MEMOIRE DE MASTER

ESPIONNAGE ECONOMIQUE EN DROIT INTERNATIONAL PUBLIC

Master général en droit
Université de Lausanne
Printemps 2016

Branche : Droit international économique
Professeur : Andreas Ziegler
Rédigé par : Anna Sidorova
Adresse : Avenue Verdeil 7, 1005 Lausanne
Téléphone : 076/410.87.79
E-mail : sidorova.annie@hotmail.com
Date de remise de la version définitive au professeur : 17 mai 2016

Table des matières

Liste des abréviations

aff.	affaire
al.	alinéa
art.	article
ATF	Arrêt(s) du Tribunal fédéral
CEDH	Convention européenne des droits de l'Homme
CIA	*Central Intelligence Agency* (Agence centrale de renseignement)
CP	Code pénal suisse
Cst.	Constitution suisse
CVRC	Convention de Vienne sur les relations consulaires
CVRD	Convention de Vienne sur les relations diplomatiques
FBI	*Federal Bureau of Investigation* (Bureau fédérale d'enquête)
KGB	Comité pour la sécurité de l'État
LCD	Loi fédérale contre la concurrence déloyale
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LOPPSI 2	Loi d'orientation et de programmation pour la performance de la sécurité intérieure
MELANI	Centrale d'enregistrement et d'analyse pour sûreté de l'information
NSA	*National Security Agency* (Agence nationale de la sécurité)
OI	organisation internationale
ONU	Organisation des Nations Unies
p.	page
Règlement de la Haye	Règlement concernant les lois et coutumes de la guerre sur terre
s.	suivant(e)
SRC	Service de renseignement de la Confédération
ss	suivant(e)s
SVR	Service des renseignements extérieurs de la Fédération de Russie
TF	Tribunal fédéral

1. Introduction

Le terme d'espionnage économique est évoqué de plus en plus fréquemment de nos jours. Il concerne les affaires qui impliquent plusieurs entités différentes : les États, les organismes privés, les organisations internationales et de simples particuliers. De l'espionnage de guerre connu depuis toujours, nous sommes passés à un autre type d'espionnage, beaucoup plus dangereux selon certains, car beaucoup plus imprévisible et sophistiqué. Les victimes potentielles ne connaissent souvent pas l'ennemi en face d'elles, notamment à cause du développement d'un nouveau type d'espionnage, le cyber-espionnage[1].

Dans ce travail, nous allons tenter de définir la notion d'espionnage économique et ses différences fondamentales avec l'espionnage de guerre dans son sens classique. Nous allons également nous pencher sur la question de l'illicéité de cette pratique au niveau international et interne. Ensuite il s'agira de faire une distinction entre cette notion et celle de l'intelligence économique, ainsi que de parler de plusieurs types d'espions qui existent. Nous allons par la suite regrouper les méthodes de protection à disposition des États, en prenant l'exemple de quelques pays choisis. Pour finir, seront exposées quelques grandes affaires d'espionnage récentes.

2. La notion d'espionnage

2.1 Espionnage dans son sens classique

Selon l'art. 29 du Règlement de La Haye, un espion en temps de guerre est une personne qui « *agissant clandestinement ou sous de faux prétextes, recueille ou cherche à recueillir des informations dans la zone d'opérations d'un belligérant, avec l'intention de les communiquer à la partie adverse*[2]. » À l'origine, c'est un terme qui fait partie du droit des conflits armés. D'ailleurs, l'espion est également défini comme « *l'individu qui se mêle aux ennemis pour les épier*[3]. » Les informations recueillies doivent être confidentielles et avoir un intérêt militaire.

[1] F. LAFOUASSE, *L'espionnage dans le droit international*, Paris, 2012, pp. 24ss.

[2] Art. 29 du Règlement de La Haye concernant les lois et coutumes de la guerre sur terre, RS 0.515.111.

[3] R. ALAIN, *Dictionnaire historique de la langue française, Le Robert*, 1994, p. 727.

Le droit national de chaque pays détermine la définition de l'acte incriminé, ainsi que les informations secrètes protégées[4].

Étant donné que l'espionnage a toujours été principalement associé aux temps de guerre, les États ont voulu prévoir dans les traités la situation d'un espion arrêté, pour lui assurer une meilleure protection. Cela explique que la doctrine s'est concentrée longuement surtout sur ce type d'espionnage, au point de dire que les espions existent seulement en temps de guerre et « *qu'on ne saurait juridiquement donner cette qualification aux individus, qui, en temps de paix, se livrent aux mêmes pratiques* », comme l'a écrit COLONIEU[5].

Les espions, lors d'un conflit armé, ne sont pas des combattants et ne bénéficient pas de privilèges, tout comme les saboteurs et les mercenaires[6]. L'espionnage n'est en soi pas prohibé par le droit de la guerre, mais est puni en vertu du droit pénal interne de chaque pays[7].

La responsabilité personnelle de l'espion peut être engagée s'il a été pris sur les faits et s'il a eu droit à un jugement. Comme nous avons déjà mentionné, l'art. 29 de la Convention de La Haye donne une définition explicite de l'espionnage qui consiste en plusieurs éléments. Selon ROUSSEAU, il est toujours préférable d'utiliser la définition internationale, surtout dans les pays qui reconnaissent la primauté du droit international sur le droit interne. Les éléments constitutifs de l'espionnage sont la clandestinité et le fait d'être surpris dans la zone d'opérations de l'État belligérant[8].

Malgré que la doctrine en droit international évoque le plus souvent uniquement l'espionnage en temps de guerre, il peut très bien avoir lieu aussi en temps de paix et peut être commis par des nationaux comme par des étrangers[9].

---

[4] J. SALMON, *Dictionnaire du droit international public*, Bruxelles, 2001, pp. 448ss.

[5] V. COLONIEU, *L'espionnage du point de vue du droit international et du droit pénal français*, Paris, 1888.

[6] R.H.F. AUSTIN, Le droit des conflits armés internationaux*, in Droit international, Bilan et perspectives*, Tome 2, Paris, 1991, pp. 830ss., voir aussi T.K. REUTER et M. FREI, *Repetitotium, Völkerrecht*, 2e éd., Zürich, 2012, p. 122.

[7] M. KÜNG, M.K ECKERT, *Repetitorium zum Völkerrecht*, Berne, 1993, p. 441 et T. STEIN, C. VON BUTTLAR, *Völkerrecht*, 13 éd., München 2012, pp. 223ss.

[8] C. ROUSSEAU, *Le droit des conflits armés*, Paris, 1983, pp. 123ss.

[9] H. ASCENSIO, E. DECAUX, A. PELLET, *Droit international pénal*, 2e éd., Paris, 2012, pp. 151.

2.2. Espionnage économique

2.2.1 Contexte général dans lequel s'est développé l'espionnage économique

Nous vivons dans une époque de développement rapide des technologies informatiques, de la technique et de la science. Le milieu informatique influence désormais toutes les sphères de la vie humaine, y compris l'économie[10]. C'est le processus de la mondialisation, la planète devient un seul « *village global*[11] *»*. Le contenu des flux transnationaux s'est transformé. Désormais ce sont les services qui occupent la première place. Notre époque est l'époque de l'information. La nécessité de récolter et d'exploiter les renseignements plus vite que le pays concurrent est devenue primordiale[12].

Tout cela fait que de nouvelles menaces inconnues jusqu'à maintenant apparaissent[13]. La sécurité informatique est un domaine des technologies informatiques relativement récent qui se développe très rapidement de nos jours. Nous assistons à un passage de l'ouverture des systèmes informatiques à leur sécurisation[14]. Les acteurs du marché sont contraints de s'adapter vite à ces changements. Selon certains, « *nous vivons des temps étranges*[15] ». Car même si politiquement nous ne sommes pas en guerre et nous ne faisons pas appel à des soldats ou à des armes, nous sommes en guerre économiquement, avec des « *belligérants en col blanc*[16] ». Les entreprises combattent entre elles pour avoir de nouvelles parts de marché et pour être plus compétitives. Les conséquences sont importantes : la déstabilisation du marché économique, la faillite des entreprises, le développement du chômage etc.

En 1996, dans un entretien donné au New York Times, le directeur du développement de Sun Microsystems[17] a dit que chaque année, 20% des connaissances de son entreprise devenaient

---

[10] A. BEZBOGOV, A. YAKOVLEV, U. MARTEMYANOV, *La sécurité des systèmes d'exploitation*, Moscou, 2008, pp. 3ss.

[11] A. LAÏDI et D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 15ss.

[12] D. DANET, L'intelligence économique : de l'État à l'entreprise, *in Les Cahiers du numérique*, Volume 3, Paris, 2002, pp. 139-170.

[13] A. BEZBOGOV, A. YAKOVLEV, U. MARTEMYANOV, *op. cit.*, pp. 3ss.

[14] A. BEZBOGOV, A. YAKOVLEV, U. MARTEMYANOV, *op. cit.*, pp. 167ss.

[15] A. LAÏDI et D. LANVAUX, *op. cit.*

[16] A. LAÏDI et D. LANVAUX, *op. cit.*

[17] Un constructeur d'ordinateurs et un éditeur de logiciels américain.

obsolètes. Les entreprises sont mises au défi constant de créer des produits encore plus innovants et de devancer la concurrence. Il ne reste qu'un seul moyen pour survivre dans cette jungle, c'est d'être en avance par rapport aux autres d'un point de vue technologique. Comment se procurer les informations nécessaires ? Si nous songeons à des moyens légaux, il s'agit bien sûr d'investir dans la recherche et développement et de contrôler le milieu autour de soi. Mais c'est la situation idéale, qui a lieu seulement si l'entreprise a du temps et de l'argent. Si elle n'en a pas, il arrive qu'elle soit tentée d'utiliser des moyens illégaux[18].

C'est pour cela que l'espionnage industriel a lieu à tous les niveaux. C'est une affaire des États, des organisations internationales et des privés. Même si un jour l'espionnage de guerre venait à disparaître, l'espionnage économique, lui, subsistera toujours. Les affaires que voit le public ne sont en réalité que le sommet de l'iceberg. 9/10^{ième} d'entre elles restent secrètes et ne sont pas révélées au public[19]. Beaucoup d'entreprises préfèrent passer sous silence ces attaques par peur de dévoiler leurs faiblesses[20].

La personne qui a largement contribué au développement de la notion de la guerre économique mondiale est Bernard Esambert, ingénieur et financier français. Selon lui, le monde est entré dans une nouvelle époque économique depuis les années 1970 et il faut s'adapter rapidement aux nouvelles règles. « *La conquête des marchés et des technologies a pris la place des anciennes conquêtes territoriales et coloniales*[21]. » Son livre contient un vrai appel aux acteurs économiques de s'adapter aux exigences de cette nouvelle époque. L'auteur souligne également que la vraie richesse est constituée désormais par les hommes, avec leur intelligence et leur savoir-faire, par l'innovation et l'invention. Dans le monde occidental des années 1990, un slogan publicitaire a été créé par une société européenne de l'électronique « *La Troisième guerre mondiale sera une guerre économique : choisissez dès à présent vos armes*. » Avant, c'était une question de conquête des territoires, maintenant c'est la conquête des marchés. Les Japonais déclarent : « *Aujourd'hui nous ne bombarderions plus Pearl Harbour, nous l'achèterions*[22]. »

[18] A. LAÏDI et D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 15ss.

[19] J. BERGIER, *L'espionnage industriel*, Paris,1969, pp. 10ss.

[20] A. LAÏDI et D. LANVAUX, *op. cit.,* pp. 7ss.

[21] B. ESAMBERT, *La guerre économique mondiale*, Paris, 1992, pp. 10ss.

[22] B. ESAMBERT, *op.cit.*

La fin de la Guerre froide ne signifie pas pour autant qu'il n'existe plus de rapports de force au niveau mondial[23]. Ce n'est plus l'idéologie qui domine le monde, mais l'économie. Nous parlons désormais des bénéfices nets, des chiffres d'affaires, des résultats boursiers, des dividendes. L'adversaire n'est plus clairement déterminé, il peut être partout. L'État n'est plus désormais l'acteur principal sur l'arène, ce sont les entreprises qui sont mises sur l'avant-scène. Le monde entier devient une énorme toile, tout ça grâce à Internet et à la globalisation.

Au début des années 90, une puissance triomphe sur la scène internationale : le Japon. Son système économique est efficace et il n'y a pas une innovation technologique qui n'est pas maîtrisée par les Japonais. C'est le premier État qui a compris le rôle essentiel de l'information et en a fait la plus importante des matières premières. A partir de 1991, ce sont les Américains qui se lancent dans la guerre économique. La culture du renseignement existe déjà dans ce pays, par ex. General Motors possède déjà depuis les années 50 un service de renseignements chargé de contrôler l'activité de ses concurrents[24].

2.2.2 Techniques utilisées dans la guerre économique

Parmi les techniques utilisées dans cette nouvelle guerre, nous pouvons citer le *benchmarking*, ou l'étalonnage, qui consiste à observer et analyser la manière de faire d'une autre entreprise et de la reproduire ensuite. C'est une technique de gestion légale tant qu'elle est pratiquée avec l'accord des entreprises concernées. Par contre le *benchmarking* offensif est une technique illégale. C'est la situation où l'analyse se fait sans le consentement du concurrent et à son détriment. Le simple fait de se faire passer pour un client et d'avoir une conversation téléphonique avec l'entreprise concernée permet déjà d'apprendre beaucoup sur elle, tout comme le fait d'envoyer un étudiant stagiaire au sein d'une entité visée. Une démarche plus poussée consiste par ex. en un lancement d'un faux appel d'offres pour voir comment l'entreprise va réagir, et connaître ainsi ses tarifs. Il y a des méthodes plus extrêmes encore, par ex. le fait de provoquer une situation d'accident pour voir les normes de sécurité dans une entreprise.

---

[23] D. LUCAS, A. TIFFREAU, *La dissuasion par l'information. Guerre économique et information : les stratégies de subversion*, Paris, 2001.

[24] A. LAÏDI, D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 15ss.

Une autre méthode est le « débauchage concurrentiel », en d'autres termes, le recrutement. Selon un chasseur de tête pour une entreprise, son travail « *c'est de déstabiliser quelqu'un qui se plaît là où il est. On lui dit qu'il est mal payé ou que l'évolution de sa carrière est coincée. On essaie tout. C'est très pervers*[25]. » Une des techniques utilisées est de faire partir petit à petit tous les cadres importants d'une société à une autre.

C'est ce qui s'est produit en 2000 avec l'usine Philips produisant des téléphones, située au Mans, et leur site de recherche à Paris, où plusieurs cadres ont l'un après l'autre quitté leur poste. La direction de l'usine s'est adressée à un cabinet d'intelligence économique pour qu'il fasse une investigation sur cette situation. Le cabinet a fait une analyse des flux téléphoniques et a identifié l'auteur des attaques. C'était une nouvelle entreprise anglaise qui a été fondée par un ancien cadre de Philips et qui a réussi à recruter 25 cadres de son ancien employeur. L'enquête menée a montré des failles importantes dans le système de sécurité de Philips. Malgré ces alertes, la maison mère a tardé de prendre les mesures nécessaires et l'inévitable s'est produit : elle n'a plus pu suivre la concurrence. Ses résultats ont chuté de 90% au premier trimestre de 2001. Près de 50% de postes ont été supprimés. Seulement 6 ans après être venu s'installer au Mans, Philips a dû partir[26].

2.2.3 Espionnage économique : pratique licite ou non ?

L'espionnage en temps de guerre est considéré comme licite, ce qui n'a jamais été contesté depuis l'époque de Grotius[27] déjà. Par contre nous ne pouvons toujours pas dire avec certitude si l'espionnage en temps de paix est licite ou non. Certains soutiennent qu'il est illicite en avançant comme argument qu'en temps de paix, contrairement au temps de guerre, la pénétration sur le territoire d'un autre État est une violation de sa loi interne, ainsi que de sa souveraineté territoriale et de son indépendance[28] car l'espionnage est un acte qui fait parfois

[25] Source anonyme, Le nouvel Economiste, Paris, 1998.

[26] A. LAÏDI, D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 230ss.

[27] Juriste du 16e siècle qui a posé les fondements du droit international.

[28] F. LAFOUASSE, L'espionnage en droit international, in *Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

appel à des moyens contraires au droit international, comme la violation de l'espace aérien ou des eaux territoriales[29].

Il y a d'autres auteurs qui affirment que l'espionnage en temps de paix est licite. Ils classent cependant cet acte dans les actes « inamicaux » car ils peuvent nuire aux bonnes relations entre États. En tout cas, une chose est sûre, c'est qu'il n'y a pas de règle conventionnelle qui l'interdit explicitement. Par contre, nombreux sont les États qui l'interdisent dans leur droit national, ce qui ne les empêche pas de le pratiquer à l'égard des autres pays[30].

La Cour suprême fédérale allemande s'est prononcée ainsi sur la question : « *From the standpoint of international law, espionage in peacetime could not be considered as unlawful. No international agreement had ever been concluded on the subject. Neither was there any usage sufficient to establish a customary rule permitting, prohibiting or otherwise regulating such activity. But equally, individual States were not prohibited by international law from enacting national rules to punish espionage activity against them (...). Despite the fact that the acts themselves were not prohibited by international law, their punishment was entirely justifiable on the basis that such activity must be effectively combatted and deterred*[31]. »

Ce raisonnement amène à dire que l'espionnage en temps de paix a une nature juridique hybride. En soi l'acte d'espionnage perpétré par un État à l'encontre d'un autre État ne viole aucune norme internationale. En même temps, l'espion appréhendé sur le territoire d'un État va être jugé en principe par les autorités de l'État qui l'a appréhendé, sauf s'il y a des motifs d'exception, comme l'immunité diplomatique[32]. Le droit international admet donc la possibilité pour chaque État de s'en défendre par ses propres moyens[33].

Nous pouvons par conséquent nous demander pourquoi il n'y a pas d'interdiction de l'espionnage au niveau international. Si les États ne veulent pas être liés par une convention

[29] G. KOHEN-JONATHAN, R. KOVAR, L'espionnage en temps de paix, *in Annuaire français de droit international*, Volume 6, Paris, 1960, pp. 239-255.

[30] F. LAFOUASSE, L'espionnage en droit international, in *Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

[31] *Espionage prosecution case, Federal Republic of Germany, Federal Supreme Court*, 30 January 1991.

[32] F. LAFOUASSE, *op. cit.*

[33] A. ZIEGLER, *Introduction au droit international public*, 3e éd., Berne, 2015, p. 281.

sur une question, c'est parce qu'ils ne veulent pas être engagés juridiquement, donc ils tirent un certain avantage d'une telle position. En réalité, les États justifient l'espionnage en évoquant le principe de la réciprocité des droits et des avantages, qui est un sous-principe de l'égalité entre États, et est nécessaire pour leur sécurité intérieure et extérieure. Il s'agit d'une fiction où le pays concerné accepte qu'il puisse être victime d'espionnage, s'il se réserve le droit de sanctionner l'auteur[34]. Il serait donc permis de *« se procurer par des voies secrètes des renseignements qu'on ne pourrait obtenir autrement, surtout lorsqu'il s'agit de se garantir de certains dangers.[35] »*

2.2.4 Éléments constitutifs de l'espionnage

La Convention de La Haye parle des moyens clandestins. Il peut s'agir de la manière dont l'agent a pénétré sur le territoire d'un autre État ou la façon dont il se sert pour avoir les informations. Est clandestine « *toute action susceptible de faire encourir à son auteur une sanction au regard de la législation pénale de l'État en cause[36]*. » Il doit s'agir en tout cas d'informations qui ne sont pas facilement accessibles et que leur propriétaire a voulu garder secrètes.

Un autre élément constitutif concerne l'objet de l'espionnage, à savoir le recueil des informations importantes aux yeux d'un État étranger. Ces informations peuvent concerner les domaines militaire, politique, économique ou technique. Pour savoir ce que nous devons entendre par « renseignement », il s'agit de nouveau se tourner vers la législation interne des États. Il peut être défini de la manière suivante : « *une information collectée et exploitée au profit de décideurs politiques[37]*. » La victime de l'espionnage est en principe un État, et ses intérêts directs ou indirects. À l'origine, l'espionnage pouvait être effectué seulement au

[34] F. LAFOUASSE, L'espionnage en droit international, *in Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

[35] HAFFTEK, *Le Droit International de l'Europe*, 1888, Chapitre IV, p. 566.

[36] HAFFTEK, *op. cit.*

[37] F. LAFOUASSE, L'espionnage en droit international, in *Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

bénéfice d'un autre État étranger. S'y sont ajoutés les partis et les organisations étrangères, ainsi que des personnes ou organismes établis à l'étranger[38].

2.2.5 Types d'espionnage économique

Nous pouvons faire une distinction entre les actes d'espionnage qui entraînent la violation de la souveraineté territoriale d'un autre État ou non. Le premier type d'espionnage concerne le cas où l'espion est présent sur le territoire étranger pour collecter les informations, et comme nous allons le voir par la suite, engage la responsabilité internationale de son État d'origine. Toutefois, en réalité, l'État espionné renonce à engager une telle responsabilité contre l'autre État pour des raisons de réciprocité.

La deuxième méthode fait appel à des moyens techniques et se fait à partir d'espaces internationaux ou du territoire de son propre État. Ici, de nouveau, la collecte est clandestine car le consentement de l'État concerné n'est évidemment pas demandé. Certains États utilisent différentes méthodes pour intercepter les communications des États étrangers. Nous allons mentionner encore une fois que, même si en droit national il existe des dispositions qui l'interdisent, en droit international ce genre d'activité n'est pas interdite. C'est pour cette raison que le réseau américain « Echelon[39] », dont nous allons parler sous le titre 6[40], existe. Concernant les espaces internationaux, tels que la haute mer et l'espace extra-atmosphérique, il existe la liberté de leur utilisation dans la communauté internationale. Il s'agit également d'une activité qui n'a rien d'illégal d'un point de vue conventionnel, même s'il y a eu des tentatives de la rendre illégale, car c'est une activité qui ne recourt pas à la force[41].

Les méthodes traditionnelles d'espionnage sont toujours de mise. En font partie par ex. l'analyse des informations publiques et le recrutement d'informateurs. Le développement des réseaux sociaux simplifie largement leur travail de nos jours. Mais le type d'espionnage qui

[38] G. KOHEN-JONATHAN et R. KOVAR, L'espionnage en temps de paix, *in Annuaire français de droit international*, Volume 6, Paris, 1960, pp. 239-255.

[39] Nom de code pour une base américaine d'interception des satellites de télécommunications.

[40] Voir le point 6.4.3., p. 32 du travail.

[41] F. LAFOUASSE, L'espionnage en droit international, *in Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

prend de l'ampleur aujourd'hui est « l'espionnage cybernétique », les actes d'espionnage qui peuvent être perpétérés au moyen d'Internet, qui possède un avantage indéniable, le fait que l'auteur reste anonyme, et peut même agir à partir d'un pays où il ne sera pas forcément poursuivi.

Par « cybercriminalité », on entend les agissements criminels qui sont perpetrés via Internet[42]. Grâce aux moyens informatiques, il est désormais possible d'accéder aux informations qui étaient inaccessibles auparavant, ce qui a permis à l'espionnage économique de prendre de l'ampleur et de s'attaquer à un plus grand nombre d'entreprises. Le « cyber-espionnage industriel » est le fait d'avoir accès au système informatique d'un tiers dans le but d'obtenir les informations sensibles et avoir un avantage sur le marché. Deux techniques sont en principe utilisées : le *social engineering*, qui est une forme d'acquisition frauduleuse des informations utilisée en matière informatique ; et des moyens techniques, comme les chevaux de Troie, des logiciels malveillants qui installent un « parasite » dans l'ordinateur de la personne visée. C'est ce parasite qui va faire les opérations au bénéfice d'une autre personne[43]. Aujourd'hui, les attaques électroniques sont ciblées et complexes. Ce sont les États principalement qui sont derrière ces attaques, mais également les entreprises privées.

Il existe des entreprises spécialisées qui révèlent ces agissements déloyaux au public[44]. Parmi ce genre d'entreprises, il y a Kaspersky Lab, une société privée russe spécialisée dans la sécurité des systèmes d'informations. En 2014, elle a révélé des informations sur les agissements de Careto, un auteur malveillant d'origine espagnole, connu aussi sous le nom de « The Mask ». Leurs attaques étaient très professionnelles et sophistiquées et visait principalement les ambassades. La Suisse a également été touchée[45].

---

[42] J. MÜLLER, *La cybercriminalité au sens étroit. Analyse approfondie du droit suisse et aperçu de quelques droits étranger*, Genève, 2012, pp. 12 ss.

[43] J. MÜLLER, *op. cit.,* pp. 170 ss.

[44] « La sécurité de la Suisse 2015 », <http://www.news.admin.ch/NSBSubscriber/message/attachments/39237.pdf> (17 mars 2016).

[45] « *Unveiling « Careto » - the masked APT (by Kaspersky Lab) »*, <http://kasperskycontenthub.com/wpcontent/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf> (17 mars 2016).

En 2015, Kaspersky Lab à rendu publique les informations sur un groupe des pirates nommé Equation Group. Il s'agit d'un groupe de cyber-espionnage de haut niveau, soupçonné d'être relié à la NSA, l'Agence nationale de la sécurité américaine. Kaspersky Lab a fait preuve d'à peu près 500 infections de logiciels par les outils du groupe dans plus de 40 pays[46].

En 2014, une entreprise américaine Symantec Corp.[47] a révélé les agissements de Regin, un outil d'espionnage très avancé utilisé dans les opérations contre les gouvernements, le monde des affaires et les privés, en tout cas depuis 2008. Il s'agissait d'une vraie surveillance de masse. Il n'y a eu aucune victime connue en Suisse pour le moment[48].

En Suisse, c'est la MELANI, la Centrale chargée par le Conseil fédéral depuis 2004 de prévenir et de résoudre les problèmes qui apparaissent dans l'infrastructure de l'information et de la communication, qui est appelée à assurer la protection des particuliers et des entreprises d'une part, et aux infrastructures nationales d'autre part[49]. La Centrale a affirmé que de nombreux renseignements précieux sont volés grâce aux systèmes qui ne sont pas détectables à l'aide des anti-virus, comme les chevaux de Troie à usage unique. Elle a laissé entendre qu'un grand nombre d'attaques provenaient d'organisations étatiques. Selon elle, cette forme d'espionnage va prendre encore plus d'ampleur avec les années.

Pour résumer, nous pouvons dire que les auteurs des attaques sont de différents types. Il peut s'agir de privés qui cherchent des informations confidentielles pour les revendre par la suite, d'entreprises qui veulent avoir accès aux secrets des concurrents et finalement, d'États qui désirent obtenir des informations militaires ou économiques[50].

---

[46] « *Equation group : questions ans answers* », <https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf> (17 mars 2016).

[47] Société américaine active dans les logiciels informatiques.

[48] « *Regin : top-tier espionage tool enables stealthy surveillance* », <http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance> (17 mars 2016).

[49] J. MÜLLER, *La cybercriminalité au sens étroit. Analyse approfondie du droit suisse et aperçu de quelques droits étranger*, Genève, 2012, p. 7.

[50] J. MÜLLER, *op. cit.*, pp. 170 ss.

À titre d'exemple, nous pouvons citer un cas de vol important de données qui s'est produit en 2009 à l'encontre de Twitter, un site de micro-blogging. Les informations confidentielles dont les perspectives financières, les procès-verbaux des réunions etc. ont été dérobées par une personne prénommée Hacker Croll, qui était le pseudonyme de François Cousteix. Il s'est introduit dans la boîte à lettres électronique d'un employé après avoir simplement répondu à une question banale de récupération de mot de passe, soit une information qu'il a pu trouver grâce aux réseaux sociaux. Il a pu se connecter de la même façon à la boîte aux lettres de la femme du directeur de Twitter. L'auteur n'a donc pas eu recours à des moyens sophistiqués. Il a pu ainsi s'introduire dans les comptes de plusieurs personnes connues, dont Barack Obama. Toutefois selon lui, il n'a pas fait ça dans le but d'un gain personnel et s'est même décrit comme un « gentil pirate ». D'après ses paroles, il a simplement voulu sensibiliser les utilisateurs des réseaux sociaux aux grands risques d'intrusion dans leur vie privée[51].

3. Domaines du droit international pouvant être touchés par l'espionnage économique : souveraineté territoriale, responsabilité internationale et droit diplomatique

La responsabilité étatique est engagée en cas d'espionnage pour le compte de l'État[52]. Les agissements des personnes ayant qualité d'organes étatiques sont imputables à l'État en question. À l'inverse, un pays ne peut pas être recherché pour les comportements des individus n'agissant pas en tant qu'organe[53]. La personne en question va dans ce cas engager sa responsabilité individuelle et l'État d'origine est obligé de la punir. La responsabilité individuelle n'est donc en principe pas engagée pour les agissements des organes étatiques. Il y a quand même une exception à cette règle, il s'agit de l'espionnage et de la trahison de guerre[54].

---

[51] « Le pirate de Twitter, Hacker Croll, condamné à 5 mois de prison avec sursis », <http://www.zdnet.fr/actualites/le-pirate-de-twitter-hacker-croll-condamne-a-5-mois-de-prison-avec-sursis-39752706.htm>(23 mars 2016).

[52] H. WEBER, *Grundkurs Völkerrecht, Das internationale Recht des Friedens und der Friedenssicherung*, Frankfurt am Main, 1977, pp. 122ss.

[53] P. DAILLIER, M. FORTEAU, A. PELLET, *Droit international public*, 8e éd., Paris, 2009, pp. 557ss.

[54] J. WEILER, A.T. NISSEL, *International law*, Volume 5, New York, 2011, pp. 350ss.

En cas d'atteinte aux services publics à l'étranger, un État peut toujours prendre des mesures nécessaires, mais doit tout de même respecter les conséquences des immunités et privilèges accordés. Par service public à l'étranger, on entend notamment les services diplomatiques. Leur défense est justifiée par la nécessité de protéger son organisation propre. En d'autres termes, ça signifie que la compétence exclusive pour le règlement des litiges revient en principe à l'État d'envoi[55].

Malgré ça, la plupart d'États prévoient dans leur législation la possibilité de poursuivre et de juger les ressortissants d'autres pays s'ils ont porté atteinte à leur sûreté nationale ou à leur crédit financier, par ex. dans le cas d'espionnage. Il est préférable de conclure les accords interétatiques qui visent les cas d'extradition pour un tel comportement. La personne sera extradée s'il est établi de façon certaine qu'elle sera jugée dans son État d'envoi[56].

Les espions n'ont pas de position particulière à l'égard du droit international car ils ne sont en principe pas considérés comme des agents étatiques officiels qui seraient envoyés pour le besoin de l'établissement des relations internationales. L'espion engage sa responsabilité individuelle et ne peut pas se voir « excusé » s'il soutient qu'il remplissait simplement les ordres de son État d'origine[57].

Si l'espionnage est si répandu qu'il constitue même une facette cachée des relations internationales et que en plus de cela, il est licite au niveau international, alors quand est-ce que la responsabilité étatique peut être engagée ? Il existe un seul cas où cela est possible, c'est le cas qui implique la violation de la souveraineté territoriale d'un autre État. Dans tous les autres actes, l'espionnage sera simplement considéré comme un « acte inamical ». Dans ce cas, il est impossible de l'imputer à l'État[58].

[55] J. VERHOEVEN, *Droit international public*, Bruxelles, 2000, pp. 623ss.

[56] P. DAILLIER, M. FORTEAU, A. PELLET, *Droit international public*, 8e éd., Paris, 2009, pp. 557ss.

[57] L. OPPENHEIM, *International law*, Volume I, Londres, 1955, p. 862.

[58] F. LAFOUASSE, L'espionnage en droit international, in *Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

4. L'intelligence économique licite par opposition à l'espionnage économique illicite

Comment définir l'intelligence économique ? DANET propose sa propre approche, qui se base sur trois dimensions : ontologique (qui concerne sa nature), téléologique (qui concerne ses buts) et méthodologique (qui concerne sa mise en œuvre). Il définit cette notion comme suit : « *un ensemble de pratiques managériales, issues de champs disciplinaires variés, et qui ont pour ambition de permettre aux dirigeants d'entreprise de mieux appréhender un environnement complexe dans lequel s'exerce une concurrence forte, mouvante et multidimensionnelle*[59].» Il s'agit d'un anglicisme qui peut aussi être défini de la manière suivante : « *l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques.*[60] »

Il est important de distinguer l'intelligence économique de l'espionnage économique, car l'intelligence économique se fait ouvertement et est en soi légale. C'est précisément cette confusion entre les deux qui fait que la notion d'intelligence économique suscite encore certaines résistances[61]. Elle peut être rapprochée tantôt à la stratégie, tantôt au marketing[62]. L'intelligence économique est également un marché, qui comme tous les autres, obéit à la loi de l'offre et de la demande. La demande vient très souvent des entreprises qui veulent s'assurer par ex. que leurs cocontractants sont solvables, avant de signer avec eux[63]. C'est donc, comme nous le constatons, un « marché de renseignement légal[64] ».

Il existe deux époques dans le développement de cette notion : la première concerne l'approche « centralisée » ou traditionnelle et la deuxième, l'approche « décentralisée ».

---

[59] D. DANET, L'intelligence économique : de l'État à l'entreprise , *in Les Cahiers du numérique*, Volume 3, Paris, 2002, pp. 139-170.

[60] A. PAECHT, rapport n° 1951 du 23 novembre 1999 tendant à la création d'une délégation parlementaire pour les affaires de renseignement, AN, p. 13.

[61] R. PAUTRAT, L'intelligence économique : un enjeu de premier eimportance toujours sous-estimé, *in Hérodote*, Paris, 2022, pp. 151-156.

[62] S. COISSARD, L. DELHALLE, S. CARLOS, Guerre économique et sécurité internationale. Une approche comparative des systèmes institutionnels d'intelligence économique, *in Revue internationale d'intelligence économique*, Volume II, Paris, 2010, pp. 233-250.

[63] B. BESSON et J-C POSSIN, *Du renseignement à l'intelligence économique. Cybercriminalité, contrefaçon, veilles stratégiques : détecter les menaces et le sopportunités pour l'entreprise*, 2e éd., Paris, 2001, pp. 167ss.

[64] B. BESSON et J-C POSSIN, *op. cit.*, p. 173.

Avant les années 1980, le fondement de l'intelligence économique était le ministère de l'Economie[65]. Contrairement à l'espionnage industriel prodigué par l'État, cette approche ne fournit pas de renseignements aux privés dans le but d'augmenter leur compétitivité sur le marché. Ici, le but final est plutôt politique ou militaire. Ce type d'intelligence a toujours son importance aujourd'hui[66]. Mais après 1980, cette vision s'est décentralisée et les auteurs-clés sont désormais de plus en plus souvent les privés[67]. C'est ce que nous pouvons appeler la « *business intelligence* » qui englobe l'espionnage des données pour les besoins commerciaux[68].

Pour comprendre la phase « centralisée » de cette notion, il s'agit de se référer au célèbre « rapport Martre[69] », du nom de l'ancien PDG d'Aérospatiale[70] qui s'est occupé de la question de la guerre économique[71]. Ce rapport est le résultat du travail collectif réalisé par le Commissariat général du Plan[72]. Le contexte est la fin de la Guerre froide avec la mondialisation des échanges et les progrès technologiques, ce qui amène au déplacement du vecteur de puissance du domaine militaire au domaine économique. La stratégie des entreprises change, elles doivent s'adapter à ce nouveau environnement. Le constat est que les acteurs économiques français n'ont pas su faire face aux nouvelles réalités et que la France est largement en retard par rapport aux pays tels que le Japon, la Suède ou les États-Unis[73].

L'intelligence économique doit être menée « en réseau » et non pas individuellement. Ce réseau est composé de professionnels qui recueillent des informations qui leur permettent de

---

[65] D. DANET, L'intelligence économique : de l'État à l'entreprise , *in Les Cahiers du numérique*, Volume 3, Paris, 2002, pp. 139-170.

[66] M. BURTON, *Government spying for commercial gain*, *in Studies in intelligence,* 1994, pp. 17-23.

[67] D. DANET, *op. cit.*

[68] M. BURTON, *op. cit.*

[69] Rapport « Intelligence économique et stratégie des entreprises », publiée en France en 1994, qui cherche à comprendre les facteurs de compétitivité sur le marché.

[70] Entreprise aéronautique française.

[71] « Intelligence économique et stratégie des entreprises. Rapport Marte », <http://bdc.aege.fr/public/Intelligence_Economique_et_strategie_des_entreprises_1994.pdf > (22 mars 2016).

[72] Institution française qui a existé entre 1946 et 2006 et qui était chargée de définir la planification économique du pays.

[73] Intelligence économique et stratégie des entreprises. Rapport Martre, *op. cit.* et A. LAÏDI et D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 15ss.

prendre les décisions pertinentes et stratégiques. Elle n'est rien sans les informations, qui ont été récoltées, traitées et analysées[74]. Il s'agit d'une approche préventive car les coûts de recherche et de développement sont de plus en plus importants et il n'est plus possible de se laisser surprendre par les concurrents[75].

De nos jours, la plupart des entreprises se dotent des services chargés de recueillir et d'analyser les renseignements et de s'occuper de l'intelligence économique. Ce n'est donc plus le cas des multinationales seulement. Il existe de plus en plus de cabinets privés qui peuvent aussi procurer ce genre de services. 95% d'informations peuvent être trouvées légalement. Par contre les autres 5% sont laissées au domaine de l'espionnage[76].

5. L'espion

5.1 Agent sous couverture officielle

Les agents sous couverture officielle, ou agents légaux, à l'étranger font partie de deux institutions : missions diplomatiques ou consulaires et organisations internationales. Il y a eu de très nombreuses affaires concernant les actes d'espionnage commis notamment par des agents diplomatiques. Les Convention de Vienne sur les relations diplomatiques et Convention de Vienne sur les relations consulaires prévoient les sanctions dans ce cas.

Il existe une expression selon laquelle « l'ambassadeur est un espion honorable ». Mais selon LAFOUASSE, elle n'a plus lieu d'être car il y a une distinction claire entre les gens qui font carrière de la diplomatie et les gens qui utilisent ce statut dans le seul but de collecter des informations clandestinement[77].

Par mission diplomatique permanente, il s'agit d'entendre un service public de l'État d'envoi de l'agent installé sur le terrain de l'État d'accueil. Les membres bénéficient de privilèges qui

[74] C. MARCON et N. MOINET, *L'intelligence économique*, 2e éd., Paris, 2011, pp. 30ss.

[75] D. ROUACH, *La veille technologique et l'intelligence économique*, 5e éd., Paris, 2010, pp. 10ss.

[76] A. LAÏDI, D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 234ss.

[77] F. LAFOUASSE, L'espionnage en droit international, in *Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136 et É. DAVID, *Éléments de droit pénal international et européen*, Bruxelles, 2009, pp. 65ss.

sont censés les aider à accomplir leurs tâches. Une des tâches de l'agent diplomatique consiste dans le fait de recueillir les informations nécessaires pour son État d'origine, pour qu'il puisse prendre les décisions d'ordre économique, politique et militaire. Dans ce cas, il s'agit d'un « espion déclaré » (« *overt spy* »)[78]. Un diplomate a une mission, qui est la collecte des informations, tout comme un espion en réalité. Sauf que les moyens pour parvenir à cette fin sont différents[79]. Mais il est obligatoire que l'agent diplomatique respecte la loi de l'État qui l'accueille[80], ce qui n'est pas toujours le cas, notamment si la personne se livre à des actes d'espionnage. Dans ce cas sa fonction prend fin et elle est déclarée *persona non grata*. L'un des deux États peut alors demander son rappel. Le rappel, qui est la sanction de son manquement aux devoirs, évite d'engager la responsabilité internationale de l'État, alors même que les actes de son agent lui sont imputables car l'acte de l'agent est en quelque sorte « *détaché* » de l'État dans ce cas, ce qui évite de compliquer les relations internationales[81].

Pendant la Guerre froide, le rappel des agents était une pratique très fréquente. Parmi les affaires internationales célèbres, nous pouvons citer le cas de renvoi par le gouvernement britannique de plus d'une centaine d'agents de l'URSS en 1971. Il justifiait le renvoi par l'activité d'espionnage des soviétiques, ce qui a été révélé par un ancien agent du KGB. Un cas pareil s'est produit en 1978 entre le Canada et Cuba. Les agents cubains ont été expulsés du territoire canadien et Cuba a alors publié un article en disant que leur comportement ne pouvait pas constituer un acte d'espionnage car ils n'ont fait qu'établir des relations avec des tierces personnes sur les questions qui ne pouvaient pas représenter une menace pour l'État d'accueil ou un tiers État[82]. A la fin de la Guerre froide, il y a eu moins d'agents diplomatiques déclarés des *persona non grata* pour des activités incompatibles avec leur

[78] F. LAFOUASSE, L'espionnage en droit international, in *Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136 et G. KOHEN-JONATHAN, R. KOVAR, L'espionnage en temps de paix, *in Annuaire français de droit international*, Volume 6, Paris, 1960, pp. 239-255.

[79] F. LAFOUASSE, *L'espionnage dans le droit international*, Paris, 2012, pp. 315ss.

[80] G.O.W. MUELLER et E.M WISE, *International criminal law*, Volume II, Londres, 1965, pp. 100ss. et L. DEMBINSKI, *The modern law of diplomacy, External missions of states and international organizations*, Dordrecht, 1988, pp. 159ss.

[81] G. KOHEN-JONATHAN et R. KOVAR, L'espionnage en temps de paix, *in Annuaire français de droit international*, Volume 6, Paris, 1960, pp. 239-255.

[82] L. DEMBINSKI, *The modern law of diplomacy, External missions of states and international organizations*, Dordrecht, 1988, pp. 159ss.

statut, ce qui en réalité est souvent un euphémisme pour l'espionnage[83]. Toutefois il serait judicieux de mentionner qu'il n'est pas toujours aisé de définir la fonction diplomatique concernant les affaires économiques. Il en résulte une zone grise entre ce qui relève des investigations économiques légales et de l'espionnage économique illégal[84].

5.2 Agent sans couverture officielle

S'agissant des agents clandestins, donc ne faisant pas partie d'une mission diplomatique officielle par ex., deux cas de figure sont possibles concernant la responsabilité de son État d'origine. La première possibilité est que l'État en question le reconnaît en tant que son agent et engage alors sa propre responsabilité car il y a un lien qui unit l'individu et le pays d'origine dans ce cas. Ou alors ce lien n'est pas établi entre les deux, et l'État en question n'intervient pas en sa faveur[85].

5.3 Particulier

S'il s'agit des faits accomplis par des particuliers qui n'agissent pas au nom de l'État et n'accomplissement pas ses injonctions, l'État ne peut pas en être tenu responsable. L'exception à ce principe peut consister dans la situation où l'État ne prend pas des mesures de précaution pour protéger les victimes d'une potentielle attaque. Dans ce cas, la responsabilité est engagée en raison du fait des organes étatiques. C'est alors une situation de la coexistence de deux types de responsabilités : celle de l'individu et celle de l'État[86].

Par contre du moment où un lien entre le particulier et l'État en question est établi, ses actes pourraient être attribués à cet État. Le problème est que la preuve d'un tel lien est difficile à apporter. Et politiquement parlant, ce n'est pas souhaitable en réalité. Mais même si l'acte est imputé à l'État, encore faut-il que cet acte viole une norme internationale, et comme nous

---

[83] E. DENZA, *Diplomatic law, Commentary on the Vienna Convention on diplomatic relations*, 3e éd., New York, 2008, pp. 78ss. et S. HOBE, *Einführung in das Völkerrecht*, 9e éd., Stuttgart 2008, pp. 379ss.

[84] L.T. LEE, *Consular law and practice*, 2e éd., Oxford, 1991, pp. 191ss.

[85] F. LAFOUASSE, L'espionnage en droit international, in *Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

[86] P. DAILLIER, M. FORTEAU, A. PELLET, *Droit international public*, 8e éd., Paris, 2009, pp. 869ss.

avons vu, il n'y a pas de norme internationale qui punit l'acte d'espionnage. Il s'agit de regarder la pratique coutumière, qui montre qu'en principe les États punissent l'agent selon leur droit pénal national, sans entreprendre de démarches diplomatiques contre l'État étranger. En réalité la réponse de l'État à un acte d'espionnage à son encontre va beaucoup dépendre « *des rapports de force, de la tension internationale, ou peut-être encore du danger encouru*. »[87]

En cas de détention d'un ressortissant étatique à l'étranger, l'État de sa nationalité peut, par contre, intervenir en sa faveur. La personne détenue a notamment le droit de s'entretenir avec un agent diplomatique ou consulaire[88].

5.4 Agent d'une organisation internationale

Il s'agit également d'un individu agissant sous couverture officielle, celle de l'agent d'une OI. Ces agents se voient accorder aussi certains privilèges et immunités à cause de leur travail qui nécessite une indépendance pour atteindre les objectifs, même si en réalité ces privilèges sont un peu moins importants que ceux des diplomates. Le débat qui existe oppose de nouveau deux intérêts : l'intérêt de l'État d'accueil à sa propre sécurité et l'intérêt de l'agent à accomplir son travail en toute indépendance[89].

Il est évidemment préférable que l'État utilise les moyens préventifs plutôt que répressifs. il est important de noter qu'il ne peut pas déclarer l'agent une *persona non grata*, contrairement à ce qui se passe avec un diplomate, car pour pouvoir le faire, les deux entités concernées, l'État en question et l'OI, doivent être « *de même nature* », soit qu'elles doivent les deux avoir la souveraineté internationale, ce qui n'est pas le cas pour les OI. En cas d'activité d'espionnage, la réaction peut être double : celle de l'OI elle-même et celle de l'État où elle siège. Quant à l'OI, si l'acte est dirigé à son encontre, elle peut licencier la personne en question pour faute grave. Si l'acte est dirigé contre le pays d'accueil, elle peut lever l'immunité de l'agent. Si la personne a agi à l'encontre de l'État, ce dernier peut soit la

[87] G. KOHEN-JONATHAN et R. KOVAR, L'espionnage en temps de paix, *in Annuaire français de droit international*, Volume 6, Paris, 1960, pp. 239-255.

[88] B. SEN, *A diplomat's handbook of international law and practice*, 3e éd., Dordrecht, 1988, pp. 370ss.

[89] F. LAFOUASSE, L'espionnage en droit international, in *Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

délivrer à ses propres tribunaux, soit l'expulser, soit les deux. En cas de demande de rappel, l'État qui accueille l'agent étranger, appelé l'État hôte, doit motiver cette demande[90].

6. Moyens juridiques de protection

6.1 Comment se protéger contre l'espionnage ?

Quelles mesures prendre pour lutter contre l'espionnage économique en tant qu'entreprise ? Le patron de Sega industrie[91], Philippe Cador s'est prononcé sur le sujet en parlant avec le journal Ouest France. Il a évoqué les précautions basiques à prendre, comme bien vérifier l'adresse d'envoi des mails, ne pas stocker les données confidentielles sur ordinateur, mais sur une clé USB, ne pas parler de sujets sensibles en public etc. [92].

Que faire pour lutter contre le cyber-espionnage ? Il s'agit surtout des améliorations au niveau technique, comme l'utilisation des anti-virus ou d'un pare-feu. Une autre solution serait d'avoir un réseau interne à une seule entreprise qui ne serait pas en contact avec l'extérieur. Le problème, c'est que ce genre de réseau peut coûter très cher[93].

Nous pouvons également nous référer au livre *The spy's guide : Office espionnage* de MELTON, qui est l'un des meilleurs spécialistes du monde de la technologie d'espionnage, membre du Conseil d'administration du Musée international d'espionnage à Washington et consultant des services de renseignements américains[94]. Dans son livre, il donne des conseils sur comment faire face au problème de l'espionnage de tous les jours. Oleg Kalouguine, ancien général-major du KGB, les services secrets russes, en écrivant un commentaire dans la préface du livre, a dit être étonné de l'existence même de ce livre qui contient des secrets, révélés au grand public, que le KGB cherchait à se procurer durant la période de la Guerre

[90] F. LAFOUASSE, *L'espionnage dans le droit international*, Paris, 2012, pp. 419ss.

[91] Société française spécialisée dans l'ingénierie et études techniques.

[92] « Les entreprises doivent se méfier des espions », <http://www.ouest-france.fr/les-entreprises-doivent-se-mefier-des-espions-2159>(23 mars 2016).

[93] J. MÜLLER, *La cybercriminalité au sens étroit. Analyse approfondie du droit suisse et aperçu de quelques droits étranger*, Genève, 2012, pp. 170 ss.

[94] H.K. MELTON, *The spy's guide : Office espionnage*, Philadélphie, 2003, pp. 11ss.

froide. Il a également souligné la façon méthodique et professionnelle utilisée par l'auteur dans sa narration[95].

L'auteur évoque notamment les méthodes pour enregistrer clandestinement la conversation durant laquelle vous êtes présent ou non, comment supprimer les dispositifs d'enregistrement dans une salle de conférence, comment avoir accès aux informations confidentielles d'une entreprise concurrente, comment obtenir les renseignements de la part des concurrents eux-mêmes, et de nombreux autres conseils[96].

6.2 Compétence personnelle et compétence réelle de l'État

Sous quel angle un État peut-il réprimer les actes d'espionnage ? Selon la compétence territoriale, il possède sur son propre territoire la souveraineté et la juridiction absolues. Mais il peut également agir sous l'angle de la compétence réelle, qui permet de poursuivre certaines infractions qui représentent un danger pour la sécurité intérieure et extérieure du pays, peu importe le lieu de commission, la nationalité de l'auteur ou de la victime. Et enfin l'État peut également fonder sa compétence en se basant sur l'atteinte portée aux services publics à l'étranger, qui en réalité peut être traitée comme une sous-catégorie de la compétence réelle. Il s'agit des services diplomatiques et consulaires ainsi que des forces armées présentes sur le territoire d'un État étranger[97].

6.3 Modes de règlement de conflits entre États en cas d'espionnage

Les États sont libres quant à la façon de régler les cas d'espionnage. Si c'est le fait d'un particulier, le droit international ne s'intéresse pas vraiment à cette possibilité car l'acte n'est pas commis par un organe étatique. Il est possible de songer à la protection diplomatique de la part de l'État dont la personne est ressortissante, mais si elle est reconnue coupable, la protection ne pourra pas avoir lieu. La définition de l'espionnage est aussi délicate pour les

[95] H.K. MELTON, *The spy's guide : Office espionnage*, Philadélphie, 2003, pp. 11ss.

[96] H.K. MELTON, *op. cit.,* pp. 39-43, 71-72, 84-85, 97-99, 100-103.

[97] F. LAFOUASSE, L'espionnage en droit international, *in Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136 et et V.G. VITZTHUM et A. PROELSS, *Völkerrecht*, 6e éd., Berlin, 2013, pp. 185ss.

tribunaux car il s'agit de démontrer que les agissements de l'individu nuisent aux intérêts étatiques. Concernant les agents diplomatiques, comme nous l'avons vu, la marche à suivre consiste en sa déclaration de *persona non grata* suivie par son rappel. Les États peuvent également procéder à l'échange des espions entre eux[98].

Au final c'est à l'État lui-même de voir « *le seuil à partir duquel une activité lui procure plus d'inconvénients que d'avantages et de rechercher alors l'accord d'un ou de plusieurs autres États en vue d'obtenir, par la voie conventionnelle, une interdiction totale ou partielle de ladite activité*[99]. » Stone a dit concernant la pratique des gouvernements : « *the psychological point, as I see it, is that the espionage situation is (...) like some situations that occasionally arise between friends and even, I understand, between husband and wife, when one of them does the sort of thing about which it isn't really any use for them to talk*[100]. »

6.4 Répression par le droit national – exemple de plusieurs pays

En principe les affaires d'espionnage ne mènent pas à un conflit interétatique, mais se règlent à l'aide du droit pénal interne du pays concerné[101].

6.4.1 La Suisse

Le service de renseignement de la Confédération suisse[102] utilise le « Radar de situation[103] » pour évaluer les dangers importants pour la Suisse chaque année. En 2015, parmi les thèmes

[98] F. LAFOUASSE, L'espionnage en droit international, *in Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136 et J. MÜLLER, *La cybercriminalité au sens étroit. Analyse approfondie du droit suisse et aperçu de quelques droits étranger*, Genève, 2012, pp. 170 ss.

[99] F. LAFOUASSE, *op. cit.*

[100] J. STONE, *Legal problèmes of espionage in conditions of modern conflict*, *in Essays on espionage and international law*, Ohio 1962, p. 39.

[101] G. KOHEN-JONATHAN et R. KOVAR, L'espionnage en temps de paix, *in Annuaire français de droit international*, Volume 6, Paris, 1960, pp. 239-255.

[102] Instrument de la politique de sécurité qui combat notamment l'espionnage, le terrorisme etc. Le service est contrôlé par le Département fédéral de la défense, de la protection de la population et des sports.

[103] Instrument qui illustre les menaces importantes pour la Suisse.

classés sous la rubrique « *Thèmes principaux* », nous retrouvons l'espionnage économique qui est placé plus ou moins au même niveau que l'espionnage contre les intérêts sécuritaires de la Suisse[104]. La dernière grande affaire qui a fait prendre conscience des risques liés à l'espionnage en Suisse a été l'affaire Snowden, que nous allons voir dans le point 7.6[105]. La situation s'est plus ou moins stabilisée depuis, mais le sujet reste toujours d'actualité à cause de ses enjeux politico-sécuritaires et économiques, et à cause d'éventuels dégâts aux OI et aux entreprises internationales établies en Suisse.

Selon le rapport publiéen 2015[106], l'espionnage économique fait partie, avec l'espionnage contre les intérêts sécuritaires de la Suisse et la surveillance de ressortissants étrangers en Suisse, de service de renseignement prohibé. Il s'agit d'abord d'une activité cachée qui « *n'est pas perçue par le public* ». Le but principal de l'espionnage économique est de récolter les informations qui seront utilisées à de différentes fins. Ces renseignements peuvent notamment trouver leur application dans le jeu contre les concurrents afin de les influencer d'une certaine façon, voire de les nuire en s'emparant des données sensibles[107].

Quels moyens de protection existent-ils dans ce cas pour la Suisse ? Il y a tout d'abord le droit pénal. Nous allons voir quelques infractions typiques pour cette matière. Mais il est nécessaire de rappeler que la procédure pénale se révèle être très longue et complexe en pratique. L'accent est de plus en plus mis sur les mesures de prévention qui doivent être utilisées notamment par les entreprises qui dépendent fortement des moyens informatiques aujourd'hui.

Le Code pénal suisse[108] réprime certains comportements relevant de la notion d'espionnage. Le premier article à citer est l'art. 272 CP intitulé « *Espionnage. Service de renseignements politiques* ». La disposition ne parle pas d'un secret, mais seulement de renseignements qui ne seraient pas accessibles pour un État étranger. L'activité des espions est de regrouper et

[104] « La sécurité de la Suisse, 2015 », <http://www.news.admin.ch/NSBSubscriber/message/attachments/39237.pdf> (17 mars 2016).

[105] Voir p. 37 du travail.

[106] « La sécurité de la Suisse 2015 », *op. cit.*

[107] « La sécurité de la Suisse, 2015 », <http://www.news.admin.ch/NSBSubscriber/message/attachments/39237.pdf> (17 mars 2016).

[108] RS 311.0.

d'analyser les données confidentielles de différentes façons, par ex. en lisant la presse, en assistant aux manifestations publiques, etc. Il doit y avoir un intérêt politique à avoir ces informations pour l'État étranger concerné. Ces renseignements doivent être transmis au préjudice de la Suisse, de ses ressortissants ou de ses organismes[109].

L'article suivant est l'art. 273 CP intitulé *« Espionnage. Service de renseignements économiques »*. Nous vivons dans une époque où les grandes entreprises sont souvent multinationales et la concurrence devient mondiale. Il est par conséquent plus compliqué de délimiter ce que sont les secrets économiques que l'État en question veut protéger. Dans cette disposition, il ne s'agit pas d'un simple renseignement, mais d'un secret de fabrication (qui est en lien avec l'élaboration du produit) ou d'un secret commercial (qui a trait au coût de production, calcul des prix etc.). Ce sont, selon le TF, « *tous les faits de la vie économique qu'un intérêt légitime commande de ne pas divulguer*[110] », ou « *toute connaissance particulière qui n'est pas de notoriété publique, qui n'est pas facilement accessible, dont un fabricant ou un commerçant a un intérêt légitime à protéger l'exclusivité et qu'en fait il n'entend pas divulguer*[111]. » Dans le contexte de cette disposition, cette donnée doit révéler un intérêt économique. L'auteur de l'infraction doit agir en faveur d'une entreprise privée étrangère ou d'un organisme privé ou officiel étranger[112]. Il n'est pas nécessaire que l'infraction soit consommée. Le simple fait de rechercher ces informations, sans forcément les trouver, tombe déjà sous le coup de l'article. Il est important de noter que cet article est soumis au principe de la protection de l'État et non pas au principe de la territorialité. Cela signifie que l'auteur sera toujours soumis au droit suisse, du moment où la victime se trouve en Suisse[113].

Dans le même ordre d'idée, nous pouvons citer les art. 179ss CP qui englobent les infractions contre le domaine secret ou le domaine privé. Nous pouvons également penser aux dispositions qui seraient applicables dans les cas d'affaires liées aux secrets économiques, comme la gestion déloyale (art. 159 CP) ou abus de confiance (art. 140 al. 1 CP).

---

[109] B. CORBOZ, *Les infractions en droit suisse*, Volume II, 3e éd., Berne 2010, pp. 440ss.

[110] ATF 65 I 330 (333) = JT 1940 I 406.

[111] ATF 103 IV 283 (284).

[112] B. CORBOZ, *Les infractions en droit suisse*, Volume II, 3e éd., Berne 2010, pp. 446ss.

[113] « La sécurité de la Suisse 2015 », <http://www.news.admin.ch/NSBSubscriber/message/attachments/39237.pdf> (17 mars 2016).

Il s'agit de mentionner également l'art. 162 CP intitulé « *Violation de secret de fabrication ou de secret commercial* ». L'auteur du délit doit être astreint au secret selon la loi ou le contrat et le révèle, cela veut dire qu'il le rapporte à une personne qui ne devait pas en avoir connaissance[114].

Du point de vue du droit pénal suisse, dans le cas de l'accès au système informatique d'une autre personne, il s'agit de l'art. 143bis al. 1 CP intitulé « *L'accès indu à un système informatique* »[115] qui protège un système qui dépend d'un ordinateur et qui n'appartient pas à l'auteur de l'attaque. L'auteur n'a pas le droit d'entrer dans ce système et y entre indûment. Une fois que la personne a accès au système, elle peut librement consulter toutes les données dont elle a besoin, ce qui tombe sous la soustraction de données réprimée à l'art. 143 al. 1 CP intitulé « *La soustraction de données* ». Il doit s'agir d'une donnée informatique, qui serait « *toute information qui peut faire l'objet d'une communication humaine*[116]. » Elle doit être conservée dans un ordinateur et ne doit pas être accessible à tous [117]. Nous estimons que la condition de l'enrichissement illégitime est aussi remplie du moment où l'auteur veut s'emparer des données personnelles car il attend d'en retirer un avantage personnel[118].

Il est important également de tenir compte de la législation sur les étrangers, qui concerne les cas où par ex. un espion se verra refuser une accrédiation diplomatique, voire même se verra prononcer une interdiction d'entrée, ou des cas où des diplomates seront désignés des *persona non grata*. Mais il s'agit de garder en tête le principe de la proportionnalité dans ces cas et faire une pesée d'intérêts en présence en tenant en compte des intérêts politiques de la Suisse, pour qui il est aussi promordial d'établir et de sauvegarder les relations avec l'étranger.

La Suisse a une position particulière grâce à son statut d'hôte d'OI et d'organes internationaux, et grâce à son rôle important dans le monde des finances. C'est pourquoi elle va continuer à être visée par les agissements des espions sur la scène internationale. Comme

---

[114] O. WENIGER, *La protection des secrets économiques et du savoir-faire (know-how). Étude comparative des droits allemand, français et suisse*, Renens, 1994, pp. 255ss.

[115] B. CORBOZ, *Les infractions en droit suisse*, Volume I, 3e éd., Berne 2010, pp. 289ss.

[116] B. CORBOZ, *Les infractions en droit suisse*, *op. cit*., . 281ss.

[117] B. CORBOZ, *op. cit.*

[118] J. MÜLLER, *La cybercriminalité au sens étroit. Analyse approfondie du droit suisse et aperçu de quelques droits étranger*, Genève, 2012, pp. 170ss.

nous avons déjà mentionné, la prévention joue un rôle primordial. Les cibles potentielles, ainsi que le Service de renseignement de la Confédération doivent prendre les mesures nécessaires[119]. Une de ces mesures est le programme Prophylax[120], qui consiste en la sensibiliation par le SRC des entreprises et des instituts universitaires aux dangers que l'espionnage fait encourir. Le même type de programme, axé spécialement sur la recherche en Suisse, est le Technopole[121].

Quant à la protection contre l'espionnage par le droit de la concurrence déloyale, nous pouvons mentionner qu'il n'y a pas de norme sanctionnant l'espionnage dans la LCD. C'est dû au fait que le législateur suisse a estimé que cela représenterait un risque pour le besoin d'informations pour les commerçants. Le seul moyen serait de se rabattre sur la clause générale de l'art. 2 LCD pour punir certains comportements déloyaux de détournement d'informations. WENIGER précise que le droit pénal actuel offre des moyens d'agir contre l'espionnage et par conséquent il ne serait pas nécessaire de les rajouter expressément dans la LCD[122].

Il est nécessaire d'évoquer également la Loi sur le renseignement (LRens) qui n'est pas encore en vigueur et dont le projet a été adopté par le Conseil fédéral en 2014. C'est une loi sur laquelle se baserait le SRC dans ses actions. Elle suscite de nombreuses interrogations et critiques, depuis le dépôt de son projet. Les partisans de la loi disent qu'elle est censée augmenter la sécurité de la Suisse et de ses citoyens et protéger de nouvelles menaces auxquelles nous devons face, notamment contre l'espionnage. Selon les défenseurs du projet, la balance entre sécurité et liberté est respectée avec cette loi car chaque mesure prise nécessitera une procédure d'approbation préalable aux niveaux juridique et politique. Ils

---

[119] « La sécurité de la Suisse 2015 », <http://www.news.admin.ch/NSBSubscriber/message/attachments/39237.pdf> (17 mars 2016).

[120] « Prophylax »,

<http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/publication/snd_publ.parsys.59158.downloadList.0556.DownloadFile.tmp/ndbprophylaxbroschuerefweb20150717.pdf> (17 mars 2016).

[121] La sécurité de la Suisse, 2015, disponible sous « http://www.news.admin.ch/NSBSubscriber/message/attachments/39237.pdf » (17 mars 2016), pp. 63ss.

[122] O. WENIGER, *La protection des secrets économiques et du savoir-faire (know-how). Étude comparative des droits allemand, français et suisse*, Renens, 1994, pp. 217ss.

invoquent que la tâche du SRC est de déceler à l'avance les menaces contre la sécurité extérieure et intérieure du pays et de les écarter le plus vite possible, ce qui sera rendu possible grâce à cette mesure[123].

Mais nombreux sont les opposants. Selon eux, la loi ne va en rien améliorer la défense anti-terroriste ou anti-espionnage, mais va augmenter l'intrusion dans la vie privée des Helvètes et constituer ainsi une grave atteinte aux libertés fondamentales européennes. Actuellement la base légale pour le renseignement civil est la LMSI, mais il s'agit dans cette loi seulement du contrôle des sources qui sont librement accessibles. La nouvelle loi pousse ce contrôle encore plus loin avec des moyens informatiques performants. Elle va soumettre à la surveillance les communications entre résidants suisses même sans aucun soupçon qu'ils ont une quelconque activité illicite. Les délais de la conservation des données personnelles seront également prolongés[124]. C'est en réalité de la surveillance « préventive », et une telle surveillance devrait être possible seulement en cas de soupçons fondés, mais non pas en l'absence de tout soupçon. Selon l'art. 13 Cst.[125] et l'art. 8 CEDH[126], toute collecte des informations concernant la vie privée des individus par l'État porte atteinte à la vie privée. Pour porter atteinte à une liberté fondamentale, il est nécessaire de remplir les trois conditions : avoir une base légale, un intérêt public et remplir le principe de la proportionnalité. Les deux premières sont plus ou moins rassemblées dans cette loi. Mais c'est la proportionnalité par rapport au but visé qui poserait problème. Dans chaque cas, concret il faudrait vérifier qu'il n'existe pas une mesure moins intrusive par rapport au but recherché. Cela veut dire que le fait de stocker les données de manière préventive n'est en tout cas pas acceptable[127]. Il serait donc largement préférable que ces problèmes se règlent au niveau de la procédure pénale comme auparavant[128].

---

[123] « Loi sur le renseignement », <http://www.vbs.admin.ch/internet/vbs/fr/home/themen/ndb/faq.html> (7 avril 2016).

[124] « Référendum contre la loi sur le renseignement », <http://www.humanrights.ch/fr/droits-humains-suisse/interieure/protection/securite/suisse-loi-renseignement> (7 avril 2016).

[125] RS 101.

[126] RS 0.101.

[127] « Référendum contre la loi sur le renseignement », *op. cit.*

[128] « La nouvelle loi sur le renseignement (LRens) : le référendum malgré les attentats », <http://www.schwaab.ch/archives/2015/11/19/nouvelle-loi-sur-le-renseignement-lrens-referendum/> (7 avril 2016).

Normalement, au mois de juin 2016 le projet devra être voté, mais la résistance est telle qu'un référendum a immédiatement été lancé, sous le nom de « *Alliance contre l'État fouineur* ». Un site Internet a également été créé pour s'opposer à cette loi[129]. Plusieurs arguments sont invoqués à son encontre. Il s'agit, comme nous avons mentionné, de l'absence de principe de la proportionnalité tout d'abord. En plus, il convient de noter que tout le monde serait potentiellement surveillé, et non pas seulement la catégorie de gens « à risque ». Et pour finir, selon les opposants de la loi, le Ministère public de la Confédération et la police disposeraient déjà de moyens suffisants pour lutter contre le terrorisme et le crime organisé[130].

6.4.2 La France

En France, l'acte d'espionnage se trouve parmi les atteintes aux intérêts fondamentaux dans le Code pénal français. Il s'agit d'une infraction politique, ce qui implique l'impossibilité d'extradition de la personne inculpée d'espionnage. Le Code pénal fait une distinction entre la trahison, le fait d'un français, et l'espionnage, le fait d'un étranger. L'espionnage en droit pénal est conçu de façon très large[131]. Mais selon certains, les normes civiles et délictuelles qui existent actuellement ne sont pas suffisantes pour protéger l'entreprise en cas de divulgation de ses secrets à des tierces personnes.

Il est possible d'engager la responsabilité d'une personne dans un tel cas sur la base de la concurrence déloyale. C'est le cas où l'auteur s'empare de l'information confidentielle sans le consentement du titulaire. En plus, selon la jurisprudence, il s'agit également de réparer le tort moral causé à l'image de l'entreprise car le public peut être amené à penser qu'elle protège mal ses données personnelles. La sanction est principalement indemnitaire. Par contre dans d'autres pays, comme aux États-Unis, elle peut être également en nature, comme le fait d'interdire l'utilisation et la communication de l'information en question.

[129] Site Internet, disponible sous « http://etat-fouineur.ch/ » (7 avril 2016).

[130] « Référendum LRens », <https://www.lrens.ch/> (7 avril 2016).

[131] F. LAFOUASSE, L'espionnage en droit international, *in Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

Un projet de loi s'inspirant de l'*Economic Espionnage Act* américain, que nous verrons plus loin[132], a été déposé à l'Assemblée Nationale en 2009. Il concerne la protection des informations économiques et propose des moyens répressifs plus efficaces pour la répression de l'espionnage économique, comme sanctionner « *l'atteinte au secret d'une information à caractère économique protégée* » (art. 1). Les peines prévues sont plus sévères et l'objet est mieux défini[133]. Les informations économiques se voient attribuées la définition suivante : « *les informations ne constituant pas des connaissances générales librement accessibles par le public, ayant, directement ou indirectement, une valeur économique pour l'entreprise, et pour la protection desquelles leur détenteur légitime a mis en œuvre des mesures substantielles conformes aux lois et usages, en vue de les tenir secrètes*[134] ».

L'autre loi qu'il est important d'évoquer est la loi LOPPSI 2 qui fixe la limite de protection. Elle aborde également le sujet de la cybercriminalité, dont fait partie l'espionnage industriel et crée, à titre d'exemple, l'infraction d'utilisation frauduleuse des données personnelles[135].

Il est important de noter que l'espionnage industriel n'est pas puni comme tel. Sont punis par contre les moyens illégaux et déloyaux utilisés pour arriver à cette fin. Une des méthodes de prévention à laquelle nous pensons en premier est le fait de bien rédiger son contrat de travail, c'est-à-dire d'y insérer une clause de confidentialité et une clause de non-concurrence. Si de telles clauses n'existent pas, le collaborateur sera astreint de toute manière à un devoir de loyauté envers son employeur. Il faut faire attention au fait que les différends relevant de ce domaine sont tranchés devant les tribunaux des Prud'hommes en tant que violation du droit de travail, ce qui souvent n'est pas une démarche assez efficace dans un cas d'une telle envergure.

Quant aux actions défensives, nous pouvons en nommer deux. La première est l'action en responsabilité civile contre celui qui révèle des informations confidentielles d'une entreprise. Il existe également une action en responsabilité délictuelle. Ce sont les cas qui concernent la

[132] Voir point 6.4.3, p. 33 du travail.

[133] « Espionnage industriel : James Bond serait-il juriste », <http://www.lepetitjuriste.fr/droit-des-affaires/droit-penal-des-affaires/espionnage-industriel-james-bond-serait-il-juriste/> (1 mars 2016).

[134] Proposition de loi sur « la protection des informations économiques ».

[135] « Se défendre contre l'espionnage industriel », <http://www.murielle-cahen.com/publications/espionnage-informatique.asp> (6 avril 2016).

concurrence déloyale et débouchent sur une sanction pénale. Il convient de noter encore que certaines professions sont plus astreintes au secret que d'autres. Il s'agit notamment des employés bancaires ou du fisc, des avocats et des notaires, etc[136].

6.4.3 Les États-Unis

Les États-Unis ont été un des premiers à avoir compris la nouvelle logique de la guerre économique. En 1993, George Bush a crée le *National Industry Security Program* qui fait le pont entre les besoins de l'industrie privée et les grandes agences de renseignement. Bill Clinton a renforcé ce dispositif dans les années 90. Il a installé le *National Economic Council* qui devait le guider pour la direction à prendre dans la diplomatie économique.

Il a également créé la « *war room* », un centre de renseignements consacré à la guerre économique. Il apparaît bien comme un promoteur de l'espionnage industriel. En 1993, il valide même un nouveau partenariat entre le gouvernement et l'industrie, qui permettra aux entreprises de profiter des compétences étatiques. La CIA, Agence centrale de renseignement américaine, travaille par conséquent avec les « *Big Three* », les trois grandes entreprises du domaine automobile, Ford, General Motors et Chrysler. L'intérêt est porté aux constructeurs d'automobile japonais. Certains renseignements sont obtenus clandestinement. L'industrie, notamment automobile, accepte de se faire assister par les agences de renseignements étatiques. Bill Clinton a mis 70 marchés de haute importance, d'un montant total de 30 milliards de dollars, sous l'encadrement des services secrets américains.

Cela veut dire que toutes les mesures seront prises pour que les entreprises américaines aient accès à des contrats essentiels. La NSA, d'abord seule, puis avec la CIA, sera en tête d'un bureau chargé de redistribuer l'information stratégique aux entreprises américaines. Ce domaine deviendra le domaine de prédilection de la NSA sous Clinton. Un véritable réseau d'espionnage électronique existant depuis les années 1948 sera révélé au grand public

[136] « Espionnage industriel : quelle réponse juridique ? », <https://www.netpme.fr/info-conseil-1/propriete-intellectuelle/contrefacon-espionnage/fiche-conseil/41504-espionnage-industriel-reponse-juridique> (7 avril 2016).

seulement en 1997[137].

En 2000, James R. Woolsey, l'ancien directeur de la CIA, a dit ouvertement que les États-Unis espionnaient ses alliés de l'Europe[138]. Il affirme que les pays de l'Europe remportent les contrats en recourant à la corruption, et par conséquent les Américains seraient légitimés eux aussi à recourir à des méthodes déloyales. Par contre ce que la CIA n'a jamais reconnu c'est le fait d'avoir recours à des agents clandestins au sein des entreprises multinationales dans le but de contrôler les entreprises européennes[139].

Les agissements de la NSA restent secrets jusqu'en 1975. Le directeur de l'agence se voit contraint de mettre au grand jour plusieurs opérations illégales des services secrets, comme l'opération Shamrock[140]. Ce sont les officiers de renseignement militaire qui ont commencé cette opération en 1945, et elle a été confiée à la NSA en 1951. Le but était de s'emparer des messages diplomatiques transférés par le circuit commercial à des grandes entreprises de télégraphie. Cette opération qui constitue une affaire d'espionnage ultra secrète est une violation des lois américaines sur les communications. Quand l'affaire est révélée, nous apprenons que la NSA utilisait un programme d'écoute à l'aide de trois grandes compagnies de téléphone américaines.

La NSA a recours aux technologies les plus sophistiquées qui existent, ce qui lui a permis en seulement quelques décennies d'intercepter et de déchiffrer les messages les plus secrets de plus d'une centaine de pays du monde[141]. En 2013, James R. Clapper, le directeur du renseignement national des États-Unis, a prononcé la phrase suivante après les révélations d'Edward Snowden : « *Ce n'est pas un secret que les services collectent des informations sur des questions économiques et financières. Ce que nous ne faisons pas, comme nous l'avons dit à de multiples reprises, est d'utiliser nos capacités de surveillance de l'étranger pour voler*

---

[137] F. CHARPIER, *L'économie, c'est la guerre : les agents secrets au service du big business*, Paris 2012, pp. 13ss.

[138] *Why we spy on out allies*, The Wall street journal, New York, 2000.

[139] A. LAÏDI et D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 234ss.

[140] « Operation Shamrock : NSA's first domestic spying program was revealed by Congress in 1975 », <http://www.pensitoreview.com/2006/05/13/operation-shamrock-nsas-first-domestic-spying-program-was-shut-down-by-congress-in-1975/> (27 mars 2016).

[141] F. CHARPIER, *L'économie, c'est la guerre : les agents secrets au service du big business*, Paris 2012, pp. 13ss.

des secrets commerciaux de compagnies étrangères au nom — ou pour leur donner des informations que nous collectons — d'entreprises américaines afin d'accroître leur compétitivité. » C'est une phrase qui, au vu de la réalité, est en contradiction totale avec la vraie politique de la NSA. Les États-Unis, tout comme de très nombreux autres États, utilisent les renseignements procurés, des fois illicitement, comme une arme puissante dans la bataille économique. C'est le cas également de beaucoup d'entités privées, comme des entreprises, qui n'hésitent pas non plus à employer parfois des méthodes déloyales dans le jeu de concurrence.

C'est dans cet ordre d'idées que nous pouvons citer l'opération « Target Tokyo » qui a été révélé en 2015 par WikiLeaks[142], selon lequel depuis 2006 les États-Uni espionnaient le gouvernement japonais, ainsi que ses entreprises, comme Mitsubishi. Cette opération a donnée accès pour les services américains à plusieurs dossiers de grande importance, politique et économique. La révélation a causé du désagrement dans les relations entre les deux pays, qui se trouvaient à ce moment en pleine discussion autour d'un traité commun.

C'est aussi WikiLeaks qui a saisi plusieurs documents qui ont dévoilé un espionnage industriel de grande ampleur contre la France pratiqué par les États-Unis, de nouveau par l'intermédiaire de la NSA. Selon Edward Snowden, tous les contrats d'une valeur de plus de 200 millions de dollars ont été visés[143]. Les rapports publiés par WikiLeaks montrent la dimension des informations recueillies par les services de renseignements américains contre la France, par ex. l'espionnage des diplomates français entre 2004 et 2012. Un document nommé « *France : développements économiques* » est censé regrouper les informations concernant les pratiques commerciales du pays, les questions liées au G8 et au G20, les contrats internationaux etc. C'est ce que le fondateur de WikiLeaks Julian Assange appelle un « *sale jeu*[144] » américain. Une centaine d'entreprises françaises sont visées par ces attaques, dont une grande partie sont des opérateurs d'importance stratégique pour la France.

---

[142] Organisation non-gouvernementale qui a pour but de publier des documents et des analyses politiques et sociales à l'échelle mondiale.

[143] F. CHARPIER, *L'économie, c'est la guerre : les agents secrets au service du big business*, Paris 2012, pp. 13ss. et Se défendre contre l'espionnage industriel, disponible sous « http://www.murielle-cahen.com/publications/espionnage-informatique.asp » (6 avril 2016).

[144] « NSA : espionnage économique, le sale jeu américain », <http://www.liberation.fr/planete/2015/06/29/espionnage-economique-le-sale-jeu-americain_1339635> (1 mars 2016).

Il s'agit de mentionner que les informations recueillies par les États-Unis doivent en partie être partagées avec les « *Five eyes* », la Grande-Bretagne, le Canada, la Nouvelle Zélande et l'Australie, qui utilisent le programme « Echelon » créé par les États-Unis, dont l'existence a été révélée seulement en 1998. Cette alliance existant depuis la Guerre froide pour surveiller les Soviétiques est désormais orientée sur le gain de la guerre économique[145]. Echelon est utilisé par les États-Unis pour défendre les intérêts des entreprises nationales. Depuis la fin de la Guerre froide, 40% des missions assignées à la CIA ont un caractère économique et elle ne cache pas que les affaires économiques sont réservées à elle[146]. Nous constatons l'implication toujours croissante des services de renseignement dans la matière de l'espionnage économique. Toutes les grandes entreprises américaines, telles que Motorola, Ford, Xerox, Digital Equipment et de nombreuses autres, ont recruté d'anciens agents des services secrets américains[147].

En 1996, le Congrès américain a adopté une loi sur l'espionnage économique, la Loi Cohen, qui punit les actes d'espionnage économique perpétrés par ou pour le compte d'un État étranger. Elle concerne tous les secrets d'affaires, donc les informations non publiques gardées secrètes. Cette loi a une double facette : la répression de l'espionnage économique au profit d'un État étranger, mais également celle des entreprises privées[148]. La répression peut être extraterritoriale dans le cas où une partie de l'acte a été commise sur le territoire américain[149]. Le but est de démotiver tout acte économique étranger sur le territoire des États-Unis[150].

[145] « NSA : espionnage économique », *op. cit.*

[146] A. LAÏDI, D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 230ss.

[147] J-J. CÉCILE, *L'espionnage Business, Guerre économique et renseignement*, Paris, 2005, pp. 210ss.

[148] B. WARUSFEL, Secret et propriété industrielle. La loi américaine sur l'espionnage économique, *in Droit et défense,* Paris, 1997, p. 64.

[149] F. LAFOUASSE, L'espionnage en droit international, *in Annuaire français de droit international*, Volume 47, Paris, 2001, pp. 63-136.

[150] A. LAÏDI, D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 234ss.

7. Grandes affaires d'espionnage économique

7.1 L'avion soviétique Tupolev Tu-144 (1960)

Un des domaines « préférés » de l'espionnage économique a toujours été l'aviation. Nous allons évoquer l'une des plus grandes affaires dans le domaine, l'« affaire du Concorde ». En 1960, l'URSS a copié l'avion Concorde pour la construction de son propre avion, Tupolev Tu-144. Parmi les personnes inculpées dans cette affaire, il y avait notamment Sergie Fabiew. Étant en réalité agent du KGB, il se présentait comme un homme d'affaires et a même monté un bureau d'études qui comptait dans ses clients Dassault et d'autres constructeurs. Il a acheté durant de nombreuses années des documents confidentiels qui devaient permettre à l'URSS de s'améliorer dans la production des avions civils supersoniques. Pour finir, la ressemblance entre les avions soviétique et américain était si grande, que l'avion Tupolev était même surnommé parfois « Concordski »[151].

7.2 Opel et Volkswagen (1993)

L'autre domaine souvent touché par l'espionnage industriel est l'industrie automobile. En 1993, José Igancio Lopez de Arriortua, cadre dirigeant d'Opel, la filiale allemande du constructeur américain General Motors, a voulu adhérer à Volkswagen. Le problème est qu'il l'a fait en emportant avec lui de nombreux documents confidentiels. Il a nié toutes les accusations et a soutenu que même s'il avait ces documents en mains, ils les a tous détruits depuis. En réalité, la police a découvert tous les dossiers chez l'un de ses proches durant une perquisition. C'est un vrai cauchemar pour l'image de Volkswagen, à un point que même le ministre de l'Economie allemande et le chancelier allemand, ainsi que le Président américain Bill Clinton s'en sont mêlés. En 1997 José Igancio Lopez de Arriortua est obligé de démissionner et de payer une amende de 400'000 marks. La même année Volkswagen devra verser plus de 100 millions de dollars à General Motors et devra en plus acheter des pièces détachées auprès de lui pour plus de 1 milliard de dollars[152].

---

[151] « Espionnage industriel : les affaires qui ont fait trembler l'économie », <http://www.capital.fr/enquetes/histoire-eco/la-saga-james-bond-objectif-fric/espionnage-industriel-les-affaires-qui-ont-fait-trembler-l-economie> (1 mars 2016).

[152] « Espionnage industriel : les affaires qui ont fait trembler l'économie », *op. cit.*

7.3 Michelin (2000)

Dans les années 2000, c'est l'affaire concernant le fabricant de pneumatiques français Michelin qui a éclaté. Un de ses chercheurs a pendant très longtemps conservé les copies des documents secrets de son employeur. Au moment de sa démission, il a voulu les vendre et pour cela il a contacté le fabricant japonais Bridgestone.

Mais les Japonais ont averti les Français et l'espion a été arrêté et mis en prison. Michelin a retenu la leçon et a changé de directeur à la sûreté du groupe pour le général Bernard Fesquet, l'ex-adjoint du directeur technique la Direction générale de la sécurité extérieure de la France. Il convient de noter que le Tribunal a peiné à trouver les moyens juridiques à mettre en œuvre pour sanctionner le comportement déloyal de l'ancien employé. Il a retenu plusieurs chefs de poursuite, mais il s'agit de normes très éparses qui ne concernent pas spécifiquement l'espionnage. Il a retenu l'abus de confiance, la révélation des secrets de fabrique selon le code de travail, ainsi que l'atteinte aux droits fondamentaux de la nation[153].

7.4 Procter&Gamble et Unilever (2001)

En 2001, Procter&Gamble a espionné son concurrent Unilever en recourant à Phoenix Consulting Group, un service de renseignements économiques. L'anecdote est qu'à cette époque, le PDG de cette société d'intelligence économique était en même temps le directeur de la *Society of competitive intelligence professionnal*, qui luttait pour promouvoir une charte déontologique dans toute la profession. Ce qui est intéressant dans cette affaire c'est que c'est le président de Procter&Gamble lui-même qui a averti son homologue de Unilever du vol de ses données. Unilever a exigé une réparation à la hauteur de 10 à 20 millions de dollars, ce à quoi Procter&Gamble a répondu qu'il estimait avoir violé seulement son règlement interne et non pas les normes légales. Il s'est par la suite excusé publiquement[154].

---

[153] « Se défendre contre l'espionnage industriel »,<http://www.murielle-cahen.com/publications/espionnage-informatique.asp>(6 avril 2016).

[154] A. LAÏDI, D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004, pp. 230ss et « Procter & Gamble en négociation avec Unilever sur une affaire d'espionnage commercial », <http://www.lesechos.fr/03/09/2001/LesEchos/18479-062-ECH_procter---gamble-en-negociation-avec-unilever-sur-une-affaire-d-espionnage-commercial.htm> (6 avril 2016).

7.5 Renault (2011) : affaire de faux espionnage ?

En 2011, Renault a soupçonné trois de ses cadres d'espionnage. Ils auraient vendu des informations secrètes concernant leur véhicule électrique. C'est la Chine qui est mentionnée comme bénéficiaire dans l'affaire, mais elle nie tous les reproches. Deux des trois cadres incriminés portent à leur tour plainte contre X pour calomnie, et le dernier pour diffamation et demande à être réintégré à son lieu de travail. Le problème était qu'il n'y avait pas de preuve réelle d'espionnage même après une enquête menée. Alors une perquisition a lieu au siège de Renault à Guyancourt. Quelque temps après, l'hypothèse d'un règlement de compte au sein de l'entreprise est évoquée. Renault parle publiquement d'une « manipulation ».

Durant le temps de l'enquête, l'affaire a pris des proportions tellement grandes que les représentants politiques s'en s'ont mêlés étant donné que l'État est le premier actionnaire de l'entreprise. Par ex., Marc Laffineur, vice-président de l'Union pour un mouvement populaire a demandé la démission ou en tout cas des excuses publiques du PDG de la société[155]. L'un des responsables de la sécurité de l'entreprise est mis en doute. Il aurait fabriqué les allégations d'espionnage et aurait été récompensé pour cela d'une somme dépassant 300'000 euros.

Ce scandale a débouché sur le départ du numéro deux de l'entreprise Patrick Pélata. Selon certaines sources, Renault aurait eu connaissance durant l'enquête du fait que les accusations d'espionnage étaient fausses. Mais Renault a démenti en arguant qu'il était nécessaire de prendre les mesures de défense du moment où le risque était grand. Les trois responsables de la sécurité ont également été licenciés. Les cadres licenciés ont été indemnisés[156].

---

[155] « De l'espionnage à la manipulation : l'affaire qui embarrasse Renault », <http://www.lemonde.fr/economie/article/2011/03/09/espionnage-chez-renault-retour-sur-une-affaire-embarrassante_1490443_3234.html> (6 avril 2016).

[156] « Chronologie de la fausse affaire d'espionnage chez Renault », <http://tempsreel.nouvelobs.com/economie/20110412.OBS1147/chronologie-de-la-fausse-affaire-d-espionnage-chez-renault.html> (6 avril 2016).

7.6 Edward Snowden (2013)

Avec le développement des réseaux sociaux, la surveillance à grande échelle et devenue plus facile pour les entreprises. Dans les années 1990, le World Wide Web[157] commençait petit à petit à se mêler de la vie sociale. C'est à ce moment que les entreprises informatiques ont fait du lobbying auprès de l'administration Clinton en demandant de minimiser la protection de la sphère privée des individus. Les données des utilisateurs sont devenues une stratégie de gain, ce qui est la base du « capitalisme numérique ». En 2014, un sondage réalisé par le cabinet de relations publiques Edelman Berland a montré que 87% des quinze mille personnes qui y ont participé ont affirmé que la loi devrait « *interdire aux entreprises d'acheter et de vendre des données sans le consentement*[158]. » Selon les personnes interrogées, le plus grand danger réside dans le fait que les entreprises peuvent le faire pour leur gain personnel. La Maison Blanche a été contrainte de réagir mais s'est contentée de promulguer un rapport qui émet des recommandations aux entreprises de limiter l'usage des données personnelles.

Cette « cyberdomination américaine » a été perturbée par les révélations d'Edward Snowden. Tout d'abord le danger de ces révélations a été politique car certains États ont redirigé leur politique économique à la suite des révélations, par ex. l'Allemagne a mis fin au contrat avec la compagnie américaine Verizon et lui a préféré Deutsche Telekom. Le gouvernement chinois a affirmé que les équipements informatiques des États-Unis étaient une menace pour sa sécurité et a demandé aux entreprises de ne plus les utiliser[159].

En 2013 les déclarations d'Edward Snowden, ex-technicien de la CIA qui a travaillé plusieurs années par la suite chez la NSA, ont permis de découvrir que la NSA, grâce à son programme Prism[160], pratiquait la surveillance au niveau mondial en ayant accès aux neuf géants d'Internet, soit notamment Google, Apple ou Facebook. Les déclarations de Snowden ont changé l'attitude envers Internet, ainsi que l'image que se faisaient les gens des entreprises et des services secrets américains. Selon lui, l'argument qui consiste à dire que « *tout les pays*

[157] Système hypertexte public fonctionnant sur Internet, qui permet de consulter des pages mises en ligne.

[158] « Géopolitique de l'espionnage. Les ramifications de l'affaire Snowden », <http://www.monde-diplomatique.fr/2014/11/SCHILLER/50926> (1 mars 2016).

[159] Géopolitique de l'espionnage. Les ramifications de l'affaire Snowden, *op. cit.*

[160] Programme américain de surveillance électronique.

font la même chose » n'est pas utilisable car aucun autre pays n'a un système d'espionnage aussi vaste que les États-Unis. Il a également parlé de la nouvelle méthode redoutable utilisée qui est le cyber-espionnage qui mène à une vraie cyberguerre. C'est une opération menée ensemble par l'État et les entreprises[161]. Ses déclarations ont clairement démontré que les intrusions américaines dépassent les actes nécessaires pour la lutte contre le terrorisme, comme c'était annoncé par Washington. Ces accusations lui ont valu une incrimination de la part des États-Unis pour espionnage, vol et utilisation illégal d'instruments gouvernementaux[162]. Une pétition a été lancée par 150'000 personnes pour lui octroyer le pardon présidentiel, mais la demande a été rejetée. Il s'est enfuit en Russie en 2013 et n'est pas prêt à retourner dans son pays d'origine, où il risque toujours 30 ans de prison[163].

8. Conclusion

Comme nous avons pu le constater, l'espionnage économique est une réalité à laquelle il est nécessaire de faire face actuellement, ce que certains acteurs du marché peinent encore à faire. Cette situation est loin de toucher à sa fin. En lisant la presse, nous pouvons remarquer que c'est un sujet qui revient pratiquement quotidiennement. Comme nous avons souligné, il est surtout important de prendre des mesures préventives et agir avant que les faits dommageables ne se produisent. Ces mesures peuvent être banales, comme le fait de ne pas parler des informations confidentielles ou de ne pas utiliser son ordinateur en public, mais aussi sophistiquées, comme le fait d'installer des moyens de protection informatiques. Il y a également un arsenal juridique qui est appelé à assurer la protection. Mais de nouveau, il n'y a

---

[161] « Espionnage industriel : les affaires qui ont fait trembler l'économie », <http://www.capital.fr/enquetes/histoire-eco/la-saga-james-bond-objectif-fric/espionnage-industriel-les-affaires-qui-ont-fait-trembler-l-economie> (1 mars 2016).

[162] « Affaire Snowden : rappel des faits », <http://www.rts.ch/decouverte/sciences-et-environnement/technologies/protection-des-donnees/6199557-affaire-snowden-rappel-des-faits.html> (6 avril 2016) et « Espionnage en Suisse : procédure pénale ouverte », <http://www.24heures.ch/suisse/espionnage-suisse-procedure-penale-ouverte/story/19678896> (1 mars 2016).

[163] « La Maison Blanche refuse le pardon présidentiel à Edward Snowden », <http://www.lexpress.fr/actualite/monde/amerique-nord/la-maison-blanche-refuse-le-pardon-presidentiel-a-edward-snowden_1702816.html> (6 avril 2016).

pas tous les pays qui sont sur un pied d'égalité dans ce domaine. À notre sens, un des plus grands dangers est l'arrivée de cyber espionnage. Nombreux sont les acteurs du marché, que ce soit les entreprises ou les privés, qui ne disposent pas encore de moyens efficaces pour le prévenir ou combattre. Un des pays les plus avancés dans ce domaine, comme cela ressort clairement du travail, sont les Etats-Unis qui disposent des moyens de protection redoutables, et qui sont également un des pays connus pour les activités d'espionnage à tous les niveaux. Comparé aux américains, les européens ont encore un travail important à faire dans en la matière. Dans le cas de la Suisse, comme nous l'avons vu, la menace de l'espionnage économique fait clairement partie des considérations politiques du pays. Nous pensons qu'il est nécessaire de prendre des mesures législatives nécessaires pour assurer une protection efficace, et il s'agit évidemment de trouver le meilleur consensus entre les moyens de protection et le respect de la vie privée des individus.

Bibliographie

Monographies :

H. ASCENSIO, E. DECAUX, A. PELLET, *Droit international pénal*, 2e éd., Paris, 2012.

J. BERGIER, *L'espionnage industriel*, Paris,1969.

B. BESSON et J-C POSSIN, *Du renseignement à l'intelligence économique. Cybercriminalité, contrefaçon, veilles stratégiques : détecter les menaces et le sopportunités pour l'entreprise*, 2e éd., Paris, 2001.

A. BEZBOGOV, A. YAKOVLEV, U. MARTEMYANOV, *La sécurité des systèmes d'exploitation*, Moscou, 2008.

J-J- CÉCILE, *L'espionnage Business, Guerre économique et renseignement*, Paris, 2005.

F. CHARPIER, *L'économie, c'est la guerre : les agents secrets au service du big business*, Paris 2012.

B. CORBOZ, *Les infractions en droit suisse*, Volume I, 3e éd., Berne 2010.

B. CORBOZ, *Les infractions en droit suisse*, Volume II, 3e éd., Berne 2010.

G. DAHM, J. DELBRÜCK, R. WOLFRUM, *Völkerrecht, Die Grundlagen, Die Völkerrechtssubjekte, Band 1*, 2e éd., Berlin, 1989.

P. DAILLIER, M. FORTEAU, A. PELLET, *Droit international public*, 8e éd., Paris, 2009.

É. DAVID, *Éléments de droit pénal international et européen*, Bruxelles, 2009.

L. DEMBINSKI, *The modern law of diplomacy, External missions of states and international organizations*, Dordrecht, 1988.

E. DENZA, *Diplomatic law, Commentary on the Vienna Convention on diplomatic relations*, 3e éd., New York, 2008.

B. ESAMBERT, *La guerre économique mondiale*, Paris, 1992.

S. HOBE, *Einführung in das Völkerrecht*, 9e éd., Stuttgart 2008.

A. HUET, R. KOERING-JOULIN, *Droit pénal international*, 3e éd., Paris, 2005.

M. KÜNG, M.K ECKERT, *Repetitorium zum Völkerrecht*, Berne, 1993.

F. LAFOUASSE, *L'espionnage dans le droit international*, Paris, 2012.

A. LAÏDI, D. LANVAUX, *Les secrets de la guerre économique*, Paris 2004.

L.T. LEE, *Consular law and practice,* 2e éd., Oxford, 1991.

D. LUCAS, A. TIFFREAU, *La dissuasion par l'information. Guerre économique et information : les stratégies de subversion*, Paris, 2001.

C. MARCON, N. MOINET, *L'intelligence économique*, 2e éd., Paris, 2011.

H.K. MELTON, *The spy's guide : Office espionnage*, Philadélphie, 2003.

J. MÜLLER, *La cybercriminalité au sens étroit. Analyse approfondie du droit suisse et aperçu de quelques droits étranger*, Genève, 2012.
G.O.W. MUELLER, E.M WISE, *International criminal law*, Volume II, Londres, 1965.
L. OPPENHEIM, *International law*, Volume I, Londres, 1955.
T.K. REUTER, M. FREI, *Repetitotium, Völkerrecht*, 2e éd., Zürich, 2012.
D. ROUACH, *La veille technologique et l'intelligence économique*, 5e éd., Paris, 2010.
C. ROUSSEAU, *Le droit des conflits armés*, Paris, 1983.
J. SALMON, *Dictionnaire du droit international public*, Bruxelles, 2001.
B. SEN, *A diplomat's handbook of international law and practice*, 3e éd., Dordrecht, 1988.
T. STEIN, C. VON BUTTLAR, *Völkerrecht*, 13 éd., München 2012.
J. VERHOEVEN, *Droit international public*, Bruxelles, 2000.
V.G. VITZTHUM, A. PROELSS, *Völkerrecht*, 6e éd., Berlin, 2013.
H. WEBER, *Grundkurs Völkerrecht, Das internationale Recht des Friedens und der Friedenssicherung*, Frankfurt am Main, 1977.
J. WEILER, A.T. NISSEL, *International law*, Volume V, New York, 2011.
O. WENIGER, *La protection des secrets économiques et du savoir-faire (know-how). Étude comparative des droits allemand, français et suisse*, Renens, 1994.
A. ZIEGLER, *Introduction au droit international public*, 3e éd., Berne, 2015.

Contributions à un ouvrage collectif :

R.H.F. AUSTIN, Le droit des conflits armés internationaux, *in Droit international, Bilan et perspectives*, Tome 2, Paris, 1991, pp. 830ss.

B. WARUSFEL, Secret et propriété industrielle. La loi américaine sur l'espionnage économique, *in Droit et défense*, Paris, 1997, p 64.

Articles :

M. BURTON, *Government spying for commercial gain*, *in Studies in intelligence,* 1994, pp. 17-23.
S. COISSARD, L. DELHALLE, S. CARLOS, Guerre économique et sécurité internationale. Une approche comparative des systèmes institutionnels d'intelligence

économique, *in Revue internationale d'intelligence économique*, Volume II, Paris, 2010, pp. 233-250.

D. DANET, L'intelligence économique : de l'État à l'entreprise , *in Les Cahiers du numérique*, volume III, Paris, 2002, pp. 139-170.

G. KOHEN-JONATHAN et R. KOVAR, L'espionnage en temps de paix, *in Annuaire français de droit international*, volume 6, Paris, 1960, pp. 239-255.

F. LAFOUASSE, L'espionnage en droit international, *in Annuaire français de droit international*, volume 47, Paris, 2001, pp. 63-136.

R. PAUTRAT, L'intelligence économique : un enjeu de premier eimportance toujours sous-estimé, *in Hérodote*, Paris, 2022, pp. 151-156.

J. STONE, *Legal problèmes of espionage in conditions of modern conflict*, *in Essays on espionage and international law*, Ohio 1962, p. 39.

Références électroniques :

« Affaire Snowden : rappel des faits », <http://www.rts.ch/decouverte/sciences-et-environnement/technologies/protection-des-donnees/6199557-affaire-snowden-rappel-des-faits.html > (6 avril 2016).

« Chronologie de la fausse affaire d'espionnage chez Renault », <http://tempsreel.nouvelobs.com/economie/20110412.OBS1147/chronologie-de-la-fausse-affaire-d-espionnage-chez-renault.html > (6 avril 2016).

« Délégation interministrielle à l'intelligence économique », <http://www.intelligence-economique.gouv.fr/qui-sommes-nous/quest-ce-que-lintelligence-economique/enjeux-pour-letat-et-les-entreprises> (29 février 2016).

« De l'espionnage à la manipulation : l'affaire qui embarrasse Renault », <http://www.lemonde.fr/economie/article/2011/03/09/espionnage-chez-renault-retour-sur-une-affaire-embarrassante_1490443_3234.html> (6 avril 2016).

« Equation group : questions ans answers (by Kaspersky Lab) », <https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf> (17 mars 2016).

« Espionnage en Suisse : procédure pénale ouverte », <http://www.24heures.ch/suisse/espionnage-suisse-procedure-penale-ouverte/story/19678896> (1 mars 2016).

« Espionnage industriel : James Bond serait-il juriste ? », <http://www.lepetitjuriste.fr/droit-des-affaires/droit-penal-des-affaires/espionnage-industriel-james-bond-serait-il-juriste/ > (1 mars 2016).

« Espionnage industriel : les affaires qui ont fait trembler l'économie », <http://www.capital.fr/enquetes/histoire-eco/la-saga-james-bond-objectif-fric/espionnage-industriel-les-affaires-qui-ont-fait-trembler-l-economie> (1 mars 2016).

« Espionnage industriel : quelle réponse juridique ? », <https://www.netpme.fr/info-conseil-1/propriete-intellectuelle/contrefacon-espionnage/fiche-conseil/41504-espionnage-industriel-reponse-juridique> (7 avril 2016).

« Géopolitique de l'espionnage. Les ramifications de l'affaire Snowden », <http://www.monde-diplomatique.fr/2014/11/SCHILLER/50926> (1 mars 2016).

« Intelligence économique et stratégie des entreprises. Rapport Marte », <http://bdc.aege.fr/public/Intelligence_Economique_et_strategie_des_entreprises_1994.pdf > (22 mars 2016).

« La Maison Blanche refuse le pardon présidentiel à Edward Snowden », <http://www.lexpress.fr/actualite/monde/amerique-nord/la-maison-blanche-refuse-le-pardon-presidentiel-a-edward-snowden_1702816.html> (6 avril 2016).

« La nouvelle loi sur le renseignement (LRens) : le référendum malgré les attentats », <http://www.schwaab.ch/archives/2015/11/19/nouvelle-loi-sur-le-renseignement-lrens-referendum/> (7 avril 2016).

« La sécurité de la Suisse 2015 », <http://www.news.admin.ch/NSBSubscriber/message/attachments/39237.pdf> (17 mars 2016).

« Le pirate de Twitter, Hacker Croll, condamné à 5 mois de prison avec sursis », <http://www.zdnet.fr/actualites/le-pirate-de-twitter-hacker-croll-condamne-a-5-mois-de-

prison-avec-sursis-39752706.htm> (23 mars 2016).

« Les entreprises doivent se méfier des espions », <http://www.ouest-france.fr/les-entreprises-doivent-se-mefier-des-espions-2159> (23 mars 2016).

« Non à l'État fouineur », <http://etat-fouineur.ch/lrens/?lang=fr> (7 avril 2016).

« Loi sur le renseignement », <http://www.vbs.admin.ch/internet/vbs/fr/home/themen/ndb/faq.html> (7 avril 2016).

« NSA : espionnage économique, le sale jeu américain », <http://www.liberation.fr/planete/2015/06/29/espionnage-economique-le-sale-jeu-americain_1339635> (1 mars 2016).

« Operation Shamrock : NSA's first domestic spying program was revealed by Congress in 1975 », <http://www.pensitoreview.com/2006/05/13/operation-shamrock-nsas-first-domestic-spying-program-was-shut-down-by-congress-in-1975/> (27 mars 2016).

« Procter & Gamble en négociation avec Unilever sur une affaire d'espionnage commercial », <http://www.lesechos.fr/03/09/2001/LesEchos/18479-062-ECH_procter---gamble-en-negociation-avec-unilever-sur-une-affaire-d-espionnage-commercial.htm> (6 avril 2016).

« Prophylax », <http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/publication/snd_publ.parsys.59158.downloadList.0556.DownloadFile.tmp/ndbprophylaxbroschuerefweb20150717.pdf> (17 mars 2016).

« Référendum contre la loi sur le renseignement », <http://www.humanrights.ch/fr/droits-humains-suisse/interieure/protection/securite/suisse-loi-renseignement> (7 avril 2016).

« Référendum LRens », <https://www.lrens.ch > (7 avril 2016).

« Regin : top-tier espionage tool enables stealthy surveillance », <http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance> (17 mars 2016).

« Se défendre contre l'espionnage industriel », <http://www.murielle-cahen.com/publications/espionnage-informatique.asp> (6 avril 2016).

« Unveiling « Careto » - the masked APT (by Kaspersky Lab) »,

<http://kasperskycontenthub.com/wpcontent/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf> (17 mars 2016).

Jurisprudence :

ATF 103 IV 283 (284).

ATF 65 I 330 (333) = JT 1940 I 406.