La Revue des droits de l'homme
Revue du Centre de recherches et d'études sur les droits fondamentaux

11 | 2017
Varia

L'exportation de systèmes de surveillance informatique par les sociétés privées européennes vers les pays tiers

Jonathan Keller

revues.org

Éditeur
Centre de recherches et d'études sur les droits fondamentaux

Édition électronique
URL : http://revdh.revues.org/2939
ISSN : 2264-119X

Référence électronique
Jonathan Keller, « L'exportation de systèmes de surveillance informatique par les sociétés privées européennes vers les pays tiers », *La Revue des droits de l'homme* [En ligne], 11 | 2017, mis en ligne le 16 janvier 2017, consulté le 23 janvier 2017. URL : http://revdh.revues.org/2939 ; DOI : 10.4000/revdh.2939

Ce document a été généré automatiquement le 23 janvier 2017.

L'exportation de systèmes de surveillance informatique par les sociétés privées européennes vers les pays tiers

Jonathan Keller

1 Lors de sa session du 18 décembre 2013, l'Assemblée Générale des Nations Unis adopta une résolution - proposée par le Brésil et l'Allemagne - reconnaissant le droit à la vie privée numérique. Cette résolution s'inscrivait à la suite de la révélation d'écoutes électroniques mondiales effectuées par les services de renseignement étasuniens. Ces atteintes à la vie privée numérique étaient justifiées par la sécurité nationale prise dans son sens le plus large. Tout d'abord, rappelons que rares sont les conventions internationales ou régionales relatives aux droits de l'homme qui parviennent à protéger efficacement le droit à la vie privée, et *a fortiori* un « *droit à la vie privée numérique* »[1] ; aucune n'est relative aux activités d'espionnage en temps de paix[2]. Cette efficacité peut être notamment appréciée au regard du respect *a priori* des normes par les États Parties à ces conventions internationales ou aux sanctions *a posteriori* invitant les États Parties à modifier leur comportement. Mais ces conventions internationales n'agissent qu'en cas de violation d'une norme de *jus cogens* accroissant ainsi la relativité du droit à la vie privée.

2 L'histoire récente est celle de l'émergence de l'emploi de nouveaux moyens de télécommunications permettant de porter des nouvelles revendications et de créer de nouvelles organisations. La « *Bataille de Seattle* »[3] l'illustre parfaitement. Les opposants à l'OMC utilisèrent les réseaux pour s'organiser jusqu'à leur suspension par les forces publiques. Les « *Révolutions Twitter* » qui se déroulèrent en 2011 en Égypte et en Tunisie sont un autre exemple. Enfin, dans un autre registre, les auteurs des attentats du 13 novembre 2015 utilisèrent les services d'application de téléphonie mobile *Telegram* pour organiser leurs crimes odieux, ce qui illustre la déviance possible de ces moyens.

3 La prévention par les forces publiques des actes terroristes comme des revendications indépendantistes ou d'autres formes de contestation, mises sur le même plan, s'accompagnent, au mieux, de l'interdiction de certains équipements, à l'instar de Blackberry en Arabie Saoudite, de réquisitions administratives ciblées en France, de partenariats publics privés avec les acteurs privés aux États-Unis ou, au pire, de la création d'un Internet purgé ou recensant toutes les requêtes qualifiées comme « déviantes » effectuées par les utilisateurs comme c'est le cas en Chine, en Corée du Nord ou en Iran.

4 Ces deux dernières hypothèses serviront ici de base. On les analysera au regard du droit français, surtout dans le contexte de la déclaration du pouvoir exécutif du 24 novembre 2015 de déroger à certaines dispositions de la Convention Européenne de Sauvegarde des Droits de l'Homme (CEDSH) prise sur le fondement des raisons impérieuses de sécurité nationale. La question de la surveillance sur Internet, défendue par des responsables politiques, a été vainement critiquée par la doctrine et combattue par de nombreuses associations à la suite de l'entrée en vigueur de la loi sur le renseignement[4]. L'article 851-3 du Code de la Sécurité Intérieure codifié par cette loi prévoit en particulier « *une mise en œuvre* » de « *réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste* » - c'est-à-dire de logiciels détectant les menaces « *à la défense et à la promotion des intérêts fondamentaux de la Nation* »[5]. Or ces logiciels sont développés par des prestataires de service, personnes morales de droit privé, et demeurent leur propriété intellectuelle exclusive.

5 Des sociétés françaises, mais également étasuniennes, fournissent ces mêmes services depuis l'avènement d'Internet à des États tiers à l'Union Européenne. Ces derniers effectuent soit des recherches de *Deep Packet Inspection*, c'est-à-dire, concrètement, de contrôle du contenu des « allées et venues » et des communications d'utilisateurs sur Internet, soit de *Stateful Packet Investigation*, c'est-à-dire de la collecte de métadonnées des télécommunications hertziennes et électroniques[6]. Or ce type d'activité offre auxdits États le contrôle de la vie numérique de leurs ressortissants, et par conséquent attentent à leur vie privée et, indirectement, à celles de leurs correspondants – d'autant plus lorsqu'ils sont ressortissants étrangers. Nous nous attacherons ici à analyser le contrat de prestation conclu entre une société prestataire dont le siège se situe sur le territoire français avec un État tiers au Conseil de l'Europe, États qui souvent maltraitent leur population grâce aux résultats des processus informatiques fournis par les prestataires français.

6 Cette situation conduit à s'interroger sur la possibilité de vendre - activité se plaçant dans le cadre de la liberté du commerce et de l'industrie - des dispositifs de surveillance - œuvre au sens de la propriété intellectuelle trouvant sa source dans la liberté d'expression - dans le cadre d'un contrat de prestation auprès d'un État tiers à l'Union Européenne. Ce contrat de prestation a pour but de détecter les recherches ou les déclarations faites sur Internet par les ressortissants dudit État, pour identifier *a minima* des menaces à l'ordre public, et *a maxima* des opposants politiques, qui dans certains pays sont, « au mieux », torturés. Autrement dit, quelle est la licéité d'un contrat de fourniture d'un logiciel, initialement œuvre de l'esprit, à des États dès lors que ceux-ci les utilisent pour réprimer la liberté d'expression de ses résidents ? Nous verrons que le logiciel de surveillance est, par sa nature d'œuvre littéraire, difficilement saisissable par les différentes sources juridiques (I). De son côté, la communauté internationale s'est saisie

de la question politique de l'exportation internationale de certains biens. Cet encadrement relève davantage du droit du commerce international que du droit international public (II).

I. L'exportation de logiciel utilisé à des fins de surveillance

7 Les exportations d'armement ou de produits manufacturés pouvant être réemployés à des fins d'armement sont encadrés par des instruments normatifs internationaux relatifs aux exportations. Ces normes soumettent les commerçants installés sur le territoire des États signataires à des régulations spécifiques avant toute exportation (B). Néanmoins, ces régulations spécifiques n'admettent pas explicitement les logiciels de surveillance dans leur *ratione materiae*. Pour appréhender cette exclusion politique, la définition préalable du logiciel doit être déterminée (A).

A) Le logiciel : œuvre dont la variation du régime dépend de l'utilisation

8 Lorsque l'outil informatique est défini par les conventions internationales, ce n'est que pour définir son inclusion[7] ou son exclusion[8] à l'égard d'un régime spécifique de protection. Le droit interne ne donne aucune définition juridique légale du logiciel. La pratique a développé certaines distinctions pour différencier les types de programme informatique. Ainsi, le logiciel est une solution informatique « *faite sur mesure* » par l'éditeur pour répondre aux besoins d'un client – son élaboration relève du contrat de prestation de service, là où le progiciel, qui relève davantage du contractuel régime de la vente, est un produit standard destiné du grand public. On se focalisera ici sur la première catégorie mais en se servant de la seconde pour illustrer les tempéraments possibles (1). Puis démonstration sera faite que les logiciels élaborés à des fins militaires décorrélés de tout support matériel échappent généralement à un contrôle *a priori* de l'Etat (2), à l'exception des moyens de cryptologie (3).

1. Le logiciel : objet juridique à régime variable

9 Œuvre par destination de la loi, le logiciel n'en reste pas moins un objet au régime juridique, en dehors de sa protection, indéfini. En effet, l'utilisation vertueuse ou délictueuse d'un logiciel entraîne un régime propre[9]. Ainsi par exemple, un logiciel multimédia affichant des contenus pornographiques répond aux mêmes restrictions imposées par le genre, c'est-à-dire par exemple un film ou une revue[10].

10 Le droit étasunien atteste d'une telle vision en énonçant que le code informatique doit être interprété comme une œuvre littéraire, c'est-à-dire jouissant de la liberté d'expression[11]. Or la liberté d'expression, tant en droit européen qu'en droit américain, souffre de tempéraments même si celle-ci se doit être « *the marketplace of ideas* » aux États-Unis[12] ou « l'un des fondements essentiels (d'une) société démocratique » en Europe [13].Ce principe prétorien a été affirmé aux États-Unis après qu'un professeur ait cherché à publier un code source relatif à un protocole de cryptologie dans une revue scientifique et que le gouvernement fédéral s'y soit opposé sur le fondement des restrictions à

l'exportation. Cette décision a eu des effets notables dans l'*Arrangement de Wassenaar*[14] à bien des égards.

11 Tout d'abord, reconnaître au code source[15] la même qualité qu'une œuvre littéraire entraîne une absence de contrôle *a priori* du logiciel par les États-Unis. Le droit d'auteur sur le logiciel – contrairement au brevet – ne peut être refusé dans l'hypothèse d'une violation de l'ordre public[16]. Ainsi lorsque contrôle il y a sur la destination du logiciel - contrôle déclenché par une plainte[17] ou demande[18] contre un acte administratif[19] devant un juge – celui-ci intervient *a posteriori* la divulgation. Les droits d'auteur existent alors toujours sur l'œuvre mais l'auteur ne peut plus divulguer en l'état son œuvre.

12 La seconde conséquence de cette assimilation de l'œuvre informatique à l'expression est l'épanouissement du logiciel sous licence libre et/ou sous licence ouverte. Ce type de contrat informatique est en quelque sorte une « perversion » du droit d'auteur. Autrement dit, les prérogatives du droit d'auteur accordées à l'auteur sont utilisées pour s'en affranchir afin de partager son œuvre logicielle sans aucune restriction et en laissant à tout à chacun la possibilité d'analyser, de modifier, d'améliorer et de partager ce logiciel. Ainsi reconnaître la divulgation d'un code de cryptologie, type de logiciel qui subit les restrictions les plus importantes quant à son régime de divulgation, dans une revue scientifique comme expression faisant l'objet d'une protection du premier amendement de la constitution américaine, suggère que les autres types de logiciels peuvent être diffusés sous forme de code source dès lors que cette diffusion est faite « efficacement », c'est-à-dire par une divulgation la plus large possible.

13 Enfin, le logiciel est une œuvre de l'esprit. Or il est très rare – même dans les contrats conclus avec les États – qu'une cession complète des droits d'auteurs soit faite. En d'autres termes, et concrètement, le prestataire crée une structure nationale *ad hoc* pour opérer la location de son logiciel à l'État en question. Cette location s'accompagne de diverses opérations de maintenance afin que le logiciel de cybersurveillance soit toujours en état et fonctionnel.

2. Le régime de droit commun sur la fourniture d'armes

14 Les industries de l'armement sont limitées quant aux modalités de leur installation et de leur exploitation. En France, elles sont soumises à un régime d'autorisation préalable en deux étapes. La première étape est mentionnée dans l'article L. 2332-1 du Code de la Défense qui soumet tout producteur de matériel militaire à l'agrément de l'État avant toute fabrication d'armes et munitions. Une telle démarche s'accompagne d'un contrôle *in concreto* par l'administration. La seconde étape concerne une demande déposée au commissariat de police ou à la brigade de gendarmerie compétente du lieu où seront produites les armes[20]. Ces exigences procédurales visent principalement les lieux de fabrication et de commercialisation de certaines catégories d'armes. Le contrôle étatique porte tant sur les opérations techniques que comptables pour contrôler l'absence de corruption de fonctionnaires étrangers[21] et la dissémination de matériels de guerre.

15 Mais ce contrôle s'exerce également sur la protection intellectuelle du matériel. Ainsi le Code de la Défense oblige le fabricant d'armes ou de matériels militaire à communiquer préalablement à tout dépôt de brevet. Cette procédure déroge au droit commun puisque l'article L. 613-20 du Code de la Propriété Intellectuelle (CPI) dans lequel l'examen d'une application militaire est fait lors de l'examen du brevet[22]. La lettre de l'article L. 613-20 du CPI ne semble s'appliquer qu'aux « *inventions, objets de demandes de brevets ou de brevets* ».

Or, un logiciel offensif ou défensif, purement logiciel c'est-à-dire n'étant pas intégré dans un matériel spécifique, reposerait exclusivement sur le droit d'auteur. Concrètement, une telle cyberarme ou tout autre moyen de cybersurveillance ne saurait en raison de cette protection faire l'objet d'une expropriation. C'est à ce niveau que l'originalité du logiciel dénote une absence de prise en compte par les pouvoirs publics.

3. L'inadéquation du logiciel de cyberarme ou de cyberdéfense à un contrôle étatique a priori

16 La question du sort des logiciels insérés dans les armes « *sophistiquées* »[23], c'est-à-dire comprenant des fonctionnalités logicielles pour parvenir à un résultat donné, doit être posée dans le cadre de cette procédure. Cette question déterminera l'enchevêtrement du logiciel dans le matériel militaire[24], c'est-à-dire le sort du cumul d'une œuvre soumise à la propriété littéraire et artistique avec une invention faisant l'objet d'une revendication d'un brevet. La réponse déterminera si la conception d'un programme d'ordinateur à des fins militaires doit être soumise aux dispositions de l'article L. 2332-1 du Code de la Défense. En principe deux éléments iraient contre cette idée. Le premier élément est que soumettre une œuvre développée par un auteur à l'appréciation étatique avant toute diffusion reviendrait à créer un régime de censure contraire au principe de la liberté d'expression. Le second est que l'ensemble de la doctrine en droit de la propriété intellectuelle appelle à une distinction entre ce qui relève du domaine pur du brevetable et de celui de la propriété littéraire et artistique lors du traitement d'une invention mise en œuvre par ordinateur[25].

17 Ainsi, l'expropriation pour des raisons de défense nationale ne saurait, par principe, y être appliquée[26] et le contrôle de l'Etat ne pourrait être fait en amont. En effet, l'invention expropriée pour des raisons de défense peut être fonctionnelle uniquement avec l'insertion du logiciel, que celui-ci soit un microgiciel[27] ou un programme d'ordinateur[28]. Celui-ci permet ainsi l'effet technique - élément justifiant l'expropriation au seul bénéfice du ministère de la Défense. Néanmoins, les droits d'auteurs sur le logiciel, composante autonome de l'invention, demeurent une variable inconnue en l'espèce. Sont-ils l'objet de la propriété exclusive de l'État, en partant du principe que l'accessoire suit le principal, ou sont-ils l'objet d'une copropriété entre l'État et l'inventeur, laissant à ce dernier la liberté d'utiliser ledit logiciel pour d'autres usages ? Nous tendrions vers cette seconde solution dans la mesure où le texte de l'article L 613-20 du CPI ne visent que « *inventions, objets de demandes de brevets ou de brevets* » et que le brevet ne concernera guère l'œuvre connexe.

18 En outre, nous penchons pour une absence d'application de l'article L 2332-1 du Code de la Défense au lieu où sont développés les logiciels composants d'un matériel militaire. En effet, notre interprétation de l'article L 613-20 du CPI appelle la remarque que les inventions mises en œuvre par ordinateur protègent certes la partie logicielle mais uniquement dans le cadre de la réalisation de cet effet technique. Cette dernière dispose d'une « *superposition de deux objets* »[29], à savoir l'écriture qui est protégée par le droit d'auteur et le processus technique ou/et le produit protégé(s)[30] par le droit des brevets[31]. À notre sens, l'invention par ordinateur dépend de l'effet technique du logiciel. L'enchevêtrement de l'appareil inventé et du logiciel créerait une apparente interdépendance entre les deux. En dépit de l'émergence de la notion juridique de cyberguerre, et même si une législation concurrente prohibe le développement, la promotion et l'utilisation de certains logiciels, cette législation exclut ce type du logiciel

du domaine des biens disponibles[32]. Ces logiciels ne peuvent pas, par principe, être distribués au grand public pour des raisons de sécurité publique, et ce même s'ils ne sont pas considérés comme des armes et que leurs auteurs jouissent toujours des droits moraux des droits d'auteur à leur égard. Néanmoins le contrôle étatique est, à l'instar de toute œuvre, postérieur à leur divulgation. La seule exception notable à cette différence de traitement est la cryptologie.

B) Les moyens de cryptologie : exception à l'absence de contrôle étatique

19 La loi du 30 décembre 1990[33] prohibait un usage civil de la cryptologie assimilant celle-ci à l'utilisation d'une arme militaire. Le fondement invoqué est de se prémunir contre toute atteinte à la sécurité nationale[34]. Ceci se justifie par la volonté de l'État Français d'exercer ses pouvoirs régaliens sur l'ensemble de son territoire par un droit d'enquête ou de réquisition administrative, et ce nonobstant l'emploi d'outil de cryptologie[35]. Ce refus d'une absence de libéralisation de la cryptologie s'explique par la volonté de prévenir toute menace intérieure dont l'élaboration serait effectuée par des communications cryptée. Les besoins du commerce électronique ont justifié un assouplissement de la réglementation de ces outils[36]. La cryptologie a pour but de « *garantir la confidentialité des communications électroniques mais aussi d'identifier de manière certaine l'auteur d'un message et d'établir l'intégrité de celui-ci* »[37]. Cette libéralisation a été initiée par la Loi pour la Confiance dans l'Économie Numérique (LCEN)[38].

20 Les dispositions de l'article 39 de la LCEN renvoient à un décret de 1939 sur les moyens de télécommunication du ministère de la Défense et est précisé par un décret de 2007 qui prévoit trois régimes distincts en fonction des opérations : un régime de tolérance ; un régime de déclaration préalable, pour certaines importations ; des demandes d'autorisations pour des exportations vers un État membre de la Communauté et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité[39].

21 L'exportation de moyen de cryptologie en dehors de l'Union Européenne est soumise au respect d'engagements internationaux pris par la France. On relèvera toutefois, que l'importation de solutions de cryptologie ne fait pas l'objet d'une autorisation ou d'un contrôle *a priori* effectifs, en témoignent les vains espoirs d'encadrement législatif des progiciels de télécommunication électronique sécurisés distribués sur des plateformes d'applications informatiques se situant à l'étranger. Limiter l'accès desdites plateformes au territoire français est en effet techniquement impossible[40] !

II. L'encadrement des régulations spécifiques par des conventions internationales

22 Le logiciel est une œuvre fonctionnelle. Néanmoins son fonctionnalisme entraîne une inadéquation avec le régime juridique encadrant les armes. Cette inadéquation se retrouve dans le droit commun des exportations de matériel militaire puisque celui-ci vise peu les logiciels (A). Il a été fait au mieux pour tenter de les limiter en les visant incidemment par des critères organiques téléologiques, c'est-à-dire en les assimilant à des éléments soumis à des restrictions spécifiques (B).

A) Le droit commun aux exportations

23 De nombreux instruments normatifs multilatéraux internationaux régulent le transfert de technologie. La norme applicable à l'exportation varie selon que la technologie soit directement ou indirectement utilisée à des fins militaires. Tout d'abord, il est utile de rappeler que les embargos décrétés par l'Organisation des Nations Unies limitent l'exportation des armes vers certains États. Au-delà de cette prohibition, la vente d'armement en droit international public s'est longtemps limitée à une liste exhaustive de plusieurs sources définies en fonction de l'armement concerné : le *Traité de non-prolifération nucléaire (TNP)* entrée en vigueur 1970 et qui regroupe 187 adhérents, à l'exception d'Israël, Cuba, l'Inde et le Pakistan) ; la *Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et de leur destruction* de 1993 ratifiée par 126 États, la *Convention sur l'interdiction de la mise au point, de la fabrication, du stockage des armes bactériologiques et à toxines* ratifiée en 1972 par 143 États. Certaines conventions internationales traitent de questions connexes comme le *Convention de Genève de 1980 sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination (CCAC)* de 1980 complétée par la *Convention sur l'interdiction de l'emploi, du stockage, de la production et du transfert des mines antipersonnel et sur leur destruction* des 3 et 4 décembre 1997, entrée en vigueur le 1er mars 1999 et signées par 135 États.

24 Toutefois, bien que ces conventions et traités portent sur la restriction de la production, de l'emploi et de la diffusion de certaines armes, leur définition reste limitée soit en raison de leur potentiel destructeur (ex : l'arme nucléaire ou les armes chimiques), soit par l'absence de contrôle direct (ex : les mines antipersonnels ou les armes « *produisant des effets traumatiques excessifs ou comme frappant sans discrimination* »), soit surtout par un effet ayant un impact corporel sur l'intégrité de la personne physique. A une telle lecture, on ne peut que songer au principe posé par l'article L132-75 du code pénal français qui distingue l'arme par nature (« *Tout objet conçu pour tuer ou blesser* »), de l'arme par destination (« *Tout autre objet susceptible de présenter un danger pour les personnes est assimilé à une arme dès lors qu'il est utilisé pour tuer, blesser ou menacer ou qu'il est destiné, par celui qui en est porteur, à tuer, blesser, ou menacer* »).

25 De tels champs d'application semblent s'éloigner de notre propos puisque le logiciel de surveillance n'occasionne aucun dommage corporel[41]. Toutefois les différents documents internationaux cités traitent des composants informatiques dans le cadre de la création des armes, et soumettent les logiciels aux mêmes dispositions que le matériel encadré par ces traités et conventions.

26 A la différence des autres conventions internationales, l'Arrangement de Wassenaar établi le 12 mai 1996 était initialement un pur instrument politique[42] dont la finalité était de limiter les exportations vers des États communistes. Il crée un système de suivi des exportations et de notification de celles-ci à l'ensemble des États partenaires. Ces exportations concernent spécifiquement les biens dits à double usages, c'est-à-dire « *toutes technologies, même civiles, sensibles et risquant d'être détournées à des fins militaires* ». Ces technologies doivent être lues en concurrence des traités déjà mentionnés qui prévoient par eux-mêmes des restrictions pour des logiciels qui rentrent directement dans leur champ d'application. Néanmoins, l'Arrangement de Wassenaar est aussi un forum international dont les lacunes ont souvent été prises à partie. Parmi elles, il y a

notamment l'absence de sanctions autres que politiques. En effet, l'exportation des armes est un enjeu important économiquement. Le rapport parlementaire de 2000 relatif à l'exportation des armes ne dit guère autre chose en déclarant qu' « *il s'agit de profits, pour les industriels, mais aussi d'emplois* »[43]. Ce marché est d'autant plus compétitif que l'exportation tant d'armes que de biens à double usage, depuis la France, relève généralement de l'appréciation de plusieurs ministères étatiques en excluant les instances européennes de toute appréciation quant à l'opportunité d'exportations de matériels létales vers des États aux politiques contestables[44].

B) Le droit applicable à l'exportation de logiciel

27 Les cyberarmes ou les moyens de cybersurveillances ne font pas en tant que tel l'objet d'une régulation étatique autre qu'une prohibition faite *a posteriori*. Il ne demeure donc que les logiciels intégrés dans des composants de matériels de guerre ou les moyens de cryptologie. Dans ces deux cas, les dispositions de l'Arrangement de Wassenaar s'appliquent. Cet acte informel international a été transposé dans l'ordre communautaire par le Règlement 428/2009/CE[45] puis par la loi 2011-266[46]. Cette loi vise indistinctement les armes de destructions massives et les biens à double usages en listant, actualisant et fusionnant les obligations administratives en droit interne imposées par des dispositions de droit international et de droit européen[47]. Ainsi seront soumises aux mêmes procédures administratives d'autorisation ou de déclaration préalable les biens à double usage[48], les fournitures nucléaires[49], les armes biologiques[50], et les armes classiques[51]. Comme en témoignent les obligations internationales[52] et européennes[53] auxquelles la France s'est engagée, ces procédures administratives sont éminemment politiques[54].

28 Il reste que le nouveau régime instauré par la loi 2011-66 simplifie cette procédure en soumettant l'ensemble des exportations à potentiel nucléaire aux mêmes dispositions. Quand l'exportation porte sur un bien à double usage, tel que défini par l'Arrangement de Wassenaar ou le Règlement 428/2009, ou sur du matériel militaire, tel que défini par l'arrêté du 17 juin 2009[55] modifié par le décret 2012-901[56], l'exportateur sera soumis à l'obtention d'une licence accordée par le SBDU[57]. Cette licence sera alternativement globale[58], générale[59] ou individuelle[60]. La qualification de la licence entraînera une variation de la durée de l'autorisation délivrée par les pouvoirs publics[61]. A l'instar de ce qui est prévu par les États-Unis, ces licences sont également conditionnées par le respect de certaines obligations contractuelles par le destinataire du matériel. Ce dernier doit s'assurer que le bien à double usage ne sera pas réexporté ou ni utilisé à d'autres fins que celles prévues par la demande d'autorisation[62]. L'exportateur sera réputé avoir respecté l'exportation conforme à la confirmation de « l'acquit à caution » fourni par le destinataire, ou une soumission de caution lorsque le destinataire est un État[63], sans contrôle *a posteriori*, en se fondant sur la bonne foi contractuelle.

29 Toutefois, cette autorisation n'est pas pérenne. Le pouvoir exécutif se réserve le droit de la suspendre ou de la retirer à tout moment[64]. Cette suspension peut être requise par l'un des membres de la commission interministérielle[65] pour des raisons purement politiques et opportunistes. Le changement de politique interne de l'État d'accueil ou de ses rapports diplomatiques avec la France justifierait cette suspension ou retrait. Dans une telle hypothèse, l'exportateur ne jouira d'aucun droit à réparation[66]. Les prérogatives régaliennes prennent le pas sur les intérêts commerciaux des personnes privées.

Néanmoins, l'État peut indirectement indemniser par des fonds d'indemnisation semi-publics comme la COFACE.

30 Ainsi nous pouvons voir que le logiciel de cyberarme ou de cybersurveillance ne fait pas l'objet d'une législation *ad hoc* et s'inscrit totalement dans la liberté de création. Néanmoins, la fourniture de tels services relève d'un choix d'opportunité politique. Or, cette protection peut s'avérer difficilement conciliable avec le droit de tiers et particulièrement avec le droit à la vie privée. Cette conciliation se complique d'autant plus lorsque le logiciel est utilisé par un Etat à l'encontre de ses concitoyens.

31 Le contrôle *a priori* de la fourniture de moyen de surveillance appartient entièrement au pouvoir politique, tant du fait de l'application des prérogatives exorbitantes du droit commun du droit de la Défense que des incertitudes autour du régime du logiciel lui-même et échappe donc au contrôle judiciaire. Le contrôle *a posteriori* de la fourniture de moyen de surveillance échappe également au contrôle du juge. Aux Etats-Unis, l'*Alien Tort Act*[67] offrait un espoir jusqu'à la décision *Kiobel*[68]. Dans cet arrêt, la Cour Suprême fédérale rappela le principe de la séparation des pouvoirs pour exonérer la responsabilité d'un fournisseur de solution logicielle étasunien facilitant les répressions civiles. Il est intéressant de relever que sur le fondement d'une compétence internationale permise par la convention contre la torture et autres peines dégradantes[69], le juge français se voit soumettre un litige similaire[70].

NOTES

1. La CEDH et la CJUE reconnaissent une atteinte à la vie privée stricto sensu par le biais d'instrument numérique. Dans ce sens voir CEDH (*Szabo et Vissy c. Hongrie*, 12/01/2016, Req. n 37138/14),) et CJUE (Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12. V**.** Florence Benoit-Rohmer,) ; pour des développements plus précis exhaustive, voir M. FARSHIAN, *Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne*, *La Revue des droits de l'homme*, mis en ligne 28/05/2015, http://revdh.revues.org/1300 et J.-P. FOEGLE, *« Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse »*, *La Revue des droits de l'homme*, mis en ligne 30/03/2016, disponible sur http://revdh.revues.org/2074 (dernière consultation le 05/11/2016).

2. F. LAFOUASSE, *L'espionnage en droit international*, AFDI vol. 47 p.63, spéc. p. 119 et s. voir également G. COHEN-JONATHAN et R. KOVAR, *l'espionnage en temps de paix*, AFDI, vol. 6, 1960 p.239-255.

3. https://fr.wikipedia.org/wiki/Manifestations_de_1999_ %C3 %A0_Seattle (dernière consultation le 21/12/12016) « *Il s'agit des premières manifestation* altermondialistes *d'envergure qui préfigurent les émeutes anti-G8 de Gênes de 2001. L'événement est symbolique et fondateur à plus d'un titre : c'est la première fois qu'une manifestation arrive à bloquer un sommet international ; les militants viennent du monde entier, agissent par la non-violence (à part quelques groupes de Black Bloc qui s'en prennent à des symboles du capitalisme) et sont réprimés*

brutalement par des policiers .La bataille de Seattle est avant tout un exemple de l'utilisation de l'information pour mobiliser au-delà même de l'évènement. ».

4. Loi 2015-912 du 24/07/2015 JORF n° 0171 du 26 juillet 2015 page 12735.

5. Art. L. 811-3. du Code de la Sécurité Intérieure- « *Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants : 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; 4° La prévention du terrorisme ; 5° La prévention : a) Des atteintes à la forme républicaine des institutions ; b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; 6° La prévention de la criminalité et de la délinquance organisées ; 7° La prévention de la prolifération des armes de destruction massive.* ». Rappelons que la définition initiale de la loi portait également « *3 Les intérêts économiques et scientifiques essentiels de la France* » qui de par sa largeur a fait réagir la société civile qui y voyait le risque d'y inclure les contrefaçons triviales d'œuvres couvertes par le droit d'auteur.

6. Une métadonnée est généralement définie comme « une donnée sur une donnée », c'est-à-dire non pas le contenu des informations en elles-mêmes mais les informations sur celles-ci. Concrètement, il s'agit par exemple des numéros de téléphones des correspondants lors d'un appel téléphonique, la durée de cet appel, si l'appel est effectué par un téléphone mobile, des relais téléphoniques...

7. Ainsi voir par exemple les ADPICS adoptés dans le cadre de l'OMC le 15/04/1995 et entrant en vigueur le 01/01/1995 et dont l'article 10 vise les « programmes informatiques ». Les ADPIC ont soumis cette œuvre au droit commun de la propriété littéraire et artistique en incluant dans leur giron les conventions internationales relatives au droit d'auteur. À noter également la directive européenne 2009/24/CE du 23/04/2009 relative à la protection juridique des programmes d'ordinateur, directive codifiant la directive 91/250/CE du 14/05/1991 concernant la protection juridique des programmes d'ordinateur.

8. Voir dans ce sens la Convention du 05/10/1973 sur la délivrance de brevets européens, spécifiquement l'article 52 qui exclut les « logiciels en tant que tels » du champ des inventions brevetables.

9. Sur ce sujet voir notre thèse Partie 1 Titre 1.

10. Ainsi par exemple la loi du 16 juillet 1949 sur les publications destinées à la jeunesse sera applicable.

11. 9th Circ. En banc, Bernstein v. United States, 176 F.3d 1132, 1999.

12. Avis dissident du Justice HOLMES dans Abrams v. United States, 250 U.S. 616, 630 (1919) ("*The ultimate good desired is better reached by free trade in ideas — that the best test of truth is the power of the thought to get itself accepted in the competition of the market.*"), expression officialisée par la Cour Suprême en 1969 (in Brandenburg v. Ohio 395 US 444).

13. CEDH 07/12/1976 Handyside c. Royaume-Uni.

14. Voir infra.

15. Le code source (écrit en langage « naturel » c'est-à-dire humain) se distingue du code objet (écrit en langage binaire).

16. Voir dans ce sens article 53 de la Convention sur le brevet européen « *Les brevets européens ne sont pas délivrés pour : a) les inventions dont l'exploitation commerciale serait*

contraire à l'ordre public ou aux bonnes moeurs, une telle contradiction ne pouvant être déduite du seul fait que l'exploitation est interdite, dans tous les États contractants ou dans plusieurs d'entre eux, par une disposition légale ou réglementaire », transposé en droit français par l'article L 611-17 du CPI.

17. Trib. Corr. Carpentras 25/06/2004 pour des systèmes de décryptage télévisuel « *Le système de traitement automatisé de donnée se définit comme tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons qui concourent à un résultat déterminé.* », voir également Crim 22/02/2011 n ° 10-82.834 note J. FRANCILLON, *Fraudes informatiques. Introductions frauduleuses de données et intrusions illégales dans un système informatique,* RSC 2013 p. 559.

18. Sur la base de la responsabilité des produits défectueux par exemple, dans ce sens N. MOLFESSIS, *Les produits en cause*, P. A., 28/12/1998 n° 155 p. 20 (§8 « *Pourquoi, en effet, faudrait-il exclure du texte les logiciels _ qui comporteraient un virus _ ou encore les biens qui constituent simplement des informations diffusées par voie informatique ou par voie de presse ? Ainsi qu'on l'a soutenu, '' il ne serait pas choquant d'affirmer que l'auteur qui divulgue par voie de presse une formule erronée dont la réalisation causerait un dommage, ou l'imprimeur à qui une erreur de composition fait classer parmi les champignons comestibles un champignon mortel, doivent répondre de la responsabilité de plein droit ''' »).

19. Voir dans ce sens par exemple l'arrêté de la Préfecture de Police du 24/06/2015 interdisant l'utilisation des applications Uberpop, Heetch, et Djump sur la base de « troubles à l'ordre public ».

20. L 2332-1 § II. C.

21. Voir dans ce sens les articles L 2332-1 et suivants du Code de la Défense où sont contrôlés « les dépenses de publicité et de représentation » de ces industries.

22. Voir J. PASSA, TRAITE DE DROIT DE LA PROPRIETE INDUSTRIELLE, LGDJ, 2013, T. 2, pp. 1059, spéc. p. 373 § 303 « *Certaines inventions sont susceptibles d'intéresser la défense nationale de telle sorte que l'État, dans l'intérêt de celle-ci, peut souhaiter s'en réserver la connaissance et l'exploitation. C'est la raison pour laquelle le ministre chargé de la Défense est habilité à prendre connaissance auprès de l'INPI, à titre confidentiel, des demandes de brevet (...). Cette phase de secret concerne toutes les inventions, y compris celles qui n'ont manifestement aucun rapport avec la défense nationale et celles (...) déposées en France sous priorité d'un dépôt étranger (...) L'intérêt du système de la mise au secret réside principalement dans la faculté d'expropriation pour les besoins de la défense nationale* ».

23. Pour reprendre l'expression de Mme M.-F. FURET, *le droit international des armes*, in LE DROIT INTERNATIONAL ET LES ARMES, note supra, spéc. p. 7.

24. Comme nous le démontrerons infra II. les matériels de communications rentrent dans une catégorie voisine mais au traitement similaire, les biens à double usage.

25. Dans ce sens voir par exemple C. CARON, *Réflexions sur la coexistence du droit d'auteur et du droit des brevets sur un même logiciel*, RIDA 2000, n° 184 pp. 3-55 et C. LE STANC EXCLUSION DE BREVETABILITE – REGLES RELATIVES AU LOGICIEL – J-CL n° 4220, §85.

26. Voir Art. L 611-10, 3 du CPI qui requiert un processus technique.

27. Ou micrologiciel, de l'anglais *firmware*. Il s'agit d'un microcode qui s'insère dans une mémoire flash dans un composant ou un matériel informatique. Voir dans ce sens X. LINANT DE BELLEFONDS, *Le droit de décompilation : une aubaine pour les cloneurs*, note supra, spéc. p. §13 : « *on peut dire, pour faire une image, qu'il est du logiciel en quelque sorte matérialisé dans le silicium dont sont composés les micro-circuits. Ces logiciels enfermés dans des puces présentes sur les circuits imprimés des matériels gèrent les processus internes de ceux-ci (notamment les ROMs) ; ces logiciels sont évidemment très solidaires du matériel, au point de ne*

pouvoir être "accédés" et étudiés qu'avec des méthodes de haute technicité qui concernent plus le pirate que l'utilisateur banal. »,

28. C'est-à-dire une « *série d'instructions pour faire fonctionner une machine calculatrice* » pour reprendre l'expression de C. LE STANC, *Logiciel : Trente ans entre droit d'auteur et brevet. Bilan ?* In MELANGES XAVIER LINANT DE BELLEFONDS, Lexis Nexis, 2007, pp. 474, spéc. p. 271-290.

29. Voir INPI, sous la direction de M. VIVANT, PROTEGER LES INVENTIONS DE DEMAIN, Coll. Propriété Intellectuelle, 2003, pp. 320, spéc. p. 91 § 67 « *Si le brevet appréhende "la recette" technique, et plus précisément les étapes d'un processus qui "font" un procédé, le droit d'auteur, qui ne concerne que la forme saisit, lui, l'écriture et l'architecture du logiciel (...). A tout le moins, la superposition des deux objets : l'écriture et la "recette" qui passe par l'écriture, débouche sur de réelles interrogations, quant à l'articulation juridique* ».

30. Sur ce sujet voir J. PASSA, DROIT DE LA PROPRIÉTÉ INDUSTRIELLE, Tome 2, LGDJ, 2013, pp. 1059 spéc. p. 80 §59 et s.

31. Par analogie à partir des exceptions du brevet d'une invention par ordinateur id. p. 93 § 67.2 : « *Sans doute, le moyen de sortir de la contradiction est de relever que le brevet ne peut couvrir que le procédé, défini à travers ses étapes, et que le droit "d'expérimentation" ne peut porter sur autre chose que cela : c'est le procédé qu'il faut pouvoir tester, la validité des enchaînements décrits, et rien d'autre. Une nette dissociation des deux objets ("recette" et écriture) est donc tout à fait concevable en l'occurrence.* ».

32. Voir dans ce sens par exemple les virus informatiques ou les méthodes d'intrusion aux systèmes automatiques de traitement de données, tous deux réprimés par l'article L 323-3-1 du Code Pénal.

33. Loi 90-1770 sur la réglementation des télécommunications dont l'article 28 instaure un régime de déclaration pour les « prestations » n'ayant pour but que « d'authentifier une communication ou d'assurer l'intégralité du message transmis » et à un régime d'autorisation pour les autres cas, c'est à dire le cryptage du message. Le second point de ce même article prévoit des peines pénales cumulables ou alternatives pour réprimer toute abstention à cette obligation.

34. Cette affirmation est d'autant plus d'actualité depuis les événements du 13 novembre 2015.

35. Voir par exemple l'article 11-1 la loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie électronique qui dispose de l'obligation pour le vendeur d'outil de cryptage de remettre, sous peine de lourdes sanctions pénales, les outils de décryptage adéquate aux « agents autorisés ».

36. Voir E. CAPRIOLI, P. AGOSTI, *La confiance dans l'économie numérique*, LPA 03/06/2005, p. 4, voir également P. LE TOURNEAU, CONTRATS INFORMATIQUE ET ELECTRONIQUES, Dalloz, 8ém éd. 2014, p. 521 « *(La cryptologie) contribue au développement du commerce électronique (principalement lorsque la prestation est immatérielle et surtout entre entreprises car elles effarouchent encore pour l'instant le consommateur)* ».

37. Voir E. CAPRIOLI, *la nouvelle réglementation sur la cryptologie : un cadre juridique enfin complet*, CCE n° 10, 10/2007, comm. 128, §1 , de plus Force est de constater que rentrent dans cette définition les équipements conçus pour assurer la protection de logiciels ou de données informatiques contre la copie ou l'utilisation illicite, en des termes plus simples des Mesures Techniques de Protection.

38. Loi n° 2004-575, 21/06/2004 JOFR 22/06/2004.

39. Voir article 30-IV de la LCEN.

40. Nous avons eu l'occasion de participer à des plaidoiries et des avis d'organisations pour contrer la volonté d'acteurs institutionnels français cherchant à obtenir des clés de décryptage d'applications mobiles appartenant à des acteurs privés (ex. whatsapp, telegram).
41. Il est intéressant de voir qu'une telle impossibilité d'un dommage se retrouve très souvent dans la littérature relative à la responsabilité du fait de l'information. En effet, l'unanimité des auteurs en droit de l'informatique rejette l'idée même qu'une information soit source d'un dommage corporel. Dans ce sens A. LUCAS, *La responsabilité du fait des choses immatérielles*, MELANGES CATALA, Litec, 2001, pp. 1023, spéc. pp. 817-826.
42. C. SORNAT, Répertoire de droit international, *Armes*, § 18 : « *Les arrangements ont un régime juridique très particulier puisqu'il ne s'agit pas de traités au sens juridique du terme, mais d'accords intergouvernementaux informels à caractère politique liant les États qui les ont acceptés.* ».
43. Voir dans ce sens J.-C. SANDRIER, C. MARTIN et A. VEYRET, RAPPORT D'INFORMATION SUR L'EXPORTATION D'ARMEMENT, 25/04/2000, n° 2334.
44. Dans ce sens voir la résolution du Parlement européen du 17 décembre 2015 sur les exportations d'armements : mise en œuvre de la position commune 2008/944/PESC qui s'avère être davantage un vœu pieu pour que la Commission se saisisse de la problématique en encadrant davantage les États.
45. Règlement du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et des transits de biens à double usage. JOUE 29/05/2009 L 134/1.
46. Loi du 14/03/2011, JO 15/03/2011.
47. Pour une étude exhaustive voir C. SORNAT, REPERTOIRE DE DROIT INTERNATIONAL, Dalloz, 08/2007 m-à-j. 01/2014, ou DIRECTION GENERALE DES DOUANES ET DROITS INDIRECTS, GUIDE SUR LES EXPORTATIONS DE BIENS ET TECHNOLOGIES À DOUBLE USAGE, 02/2014
48. Voir le règlement 428/2009 transposant et organisant les dispositions de l'Arrangement de Wassenaar dans l'Union Européenne.
49. Voir le Traité de Washington sur la non-prolifération des armes nucléaires du 01/07/1968 (JO 25/09/1992).
50. Voir le protocole concernant la prohibition d'emploi à la guerre de gaz asphyxiants, toxiques ou similaires et de moyens.
51. Voir les articles 6 et 7 du Traité sur le commerce des armes, commentaire par A.-N. DUMOUCHEL, note supra. p. 33, voir également p. 38 les critères d'évaluation de l'État destinataire des armes classiques.
52. Composé de délégués issus du ministère de la Défense, du Ministère des Affaire Étrangères et du MINEFI.
53. Voir le Code de conduite de l'Union Européenne en matière d'exportation d'armements de du 13/12/2008 (JOUE L 335/99à qui fait état de 8 critères à prendre en compte, voir F. VALLEE et F. BAUDE, DROIT DE LA DEFENSE, p. 795 note de base n° 1 « *1. Respect des obligations et des engagements internationaux des États, Membres, en particulier des sanctions adoptées par le Conseil de sécurités des Nations Unies ou l'Union Européenne, des accords en matière, notamment de non-prolifération, ainsi que des autres obligations internationales ; 2. Respect des droits de l'homme dans le pays de destination finale et respect du droit humanitaire international par ce pays ; 3. Situation intérieure dans le pays de destination finale ; 4. Préservation de la paix, de la sécurité et de la stabilité régionales ; 5. Sécurité nationale des États membres et des territoires dont les relations extérieures relèvent de la responsabilité d'un État membre (...) ; 6.*

Comportement du pays acheteur à l'égard de la communauté international ; 7. Existence d'un risque de détournement de la technologie ou des équipements militaires dans le pays acheteur ou de réexportation de ceux-ci dans des conditions non souhaitées ; 8. Compatibilité des exportations de technologie ou d'équipements militaires avec la capacité technique et économique du pays destinataire, compte tenu du fait qu'il est souhaitable que les États répondent à leurs besoins légitime de sécurité et de défense en consacrant un minimum de ressources humaines et économiques aux armements ».

54. A. COLLET, « *Toute exportation d'armement traduit une volonté politique. Elle implique les choix de l'Etat client et de la destination en fonction de la situation du moment et relève de la même dialectique que l'envoi d'un porte-avions ou d'une force militaire. Elle comporte une connotation diplomatique même si des préoccupations économiques sont également présentes : il s'agit d'adresser de façon ostensible à un gouvernement un message d'amitié ou de réprobation. Pour faire respecter sa volonté politique, l'Etat dispose d'un moyen efficace : la réglementation* ». 1998 p. 63.

55. NOR DEFD0908305A.

56. Décret n° 2012-901 du 20/07/2012 relatif aux importations et aux exportations hors du territoire de l'Union Européenne de matériels de guerre, armes et munitions et de matériels assimilés et aux transferts intracommunautaires de produits liés à la défense NOR DEFD1207449D.

57. Service des biens à double usage – direction générale de la compétitivité, de l'industrie et des services – Ministère du redressement productif.

58. Voir DGCIS, GUIDE DE L'EXPORTATEUR, 10/2013, pp. 14, spéc. p. 6 : « *Cette licence, accordée pour 2 ans, permet à son titulaire d'exporter, sans limite de quantité ou de valeur, un ou plusieurs biens exhaustivement listés vers un ou plusieurs utilisateurs finaux spécifiques. Ce dispositif vise à faciliter le processus d'autorisation d'exportation en évitant des demandes récurrentes. En contrepartie de cette liberté laissée à l'exportateur, celui-ci doit mettre en place un processus interne de contrôle et effectuer un reporting semestriel auprès du SBDU.* » ; Voir également DIRECTION GENERALE DES DOUANES ET DROITS INDIRECTS, GUIDE SUR LES EXPORTATIONS DE BIENS ET TECHNOLOGIES À DOUBLE USAGE, p. 9 « *Adaptée aux flux importants, elle permet à son titulaire d'exporter des biens à double usage sans limitation de quantité ou de contrôle.* ».

59. DIRECTION GENERALE DES DOUANES ET DROITS INDIRECTS, GUIDE SUR LES EXPORTATIONS DE BIENS ET TECHNOLOGIES À DOUBLE USAGE « *Il s'agit de licences créées au niveau national qui couvrent quatre types de catégories très précises de biens (biens industriels, produits chimiques, graphite, certains éléments génétiques et organismes génétiquement modifiées) vers certains pays. Elles permettent d'exporter les biens en questions en quantité illimitée vers certaines destinations.* ».

60. DGCIS, GUIDE DE L'EXPORTATEUR, p. 6 « *Il 'agit de l'autorisation de droit commun pour un bien à double usage. Elle est valable 2 ans et permet l'exportation de ce bien à partir de tout Etat-Membre de l'Union Européenne. Elle est accordée pour un ou plusieurs biens de même nature et précise expressément le destinataire, l'utilisateur final, l'utilisation finale, la quantité et la valeur des biens à exporter* ».

61. Ainsi, les licences individuelles et globales sont accordées pour une période maximale de trois années, alors que la licence générale sera accordée par période d'une année renouvelable.

62. Voir Art. R. 2335-17-1 du Code de la défense dont le 5° « *l'utilisation et l'utilisateur final du matériel de guerre ou du matériel assimilé, s'ils sont connus* » et 6° »*la justification que le destinataire du matériel de guerre ou des matériels assimilés a été informé de la restriction à*

l'exportation dont l'autorisation d'exportation est assortie » ; voir également F. BAUDE et F. VALLEE, DROIT DE LA DEFENSE p. 795 § 1609 qui parle d'un « *effet extraterritorial d'exigences réglementaires françaises* ».

63. Voir Art. R 2335-35 du Code de la défense.

64. Voir Art. R 2335-14-I du code de la défense.

65. C'est-à-dire le délégué du ministère de la Défense, du Ministère des Affaire Étrangères, du MINEFI ou le Premier Ministre.

66. CE, Ass. 29/06/1962, Sté Manufacture des machines du Haut Rhin, AJDA 1962 p. 580. le Conseil d'État déclara « *la société requérante ne pouvait ignorer l'aléa que comportait nécessairement la passation d'un tel contrat, elle devait normalement envisage l'éventualité où pour des motifs légitimes, tirés notamment de l'intérêt de la défense nationale et de la conduite de la politique extérieure de la France, l'autorisation d'exporter à destination de la Syrie le matériel de guerre qu'elle avait fabriqué lui serait refusée ; ayant ainsi assumé ce risque en toute connaissance de cause, elle ne saurait utilement prétendre à faire supporter par l'État les conséquences onéreuses qui sont résultées pour elle de l'impossibilité où elle s'est trouvée de mener à son terme l'exécution de son marché* ».

67. Ch. 20, § 9, 1 Stat. 73 (1789) codifiée à l'article USC §1350

68. Cour Suprême Kiobel v. Royal Dutch Petroleum Co. 569-10-491, note H. MUIR WATT RCDIP, 2013, 3, p. 595

69. Article 689-3 du CPP *« Pour l'application de la Convention européenne pour la répression du terrorisme, signée à Strasbourg le 27 janvier 1977, et de l'accord entre les États membres des Communautés européennes concernant l'application de la convention européenne pour la répression du terrorisme, fait à Dublin le 4 décembre 1979* », Article 689-4 du CPP « *Pour l'application de la convention sur la protection physique des matières nucléaires, ouverte à la signature à Vienne et New York le 3 mars 1980* », Article 689-5 du CPP : « *Pour l'application de la convention pour la répression d'actes illicites contre la sécurité de la navigation maritime et pour l'application du protocole pour la répression d'actes illicites contre la sécurité des plates-formes fixes situées sur le plateau continental, faits à Rome le 10 mars 1988,* », Article 689-6 du CPP : « *Pour l'application de la convention sur la répression de la capture illicite d'aéronefs, signée à La Haye le 16 décembre 1970, et de la convention pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile, signée à Montréal le 23 septembre 1971* », Article 689-7 du CPP « *Pour l'application du protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale, fait à Montréal le 24 février 1988, complémentaire à la convention pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile, faite à Montréal le 23 septembre 1971* », Article 689-8 du CPP« *Pour l'application du protocole à la convention relative à la protection des intérêts financiers des Communautés européennes fait à Dublin le 27 septembre 1996 et de la convention relative à la lutte contre la corruption impliquant des fonctionnaires des Communautés européennes ou des fonctionnaires des États membres de l'Union européenne faite à Bruxelles le 26 mai 1997* » et 689-9 du CPP « *Pour l'application de la convention internationale pour la répression des attentats terroristes, ouverte à la signature à New York le 12 janvier 1998* ».

70. Voir FEDERATION INTERNATIONALE DES DROITS DE L'HOMME, *La société Qosmos placée sous le statut de témoin assisté : une avancée importante dans l'affaire en cours*, mis en ligne le 14/04/2015, disponible sur https://www.fidh.org/fr/regions/maghreb-moyen-orient/syrie/la-societe-qosmos-placee-sous-le-statut-de-temoin-assiste-une-avancee (dernière consultation le 21/12/2016).

RÉSUMÉS

A l'heure du tout connecté, des prestataires de service fournissent à des États tiers de l'Union Européenne des solutions logicielles interceptant et surveillant les communications entre personnes privées. Cette surveillance permet, dans certains États, de poursuivre des dissidents. La présente étude s'intéresse aux modalités d'exportations de ce type de logiciels.

At the age of the almighty connected, services companies provide to European Union's third party states, softwares which allow those state to intercept and monitor communication between private persons. Those interception can bring the repression of dissents. This study will focus on the modalities of the exportation of such softwares.

INDEX

Mots-clés : exportations, logiciel, compétence extraterritoriale, opportunité politique
Keywords : exports, software, extraterritorial jurisdiction, political opportunities

AUTEUR

JONATHAN KELLER

Jonathan Keller effectue sa thèse "La notion d'auteur dans le monde des logiciels" au sein du CREDOF. Il est également juriste de l'association La Paillasse et l'un des membres co-fondateur de l'association *Hackers against Natural Disasters*.