immatériels)		

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Canada	*		*	Loi sur les licences d'importation et d'exportation; et la Liste des marchandises d'exportation contrôlée	Ministère des affaires étrangères et du commerce international	*			
Rép tchèque	*		*	Loi sur le contrôle des exportations et importations de biens et technologies soumis à des régimes internationaux de contrôle	Ministère de l'industrie et du commerce	?	?		
Danemark	*	*	*	Décret relatif à l'exportation de biens, technologies et savoir-faire à double usage	Agence danoise du commerce et de l'industrie	*			

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Finlande	*	*	*	Loi sur le contrôle des exportations de biens à double usage ; Décret sur l'exportation des biens à double usage ; et Décision du Ministère du commerce et de l'industrie sur les licences d'exportation de produits à double usage (janvier 1997)	Ministère du commerce et de l'industrie	*			
France	*	*	*	Divers textes législatifs, décrets et arrêtés (voir le corps du texte)	Service Central de la Sécurité des Systèmes d'Information (SCSSI)			*	*
Allemagne	*	*	*	?	Ministère fédéral de l'économie (BMWi)	?	?		
Grèce	*	*	*	?	?	?	?		

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Hongrie	*		*	?	Ministère des affaires économiques	?	?		*
Islande				Sans objet	Sans objet	Sans objet	Sans objet		
Irlande	*	*	*	Control of Exports Act 1983 ; Control of Exports Order (1996); Règlement des Communautés européennes (Contrôle des exportations de biens à double usage) (1996); et Customs Act (1956)-	*Export Licensing Unit of Department of Enterprise, Trade & Employment*	*	?		
Italie	*	*	*	Loi no. 89, 24 février 1997	Ministère du commerce extérieur (*Ministerio del commercio con l'estero*)	*	Indéterminé	*	Non

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Japon	*	Non	*	Loi sur les changes et le commerce extérieur (No.228, 1949); Arrêté interministériel sur les changes (No.260, 1980); Arrêté interministériel sur le contrôle des exportations (No.63, 1949); et Notification du Bureau de l'administration du commerce international (No.492, 1992)	Ministère du commerce international et de l'industrie (MITI)	*	Non	Non	Non
Corée	*	Non	*	Avis public sur l'exportation et l'importation de biens stratégiques	Ministère du commerce, de l'industrie et de l'énergie	*	?	Non	Non
Luxembourg	*	*	*	?	?	?	?	Non	Non
Mexique	Non	Non	Non	Sans objet	Sans objet	Sans objet	Sans objet	Non	Non

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Pays-Bas	*	*	*	Loi sur les importations et exportations (Recueil des lois néerlandaises 1962, 295) ; et Décision ministérielle concomitante sur l'exportation de biens stratégiques (Recueil des lois néerlandaises 1963, 128).	L'Agence centrale pour l'importation et l'exportation, qui relève du Ministère des affaires économiques	*	* (pas de contrôle sur les exportations de biens immatériels)	* (Lois connexes sur les télécoms)	Non
Nouvelle-Zélande	*	Non	*	*Customs and Excise Act 1996 ;* et Customs Prohibition Order 1996	*International Security & Arms Control Division* qui relève du Ministry of Foreign Affairs and Trade	Non	* (pas de contrôle sur les exportations de biens immatériels)	Non	Non

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Norvège	*	Non	*	Loi relative au contrôle des exportations de biens, services, technologies etc. stratégiques ; Règlement pour l'application du contrôle des exportations de biens, services, technologies etc. stratégiques et Liste des biens et technologies à double usage	Ministère des affaires étrangères	*	?	Non	Non
Pologne	*	Non	*	?	?	?	?	Non	* (autorisation requise)

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Portugal	*	*	*	?	Direction générale du commerce	?	?	Non	Non
Espagne	*	*	*	*Real Decreto por el que se aprueba el Reglamento del Comercio Exterior de Material de Defensa y de Doble Uso*	*Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso*	*	*	Non	* (contrôle sur les technologies destinées à un usage dans le domaine de la sécurité nationale)
Suède	*	*	*	Loi sur les produits stratégiques; et Arrêté sur les produits stratégiques	Inspection pour les produits stratégiques	*	?	Non	Non
Suisse	*	Non	*	Loi fédérale sur le contrôle des biens utilisables à des fins civiles et militaires et des biens militaires spécifiques et l'Ordonnance concernant l'exportation, l'importation et le transit de biens à double usage et biens militaires spécifiques	Office fédéral des affaires économiques extérieures	*	Non	Non	Non

PAYS	PARTIE À WASSENAAR	MEMBRE DE L'UE	CONTRÔLE DES EXPORTATIONS	LEGISLATION APPLICABLE	AUTHORITE DE TUTELLE	APPLICATION DE LA NOTE GENERALE RELATIVE AUX LOGICIELS	TRAITEMENT DIFFÉRENT SI LES LOGICIELS SONT SOUS FORME "TANGIBLE" OU "IMMATÉRIELLE"?	CONTROLES INTERIEURS	CONTROLE DES IMPORTATIONS
Turquie	*	Non	*	Loi relative au contrôle des entreprises industrielles privées produisant des armes, des véhicules, des équipements et des munitions de guerre et Article 3. du Décret sur le régime des exportations	Ministère de la défense nationale et Sous secrétariat au commerce extérieur	*	*	Non	Non
Royaume-Uni	*	*	*	*Export of Goods (Control) Order* modifié par les *Dual-Use and Related Goods (Export Control) Regulations*	*Export Control Department* qui relève du *Department of Trade and Industry*	*	* (pas de contrôle sur les exportations de biens immatériels)	Non	Non
Etats-Unis	*	Non	*	*Export Administration Regulations;* et *Commerce Control List*	*Bureau of Export Administration* qui relève du *Department of Commerce*	* (les E-U appliquent partiellement la Note sur les logiciels en imposant une limite de 40bits)	Non	Non	Non

ANNEXE II : L'ARRANGEMENT DE WASSENAAR (Extraits uniquement)

Arrangement de Wassenaar

relatif au contrôle des exportations d'armes conventionnelles

et de biens et technologies à double usage

Déclaration finale

1. Les Représentants de l'Australie, de l'Autriche, de la Belgique, du Canada, de la République tchèque, du Danemark, de la Finlande, de la France, de l'Allemagne, de la Grèce, de la Hongrie, de l'Irlande, de l'Italie, du Japon, du Luxembourg, des Pays-Bas, de la Nouvelle-Zélande, de la Norvège, de la Pologne, du Portugal, de la Fédération de Russie, de la République slovaque, de l'Espagne, de la Suède, de la Suisse, de la Turquie, du Royaume-Uni et des Etats-Unis se sont réunis à Wassenaar (Pays-Bas) les 18 et 19 décembre 1995.

2. Les représentants sont convenus d'établir l'Arrangement de Wassenaar relatif au contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage.

3. Les représentants ont établi les éléments initiaux du nouvel Arrangement, à soumettre à leurs gouvernements respectifs pour approbation.

4. Ils ont également établi un Comité préparatoire plénier qui débutera ses travaux en janvier 1996.

5. Les représentants sont convenus de situer le Secrétariat de l'Arrangement de Wassenaar à Vienne (Autriche). La première Assemblée plénière aura lieu à Vienne les 2 et 3 avril 1996.

Palais de la paix à la Haye (Pays-Bas), le 19 décembre 1995.

Eléments initiaux

(Extraits uniquement)

Tels qu'adoptés par l'Assemblée plénière les 11 et 12 juillet 1996

I. Objet

1. L'*Arrangement de Wassenaar* a été élaboré afin de contribuer à la sécurité et à la stabilité régionales et internationales, en favorisant la transparence et une responsabilité accrue en matière de transferts d'armes conventionnelles et de biens et technologies à double usage, prévenant ainsi les accumulations déstabilisantes. Les Etats participants chercheront, par leurs procédures nationales, à garantir que les transferts de ces biens ne contribuent pas au développement ou au renforcement de capacités militaires affaiblissant ces objectifs, et ne soient pas détournés pour soutenir ces capacités.

2. Il complétera et renforcera, sans faire double emploi avec eux, les régimes existants en matière de contrôle des armes de destruction massive et de leurs vecteurs, ainsi que les autres mesures reconnues au plan international destinées à promouvoir la transparence et une responsabilité accrue, en se concentrant sur les menaces pour la paix et la sécurité internationales et régionales pouvant résulter des transferts d'armements et de biens et technologies sensibles à double usage pour lesquels les risques sont considérés comme les plus importants.

3. Cet arrangement vise également à intensifier la coopération en vue d'empêcher l'acquisition d'armements et de biens à double usage sensibles à des fins militaires, si la situation dans une région ou le comportement d'un Etat est, ou devient, un motif de préoccupation sérieuse pour les Etats participants.

4. Cet arrangement ne sera dirigé contre aucun Etat ou groupe d'Etats et ne fera pas obstacle aux transactions civiles de bonne foi. En outre, Il n'interférera pas avec le droit des Etats d'acquérir des moyens légitimes de défense conformément à l'Article 51 de la Charte des Nations unies.

II. Champ d'application

1. Les Etats participants se réuniront régulièrement afin de s'assurer que les transferts d'armes conventionnelles et de biens et technologies à double usage se font de façon responsable et dans le sens de la paix et de la sécurité internationales et régionales.

2. A cette fin, les Etats participants échangeront, à titre volontaire, des informations qui renforceront la transparence, conduiront à des échanges de vue entre tous les Etats participants à propos des transferts d'armes ainsi que des biens et technologies sensibles à double usage, et aideront à élaborer une compréhension commune des risques liés au transfert de ces biens. Sur la base de ces informations, ils évalueront les possibilités de coordonner les politiques nationales de contrôle en vue de lutter contre ces risques. Les informations qui feront l'objet de ces échanges comprendront toutes les questions que les Etats participants souhaitent, à titre individuel, porter à l'attention des autres, et notamment, pour ceux des Etats qui souhaiteraient le faire, des notifications allant au-delà de celles ayant fait l'objet d'un accord.

3. La décision de transfert ou de refus de transfert de tout bien relève exclusivement de la responsabilité de chaque Etat participant. Toutes les mesures adoptées dans le cadre de l'arrangement seront conformes à la législation et aux politiques nationales et seront mises en oeuvre sur la base de la compétence nationale discrétionnaire.

4. Conformément aux dispositions du présent arrangement, les Etats participants sont convenus de notifier les transferts et les refus de transferts. Ces notifications concerneront tous les Etats non-participants. Néanmoins, à la lumière des échanges d'informations générales et spécifiques, la portée de ces notifications, ainsi que leur pertinence par rapport aux objectifs de l'arrangement, seront réexaminées. La notification d'un refus n'entraînera pas d'obligation pour les autres Etats participants de refuser des transfert similaires. Toutefois, un Etats participant notifiera, de préférence dans les 30 jours, et sans dépasser un délai 60 jours, à tous les autres Etats participants l'approbation d'une licence qui a été refusée par un autre Etat participant pour une transaction essentiellement identique au cours des trois années précédentes.

5. Au début du présent arrangement, les Etats participants conviennent que les travaux concernant de nouvelles directives et procédures se poursuivront rapidement, en prenant en considération l'expérience acquise. Cela comportera notamment un examen du domaine des armes conventionnelles à couvrir en vue d'étendre les informations et notifications au-delà des catégories décrites à l'Annexe 3. Les Etats participants sont convenues de débattre de façon plus approfondie de la façon de traiter les zones de chevauchement entre les différentes listes.

6. Les Etats participants conviennent de faire le point régulièrement sur le fonctionnement général du présent arrangement, et ce à compter de 1999.

III. Listes de contrôle

1. Les Etats participants contrôleront tous les biens inclus dans la Liste des biens et technologies à double usage et dans la Liste des munitions (voir Annexe 5) dans le but d'empêcher les transferts ou re-transferts qu'ils n'auraient pas autorisés.

2. La Liste des biens et technologies à double usage (niveau 1) comporte deux annexes : l'une composée de biens sensibles (niveau 2), et l'autre d'un nombre limité de biens très sensibles (sous-ensemble du niveau 2).

3. Les listes seront régulièrement revues, afin de prendre en compte les évolutions technologiques et l'expérience acquise par les Etats participants, notamment dans le domaine des biens et technologies à double usage critiques pour les capacités militaires locales. A cet égard, des études seront menées, qui coïncideront avec le premier réexamen des listes en vue de fixer un niveau de transparence adapté pour les biens concernés.

IV. Procédures pour l'échange d'informations générales

1. Les Etats participants conviennent d'échanger des informations générales concernant les risques associés aux transferts d'armes conventionnelles et de biens et technologies à double usage afin d'envisager, là où cela serait nécessaire, la portée d'une coordination des politiques nationales de contrôle pour lutter contre ces risques.

2. Une liste d'éléments possibles pour l'échange d'informations générales concernant les Etats non-participants figure à l'Annexe 1.

V. Procédures pour l'échange d'informations concernant les biens et technologies à double usage

1. Les Etats participants notifieront les licences concernant les biens figurant sur la Liste des biens et technologies à double usage refusées à des Etats non-participants, lorsque les raisons du refus sont en rapport avec les objectifs du présent arrangement.

2. S'agissant du niveau 1, les Etats participants notifieront, sur une base agrégé, deux fois par an, toutes le licences refusées conformément aux objectifs du présent arrangement aux Etats non-participants. Le contenu indicatif de ces notifications de refus est indiqué à l'Annexe 2.

3. Pour les biens du niveau 2 et de son sous-ensemble de biens très sensibles, les Etats participants notifieront, sur une base individuelle, toutes les licences refusées conformément aux objectifs du présent arrangement aux Etats non-participants. Les Etats participants conviennent que la notification devra être faite sans délai et en temps utile, de préférence dans les 30 jours, et au plus tard dans un délai de 60 jours, à compter de la date du refus. Le contenu indicatif de ces notifications de refus est décrit à l'Annexe 2.

4. Pour les biens du niveau 2, les Etats participants notifieront, sur une base agrégé, deux fois par an, les licences délivrées ou les transferts réalisés, lorsqu'ils sont en rapport avec les objectifs du présent arrangement, vers les Etats non-participants. Le contenu indicatif de ces notifications de licence/transfert est indiqué à l'Annexe 2.

5. Les Etats participants exerceront une extrême vigilance pour les biens inclus dans le sous-ensemble du niveau 2 en appliquant à leur exportation des conditions et des critères nationaux. Ils discuteront et compareront ultérieurement les pratiques nationales.

6. Les Etats participants conviennent que toute information sur des transferts spécifiques, allant au-delà de celles prévues ci-dessus, peut être demandée, entre autres, par le canal diplomatique habituel.

VI. Procédures pour l'échange d'informations concernant les armes

...

VII. Réunions et administration

1. Les Etats participants se réuniront périodiquement afin d'adopter des décisions concernant le présent arrangement, ses objectifs et son élaboration ultérieure, de revoir les listes des biens contrôlés, d'envisager les moyens de coordonner les efforts afin de favoriser le développement de systèmes efficaces de contrôle des exportations, et de discuter d'autres questions pertinentes d'intérêt commun, y compris des informations à rendre publiques.

2. Des réunions plénières se tiendront au moins une fois par an et seront présidées par un Etat participant selon un rythme de rotation annuel. Les besoins financiers de l'Arrangement seront couverts par des budget annuels qui seront adoptés lors des réunions plénières.

3. Des groupes de travail pourront être mis en place, s'il en est décidé ainsi lors de la réunion de l'Assemblée plénière.

4. Un Secrétariat sera créé, doté des moyens nécessaires en personnel pour assumer les fonctions qui lui seront confiées.

5. Toutes les décisions dans le cadre du présent arrangement seront adoptées par consensus entre les Etats participants.

VIII. Participation

Le nouvel arrangement sera ouvert, sur une base globale et non discriminatoire, aux futures adhérents satisfaisant aux critères fixés à l'Annexe 4. L'admission de nouveaux participants se fera sur la base du consensus.

IX. Confidentialité

Les informations échangées resteront confidentielles et seront traitées comme des communications diplomatiques protégées. Cette confidentialité s'étendra à toute utilisation qui serait faite de ces informations et à toute discussion entre les Etats participants.

Annexe 5

Liste des biens et technologies à double usage et Liste des munitions

(Extraits uniquement)

SOUMISES A L'ASSEMBLEE PLENIERE A VIENNE

les 11 et 12 juillet 1996

Ces listes reflètent les accords enregistrés dans l'Annexe 5 aux Eléments initiaux en date du 19 décembre 1995 et des modifications d'ordre rédactionnel appropriées convenues par le Groupe de rédaction le 16 mars 1996.

La catégorie 2 de l'Annexe 1 reflète les amendements décidés par l'Assemblée plénière en date des 2 et 3 avril 1996.

LISTE DES MARCHANDISES A DOUBLE USAGE

Note : Les termes entre "guillemets" sont des termes qui sont définis. Voir les "Définitions de termes utilisés dans les groupes 1 et 2".

NOTE GÉNÉRALE SUR LA TECHNOLOGIE

L'exportation de "technologie" "nécessaire" au "développement", à la "production" ou à l'"utilisation" de produits visés par la Liste de marchandises à double usage est contrôlée conformément aux dispositions de chaque catégorie. La "technologie" relative à un produit visé reste visée même lorsqu'elle est applicable à un produit libre quelconque.

Les contrôles ne s'appliquent pas à la "technologie" minimale nécessaire à l'installation, à l'exploitation, à la maintenance (vérification) et à la réparation des produits libres ou dont l'exportation a été autorisée.

N.B. Cette clause ne libère pas la "technologie" de réparation visée par les chiffres 1.E.2.e & 1.E.2.f et 8.E.2.a & 8.E.2.b.

Les contrôles ne s'appliquent pas à la "technologie" "relevant du domaine public", à la "recherche scientifique fondamentale" ni à l'information minimale nécessaire au dépôt de demandes de brevets.

NOTE GÉNÉRALE RELATIVE AUX LOGICIELS

La liste des marchandises à double usage ne vise pas les “logiciels” qui, soit :

1. sont couramment à la disposition du public du fait qu'ils sont :
   a. *vendus directement sur stock, sans restriction, à des points de vente au détail :*
      1. *en magasin;*
      2. *par correspondance; ou*
      3. *sur appel téléphonique; et*
   b. *conçus pour être installés par l'utilisateur sans assistance ultérieure importante de la part du fournisseur; soit*
2. “relèvent du domaine public”.

CATEGORIE 5 - PARTIE 2 - SECURITE DE L’INFORMATION

Partie 2 - “SECURITE DE L’INFORMATION”

Note : Le statut des équipements, des logiciels, des systèmes des ensembles électroniques spécifiques à une application donnée, des modules, des circuits intégrés, des composants ou des fonctions assurant la sécurité de l’information est défini dans la catégorie 5, partie 2, même s’il s’agit de composants ou d’ensembles électroniques d’autres matériels.

5A2 SYSTÈMES, ÉQUIPEMENTS ET COMPOSANTS

a. Systèmes, équipements, ensembles électroniques spécifiques à une application donnée, modules et circuits intégrés assurant la sécurité de l’information, comme suit, et leurs autres composants spécialement conçus :

Note : Pour les systèmes globaux de navigation par satellites recevant des équipements contenant ou employant le déchiffrement (à savoir, GPS ou GLONASS), voir le chiffre 7.A.5.

1. conçus ou modifiés pour utiliser la cryptologie faisant appel à des techniques numériques pour assurer la sécurité de l’information ;

2. conçus ou modifiés pour effectuer des fonction cryptoanalytiques ;

3. conçus ou modifiés pour utiliser la cryptologie faisant appel à des techniques analogiques pour assurer la sécurité de l’information ;

Note : Le chiffre 5A.2a.3 ne vise pas les équipements suivants :

1. *équipements utilisant des techniques de mélange de bandes fixes ne dépassant pas 8 bandes et où les changements de transposition ne s’effectuent pas plus d’une fois toutes les secondes ;*

2. *équipements utilisant des techniques de mélange de bandes fixes dépassant 8 bandes et où les changements de transposition ne s’effectuent pas plus d’une fois toutes les dix secondes ;*

3. *équipements utilisant des techniques de mélange de bandes fixes dépassant 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ;*

4. *équipements de fac-similé;*

5. *équipements de radiodiffusion pour audience restreinte ;*

6. *équipements de télévision civile.*

a) conçus ou modifiés pour supprimer les émanations compromettantes de signaux porteurs d'information ;

Note : Le chiffre 5A.2.a.4 ne vise pas les équipements spécialement conçus pour supprimer les émanations pour des raisons de santé ou de sécurité.

5) conçus ou modifiés pour employer des techniques cryptologiques pour générer le code d'étalement pour le spectre étalé ou le code de saut pour les systèmes à agilité de fréquence ;

6) conçus ou modifiés pour assurer une sécurité multi-niveau ou une isolation de l'utilisateur certifiées ou certifiantes à un niveau dépassant la classe B2 de la norme "Trusted Computer System Evaluation Criteria" (TCSEC) ou d'une norme équivalente ;

7) systèmes de câble de télécommunication conçus ou modifiés en faisant appel à des moyens mécaniques, électriques ou électroniques pour détecter les intrusions subreptices.

Note : Le chiffre 5A.2 ne vise pas ce qui suit :

a) les cartes à microprocesseur personnalisées ou leurs composants spécialement conçus, présentant l'une des caractéristiques suivantes :

1. *incapables d'encrypter le trafic de messages ou les données fournies par l'utilisateur ou leurs fonctions de gestion de clef associée ; ou*

2. *destinées à servir uniquement avec les équipements ou systèmes non visés aux points 1 à 6 de la note au chiffre 5A.2.a.3 ou aux points b à h de la présente note ;*

b. les équipements employant des techniques de compression ou de codage de données fixes ;

c. équipements de réception pour la radiodiffusion, la télévision payante ou la télévision similaire réservée à un nombre limité de téléspectateurs du grand public, sans capacité de chiffrement numérique et où le déchiffrement numérique est limité aux fonctions vidéo, audio ou de gestion ;

d. radiotéléphones portatifs ou mobiles destinés a l'usage civil, (p. ex. pour l'emploi avec les systèmes de radiocommunications cellulaires commerciaux civils) qui ne sont pas en mesure de procéder au chiffrement de bout en bout ;

e. fonctions de déchiffrement spécialement conçues pour permettre l'exécution de logiciels protégés, à condition que ces fonctions ne soit pas accessibles à l'utilisateur ;

f. équipements de contrôle d'accès, tels que machines automatiques de distribution de billets, imprimantes libre-service de relevés de comptes ou terminaux de points de vente, protégeant les mots de passe, numéros d'identification personnels ou autres données similaires empêchant l'accès non autorisé à des installations, mais ne permettant pas le chiffrement des fichiers ou des textes, sauf lorsqu'il est directement lié à la protection des mots de passe ou des numéros d'identification personnels ;

g. équipements d'authentification des données qui calculent un code d'authentification de message ou un résultat similaire afin d'assurer qu'aucune modification de texte n'a été effectuée ou d'authentifier les utilisateurs, mais qui ne permettent pas de chiffrer des données, textes ou autres supports, sauf pour ce qui est nécessaire à l'authentification ;

h. équipements cryptologiques spécialement conçus et limités pour servir dans des machines d'opération bancaires ou financières, telles que machines automatiques de distribution de billets, imprimantes libre-service de relevés de comptes ou terminaux de points de vente.

5.B.2 <u>EQUIPEMENTS D'ESSAI, DE CONTRÔLE ET DE PRODUCTION</u>

a. Equipements spécialement conçus pour :

1. le développement des équipements ou des fonctions visés à la Catégorie 5, Partie 2, y compris les équipements de mesure ou d'essai ;

2. la production des équipements ou des fonctions visés à la Catégorie 5, Partie 2, y compris les équipements de mesure, d'essai, de réparation ou de production ;

b. Equipements de mesure spécialement conçus pour évaluer et valider les fonctions de sécurité de l'information visés aux chiffres 5A.2 ou 5D.2.

5.C.2 <u>MATERIAUX</u> - Néant

5.D.2 <u>LOGICIEL</u>

a. logiciel spécialement conçu ou modifié pour le développement, la production ou l'utilisation des équipements ou logiciels visés à la Catégorie 5, Partie 2 ;

b. logiciel spécialement conçu ou modifié pour le soutien de la technologie visée au chiffre 5E.2 ;

c. logiciel spécifique, comme il suit :

1. logiciel présentant les caractéristiques ou exécutant ou simulant les fonctions des équipements visés aux chiffres 5A.2 ou 5B.2 ;

2. logiciel destiné à certifier le logiciel vise au chiffre 5D.2.c.1 ;

<u>Note</u> : Le chiffre 5D.2 ne vise pas :

a. le logiciel nécessaire à l'utilisation des équipements exclus du contrôle aux termes de la note relative au chiffre 5A.2 ;

b. le logiciel réalisant l'une des fonctions des équipements exclus du contrôle aux termes de la note relative au chiffre 5A.2.

5E2 TECHNOLOGIE

a. Technologie, au sens de la note générale de technologie, pour le développement, la production ou l'utilisation des équipements ou du logiciel visés à la Catégorie 5, Partie 2.

DÉFINITIONS DES TERMES UTILISÉS DANS CES LISTES

(Extraits uniquement)

On trouvera dans ce document les définitions des termes utilisés dans ces listes, par ordre alphabétique.

Note : Les définitions s'appliquent dans l'ensemble des Listes et de leurs Annexes. Les références sont purement indicatives et n'ont pas d'incidence sur l'application universelle des termes définis dans l'ensemble de ces Listes et de leurs Annexes.

Les catégories correspondantes sont indiquées entre parenthèses, à la droite du terme défini.

"Calculateur numérique" (4,5)

Les termes "calculateur numérique" désignent un équipement capable, sous forme d'une ou de plusieurs variables discrètes, d'assurer toutes les fonctions suivantes :

a. accepter des données;

b. emmagasiner des données ou des instructions dans des dispositifs d'emmagasinage fixes ou modifiables (par réécriture);

c. traiter des données au moyen d'une séquence emmagasinée d'instructions modifiable; et

d. assurer la sortie de données.

N.B. Les modifications de la séquence emmagasinée d'instructions comprennent le remplacement de dispositifs d'emmagasinage fixes mais non une modification matérielle du câblage ou des interconnexions.

"Carte à microprocesseur personnalisée" (5)

Les termes "carte à microprocesseur personnalisée" désignent une carte à microprocesseur (carte à puce) contenant un microcircuit, conformément à la Norme ISO/CEI 7816, qui a été programmé par l'émetteur et ne peut être modifié par l'utilisateur.

"Code objet" ou "langage objet" (4,5,6,7,9)

Les termes "code objet" ou "langage objet" désignent une forme exécutable par la machine d'une expression appropriée d'un ou de plusieurs processus ("code source" ou "langage source") traduit par un système de programmation.

"Cryptologie" (5)

Le terme "cryptologie" désigne la discipline qui englobe les principes, moyens et méthodes servant à la transformation des données afin d'en dissimuler le contenu informatif, empêcher sa modification sans détection ou empêcher son utilisation sans autorisation. La "cryptologie" est limitée à la transformation d'informations par l'emploi d'un ou de plusieurs paramètres secrets (par exemple, des variables cryptologiques) ou de la gestion de clef associée.

N.B. Les termes ‹paramètre secret› désignent une constante ou une clef non portée à la connaissance d'autres personnes ou partagée uniquement au sein d'un groupe.

“Domaine public (relevant du)” (Note sur la technologie, Note sur le logiciel)

Les termes “relevant du domaine public” qualifient la “technologie” ou le “logiciel” divulgué sans qu'il soit apporté de restriction à sa diffusion ultérieure.

N.B. Les restrictions relevant de ‹copyright› n'empêchent pas une “technologie” ou un “logiciel” d'être considéré comme “relevant du domaine public”.

“Fixe” (5)

Le terme “fixe” signifie que l'algorithme de codage ou de compression ne peut accepter des paramètres fournis de l'extérieur (par exemple, variables cryptologiques ou à clés) et ne peut être modifié par l'utilisateur.

“Logiciel” (Deux listes)

Le terme “logiciel” désigne une collection d'un ou de plusieurs “programmes” ou “microprogrammes” fixée sur tout support d'expression tangible.

“Nécessaire” (5,6,9, Note sur la technologie)

Le terme “nécessaire”, lorsqu'il s'applique à la “technologie” ou au “logiciel”, désigne uniquement la portion particulière de “technologie” ou de “logiciel” qui permet d'atteindre ou de dépasser les niveaux de performance, caractéristiques ou fonctions visés. Cette “technologie” ou ce “logiciel” “nécessaire” peut être commun(e) à différents produits.

“Programme” (2,4,5,6)

Le terme “programme” désigne une séquence d'instructions pour la mise en oeuvre d'un processus sous une forme, ou transposable dans une forme, qu'un calculateur électronique puisse exécuter.

“Sécurité de l'information” (5)

Les termes “sécurité de l'information” désignent tous les moyens et fonctions assurant l'accessibilité, la confidentialité, ou l'intégrité de l'information ou des télécommunications, à l'exclusion des moyens et fonctions prévus pour la protection contre les défaillances. Cela comprend notamment la “cryptologie”, la crypto-analyse, la protection contre les émanations compromettantes et la sécurité du calculateur.

N.B. Le terme ‹crypto-analyse› désigne l'analyse d'un système cryptologique ou de ses entrées et sorties pour dériver des variables confidentielles ou des données sensibles comprenant du texte en clair.

“Technologie” (Note sur la technologie et les deux listes)

Le terme “technologie” désigne les renseignements spécifiques nécessaires au “développement”, à la “production” ou à l'“utilisation” d'un produit. Ces renseignements

revêtent la forme de documentation technique ou d'assistance technique. La "technologie" visée est définie dans la Note générale sur la technologie et dans la Liste des marchandises à double usage.

N.B. 1 : Les termes ‹documentation technique› désignent des données pouvant se présenter sous des formes telles que bleus, plans, diagrammes, maquettes, formules, tableaux, dessins et spécifications d'ingénierie, manuels et instructions écrits ou enregistrés sur des supports ou dispositifs tels que disques, bandes magnétiques, mémoires mortes.

N.B. 2 : Les termes ‹assistance technique› désignent une assistance pouvant revêtir des formes telles que : instructions, procédés pratiques, formation, connaissances appliquées, services de consultants. L'‹assistance technique› peut impliquer un transfert de ‹documentation technique›.

NOTES INTERPRÉTATIVES ET CONDITIONS DE VALIDITÉ
(Extraits uniquement)

LISTE DES BIENS ET TECHNOLOGIES À DOUBLE USAGE

Note générale sur la technologie (NF (95) CA WP1)

Les Gouvernements conviennent que les transferts de "technologie" conformément à la Note générale sur la technologie, pour la "production" ou le "développement" d'éléments figurant sur cette liste seront traités avec vigilance conformément aux politiques nationales et aux finalités du présent régime.

Note générale sur la technologie (WG2 GTN TWG/WP1 Revised 2)

Il est entendu que l'on attend des Gouvernements Membres qu'ils exercent des contrôles sur la "technologie" immatérielle, dans toute la mesure que permet leur législation.

Note générale sur le logiciel (NF (95) CA WP1)

Les Gouvernements conviennent que les transferts de "logiciel", pour la "production" ou le "développement" d'éléments figurant sur cette liste seront traités avec vigilance conformément aux politiques nationales et aux finalités du présent régime.

Catégorie 5, Partie 2

Note relative à la validité

> *Le contrôle prévu au chiffre 5.A.2.a.1 demeurera en vigueur pour une période de deux ans à compter de la date d'entrée en vigueur de la Liste des biens et technologies à double usage, et sa reconduction sous sa forme actuelle exigera un accord unanime.*

N.B. Dans l'éventualité où un examen régulier de la Catégorie 5 - Partie 2 de la liste interviendrait avant l'expiration de la présente Note relative à la validité, les éventuelles décisions prises à l'issue de l'examen de la liste l'emporteraient sur les dispositions de cette Note.