Export de logiciels libres de chiffrement : le modèle américain (ITAR, EAR)

Par Lucie Blaye, juriste spécialisée en droit des logiciels

« Nous faisons vraiment la course entre nos capacités à construire et déployer la technologie, et leur faculté à créer et mettre en œuvre des lois et des traités. Aucun des deux côtés n'est susceptible de céder ou gagner en sagesse tant qu'il n'a pas perdu définitivement la course.[1] »

Devant l'utilité et la nécessité de faire appel à un mécanisme de chiffrement pour sécuriser les communications, les États-Unis ont investi beaucoup de moyens pour faire avancer la recherche en cryptographie. Compte tenu de l'usage militaire qui peut en être fait, il leur a semblé légitime de poser des restrictions quant à l'export de telles ressources afin de se préserver d'éventuelles réutilisations à leur encontre. Ce faisant, les États-Unis ont intégré la majorité des dispositions prévues dans le cadre l'arrangement de Wassenaar du 12 juillet 1996 (convention réglementant plus généralement l'export de matériels relatifs à l'armement) afin de contrôler les situations selon lesquelles une personne diffuse un logiciel de chiffrement – ou un produit utilisant un logiciel de chiffrement –, mais aussi dans le cas où une personne utilise ou embarque un logiciel de chiffrement dans ses propres produits commercialisés ou exploités à l'extérieur des États-Unis.

Dans le cadre d'une application stricte de ces dispositifs, le gouvernement américain avait ainsi condamné le 1er juillet 2009 le Professeur J. Reece Roth de l'Université du Tennessee à quatre ans de prison pour avoir autorisé deux étudiants étrangers, faisant leurs études aux États-Unis, à accéder à des informations concernant un projet militaire. La révélation de telles données techniques sur un drone de l'Air Force avait été assimilée à un export, cette notion englobant toute expédition ou transition d'articles en dehors des États-Unis.

Cette régulation, relativement contraignante et procédurale, semble difficilement combinable avec la logique de libre diffusion intrinsèque aux logiciels libres et Open Source. En effet, ces projets collaboratifs font appel à la contribution de développeurs de tout pays et, dans un tel contexte international, il conviendrait par exemple de veiller à respecter la réglementation américaine (et l'ensemble des réglementations nationales) dès lors qu'un logiciel de chiffrement est édité ou hébergé sur le sol américain.

En pratique, ces deux logiques ont des liens plus étroits et qu'il ne peut y paraître. En effet, l'usage de logiciels de chiffrement et déchiffrement cryptographique s'est vu démocratisé en 1991 grâce à l'intervention de Philip Zimmermann et son logiciel libre PGP (Pretty Good Privacy qui garantit la confidentialité et l'authentification pour la communication de données) – qu'il a, à l'époque, mis à disposition des internautes outrepassant la législation en matière de restrictions à l'exportation[2]. Conséquemment, et reconnaissant à ce titre l'intérêt de l'Open Source, le gouvernement américain a, 5 ans plus tard, mis en place des mesures dérogatoires spécifiques aux logiciels de chiffrement libres et open source.

Particulièrement importante compte tenu du nombre de projets libres concernés, la réglementation américaine de l'export de logiciels libres de chiffrement sera l'objet de ce premier article. Après une recontextualisation dans le cadre international (I), nous détaillerons le régime de l'EAR (II) qui prévoit en son sein des exceptions (III) et des dispositions spécifiques concernant le

1 We are literally in a race between our ability to build and deploy technology, and their ability to build and deploy laws and treaties. Neither side is likely to back down or wise up until it has definitively lost the race. John Gilmore, FreeS/WAN project founder

2 Une enquête a été ouverte par le gouvernement américain de 1993 à 1996, mais sans donner de suite.

libre et l'open source (IV) permettant la construction de projets libres (V).

I) Encadrement juridique international

Afin de permettre la circulation de logiciels de chiffrement la plus paisible possible, les règles sont harmonisées aux différentes échelles : règles internationales telles que l'arrangement de Wassenaar de 1996 (A) ou encore règles nationales comme celle des États-Unis (B).

A) L'arrangement de Wassenaar :

Le 12 juillet 1996, un groupe de 33 pays mené par les États-Unis a adopté l'arrangement multilatéral de Wassenaar sur le contrôle des exportations d'armements conventionnels et de biens et technologies à double usage. Il regroupe aujourd'hui 41 États.

Cet arrangement est destiné à renforcer la sécurité régionale et internationale en promouvant "la transparence et une plus grande responsabilité dans les transferts d'armes et de biens à double usage afin de prévenir les accumulations déstabilisantes". Les signataires de l'arrangement ont donc convenu de la création d'une coopération entre eux.

Dispositif d'ordre non contraignant, chaque signataire peut ensuite intégrer les directives de l'arrangement dans sa législation. Pour ce faire, il s'engage à effectuer un contrôle des exportations en vertu de sa législation nationale et à rendre compte, pour des questions de transparence, des transferts d'armements conventionnels et des biens à double usage jugés sensibles, ainsi que toute technologie à double usage très sensible.

Des listes de contrôles sont établies pour identifier ces biens à double usage et donner une ligne directrice aux régulations auxquelles ils doivent être soumis. Chaque liste de contrôle est mise à jour tous les ans en fonction de l'évolution des technologies.

L'arrangement de Wassenaar pose les conditions d'exportation des éléments de chiffrement (catégorie 5 partie 2). Cependant, chaque pays transpose de la manière qui lui convient chaque directive de l'arrangement. Celui-ci ne pose donc que des principes auxquels les législateurs nationaux peuvent apporter des exceptions, comme celle de la *License Exception TSU* aux États-Unis.

B) Législation américaine :

L'ITAR ou i*nternational Traffic in Arms Regulations* de 1976 est un ensemble de réglementations établies par le gouvernement américain pour effectuer un contrôle des importations et exportations relatives à la défense, rassemblé dans l'*U.S. Munition List*. Cette liste, actualisée régulièrement, oblige à ne pas communiquer les informations concernant la défense et la technologie militaire à des personnes extérieures aux USA, sauf exception.

Ce règlement s'applique entre autres sur tous les systèmes informatiques, qu'il s'agisse d'équipement ou logiciel, servant ou pouvant servir à contrôler ou compléter ces équipements. En outre, le terme « exportation » doit être interprété de manière très large, la définition englobant les exports et les transmissions d'éléments en dehors des États-Unis. Seront donc considérée comme des exportations toute activité opérée sur internet avec notamment la présence de données techniques pouvant potentiellement être utilisées à des fins militaires, les données restant accessibles à des personnes localisées dans le monde entier.

La signature de l'arrangement de Wassenaar de la part des États-Unis a fondamentalement changé leur vision sur les supports de chiffrement. Ils évoluent donc de l'ITAR qui considère ceux-ci comme des armes militaires à une réglementation moins restrictive qui est l'EAR. Devant la banalisation des opérations utilisant des techniques de chiffrement, l'ITAR n'est plus utilisé dans le contexte des exports de ces logiciels. Depuis le 30 décembre 1996, ce pouvoir est dévolu au Ministère du Commerce, dans un service de régulation destiné aux produits de chiffrement commerciaux. Ainsi, la régulation des logiciels de chiffrement a été transférée de la liste de munition (*U.S. Munitions List*) à la liste de surveillance du commerce (*the Commerce Control List (CCL)*) dépendant du règlement de l'administration aux exportations des États-Unis *(EAR)*.

Cela à l'exception de certains logiciels de chiffrement exclusivement développés pour un usage militaire qui resteront concernés par la réglementation ITAR (concernant l'intégration au sein de matériels référencés par l'*USML*). Le §121-8 revient sur le fait que tout export de logiciel répondant à une telle description peut s'effectuer suite à la demande d'une *technical data licence*. Il est prévu que toute personne ou entreprise aux États-Unis qui importe ou exporte des produits contenus dans l'*U.S. Munition List* doit s'enregistrer au niveau du département de l'État concerné. De plus, un pouvoir de contrôle est laissé au président des États-Unis sur les importations et exportations d'armement grâce à l'*Arms Export Control Act*

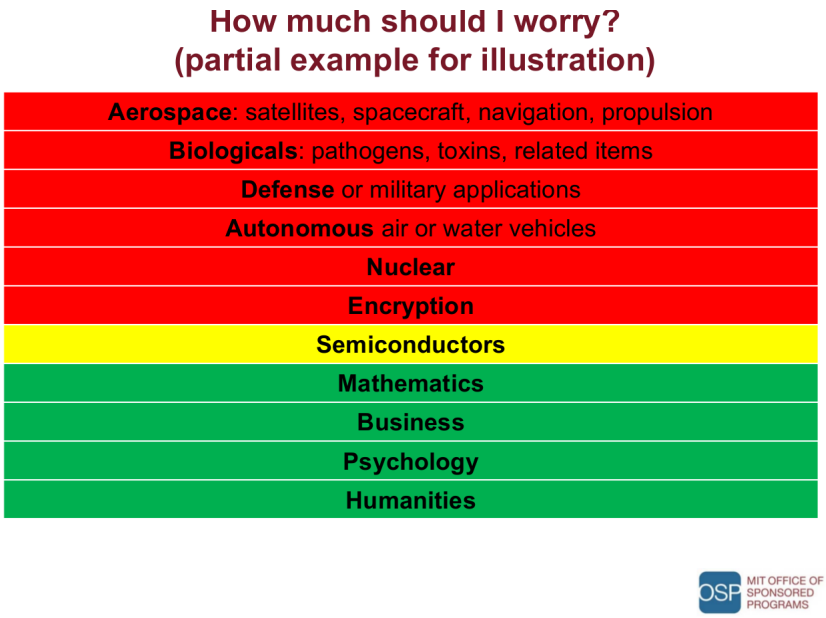
En synthèse, chaque *Department* (ministère) dispose de ses propres pouvoirs de contrôle et de sanction et la régulation de l'export s'effectue de la manière suivante :

Export de produits	Régime	Sanctions
Liés à la défense, données techniques et services.	Department of State (ITAR)	Les sanctions pénales : • pour une personne : jusqu'à un million de dollars par infraction et 10 ans d'emprisonnement • pour une entreprise : jusqu'à un million de dollars Les sanctions civiles s'élèvent à $500 000 et à des confiscations. Cependant, toute entreprise ne respectant pas les obligations du règlement peut se retrouver sur une liste noire pendant une période allant de 5 à 10 ans et par conséquent se verrait privée du privilège de vente ou prestation de service auprès du gouvernement américain.
Commerciaux (équipements, matériel, logiciels et technologie).	Department of Commerce (EAR)	Sanctions pénales : un million de dollars (avec peine de 20 ans d'emprisonnement pour les personnes physiques) Sanctions civiles sont allégées à $250 000.
À destination de pays faisant l'objet d'embargos	Department of the Treasury (OFAC)	Sanctions pénales : un million de dollars (avec peine de 20 ans d'emprisonnement pour les personnes physiques) Sanctions civiles sont allégées à $250 000.

Note : les individus sont aussi sujets à la réglementation : le fait de transporter un ordinateur ou une clé USB avec un contenu sujet à ladite réglementation en dehors des États-Unis ou montrer un algorithme à une personne étrangère est considéré comme un export selon la loi américaine[3].

3 Il existe une exception pour les voyages nommée BAG (§ 740.14 BAGGAGE de la réglementation EAR).

Illustration 1: David Quimby (MIT)
http://osp.mit.edu/sites/osp/files/u42/osp_forum_26may2011exportcontrols.pdf



II) Que prévoit la réglementation EAR ?

Dans son règlement EAR, le ministère du Commerce prévoit que ces dispositions s'appliquent à tous les exports et réexports de produits de chiffrement à des individus, entreprises commerciales et autres utilisateurs finaux sans lien avec le gouvernement. Ce contrôle s'applique à tous les biens à double usage, c'est-à-dire qu'ils sont susceptibles d'avoir une utilisation tant civile que militaire.

La notion d'exportation aura la même définition que celle posée par la réglementation ITAR, et le règlement EAR ajoute la notion de réexport qui englobe toutes les expéditions et les transmissions d'éléments sujets au règlement EAR entre les pays étrangers.

Quant au matériel concerné, il s'agit de la technologie et les logiciels exportés ou réexportés sans tenir compte du média ou de la méthode (cela regroupe entre autres la consultation, la conversation téléphonique, les conférences, Internet, messages électroniques...).

La Commerce Control List (CCL), dans sa catégorie 5 nommée « Télécommunications et « Sécurité de l'information » », Partie 2 « Sécurité de l'information » pose les principes de contrôles liés aux logiciels de chiffrement.

Ainsi, dans la partie D « Logiciel », on peut apprendre que les contrôles à l'export inclus dans 5D002.a,c. 1 ou dans le ECCN 5A002 comprennent les codes source de produits de chiffrement sauf dans le cas des exceptions établies dans les paragraphes 740.13(e) et § 734.3(b)(3) de la réglementation EAR qui seront expliqués dans le paragraphe B de cet article. De plus, une mention est insérée excluant aussi les codes objets dont le code source respecte les critères cités de la réglementation EAR.

Afin de comprendre les enjeux de cette réglementation s'appliquant aux logiciels de chiffrement, il convient de poser une méthode pour permettre une autoclassification (A) pour identifier les exceptions (B) conduisant à une *License Exception* (C).

A) Méthode pour élaborer une autoclassification

Une note insérée en préambule de la catégorie 5D002 (relative aux logiciels) indique que les logiciels de chiffrement sont contrôlés à cause de leurs capacités fonctionnelles et non pour les valeurs informationnelles qu'ils contiennent. De plus, de tels logiciels ne se voient pas accorder le

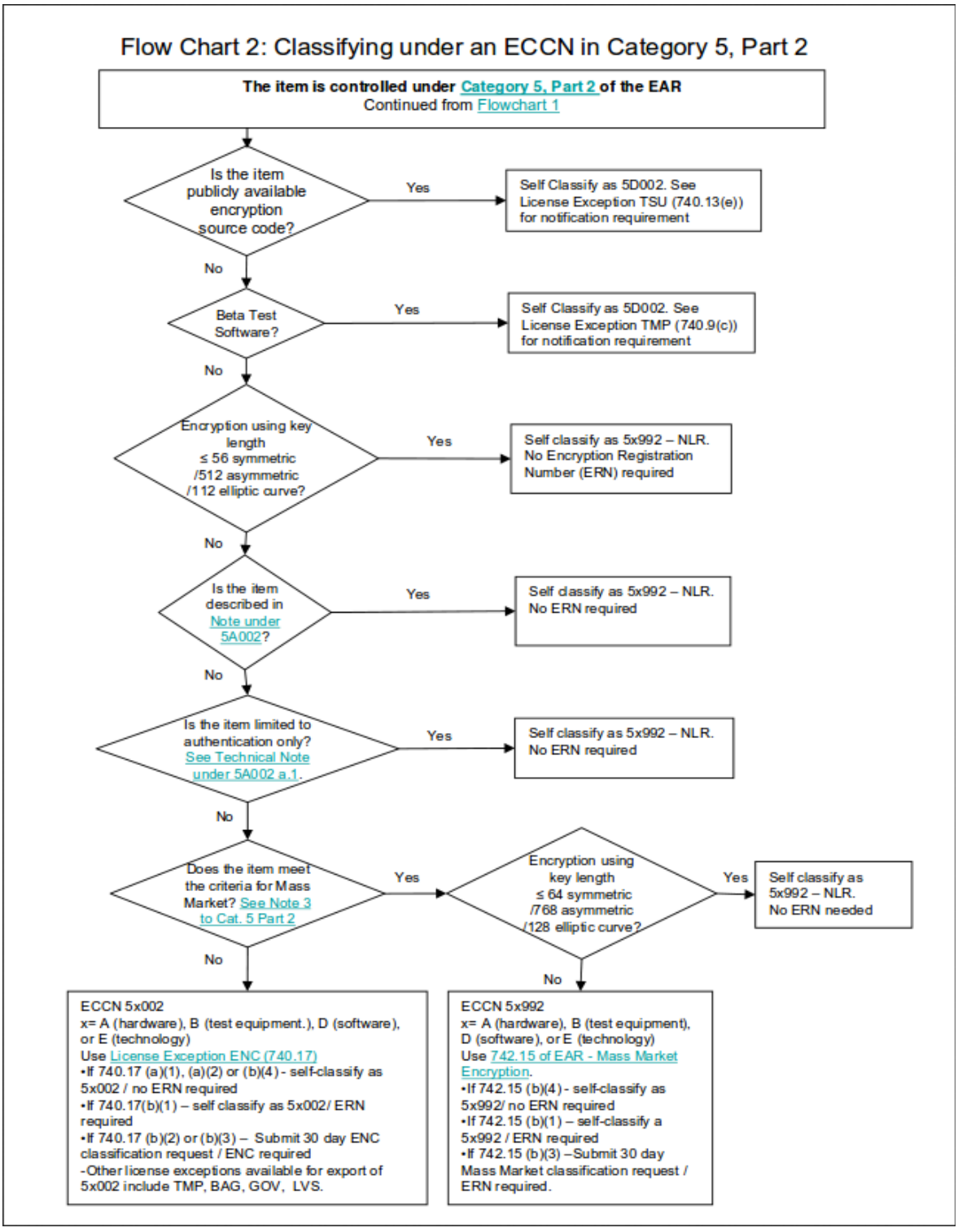
même traitement du règlement EAR que les autres logiciels et pour des raisons d'exportation, le logiciel de chiffrement est traité selon les mêmes dispositions que les systèmes de sécurité de l'information et les composants des équipements (5A002).

Cependant, il existe des exceptions et il convient de préciser la manière de bien identifier quelles sont les méthodes pour permettre une auto-classification du logiciel.

Le schéma ci-dessous donne un aperçu sur la façon d'auto-classer des produits et de les exporter selon leur classification :

Illustration 2: http://www.bis.doc.gov/index.php/forms-documents/doc_view/328-flowchart-2

Pour plus de renseignements : http://www.bis.doc.gov/index.php/policy-guidance/encryption/registration



B) Conditions d'application de l'EAR (§734.3(b)(3) et §734.7)

Le paragraphe §734.3(b)(3) encadre les produits qui ne sont pas concernés par la réglementation EAR : les technologies et les logiciels mis à disposition du public sauf ceux classés sous ECCN 5D002 sur la *Commerce Control List* qui :

- Sont ou ont été publiés comme décrit dans le §734.7 (développé par la suite)
- Sont le résultat de recherches fondamentales (§734.8)
- Ont une visée éducative (§734.9)
- Sont inclus dans certaines demandes de brevets (§734.10)

Note : un livre ou tout autre support matériel exposant des techniques de chiffrement ne sont pas soumis au règlement EAR.

Les informations qui sont ou ont été publiées doivent respecter des conditions qui sont développées dans le paragraphe §734.7 (Information publiée et logiciel) qui met en relief deux conditions : la publication (1) et la distribution (2).

1. La publication (§734.7)

Une information est publiée quand elle devient généralement accessible par le public sous quelle que forme que ce soit, incluant :

- Des publications dans des périodiques, livres, imprimés, électroniques ou sur tout autre support rendant disponible la distribution à tout membre du public ou à une communauté de personnes intéressées par un même sujet scientifique, que ce soit gratuit ou à un certain prix qui ne dépasse pas le prix de reproduction et de distribution ;
- Brevets et demandes « ouvertes » de brevets disponibles auprès des bureaux compétents ;
- Conférence accessible au public (il faut que le public puisse prendre des notes).

2. La distribution (§734.7)

La seule condition liée à la distribution inclue la notion de prix : il faut que la mise à disposition du public le soit à titre gratuit ou à un prix n'excédant pas le prix de reproduction et de distribution.

De plus, il est précisé que malgré les précisions apportées précédemment, il faut noter que les logiciels de chiffrement contenus dans le *Commerce Control List* restent soumis à l'EAR, exception faite des codes source des logiciels de chiffrement disponibles au public qui respectent le paragraphe 740.13(e) de l'EAR.

Note : l'EAR, dans ses différentes parties, développe des questions auxquelles sont apportées des réponses sur les divers points portant à confusion (Section A, B et G dans le contexte).

C) Régime de l'exception de la réglementation EAR (License Exception (§740.13(e))

Le paragraphe exposant la License Exception TSU (Technologie and Software Unrestricted) est très fourni dans ses conditions, il convient donc de présenter en premier lieu l'encadrement du §740.13 de cette *License* (1), puis de s'intéresser au cas spécifique de la mise à disposition du public (§740.13(e)) de tels codes source de chiffrement (2), et enfin de voir les conditions liées à la notification (3).

1) Portée de la *License Exception TSU*

Le paragraphe §740.13 a pour portée d'accorder des permissions d'export et de réexport des technologies et des logiciels opérationnels. Cela englobe le minimum de technologie nécessaire pour l'installation, l'opération, la maintenance (vérification) et la réparation de telles marchandises ou des logiciels qui sont légalement exportés ou réexportés sous licence, la *License Exception*. Sont exclues les technologies permettant le développement ou la production et est incluse la technologie d'usage servant les extensions garantissant la sécurité et l'usage efficace des marchandises ou des logiciels.

Le 14 janvier 2000 est créée la catégorie « Code source de chiffrage à accès libre » ("*unrestricted encryption source code*") qui permet de ne pas soumettre au contrôle effectué pour les *Encryption Items* de la Licence Exception TSU. Le 19 octobre 2000, cela s'est étendu aux codes objets compilés des logiciels issus de la catégorie « Code source de chiffrage sans restriction ». Dans ces deux cas, le code source ou le code objet doit respecter la condition posée par EAR : « mis à disposition du public ». De plus, le logiciel doit être disponible gratuitement ou à un prix ne dépassant pas les frais de reproduction et de distribution.

Le paragraphe §740.13(2) met en relief les dispositions et la destination liées à la technologie définie précédemment. S'agissant des dispositions, il existe deux conditions : le logiciel d'opération est le minimum nécessaire pour faire fonctionner un équipement autorisé à l'export et au réexport et le logiciel d'opération est sous forme de code objet. Quant à la destination, le logiciel et la technologie peuvent être exportés vers n'importe quelle destination pour laquelle l'équipement dans lequel ils sont intégrés a été ou est légalement exporté ou réexporté.

De plus, les mises à jour de logiciels sont autorisées si elles sont limitées à la correction d'erreurs du logiciel légalement exporté (740.13(c)).

2) Mise à disposition du public des codes source de chiffrement (740.13(e))

Le paragraphe §740.13(e) (*publicly available encryption source code*) autorise les exports et les réexports de codes sources de logiciels de chiffrement. Ces codes sources sont éligibles à la *Licence Exception* TSU (*Technology and Software Unrestricted*)[4]

Larry Christensen, ancien directeur de la Politique de la régulation du BXA (Regulatory Policy) recommande d'utiliser un mécanisme de décision pour déterminer la License Exception appropriée :

- Déterminer si le logiciel ou la technologie peuvent être qualifiés de disponibles au public ce qui permettra de le placer en dehors de la réglementation EAR.
- Sinon, déterminer si le logiciel est en dehors de la portée des contrôles effectués sur les logiciels de chiffrement (*Encryption Items* ou EI).
- Est-ce que le logiciel peut se voir englobé dans la définition de la *License Exception* ?

Le code source est éligible à cette *License Exception* même s'il est soumis à un accord exprès de licence à titre onéreux ou des royalties pour une production commerciale ou vente de tout produit développé en utilisant le code source.

Cependant, des restrictions sont prévues en soustrayant tout export ou réexport de logiciels de chiffrement classé ECCN 5D002 qui ne correspondent pas aux exigences du paragraphe (e)(1) (sur la portée du paragraphe, voir supra), même si le logiciel incorpore ou est spécialement créé pour utiliser d'autres logiciels de chiffrement qui répondent aux exigences de ce paragraphe (e)(1). En outre, les exportations vers les pays sujets à un embargo sont proscrites.

3) Notification (§740.13(e)(3))

Il convient de notifier le BIS (Bureau of Industry and Security) et le ENC Encryption Request

4 Cette Licence Exception autorise les exports et ré-exports de technologies et logiciels, leur vente, leur mise à jour et les codes sources de chiffrement qui sont considérés disponibles au public selon le §734.3(b)(3).

Coordinator de la NSA par mail de l'adresse URL du code source accessible par le public ou fournir aux deux une copie de ce code source. Toute modification devra par ailleurs leur être signalée. De plus, il convient de leur préciser tout changement d'adresse internet du site intégrant le code source, mais les modifications sur internet de ce code ne doivent pas être portées à leur connaissance.

Les notifications ou copies doivent être effectuées aux l'adresse suivante : crypt@bis.doc.gov et à enc@nsa.gov.

La Licence Exception TSU autorise l'export de codes source contrôlés par l'ECCN 5D002 ou, si ce n'est pas le cas est considéré publiquement disponible selon la section 734.3(b)(3).

Certains produits contrôlés par la catégorie 5, partie 2 ne nécessitent pas d'enregistrement. Sont inclus :

- Les produits classés 5x992, à savoir :
    - Des produits avec des clefs dont la taille n'excède pas 56 bits symétrique, 512 bits asymétriques et/ou 112 bits courbe elliptique ;
    - Produits de consommation de masse avec des clefs dont la taille n'excède pas 64 bits symétrique, 768 bits asymétriques et/ou 128 bits courbe elliptique
    - Produits qui utilisent le chiffrement simplement pour des raisons d'authentification.
- Des produits/transactions 5x002 :
    - Certains produits/transactions sont éligibles aux exceptions ENC sans modalités d'enregistrement à destination du secteur privé (740.17(a)(1)), un subsidiaire américain (740.17(a)(2))
    - Certains produits qui ne demandent qu'une notification avant export tels que les logiciels de chiffrement mis à disposition du public avec un code source sous Licence Exception TSU (740.13(e)) et les logiciels de test bêta sous Licence Exception TMP (740.9).

Pour plus de renseignements sur l'enregistrement :
Site du Bureau of Industry and Security :
http://www.bis.doc.gov/index.php/policy-guidance/encryption/registration
http://www.bis.doc.gov/index.php/policy-guidance/encryption/encryption-faqs

Document explicatif de la procédure SNAP-R :
http://www.bis.doc.gov/index.php/forms-documents/doc_view/329-example-view-in-snap-r

III) Les exceptions :

La « Karn case » rappelle que l'exception de domaine public ne s'applique pas en cas de logiciels de chiffrement. Cependant, la Cour Suprême va différencier le support de chiffrement : les cours et les écrits académiques peuvent être exportés sans accord préalable du gouvernement. Par conséquent, les réglementations ITAR et EAR ne sont pas applicables aux principes scientifiques, mathématiques ou d'ingénierie qui sont enseignés à l'école et à l'université ou des informations qui composent légitimement le domaine public[5].

On pourra donc faire la différence les exceptions et les exemptions :

Exceptions :	Exemptions (informations publiée et accessible au public)
• Domaine public	• Informations disponibles dans les kiosques

5 Domaine public (définition en droit américain) : création non protégée par le copyright. La création n'est jamais protégeable par le copyright ou est entrée dans le domaine public dû à l'expiration des droits.

- Finalité éducative
- Recherche fondamentale

à journaux, les librairies, sur internet, par mail...
- Dans les bibliothèques
- Brevets et dépôts de brevet publiés
- Conférences, meetings, séminaires aux États-Unis, accessibles au public
- Logiciels mis à disposition du public
- Recherche fondamentale.[6]

VI) Quid de l'Open Source et du libre selon le régime américain ?

Comme nous venons de le voir, les logiciels de chiffrement classés sous l'ECCN 5D002 restent sujets aux réglementations EAR, exception faite des codes source des logiciels mis à disposition du public (si le §740.13(e) s'applique en l'espèce aux fins d'invoquer la *License Exception TSU*).

Il faut de plus prendre en considération que les critères précédents ne s'appliquent que dans le cadre de la législation américaine, c'est-à-dire que pour les résidents des États-Unis. Pour les développeurs d'autres pays, la législation peut s'inspirer des arrangements de Wassenaar (notamment si son pays de résidence est signataire à ce traité) mais ne pas comporter d'exception pour les logiciels de chiffrement libres ou open source[7].

Deux situations nous intéressent principalement : celle dans laquelle on diffuse un produit qui utilise un logiciel de chiffrement (A) et celle dans laquelle on utilise ou intègre un logiciel de chiffrement (B).

A. Export d'un logiciel libre de chiffrement

Ces logiciels pourront donc être diffusés, suite à notification, dans des pays autres que ceux interdits par le ministère du Trésor, s'ils respectent les conditions suivantes :

- Il faut que le code source soit notifié au niveau du BIS et de l'ENC Encryption Request Coordinator de la NSA (procédure expliquée dans le 2.B).
- Le prix du logiciel ne doit pas excéder le coût de reproduction et de distribution.

Il faut cependant noter que s'agissant des entreprises ou personnes diffusant des logiciels libres ou open source moyennant un paiement ne disposent pas des exceptions prévues par le gouvernement américain et doivent par conséquent disposer d'autorisations précises avant tout export.

On peut notamment citer la société Red Hat qui propose des logiciels libres payants, qui met à disposition de tout intéressé les différentes notifications et autorisations dont l'entreprise a dû se doter pour exporter ses solutions.[8]

Les États-Unis étant le berceau des mouvements libres et open source, il est intéressant de constater que cet aménagement spécifique de la législation américaine est particulièrement adapté à ce type de diffusion : la seconde condition étant automatiquement remplie du fait de la licence (qui est gratuite) et il suffit donc de notifier les autorités compétentes dans les règles précitées pour être conforme à la législation.

B. Le logiciel de chiffrement embarqué

Dans cette hypothèse, c'est le produit fini incluant le logiciel de chiffrement qui sera considéré et non pas simplement le logiciel comme composant propre d'un ensemble.

6 Toute recherche non divulguée ou « propriétaire » est soumise à l'EAR pour les conditions liées à l'export.
7 Un article complétera bientôt ce premier travail en se concentrant sur la législation française relative à l'exportation de matériels de chiffrement.
8 http://www.redhat.com/f/pdf/licenses/ProductTechnologyMatrix.pdf

Il faut envisager deux situations différentes : le cas où le produit fini peut être classé comme matériel militaire (1) et le cas contraire (2).

1. Logiciel embarqué dans du matériel militaire

Que l'on se place au niveau de l'export américain ou de tout autre pays, le matériel de chiffrement ne sera pris en compte que dans un deuxième temps, la principale analyse s'opérera sur le matériel à l'export et sur les autorisations autour. En outre, le logiciel peut être considéré comme essentiel au bon fonctionnement du matériel et ne nécessitera pas d'analyse comme élément indépendant du matériel militaire.

Dans ce cas de figure, il faut prendre en considération la réglementation ITAR qui va réguler entièrement les exportations de matériels militaires et donc se référer à l'*U.S. Munition List.*

2. Logiciel embarqué dans du matériel non militaire

Là encore, le matériel sera considéré du point de vue militaire et sera écarté du régime législatif correspondant à l'export de matériels militaire de la réglementation ITAR.

Puis, il conviendra de respecter toutes les règles du pays d'exportation, mais aussi d'importation, dont voici un rappel pour les États-Unis :

- Il ne faut pas que le pays de destination soit sujet à l'embargo des États-Unis ;
- Il faut que le code source soit notifié au niveau du BIS et de l'ENC Encryption Request Coordinator de la NSA (procédure expliquée dans le 2.B) ;
- Le prix du logiciel ne doit pas excéder le coût de reproduction et de distribution.

Si tous ces critères sont respectés, il faut procéder à la notification de la NSA et du BIS[9]. Dans le cas où toutes les conditions de notification n'auraient pas été respectées, certaines entreprises peuvent être inscrites sur une liste noire interdisant toute importation sur le territoire souhaité.

V) Quid des projets libres ?

Pour conclure ce premier article, il est intéressant de constater la pratique des projets libres et Open Source suffisamment importants pour avoir considéré la question.

En effet et bien que les restrictions semblent allégées pour les logiciels de chiffrement open source, la procédure de notification peut représenter un frein pour les petites entreprises ou organisations américaines, ou tout autre entité qui hébergerait ses logiciels de chiffrement aux États-Unis. Cependant, il faut noter que le cycle de développement très court qui caractérise le logiciel libre (release early, release often) est totalement pris en compte dans la législation américaine (une seule notification du site web sur lequel sont mis à disposition les logiciels de chiffrement étant nécessaire).

Certains ont trouvé une parade à la législation américaine, tel que Debian, qui a fait le choix de séparer les logiciels de chiffrement dans une archive particulière en dehors des États-Unis.

Debian est un système d'exploitation dont les capitaux et les ressources sont détenus par un organisme enregistré à but non lucratif : Software in the Public Interest (SPI). L'engagement commercial étant nécessaire sur internet pour pouvoir se voir verser des dons, la sécurisation doit être optimale, d'où l'utilisation de logiciels de chiffrement. Ces logiciels ne sont donc pas localisés aux États-Unis, mais basés sur un serveur connu sous le nom de serveur « non-US ».

Cependant, cette solution comporte des limites quant à la responsabilité des développeurs américains qui apporteraient leurs contributions sur ces logiciels de chiffrement.

Il existe aussi le type de site qui, pour plus de compréhension, met à disposition du public toute la méthodologie mise en place pour procéder à la notification ou à l'autorisation comme le site de

9 Pour plus de renseignements, se référer à la parie II C 3).

Freedesktop[10]. Ce site rappelle aussi les règles liées à l'exportation sur une page entièrement dédiée.

Enfin, il existe la solution Apache qui a dédié une page entière de son site, dédiée aux exports de ses produits.

10 http://www.freedesktop.org/wiki/Software/fprint/US_export_control/