AIX-MARSEILLE UNIVERSITÉ
FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE
INSTITUT DE RECHERCHE ET D'ÉTUDES EN DROIT DE L'INFORMATION ET DE LA COMMUNICATION

L'INFLUENCE DES ÉTATS-UNIS SUR LE DROIT DU RÉSEAU INTERNET

MÉMOIRE POUR L'OBTENTION DU
MASTER « DROIT DES MÉDIAS ET DES TÉLÉCOMMUNICATIONS »

PRÉSENTÉ PAR
M. VALENTIN BOULLIER

RÉALISÉ SOUS LA DIRECTION DE
M. FRÉDÉRIC LAURIE
MAÎTRE DE CONFÉRENCES EN DROIT PUBLIC À L'UNIVERSITÉ D'AIX-MARSEILLE

ANNÉE UNIVERSITAIRE 2013-2014

M. VALENTIN BOULLIER – L'INFLUENCE DES ÉTATS-UNIS SUR LE DROIT DU RÉSEAU INTERNET

IREDIC, 2013-2014.

AIX-MARSEILLE UNIVERSITÉ
FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE
INSTITUT DE RECHERCHE ET D'ÉTUDES EN DROIT DE L'INFORMATION ET DE LA COMMUNICATION

L'INFLUENCE DES ÉTATS-UNIS SUR LE DROIT DU RÉSEAU INTERNET

MÉMOIRE POUR L'OBTENTION DU
MASTER « DROIT DES MÉDIAS ET DES TÉLÉCOMMUNICATIONS »

PRÉSENTÉ PAR
M. VALENTIN BOULLIER

RÉALISÉ SOUS LA DIRECTION DE
M. FRÉDÉRIC LAURIE
MAÎTRE DE CONFÉRENCES EN DROIT PUBLIC À L'UNIVERSITÉ D'AIX-MARSEILLE

ANNÉE UNIVERSITAIRE 2013-2014

M. VALENTIN BOULLIER – L'INFLUENCE DES ÉTATS-UNIS SUR LE DROIT DU RÉSEAU INTERNET

IREDIC, 2013-2014.

NOTES PRÉLIMINAIRES

Avant d'aborder ce mémoire, il nous semble important d'apporter diverses précisions.

Premièrement, l'écriture du mot « Internet » soulève de nombreuses difficultés : en effet, de nombreuses personnes estiment qu'il s'agit de « l'Internet » et utilisent l'expression « l'internet » ou « l'Internet ». Nous avons privilégié, dans la mesure du possible, « l'internet » et « gouvernance d'internet ». En effet, si les usages ne sont pas encore fixés, le Journal officiel du 16 mars 1999 mentionne un « Vocabulaire de l'information et de l'internet ». La majuscule est ainsi abandonnée. Concernant « la gouvernance d'internet », cette expression est usitée par l'*ICANN* sur son site web et dans ses documents.

Deuxièmement, l'accès à plusieurs sources est restreint, en raison de la confidentialité de certaines informations. Par voie de conséquence, certains paragraphes sont plus riches en informations.

Troisièmement, nous avons cité plusieurs articles de journaux. Nous avons privilégié les sources pouvant être considérées comme fiables, comme *Le Monde* ou *The Guardian.*

Enfin, les traductions de textes écrits en langue anglaise sont libres. Certaines phrases ont été laissées en anglais, une traduction libre pouvant porter atteinte à l'esprit de la phrase.

REMERCIEMENTS

Je tiens, avant d'aborder ce mémoire, à remercier M. Frédéric Laurie pour avoir accepté de diriger celui-ci et d'avoir orienté mes recherches sur un sujet passionnant.

Je remercie de même l'équipe de l'IREDIC.

TABLE DES ABRÉVIATIONS

ACAC	Accord commercial anti-contrefaçon
ACTA	*Anti-Counterfeiting Trade Agreement*
AFNIC	Association Française pour le Nommage Internet en Coopération
AoC	*Affirmation of Commitment*
CNRS	Centre national de la recherche scientifique
CPCE	Codes des Postes et des Communications Électroniques
DARPA	*Defense Advanced Research Projects Agency*
DNS	*Domain Name System*
DoC	*Department of Commerce*
FCC	*Federal Communications Commission*
FISA	*Foreign Intelligence Surveillance Act*
FISAA	*Foreign Intelligence Surveillance Amendment Act of 2008*
GAC	*Governmental Advisory Committee*
GCHQ	*Government Communications HeadQuarters*
IANA	*Internet Assigned Numbers Authority*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IETF	*Internet Engineering Task Force*
IGP	*Internet Governance Project*
IRTF	*Internet Research Task Force*

IP	*Internet Protocol*
ISOC	*Internet Society*
ISP	*Internet Service Provider*
JPA	*Joint Project Agreement*
LPM	Loi de programmation militaire
MoU	*Memorandum of Understanding*
NSA	*National Security Agency*
NSF	*National Science Foundation*
NSI	*Network Solutions Inc.*
NTIA	*National Telecommunications and Information Administration*
OMPI	Organisation Mondiale de la Propriété Intellectuelle
OTAN / NATO	Organisation du Traité Atlantique-Nord / *North Atlantic Treaty Organization*
PAA	*Protect America Act*
PIPA	*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011*
RFC	*Request for Comments*
RIPA 2000	*Regulation of Investigatory Powers Act 2000*
SOPA	*Stop Online Privacy Act*
TCP/IP	*Tranmission Control Protocol / Internet Protocol*
TLD	*Top-Level Domain*
UE	Union européenne

UIT	Union Internationale des Télécommunications
UKUSA	*United Kingdom – United States Communications Intelligence Agreement*
URS	*Uniform Rapid Suspension system*
USA FREEDOM ACT	*Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring*
USA PATRIOT ACT	*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*
VPN	*Virtual Private Network*
WCIT	*World Conference on International Telecommunications*
WSIS	*World Summit on the Information Society*

SOMMAIRE

INTRODUCTION

PARTIE I - Les limites de l'influence américaine sur la gestion des infrastructures physiques et la gouvernance d'internet

CHAPITRE I – L'influence américaine sur la gestion des infrastructures physiques de l'internet

CHAPITRE II – La contestation grandissante de l'influence américaine sur la gouvernance d'internet

PARTIE II - Le renforcement de l'influence américaine sur l'internet via des moyens juridiques et extra-juridiques

CHAPITRE I - Les initiatives juridiques tendant au renforcement de l'influence américaine sur internet

CHAPITRE II - Le renforcement de l'influence américaine via des moyens extra-juridiques

CONCLUSION

INTRODUCTION

Considéré comme un réseau libre permettant le développement du web, le réseau internet est pourtant le fruit de considérations techniques, politiques mais surtout diplomatiques. L'internet est aujourd'hui au cœur d'une société qui se veut de plus en plus connectée. Si le web est communément confondu avec l'internet, la distinction est nécessaire afin de comprendre comment ce dernier a été construit et développé. Toutefois, pour les besoins de ce mémoire, nous considérerons le web comme partie intégrante de l'internet afin de comprendre comment les États-Unis ont construit le réseau et le protocole afin d'asseoir leur influence sur un mode de communication aujourd'hui irremplaçable.

Cette influence est pourtant de plus en plus contestée, et ce tant par certains États que par les utilisateurs du réseau. Si l'influence américaine sur le réseau est historique, pour des raisons politiques, économiques et surtout techniques, cette influence est de plus en plus difficile à conserver. Si, de prime abord, l'internet semble avoir aboli les frontières, il apparaît que celles-ci demeurent.

Les « modèles de l'internet » sont nombreux. S'il est possible de distinguer de nombreuses couches, comme le modèle TCP/IP comportant quatre couches, nous avons choisi de retenir, pour des raisons pratiques et didactiques, un modèle en trois couches. Ce modèle est cité dans le rapport « Internet : pour une gouvernance ouverte et équitable », présenté par Nathalie Chiche (Conseil économique, social et environnemental, 11 décembre 2013) mais également dans un article de Bernard Benhamou[1]. La paternité de ce modèle en trois couches semble devoir être attribuée à Yochai Benkler, enseignant à la Faculté de Droit de Harvard. Ainsi, le réseau internet reposerait sur trois couches : la couche physique, comprenant les infrastructures physiques, la couche logique, recouvrant les normes, et enfin la couche numérique, relative aux informations échangées. Comme le note l'étude de la section des Affaires européennes et internationales dans son rapport, « l'étanchéité entre ces trois différentes couches a pour effet de séparer les fonctions de transport et de traitement des informations et place, de fait, chaque entité connectée sur un pied d'égalité »[2]. Ce modèle a ainsi servi à l'élaboration du plan de cette étude.

1 BENHAMOU (B.), « Organiser l'architecture de l'Internet », www.diplomatie.gouv.fr, date de mise en ligne inconnue, consulté le 10 août 2014, disponible à l'adresse <http://www.diplomatie.gouv.fr/fr/IMG/pdf/OrganiserlarchitecturedelInternetBernardBenhamou-2.pdf>, publication initiale dans *Esprit*, mai 2006.

2 CHICHE (N.), *Internet : pour une gouvernance ouverte et équitable*, rapport au Conseil économique, social et environnemental, 11 décembre 2013, p.11.

Le réseau internet a été développé par les États-Unis dans le but d'assurer une redondance des informations en cas de conflit. Si l'origine militaire du réseau ne peut être contestée, la dimension scientifique ne peut pour autant être occultée : le développement de l'internet résulte de la coopération entre chercheurs américains et non-américains. Les États-Unis ont rapidement appréhendé l'intérêt de l'internet, et ont développé celui-ci selon un modèle essentiellement américain. Ils ont également perçu le vecteur d'influence que pouvait constituer le réseau. Si les infrastructures physiques sont – en partie – protégées de l'influence américaine grâce au droit international, la gouvernance d'internet a très rapidement été maîtrisée par les États-Unis. Cependant, celle-ci tend à s'internationaliser sous l'impulsion de puissances régionales et de plusieurs institutions internationales. Par voie de conséquence, les États-Unis ne peuvent conserver durablement leur influence dans le domaine de la gouvernance d'internet : le modèle multi-parties prenantes *(Multistakeholder)*, en plein développement, constitue un rempart face à la puissance nord-américaine.

Toutefois, la première puissance mondiale n'entend pas abandonner son emprise sur le réseau, et travaille actuellement à renforcer son influence sur le réseau. Les États-Unis étendent ainsi leur influence *via* le Web, en opérant des programmes permettant une captation massive des données échangées. Ces programmes sont mis en œuvre par les puissantes agences de renseignements, et bénéficient d'une certaine légalité. Par ailleurs, les États-Unis ont élaboré une législation adéquate leur permettant de conserver la maîtrise de l'internet et du web. L'emprise de la première puissance mondiale est telle que plusieurs propositions de lois, comme *SOPA* et *PIPA*, ont engendré de nombreuses contestations au niveau international. Ainsi, l'influence de la législation américaine ne peut être contestée. L'Union européenne tente cependant de « contenir » cette influence, avec des résultats pour le moment limités. En effet, les campagnes de lobbying réalisées par les grandes sociétés américaines constituent un frein à l'influence européenne.

Les États-Unis renforcent ainsi leur influence *via* des moyens juridiques, mais également *via* des moyens *hardware* et *software*, c'est-à-dire, *via* des moyens matériels ou logiciels.

Ainsi, l'influence des États-Unis sur le droit du réseau internet est-elle de plus en plus limitée ou demeure-t-elle manifeste ?

Il apparaît que l'influence américaine sur le réseau est de plus en plus contestée, et, par voie de conséquence, de plus en plus limitée. Si les États-Unis disposent d'une capacité d'influence limitée sur les infrastructures physiques de l'internet, les puissances régionales, comme l'Europe ou le Brésil, tentent de promouvoir une internationalisation de la gouvernance. Pour autant, l'*ICANN*, société de droit américain, est le symbole de l'influence américaine sur le réseau, même si celle-ci

apparaît de plus en plus relative (Partie I). Cependant, la première puissance mondiale redéploie son influence sur le réseau. En effet, les États-Unis utilisent des moyens juridiques et des moyens extra-juridiques, *hardware* et *software* afin d'imposer un modèle américain de l'internet et du Web. Les programmes de surveillance opérés par les puissantes agences du renseignement assurent ainsi aux États-Unis la maîtrise du réseau (Partie II).

PARTIE I

Les limites de l'influence américaine sur la gestion des infrastructures physiques et la gouvernance d'internet

Le réseau internet repose sur des infrastructures physiques, composées des satellites et des câbles sous-marins. Ces derniers assurent le transit de l'écrasante majorité des communications mondiales. Ainsi, les communications téléphoniques ne pourraient aboutir sans les câbles sous-marins. Ceux-ci assurent également la communication d'autres données. Si l'image de la « toile » illustre le web, il s'avère que les câbles constituent également une « toile » permettant l'existence de l'internet. Les satellites assurent également, notamment dans les zones peu peuplées, l'accès au réseau. Malgré leur importance, ces infrastructures physiques sont relativement peu soumises à l'influence américaine, et ce tant pour des raisons historiques que juridiques (Chapitre I). En revanche, les États-Unis déploient pleinement leur influence sur la gouvernance d'internet, grâce notamment à leur emprise sur l'*ICANN*. Si certains observateurs estiment que l'*ICANN* acquiert une plus grande indépendance, il s'avère que les États-Unis exercent toujours une influence sur cet acteur majeur. En revanche, il apparaît que l'influence américaine sur la gouvernance d'internet est de plus en plus limitée, notamment grâce aux puissances régionales (Chapitre II).

CHAPITRE I

L'influence américaine sur la gestion des infrastructures physiques de l'internet

L'influence américaine sur les satellites est limitée, en raison de l'internationalisation de la gestion des ressources satellitaires (Section 2). De même, l'installation, la maintenance et la gestion des câbles sous-marins obéissent à des règles internationales (Section 1).

Section 1 – Une influence historiquement limitée pour l'installation et la gestion des câbles sous-marins

Les câbles sous-marins sont au cœur du réseau internet. Héritiers des câbles sous-marins télégraphiques, les câbles actuels constituent la « colonne vertébrale » (§1). L'influence américaine est cependant limitée grâce au droit international (§2).

§1 – Les câbles sous-marins, des infrastructures au cœur des réseaux de données numériques

L'utilisation des câbles sous-marins est ancienne, et leur installation date du développement du télégraphe (A). Ils demeurent aujourd'hui des installations de base et assurent l'existence du réseau internet (B).

A – Les câbles sous-marins, du télégraphe à l'internet

Les premiers câbles sous-marins furent posés au milieu du XIX^{ème} siècle. Si le développement mondial du réseau internet a encouragé la pose de nouveaux câbles, la nécessité d'installer ceux-ci au fond des mers et océans est apparue avec le développement d'une invention cruciale dans le développement économique mondial, le télégraphe, « cet Internet de l'ère victorienne »[3]. Le XIX^{ème} siècle constitue l'âge d'or du Royaume-Uni, puissance coloniale dominant le monde et terreau de la révolution industrielle. Malgré la rivalité historique avec l'autre grande puissance du siècle, la France, le Royaume-Uni souhaita développer les communications entre les deux pays. Ainsi, le remorqueur *Goliath* devient le premier navire à poser un câble. Celui-ci, notamment composé de gutta-percha, relia la France et le Royaume-Uni durant l'été 1850. Ce câble ne fonctionna que sur une période extrêmement brève (certaines sources avancent une durée de

3 CHAUBET (F.), « La mondialisation culturelle », P.U.F. « Que sais-je ? », 2013, p. 36.

onze minutes), en raison de l'accrochage du câble par un pêcheur[4]. Si les principaux problèmes sont désormais identifiés, comme le risque d'accrochage, la nécessité d'un balisage efficient, ou encore la procédure de pose, il faudra encore quelque temps pour qu'un câble reliant le Royaume-Uni et la France soit totalement opérationnel et permette la transmission des câbles télégraphiques. En effet, de nombreux sondages sous-marins seront effectués afin de pouvoir assurer la pose de nouveaux câbles[5]. Un nouveau câble fut posé peu de temps après, « les anglais, financiers et maîtres d'œuvre du dispositif en assurant l'exploitation »[6]. Les britanniques dominèrent longtemps ce secteur. Peu de temps après, et après quelques échecs, le premier câble transatlantique fut posé. 1866 demeurera une année capitale dans le domaine des télécommunications. Le navire *Great Eastern* devint l'un des premiers navires câbliers, et put « […] embarquer dans ses trois gigantesques cuves les 4300 km de câble pesant 3870 tonnes »[7]. En quelques décennies seulement, un réseau mondial fut installé. La durée de transmission et de diffusion diminua considérablement. Nous retiendrons, afin de mieux cerner l'impact sur la population de l'installation des câbles sous-marins le poème de Rudyard Kipling, *« The Deep-Sea Cables »* : « Ils ont réveillé les Choses éternelles ; ils ont tué leur père Temps »[8]. Si des pannes surgissent aujourd'hui occasionnellement, la fiabilité du réseau actuel est sans commune mesure avec l'état du réseau de la fin du XIX^{ème} siècle. En effet, Pascal Griset, chercheur au CNRS, note dans un article que « sur les 11 364 miles de câbles posés avant 1862, à peine 25 % étaient en état de fonctionnement »[9].

L'influence américaine sur l'installation des premiers câbles sous-marins télégraphiques ne fut pas négligeable, malgré la puissance de la Grande-Bretagne et de la France. En effet, l'installation du premier câble direct en 1869 entre les États-Unis et la France connut quelques problèmes. Le câble fut posé sans l'aval du gouvernement américain, ce qui donna lieu à un incident diplomatique, obligeant le président américain de l'époque, Ulysse S. Grant, à intervenir :

---

4 GRISET (P.), « Les câbles sous-marins : 150 ans de rebondissements », *La lettre de l'autorité de régulation des communications électroniques et des postes*, mai-juin 2008, n°61, p. 26.

5 ANONYME, « Communications sous-marines », www.ifremer.fr, date de mise en ligne inconnue, mis à jour le 24 février 2012, consulté le 13 mars 2014, disponible à l'adresse <http://wwz.ifremer.fr/grands_fonds/Les-enjeux/Les-applications/Communications>.

6 GRISET (P.), « Les câbles sous-marins : 150 ans de rebondissements », *La lettre de l'autorité de régulation des communications électroniques et des postes, op. cit.*, p. 26.

7 ANONYME, « Les câbles télégraphiques sous-marins », www.cite-telecoms.com, date de mise en ligne inconnue, consulté le 13 mars 2014, disponible à l'adresse <http://www.cite-telecoms.com/histoire/200-ans-de-telecoms/lage-classique-des-annees-1790-aux-annees-1950/les-cables-telegraphiques-marins/>.

8 KIPLING (R.), « The Deep-Sea Cable », première publication *in English Illustrated Magazine*, mai 1893 : *« [...}]They have wakened the timeless Things; they have killed / their father Time / Joining hands in the gloom, a league from the last of the sun./ Hush! Men talk to-day o'er the waste of the ultimate slime,/ And a new Word runs between: whispering, 'Let us be one!' »*, disponible à l'adresse <http://www.kiplingsociety.co.uk/poems_cables.htm>.

9 GRISET (P.), « Un fil de cuivre entre deux mondes : les premières liaisons télégraphiques transatlantiques », *in : Quaderni*, n. 27, Automne 1995, p. 107.

« Adoptant une attitude qui servit par la suite de référence, il refusa d'accorder l'autorisation tant que la compagnie ne renoncerait pas à un privilège de monopole qui semblait lui avoir été accordé par l'Administration française. Il posa également comme condition que, dans le futur, les entreprises américaines se voient accorder les mêmes autorisations en France »[10]. Ainsi, malgré la puissance française, les États-Unis réussirent à développer une influence certaine sur les réseaux de communications. Cette influence continua à se développer, pour atteindre un paroxysme dès la fin de la Seconde Guerre Mondiale.

En 1956, soit un siècle environ après la pose du premier câble sous-marins, le premier câble téléphonique fut installé. Les câbles télégraphiques furent débranchés les uns après les autres. La dernière grande innovation du XX^{ème} siècle dans le domaine des câbles sous-marins fut l'installation en 1998 du premier câble à fibre optique.

B – Les câbles sous-marins, colonne vertébrale stratégique des télécommunications modernes

Malgré la fin du télégraphe, les câbles sous-marins demeurent capitaux pour les télécommunications modernes (annexe 1). Ils restent en effet une infrastructure physique de base pour l'internet, et l'intérêt qui leur est porté par les agences de renseignements, et notamment par la *NSA (National Security Agency)* et le *GCHQ (Government Communications Headquarters)* démontre une importance toujours d'actualité. Cependant, l'influence américaine dans ce domaine, si elle est considérable dans la sphère extra-juridique, est relativement faible dans la sphère juridique.

Ce secteur constitue un secteur stratégique, et la moindre panne peut avoir de fortes répercussions sur le trafic des données numériques. Les câbles constituent ainsi une véritable « colonne vertébrale » des télécommunications modernes (annexe 2) et relient l'ensemble des continents à l'exception de l'Antarctique. 95 % du trafic transocéanique de « voix » et de données est assuré par les câbles[11]. Actuellement, huit cent mille kilomètres de câbles sous-marins sont en service[12]. La consultation de la carte des câbles sous-marins[13] permet de définir des « pôles » de concentration des câbles : bien évidemment, ceux-ci sont identiques aux pôles économiques.

En effet, l'essentiel des câbles est concentré dans le nord de l'Océan Atlantique (pour les

10 *Ibid.*, p. 107.
11 CARTER (L.), BURNETT (D.) *et alii*, « Submarine cables and the oceans : connecting the world », rapport de l'*ICPC (International Cable Protection Committee)*, décembre 2009, p. 3.
12 LE GALL (F.), « Les câbles sous-marins de fibre optique », www.ariase.com, date de mise en ligne inconnue, consulté le 4 mai 2014, disponible à l'adresse : <http://www.ariase.com/fr/reportages/navire-cablier-rene-descartes.html>
13 Une carte peut être consultée à l'adresse <http://www.submarinecablemap.com/>

liaisons entre l'Europe et les États-Unis), en mer de Chine et à l'ouest de l'océan Atlantique. Si les puissances économiques sont particulièrement connectées, d'autres zones à densité très faible de population sont également connectées par des câbles. Par exemple, l'Islande est reliée à cinq câbles et le Groenland à un câble, tout comme les îles Marshall ou Mayotte. La mer Méditerranée est également parsemée de nombreux câbles. Le « paysage câblier » n'est pas figé et est en constante mutation : de nombreux câbles seront posés dans les prochaines années, et un projet de câble sous l'Arctique est en cours de réalisation.

Il est à noter que Marseille est un point stratégique pour les télécommunications méditerranéennes, plusieurs câbles atterrissant dans la Cité phocéenne. Par ailleurs, « la Ville sans nom » est particulièrement affectée par les agissements de la *NSA*, un câble sous-marin y atterrissant ayant fait l'objet d'une attention particulière de la célèbre agence de renseignement.

Un territoire peut se retrouver isolé et « déconnecté » de l'internet en cas de panne ou de rupture d'un câble sous-marin. Par exemple, le câble « SeaMeWe-4 » reliant Marseille à Singapour en reliant également de nombreux autres pays, tels que l'Algérie, le Pakistan, l'Inde, ou encore la Thaïlande, fut sectionné en avril 2013, et engendra des perturbations dans plusieurs territoires[14].

Si l'expertise française en matière de câbles télégraphiques sous-marins était limitée, celle-ci s'est fortement développée, et de grands groupes français disposent dorénavant d'une expertise certaine en la matière. Par exemple, la filiale d'Orange en charge des câbles sous-marins a posé environ 170 000 kilomètres de câbles[15], et dispose d'une flotte de 5 navires câbliers[16]. Un sixième navire a été lancé durant l'été 2014. De même, le groupe Alcatel a récemment signé un important contrat dont le montant s'élève à plusieurs centaines de millions de dollars américains avec un consortium rassemblant quinze opérateurs de télécommunications afin de procéder à la pose de nouveaux câbles[17]. Enfin, il convient de noter l'expertise du groupe Nexans.

§2 – Une influence américaine limitée

L'influence juridique américaine est en la matière relativement limitée, malgré le poids

14 BONVOISIN (G.), « Câbles Internet sous-marins : plusieurs pays affectés par une rupture », www.cnetfrance.fr, mis en ligne le 2 avril 2013, consulté le 13 mars 2014, disponible à l'adresse <http://www.cnetfrance.fr/news/cables-Internet-sous-marins-plusieurs-pays-affectes-par-une-rupture-39788887.htm>.

15 ANONYME, « France Télécom Marine devient Orange Marine », communiqué de presse, 16 juillet 2013, disponible à l'adresse <http://www.orange.com/fr/presse/communiques/communiques-2013/France-Telecom-Marine-devient-Orange-Marine>, p. 1.

16 ANONYME, « présentation », http://marine.orange.fr, date de mise en ligne inconnue, mis à jour le 25 février 2014, disponible à l'adresse <http://marine.orange.com/fr/qui-sommes-nous/presentation>

17 ANONYME, « Alcatel-Lucent and Sea-Me-We 5 consortium to strengthen ultra-broadband undersea connectivity between Singapore and France », www.alcatel-lucent.com, mis en ligne le 7 mars 2014, consulté le 4 mai 2014, disponible à l'adresse <http://www.alcatel-lucent.com/press/2014/alcatel-lucent-and-sea-me-we-5-consortium-strengthen-ultra-broadband-undersea-connectivity-between>

diplomatique de la première puissance mondiale. Les conventions internationales permettent en effet de limiter cette influence (A). De mêmes, plusieurs puissances régionales tentent à leur tour de développer une certaine « maîtrise » dans le domaine des câbles sous-marins (B).

A – Le régime juridique des câbles sous-marins

Le droit régissant les câbles sous-marins est à la fois international et national. Ainsi, les articles L. 72 et suivants du Code des postes et des communications électroniques français mettent en place un régime juridique spécifique aux câbles sous-marins en cas de dommage causé à l'un d'entre eux. En effet, l'article L. 72 du Code dispose que « Toute personne qui, par négligence coupable et notamment par un acte ou une omission punis de peines de police, rompt un câble sous-marin ou lui cause une détérioration qui peut avoir pour résultat d'interrompre ou d'entraver, en tout ou partie, les communications électroniques, est tenue, dans les vingt-quatre heures de son arrivée, de donner avis aux autorités locales du premier port où abordera le navire sur lequel il est embarqué, de la rupture ou de la détérioration du câble sous-marin dont il se serait rendu coupable ». Si l'auteur du dommage manque à cette obligation de déclaration, l'article L. 72 prévoit une amende de 3750 euros et « éventuellement » quatre mois d'emprisonnement. De même, les articles L. 82 à L. 86 contiennent des dispositions s'appliquant exclusivement aux infractions commises dans les eaux territoriales. Enfin, de nombreuses dispositions nationales s'appliquent aux câbles sous-marins, et ceux-ci bénéficient par exemple d'un régime fiscal particulier.

Malgré de riches dispositions nationales, les câbles sous-marins sont frappés du sceau du droit international. Si l'incident diplomatique impliquant la France et les États-Unis peut sembler anecdotique, il révèle au contraire l'aspect éminemment international qui peut affecter les câbles sous-marins et leur régime. Le télégraphe ayant été perçu comme une invention fondamentale pour le progrès de l'humanité (ou plutôt, de la « civilisation »[18] pour une ère marquée par les expansionnismes colonialistes), le droit s'appliquant à des câbles traversant les eaux internationales et nationales devait être marqué par une internationalisation juridique. La Convention internationale pour la protection des câbles sous-marins réunit au début de l'année 1884 (le procès-verbal de signature est en date du 14 mars 1884) des délégations de nombreux pays : Allemagne, Belgique, Brésil, Costa-Rica, Royaume-Uni, France, États-Unis. Vingt-six pays étaient représentés. L'influence américaine était limitée, et la délégation ne formulera aucune déclaration au moment de la signature de la Convention, contrairement aux délégations néerlandaise, belge, suédoise et

18 « J'étais réticent à l'idée de priver la civilisation de moyens de communication nouveaux tels que ceux qui étaient proposés », Ulysse S. Grant, 18ème président des États-Unis, citation tirée de GRISET (P.), « Un fil de cuivre entre deux mondes : les premières liaisons télégraphiques transatlantiques », *op. cit.*, p. 107.

norvégienne, et surtout anglaise. L'apport de la Convention de 1884 est considérable. Ses dispositions envisagent notamment la détérioration des câbles et l'engagement de la responsabilité des auteurs de dommages causés aux câbles. Ainsi, l'article 2 dispose notamment que « La rupture ou la détérioration d'un câble sous-marin, faite volontairement ou par négligence coupable, et qui pourrait avoir pour résultat d'interrompre ou d'entraver, en tout ou partie, les communications télégraphiques est punissable, sans préjudice de l'action civile en dommages-intérêts ». Il convient de relever la similarité de cet article avec l'article L. 72 du Code des postes et des communications électroniques français. De surcroît, ce dernier mentionne explicitement la Convention de 1884 en son article L. 77, relatif aux eaux internationales.

Si cette Convention internationale constitue la première pierre du régime juridique internationale des câbles sous-marins, plusieurs autres textes internationaux contiennent des dispositions applicables aux câbles sous-marins. La Convention des Nations unies sur le droit de la mer (Convention de *Montego Bay*) de 1982 mentionne en effet les câbles sous-marins, et détermine notamment les droits en fonction des zones maritimes envisagées. Par exemple, les États peuvent installer, à leur convenance, des câbles sous-marins sur le plateau continental (article 79, alinéa 1er), et « l'État côtier ne peut entraver la pose ou l'entretien de ces câbles [...] ». De même, l'alinéa 5 de l'article 79 dispose que « Lorsqu'ils posent des câbles […] sous-marins, les États tiennent dûment compte des câbles […] déjà en place. Ils veillent particulièrement à ne pas compromettre la possibilité de réparer ceux-ci ». L'article 112 dispose notamment que « Tout État a le droit de poser des câbles […] sous-marins sur le fond de la haute mer, au-delà du plateau continental ». La zone économique exclusive (ZEE) fait également l'objet d'une attention particulière, l'article 58 disposant notamment que « tous les États, qu'ils soient côtiers ou sans littoral, jouissent […] de la liberté de poser des câbles […] sous-marins », les États devant cependant tenir compte « des droits et des obligations de l'État côtier ». Enfin, la rupture ou la détérioration desdits câbles est envisagée. Les États-Unis n'ont pas ratifié la Convention de *Montego Bay*, et ce malgré les appels de plusieurs présidents[19].

B – Les puissances régionales, frein à l'influence américaine

Les révélations d'Edward Snowden ont également contribué à une réduction de l'influence américaine. En effet, ces révélations ont engendré de nombreux incidents diplomatiques et ont fourni à des puissances régionales les arguments nécessaires pour déployer à leur tour leur influence

19 LE GALL (J.), « Les trente ans de la Convention des Nations unies sur le droit de la mer (10 décembre 1982 – 10 décembre 2012) – Partie 2 », www.marine-oceans.com, mis en ligne le 8 octobre 2012, consulté le 10 mai 2014, disponible à l'adresse <http://www.marine-oceans.com/les-grands-dossiers-de-marine-et-oceans/3734-les-trente-ans-de-la-convention-des-nations-unies-sur-le-droit-de-la-mer-10-decembre-1982-10-decembre-2012-partie-2>

sur le réseau internet. Outre l'Union européenne, le Brésil a invoqué ces révélations afin d'adopter une nouvelle position sur la scène internationale. La présidente du Brésil, Madame Dilma Rousseff, avait en effet reporté une importante visite qu'elle devait effectuer aux États-Unis. Un article publié sur le site web de *Reuters* précise que les télécommunications entre l'Europe et le Brésil « s'appuient sur un câble sous-marin américain »[20]. De surcroît, il apparaît que ce câble n'autorise que le « transport » de la voix[21]. Le nouveau câble, qui sera déployé très prochainement, mesurera six mille kilomètres de long « pour un coût de 77 000 reais *(sic)* [environ 24 000 euros] par kilomètre »[22]. Malgré ce coût important, nécessitant des aides, la présidente du Brésil est déterminée à encourager ce projet afin de sauvegarder les droits et libertés fondamentaux de ses citoyens, tout en augmentant la capacité d'influence brésilienne sur la scène internationale.

Cependant, le Brésil n'est pas la seule puissance à tenter de contrer la « pieuvre américaine ». La Chine, alliée traditionnelle de la Fédération de Russie, et généralement hostile à la puissance américaine, tente également de devenir un acteur de premier plan dans le domaine des câbles sous-marins. Selon Monsieur Winston Qiu, la Chine tente de bénéficier du recul des opérateurs de télécommunications américaines *(« carriers »)* dans ce domaine[23]. Ces derniers se détournent en effet des câbles sous-marins en raison d'un faible retour sur investissement.

Au-delà des puissances régionales traditionnelles ou nouvelles, notre regard doit se porter vers le continent africain. L'Afrique occupe en effet une place stratégique : de nombreux câbles sous-marins y atterrissent. Ainsi, l'Égypte constitue un « verrou », et ce tant pour le trafic maritime que pour les câbles sous-marins. Certes, si l'installation, la gestion et la maintenance des câbles est généralement d'origine occidentale, les puissances régionales africaines peuvent également tenter de s'immiscer dans un domaine très fermé : « Tout le système de production, d'expertise, de pose et de maintenance est concentré dans quelques pays, dont l'Afrique du Sud est le seul représentant africain »[24].

L'influence américaine sur les câbles sous-marins n'est cependant pas négligeable. Les États-Unis disposent en effet de moyens extra-juridiques (lobbying, boîtiers d'interception, *etc.*) et

20 EMMOTT (R.), « Brazil, Europe plan undersea cable to skirt U.S. spying », www.reuters.com, mis en ligne le 24 février 2014, consulté le 8 mai 2014, diponible à l'adresse <http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224>

21 *Ibid.*

22 TORRES (I.), « Dilma Rousseff défie le Big Brother américain », www.courrierinternational.com, mis en ligne le 12 mars 2014, disponible à l'adresse <http://www.courrierinternational.com/article/2014/03/12/dilma-rousseff-defie-le-big-brother-americain>

23 QIU (W.), « Why It Is China's Turn to Lead the Submarine Cable Industry », www.telecomramblings.com, mis en ligne le 11 février 2014, consulté le 8 mai 2014, disponible à l'adresse <http://www.telecomramblings.com/2014/02/chinas-turn-lead-submarine-cable-industry/>

24 ERIC (B.), « Internet et ses frontières en Afrique de l'Ouest », *Annales de géographie*, 2005/5, n°645, p. 557.

juridiques afin de garder intact leur « rayonnement » mondial. La meilleure illustration est sans aucun doute la situation de l'île de Cuba[25]. Ce pays, soumis à un blocus important de la part des États-Unis, disposait jusqu'à maintenant d'un accès à l'internet grâce aux communications satellites. Cependant, un câble sous-marin a été très récemment activé entre Cuba et le Venezuela, par la société Alcatel Shangaï Bell. Il convient cependant de noter que plusieurs sources mentionnent que si l'embargo américain est la raison invoquée par Cuba, la censure exercée sur les moyens de communications par le régime cubain demeure. Toutefois, il est nécessaire de relever que le câble « atterrit » (terme technique usité dans le domaine) au Venezuela, pays hostile à la politique américaine.

De même, le conflit existant entre les États-Unis et Huawei a été à l'origine de perturbations dans l'installation d'un nouveau câble sous-marin. L'État chinois est en effet un actionnaire très important de Huawei. Or, cette entreprise est soupçonnée par les États-Unis d'espionner pour le compte de l'État chinois : « l'administration Obama redoute que le gouvernement chinois ne soit en mesure d'intercepter le contenu des communications transitant par ce câble, voire de les perturber »[26]. Le câble concerné, devant être installé par Huawei, devait relier les États-Unis et l'Ancien monde, et ainsi améliorer le *trading* haute-fréquence. Or, cette activité étant plus que stratégique, les États-Unis ont brandi, une nouvelle fois, la sécurité des télécommunications. La réaction des États-Unis fut en effet immédiate : « Washington a fait savoir aux opérateurs IP que le fait d'utiliser ce câble leur ferait immédiatement perdre le bénéfice des contrats fédéraux de l'administration »[27]. Hibernia Networks, qui avait sélectionné Huawei pour la pose du câble, a stoppé les discussions avec la société chinoise. Ainsi, l'influence américaine demeure sur les câbles sous-marins.

De même, l'influence américaine s'exerce pleinement en dehors de l'installation des câbles sous-marins, notamment avec l'installation de boîtiers d'interception, le développement de bases de renseignements ou encore le lobbying exercés sur les entreprises du secteur. Ainsi, si l'influence n'était pas entièrement apparente (du moins, aux yeux de l'opinion publique) avant les révélations de monsieur Edward Snowden, celle-ci est dorénavant exposée à la vue et au sus de tous.

Il convient à présent d'étudier l'influence exercée par les États-Unis sur les satellites. Il est

25 EFE (Agence), « Undersea Fiber-Optic Cable from Venezuela reaches Cuba », www.laht.com, date de mise en ligne inconnue, consulté le 4 mai 2014, disponible à l'adresse <http://www.laht.com/article.asp?ArticleId=386513&CategoryId=10718>

26 COL (P.), « Du mou dans le câble : conflit ouvert entre les USA et la Chine », www.zdnet.fr, mis en ligne le 16 février 2013, consulté le 8 mai 2014, disponible à l'adresse <http://www.zdnet.fr/actualites/du-mou-dans-le-cable-conflit-ouvert-entre-les-usa-et-la-chine-39787292.htm>

27 *Ibid.*

cependant nécessaire de noter que le processus de privatisation d'Intelsat a été particulièrement opaque, et que peu de documents ont été publiés.

Section 2 – L'influence américaine sur les satellites

Si toutes les terres ne peuvent être reliées à la « toile » des câbles sous-marins, elle ne sont pas pour autant isolées du réseau internet. Les satellites permettent en effet de pouvoir accéder à internet en tous points de la planète, et peuvent parfois servir de matériel de redondance dans l'hypothèse où un câble sous-marin serait rompu. La maîtrise des technologies satellitaires est l'apanage de certains pays développés, bien que la plupart des pays disposent de satellites de communications ou peuvent utiliser des ressources satellitaires d'autres pays. INTELSAT est l'exemple le plus probant afin d'illustrer l'influence américaine. Si sa construction a été internationale (§1), il s'avère que sa privatisation a pu être opérée grâce à l'accord des États-Unis (§2).

§1 – La construction d'Intelsat

Les satellites étant des ressources stratégiques majeures, leur lancement et leur entretien est réglementé. En effet, des conventions internationales tentent de combiner la souveraineté des États à accéder aux services de communication – et donc, notamment, à l'internet – et la rareté de la ressource (orbite, fréquences, *etc.*). L'organisation du système satellitaire est assurée par de nombreuses organisations internationales. Ainsi, un État ne peut disposer d'une maîtrise totale dudit système. Si de nombreuses organisations internationales existent, INTELSAT est l'organisation la plus pertinente pour illustrer nos propos, et démontrer que l'influence américaine sur ce domaine est relativement faible.

INTELSAT a été créée en 1964, durant la période la Guerre froide, et est devenue en 1971 une organisation internationale « de plein exercice »[28]. Pour Anne-Thérèse Nguyen, la volonté des États-Unis de conserver leur influence sur les télécommunications peut s'illustrer par deux événements : « la création de l'organisation spatiale INTELSAT et l'immédiate mainmise des États-Unis sur cette institution, la résolution NSAM 338 de 1965 »[29]. L'influence américaine est si prégnante que cette institution « protège les États-Unis de tout système concurrent »[30]. Cependant, il apparaît que le monopole américain sera limité par les programmes français. De même, même si les

28 COL (P.), « Du mou dans le câble : conflit ouvert entre les USA et la Chine », www.zdnet.fr, mis en ligne le 16 février 2013, consulté le 8 mai 2014, disponible à l'adresse <http://www.zdnet.fr/actualites/du-mou-dans-le-cable-conflit-ouvert-entre-les-usa-et-la-chine-39787292.htm>

29 NGUYEN (A.-T.), « Les échanges technologiques entre la France et les États-Unis : les télécommunications spatiales (1960-1985 », *Flux*, 2001/1, n°43, p. 19.

30 *Ibid.*, p. 20.

satellites peuvent être nécessaires pour pouvoir accéder à l'internet, l'essentiel du trafic transite *via* les câbles sous-marins. Toutefois, il convient de noter qu'INTELSAT fournit toujours des services aux fournisseurs d'accès à l'internet[31].

Enfin, il convient de noter que les ressources satellitaires sont strictement contrôlées par des institutions internationales. Certes, les États-Unis utilisent leur puissance diplomatique, mais ne peuvent entraver la volonté d'un État de placer un satellite sur orbite.

§2 – La privatisation d'Intelsat

INTELSAT est privatisé en 2001 : le 18 juillet 2001, les actifs financiers sont transférés à une compagnie privée. Cette privatisation a été ardemment souhaitée par les États-Unis, qui ont, pour accélérer le processus, brandit la menace d'une fermeture de l'accès au marché national des télécommunications[32]. En mars 2000, la loi *ORBIT ACT* acta la privatisation de l'organisation, en imposant « qu'INTELSAT soit transformé en une société privée, à but non-lucratif, doté d'un conseil d'administration qui serait largement indépendant des signataires originaires »[33]. Cette privatisation aurait pu avoir pour conséquence une limitation de l'influence américaine. Or, celle-ci a été voulue par les États-Unis : il convient ainsi de noter que ce processus a été mené grâce à la *FCC (Federal Communications Commission). Intelsat Ltd.* est une *holding* basée aux Bermudes. De même, le rapport cité *supra* précise qu'« à la fin des années 1990, le Gouvernement des États-Unis a également estimé qu'il serait dans les intérêts des consommateurs et des entreprises des États-Unis qu'INTELSAT soit privatisé »[34]. Les États-Unis ont donné leur accord, la privatisation d'INTELSAT n'étant pas contraire aux traités commerciaux précédemment ratifiés.

Malgré la puissance économique d'INTELSAT, il convient également de noter que de nombreuses sociétés, non-américaines, sont spécialisées dans le lancement de satellites.

31 http://www.intelsat.com/services/

32 HUBERT-RODIER (J.), « Satellites : les États-Unis cherchent à accélerer la privatisation d'Intelsat », www.lesechos.fr, mis en ligne le 30 avril 1996, consulté le 15 juin 2014, disponible à l'adresse <http://www.lesechos.fr/30/04/1996/LesEchos/17139-033-ECH_satellites--les-etats-unis-cherchent-a-accelerer-la-privatisation-d-intelsat.htm>

33 GAO *(Government Accountability Office),* « Intelsat Privatization and the implementation of the ORBIT Act », *Report to Congressional Requesters,* septembre 2004, p. 6.

34 *Ibid.*, p. 6.

CHAPITRE II

La contestation grandissante de l'influence américaine sur la gouvernance d'internet

Le protocole TCP/IP constitue la racine de l'internet, qui demeure une construction américaine malgré l'intervention de scientifiques étrangers, et notamment français. De même, l'influence américaine s'exerce pleinement sur la gouvernance d'internet (Section 1). Toutefois, cette influence est de plus en plus limitée par les puissances régionales (Section 2).

Section 1 – Une influence américaine toujours très présente

Le protocole TCP/IP est la racine de l'internet (§1). L'*ICANN*, association de droit californien, est un acteur au cœur de la gouvernance d'internet qui demeure, malgré de nombreuses tentatives d'indépendance, sous contrôle américain (§2). Enfin, l'influence américaine peut également s'exercer sur d'autres acteurs de la gouvernance d'internet (§3).

§1 – Le protocole TCP/IP, racine de l'internet

A – L'internet, une construction américaine

L'internet est une construction américaine qui a nécessité la collaboration de scientifiques américains et non-américains. Si la DARPA est à l'origine de ce réseau, les utilisations civiles ont très vite été développées. L'internet est ainsi rapidement devenu un réseau destiné aux universitaires. Malgré le développement des utilisations civiles et la collaboration de scientifiques étrangers, les États-Unis ont strictement contrôlé le développement du réseau en prenant soin de conserver une maîtrise physique totale. De même, la première puissance mondiale a rapidement tenté de contrôler la gouvernance d'internet afin d'acquérir la suprématie technique.

B – Le protocole TCP/IP

TCP/IP est un protocole permettant l'échange de données. Le *RFC-1122* décrit le TCP comme un protocole de transport pour l'internet[35]. Celui-ci permet donc d'acheminer des « paquets de données » sur le réseau internet. Il a notamment été conçu par Robert Kahn et Vinton Cerf, deux

35 *« the primary virtual-circuit transport protocol for the Internet suite »*, RFC-1122, consultable sur le site web de l'*IETF*.

pionniers de l'internet.

§2 – L'ICANN, société de droit californien au cœur de la gouvernance d'internet

L'*ICANN* est un acteur au cœur de la géopolitique mondiale, notamment de par ses missions (A). L'association de droit californien exerce ainsi un véritable contrôle sur les bureaux et offices d'enregistrement (B). Malgré la volonté d'une indépendance accrue, les États-Unis entretiennent toujours des relations « privilégiées » avec l'*ICANN* (C).

A – L'ICANN au cœur de la géopolitique mondiale

1 – Les origines de l'ICANN

L'*ICANN (Internet Corporation for Assigned Names and Numbers)* ne fut pas le premier organisme à être chargé de l'attribution des noms de domaine. Elle fut créée en 1998 afin de se substituer au *NSI (Network Solutions Inc.).* Ce dernier était en effet l'organisme en charge de l'attribution des noms de domaine, et en détenait alors le « monopole d'attribution »[36]. La compétence du *NSI* en matière de l'attribution de noms de domaine était fondée sur un contrat conclu avec le gouvernement fédéral américain, représenté par la *NSF (National Science Foundation)*[37], une agence fédérale « indépendante »[38]. L'enregistrement de noms de domaine était à l'origine gratuit. Cependant, en 1995, *Network Solutions Inc.* fut autorisée par la *NSF* à réclamer la somme de 50 dollars « par an et pour les deux premières années »[39] aux personnes souhaitant enregistrer un nom de domaine. Toutefois, ce système cristallisa de nombreuses critiques, notamment basées sur le monopole détenu par *Network Solutions Inc.* Ainsi, le Conseil d'État, dans son rapport de 1998 « Internet et les réseaux numériques », attira l'attention sur cette problématique[40].

Ces contestations permirent l'émergence d'un nouvel organisme, l'*ICANN*. L'Administration Clinton (1993-2001), en 1997, souhaita[41] privatiser le *DNS (Domain Name System),* « de manière à

36 GAVALDA (Ch.) et SIRINELLI (P.), *Lamy droit des médias et de la communication,* tome 2, Lamy, encyclopédie annuelle, 2013 étude 465-31.

37 « Network Information Services Manager(s) for NSFNET and the NREN : INTERNIC Registration Services COOPERATIVE AGREEMENT NO. NCR-9218742 », disponible sur http://archive.icann.org.

38 ANONYME, « About the National Science Foundation », http://nsf.gov, date de mise en ligne inconnue, consulté le 7 février 2014, disponible sur : <http://nsf.gov/about/>

39 *Statement of Policy on the Management of Internet Names and Adresses*, 5 juin 1998, registre : 980212036-8146-02, date de mise en ligne inconnue, consulté le 7 février 2014, disponible sur le site www.ntia.doc.gov.

40 GAVALDA (Ch.) et SIRINELLI (P.), *Lamy droit des médias et de la communication,* tome 2, Lamy, encyclopédie annuelle, étude 465-31.

41 *Clinton Administration's Framework for Global Electronic Commerce, http://clinton4.nara.gov/WH/New/Commerce/read.html*

augmenter la concurrence et à faciliter la participation internationale dans son *management* »[42]. Le système mis en place par la *NSF* et l'organisme *NSI* fut l'objet de critiques en raison d'un manque de concurrence[43]. Le secrétaire au *Department of Commerce*, M. William Daley, fut chargé de cette mission.

L'année 1998 fut charnière pour l'internet tel que nous le connaissons aujourd'hui. La *NTIA (National Telecommunications and Information Administration)* publia un *Proposal to Improve the Technical Management of Internet Names and Adresses.* Le 20 février 1998, le *« Green Paper »* fut publié, et il fut possible de transmettre ses commentaires et observations[44]. Le *« Green Paper »* permit de délimiter plusieurs principes devant être les principes fondateurs du nouveau système : la stabilité (*« stability »*), la concurrence (*« competition »*), une coordination dite ascendante et émanant du secteur privé (*« private, bottum-up coordination »*) et la représentation de la diversité des usagers du réseau (*« representation »*). Le seul moyen d'assurer l'effectivité de ces principes était, selon la *NTIA*, de créer un nouveau système basé sur une nouvelle entité privée et à but non lucratif. Ainsi, un transfert des compétences de l'*IANA (Internet Assigned Numbers Authority)* vers la nouvelle entité fut réalisé. Le *« Green Paper »* prend soin de préciser que le Gouvernement des États-Unis, grâce au rôle coordinateur du *Department of Commerce*, participera à la transition des compétences et fonctions. Par la suite, la *NTIA* publia le *Statement of Policy on the Management of Internet Names and Adresses* le 5 juin 1998[45](*« White Paper »)*, reprenant les principes énoncés *supra.* Ainsi, l'histoire du *DNS* est marquée par le sceau du Gouvernement fédéral nord-américain. Malgré toutes les volontés d'internationalisation et d'ouverture à la concurrence, la nouvelle entité, l'*ICANN*, sera également fortement influencée par la volonté du *Department of Commerce*, et donc par le Gouvernement fédéral.

2 – La création de l'ICANN

L'*ICANN* a été créée le 18 septembre 1998, et est constituée comme une société sans but

42 *Statement of Policy on the Management of Internet Names and Adresses, 5 juin 1998,* numéro de registre : 980212036-8146-02, *Fed. Reg. : June 10, 1998, vol. 63, n. 111, pp. 31741-31751,* disponible sur les sites www.ntia.doc.gov et sur www.icann.org.

43 *« There is widespread dissatisfaction about the absence of competition in domain name registration », Improvement of Technical Management of Internet Names and Adresses ; Proposed Rules,* numéro de registre : *980212036-8036-01,* disponible sur <http://www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-Internet-names-and-addresses-proposed->

44 Les commentaires transmis à la *NTIA* peuvent être trouvés à l'adresse suivante : <http://www.ntia.doc.gov/legacy/ntiahome/domainname/proposals/comments/comments.html>

45 Statement of Policy on the Management of Internet Names and Adresses, 5 juin 1998, numéro de registre : *980212036-8146-02, Fed. Reg. : June 10, 1998, vol. 63, n. 111, p. 31741-31751,* disponible sur les sites www.ntia.doc.gov et sur www.icann.org.

lucratif, structurée et gérée dans un but « exclusivement caritatif, éducatif, et scientifique »[46] au sens de la loi californienne. Elle est donc une société de droit américain[47], dont le siège se situe à Los Angeles (Marina del Rey). Malgré cette domination totale du droit californien, et donc étasunien, les statuts précisent que le but de l'*ICANN* est de promouvoir l'intérêt général, l'internet ne constituant la « propriété d'aucune nation, individu ou société ». Cet organisme a reçu les fonctions auparavant supervisées par l'*IANA* par un accord conclu le 9 février 2000 avec le gouvernement américain[48].

L'influence américaine sur l'*ICANN* est patente. Au-delà de sa soumission aux lois de Californie, les États-Unis ont pris soin de conserver une forte influence sur le nouvel organisme. En effet, malgré les contestations de l'ancien système *NSI,* le Gouvernement a souhaité conserver un contrôle de la nouvelle société en concluant avec celle-ci un contrat, un *Memorandum of Understanding.* Ainsi, la création de l'*ICANN* n'a pas permis de dissocier le *DNS* du Gouvernement étasunien. Les autres puissances mondiales, mais également l'Union européenne, n'ont, à cette période-clé de l'Histoire, « pas su faire prévaloir leurs vues »[49], et l'*ICANN* est demeurée une société sous contrôle des États-Unis.

La forme de l'*ICANN* est également l'objet de nombreuses observations. Certains auteurs ont ainsi pu employer l'expression « objet juridique non identifié »[50]. Ainsi, selon Mme Françoise Massit-Folléa, l'*ICANN* « n'est pas une instance de normalisation technique, […], pas une agence gouvernementale, […], pas une agence intergouvernementale, […], pas une banale association à but non-lucratif, […], pas une organisation ”ouverte” ». Le rapport[51] présenté par Mme Nathalie Chiche au Conseil économique, social et environnemental rejoint cette argumentation, en rejetant les qualifications d'agence gouvernementale et d'instance « de normalisation technique »[52]. En effet, la forme de l'*ICANN* est la conséquence de préoccupations économiques mais également politiques. L'*ICANN* a donc été l'objet de nombreuses contestations, notamment en raison de sa forme. Cette incertitude peut en partie être justifiée par l'équilibre sur lequel repose cet organisme, cet équilibre étant le fruit de préoccupations nationales (notamment en raison des contestations chinoise et russe),

46 Art. 3, *Articles of Incorporation of Internet Corporation for Assigned Names and Numbers.*
47 *Ibid.*
48 *Contract Between ICANN and the United States Government for Performance of the IANA Function,* 9 février 2000, <http://www.icann.org/en/about/agreements/iana/iana-contract-09feb00-en.htm>
49 CHICHE (N.), *Internet : pour une gouvernance ouverte et équitable,* rapport au Conseil économique, social et environnemental, *op. cit.*, p.12.
50 MASSIT-FOLLÉA (F.), « La gouvernance de l'Internet. Une internationalisation inachevée », *Le Temps des médias,* 2012/1 n°18. DOI : 10.3917/tdm.018.0029, p.33.
51 CHICHE (N.), *Internet : pour une gouvernance ouverte et équitable,* rapport au Conseil économique, social et environnemental, *op. cit.*
52 *Ibid.*, p.13.

régionales, et mondiales. L'*ICANN* est donc tenue de s'adapter à toutes ces préoccupations, mais toujours en prenant en compte l'influence américaine historique et actuelle. Malgré les tentatives d'internationalisation de l'organisme, celui-ci reste « perçu comme mystérieux et opaque »[53]. Les récentes révélations d'espionnage tendent à renforcer les inquiétudes.

3 – L'influence américaine lors de la création de l'ICANN

L'influence américaine sur l'*ICANN* est présente depuis sa création, celle-ci répondant à la volonté américaine de remplacer un système très contesté. En dépit des souhaits d'autres puissances consistant en une internationalisation, les États-Unis ont dès l'origine imaginé l'*ICANN* comme une construction américaine. Pour certains auteurs, le gouvernement américain « poursuit l'objectif naturel de garder le contrôle du DNS tout en le légitimant en l'″universalisant″ par l'entremise de l'ICANN »[54]. Ainsi, « l'Icann est en fait le fruit d'une construction unilatérale de la part des États-Unis »[55]. Le *Memorandum of Understanding (MoU)* du 25 novembre 1998, est un contrat conclu entre l'*ICANN* et le *Department of Commerce* par lequel ce dernier souhaitait s'assurer de la capacité du secteur privé à pouvoir gérer « le management technique du DNS »[56]. Il est intéressant de noter que le *DoC* fonde son autorité en cette matière sur des normes américaines et non internationales, tandis que l'*ICANN* fonde la sienne sur ses statuts. En vertu du *MoU,* le *Department of Commerce* conserva la maîtrise sur l'*ICANN*. Ce contrat prévoyait notamment une coopération entre les deux parties afin de « concevoir, développer, et tester les mécanismes, méthodes, et procédure pour effectuer le management des fonctions DNS suivantes »[57], et ce de manière conjointe. Une liste comportant cinq fonctions avait été établie. De plus, les deux parties devaient « concevoir, développer, et tester les mécanismes, méthodes, et procédures qui achèverait la transition sans perturber l'opération fonctionnelle d'Internet »[58]. La supervision du département du commerce était donc totale. Un terme voisin de « supervision » (*« oversight »*) était employé, dans le sens où le *DoC* devait assurer la surveillance des activités réalisées en vertu du contrat[59]. De surcroît, le *DoC* avait consenti à mettre à la disposition de l'*ICANN* son expertise et ses conseils. Cette maîtrise « totale » était particulièrement contestée, et était à l'origine de nombreuses inquiétudes.

53 DREYFUS (N.), « La gouvernance de l'Internet L'Icann : entre régulation et gouvernance », *RLDI*, avril 2012, n°81, p. 119.
54 MOUNIER (P.), « L'ICANN : Internet à l'épreuve de la démocratie », *Mouvements*, 2001/5 no18, DOI : 10.3917/mouv.018.0081, p. 82.
55 *Ibid.*, p. 119.
56 *Memorandum of Understanding* conclu le 25 novembre 1998, disponible sur les sites www.icann.org et www.ntia.gov.
57 *Ibid.*
58 *Ibid.*
59 *« Provide general oversight of activities conducted pursuant to this Agreement », Memorandum of Understanding,* conclu le 25 novembre 1998, *op. cit.*

Le *Memorandum of Understanding* devait prendre fin le 30 septembre 2000. Cependant, celui-ci fut amendé à de nombreuses reprises, et le dernier amendement date du 17 septembre 2003. Les six amendements peuvent être consultés sur le site web de l'*ICANN*. Le *MoU* expira le 30 septembre 2006, mais l'emprise américaine perdura, puisque le *MoU* fut par la suite remplacé par le *JPA (Joint Project Agreement)*[60]. Il est très intéressant de noter que l'amendement 1, en date du 10 novembre 1999, soit peu de temps après la création de l'*ICANN*, prévoyait notamment que si le département du commerce américain retirait la reconnaissance accordée à l'*ICANN*, celle-ci s'engageait à transmettre au département tous les droits qu'elle détenait en vertu des contrats conclus avec les offices et les bureaux d'enregistrement[61]. Le département du commerce américain pouvait ainsi continuer à exercer une réelle influence s'il choisissait de ne plus reconnaître l'*ICANN*.

De plus, le *MoU* n'est pas le seul contrat conclu entre l'*ICANN* et le département du commerce américain. En effet, en plus de l'accord conclu entre l'*ICANN* et la *NTIA* le 9 février 2000, un autre accord fut conclu avec le département du commerce en 1999[62].

De surcroît, l'*ICANN*, en tant que société de droit privé à but non-lucratif constituée selon les lois californiennes, est soumise au droit américain. Ce point peut notamment être illustré par une résolution en date du 20 décembre 2012, qui contient notamment l'expression « attendu qu'en vertu des statuts de l'ICANN et de la loi californienne »[63]. Si cette résolution est relative à un supplément de rémunération pour un membre important de la société, l'emploi d'une telle expression peut parfaitement illustrer l'influence de la loi californienne.

4 – Les missions de l'ICANN

La mission principale de l'*ICANN* « est de coordonner, à un niveau général, les systèmes mondiaux d'identificateurs uniques d'internet et notamment d'en assurer la stabilité et la sécurité d'exploitation »[64]. Si l'*ICANN* est chargée de la gestion du *Domain Name System*, elle est également responsable de l'accréditation des *registrars*, c'est-à-dire les bureaux d'enregistrement des noms de domaine. Les autres identificateurs uniques sont d'une part les adresse *IP*, d'autre part les *AS*

60 FROOMKIN (M.), « Almost Free : An Analysis of ICANN's ″affirmation of Commitments″ », *9 J. on Telecomm. & High Tech. L. 187*, 2011, p. 192 (disponible sur le site de la *New York University School of Law* à l'adresse <http://www.law.nyu.edu/sites/default/files/ECM_PRO_067688.pdf>)

61 *« If DOC withdraws its recognition of ICANN or any successor entity by terminating this MOU, ICANN agrees that it will assign to DOC any rights that ICANN has in all existing contracts with registries and registrars »*, *Memorandum of Understanding*, premier amendement , signé le 10 novembre 1999.

62 *Cooperative Research and Development Agreement Between ICANN and US Department of Commerce*,

63 Résolution du 20 décembre 2012, publiée le 22 décembre 2012, consultée le 11 février 2014, disponible sur : <http://www.icann.org/en/groups/board/documents/resolutions-20dec12-en.htm>.

64 Art. 1Er, sect. 1, al. 1Er du Règlement de l'*ICANN*.

(Autonomous System), et enfin « les numéros des ports de protocoles et des paramètres »[65]. Malgré ses importantes prérogatives et son rôle central dans le fonctionnement de l'internet, *l'ICANN* qualifie parfois son rôle de « très limité »[66]. L'*ICANN* est un organisme coordinateur entre ces différents identificateurs. Les *« Green Paper »* et *« White Paper »*, mais également le *MoU*, avaient mis en avant le terme de coordination, en délimitant un principe fondateur du nouveau système qui devait alors être mis en place : *« private, bottum-up coordination »*. Toutefois, il peut être intéressant de noter que si le terme de coordination est explicite dans l'énonciation de ce principe, il est également présent de manière implicite dans les trois autres principes énoncés : en effet, la stabilité, la concurrence et la représentation de la diversité des usagers des réseaux impliquent une coordination effective dans la gestion du réseau. L'ensemble des principes énoncés ci-dessus avaient été repris dans le *MoU*.

L'*ICANN* va donc être dotée d'une mission de coordination des « systèmes mondiaux d'identificateurs ». Or, la coordination de tels systèmes ne peut être effective que grâce à une coordination internationale et impliquant notamment les acteurs privés. L'*ICANN* va donc être tenue d'adopter une structure adéquate.

5 – La structure de l'*ICANN*

L'*ICANN* est structurée selon un modèle pluripartite. L'organisme est notamment doté d'un conseil d'administration qui regroupe seize membres possédant un droit de vote et cinq autres membres sans droit de vote : ce sont les agents de liaison. Les règlements de l'*ICANN* détaillent les conditions requises pour pouvoir devenir un administrateur ou un agent de liaison.

B – L'influence de l'ICANN sur les offices et bureaux d'enregistrement

L'*ICANN* est notamment responsable de l'accréditation des bureaux d'enregistrement pour certains *Top Level Domains.* Ces *« registrars »* sont des organismes « ayant pour activité l'enregistrement des noms de domaine »[67].Les bureaux d'enregistrement vont jouer le rôle d'intermédiaire entre les personnes physiques ou morales souhaitant obtenir un nom de domaine, et l'office d'enregistrement. La société *NSI* (aujourd'hui *Network Solutions)*, source de critiques lorsqu'elle détenait le monopole pour l'attribution des noms de domaine, est à ce jour un bureau d'enregistrement accrédité par l'*ICANN*. Afin de devenir un *« registrar »*, il est parfois nécessaire de postuler auprès de l'*ICANN* en déposant un dossier de candidature, comprenant notamment un

65 Art. 1, sect. 1, 1°, c, des règlements de l'*ICANN* (*« Bylaws »*).
66 https://www.icann.org/fr/about/learning/faqs#dns
67 FÉRAL-SCHUHL (C.), *Cyberdroit, le droit à l'épreuve de l'Internet*, Dalloz, collection Praxis Dalloz, 2008, p.537.

chèque de trois mille cinq cents dollars américains. En effet, plusieurs *« Top Level Domain »* ne peuvent être réservés qu'auprès de bureaux d'enregistrement accrédités par *l'ICANN*, comme .aero, .asia, .biz., .cat, .info, .museum ou encore .xxx. Ce dernier fera l'objet d'une étude particulière, car démontrant notamment l'influence américaine actuelle sur l'*ICANN*, et qui a donné lieu à l'affaire « Pigalle du Net ». La liste des bureaux d'enregistrement accrédités par l'*ICANN* est très aisément consultable[68]. Il est important de noter que l'accord d'accréditation de bureau d'enregistrement a été modifié le 21 mai 2009. Cette version ainsi que la version antérieure peuvent toutes les deux être consultables librement sur le site de l'*ICANN*. Cependant, il est possible de devenir un bureau d'enregistrement en réclamant une accréditation auprès des offices d'enregistrement.

L'office d'enregistrement est l'organisme unique en charge de « l'attribution et la gestion des noms de domaine rattachés à chaque domaine de premier niveau du système d'adressage par domaines de l'Internet correspondant aux codes pays du territoire national ou d'une partie de celui-ci »[69]. En France, l'office d'enregistrement est l'AFNIC (Association Française pour le Nommage Internet en Coopération). Il est à noter que l'AFNIC, association constituée sous le régime de la loi du 1er juillet 1901, et descendant de l'« Institut National de Recherche en Informatique et en Automatique » (INRIA) s'était vue confier la mission de gérer le .fr par l'*IANA*, organisme américain. L'AFNIC a été désignée par un arrêté en date du 25 juin 2012 comme office d'enregistrement. L'article L. 45 alinéa 2 du code des postes et des communications électroniques dispose en effet que « le ministre chargé des communications électroniques désigne, par arrêté, l'office d'enregistrement de chaque domaine, après consultation publique, pour une durée fixée par voie réglementaire ». Suite à une décision du Conseil constitutionnel en date du 6 octobre 2010, le dispositif posé par l'article L. 45 avait été jugé contraire à la Constitution.

Les relations entre l'organisme américain et l'AFNIC sont en effet formalisées. Pour M. Bertrand du Marais, « l'origine américaine des pratiques et des règles de l'Internet […] et l'influence du droit de la concurrence viennent en effet limiter considérablement les marges de manœuvre dont bénéficiaient traditionnellement les pouvoirs publics français dans l'organisation des services publics »[70]. La formalisation des relations entre l'AFNIC et l'*ICANN* s'illustre notamment par la signature de lettres d'intention croisées le 26 octobre 2011. Ainsi, l'AFNIC, dans la lettre remise à l'*ICANN*, souhaite que cette dernière « maintienne un système efficace, sécurisé, réactif et fiable », tout en souhaitant que la fonction IANA « soit assurée de manière ouverte et transparente ». De surcroît, l'AFNIC s'engage à verser à l'*ICANN* une contribution « sur une base purement

68 La liste peut être consultée à l'adresse suivante : <https://www.icann.org/registrar-reports/accredited-list.html>
69 Art. L. 45 du code des postes et des communications électroniques.
70 DU MARAIS (B.), « Le service public du nommage », *AJDA*, 2003, p. 1590.

volontaire ». La référence à la législation nationale, et donc française, n'est pas évincée. Ainsi, la lettre d'intention signée par l'*ICANN* précise que « la plupart des questions de politiques de registres soulevées dans le cadre de l'utilisation du .fr sont de nature locale et doivent être traitées au niveau local conformément à la législation nationale ». Cependant, si ces questions de politiques de registres sont susceptibles d'avoir un impact sur « la sécurité, la stabilité ou l'interopérabilité du DNS à un niveau mondial », leur résolution devra alors s'inscrire dans un cadre international.

C – Les liens actuels de l'ICANN avec les institutions gouvernementales américaines

Les récentes révélations relatives à l'interception massive de communications électroniques ont renforcé les contestations relatives à la gouvernance d'Internet. L'*ICANN* s'est défendue en réclamant elle-même une plus grande indépendance vis-à-vis des États-Unis, mais également en rappelant que la structure de l'*ICANN* était éminemment internationale et transparente. Le principe de transparence s'illustre notamment par la publication de comptes-rendus et de rapports préliminaires. Le rapport annuel de 2011 illustre cette volonté d'indépendance : « le modèle multilatéral de l'ICANN est fondé sur l'ouverture, l'inclusion, la confiance et la collaboration. Il a pour but de servir l'intérêt général au niveau mondial. Quand toutes les voix sont entendues, aucune voix unique ne peut dominer une organisation »[71].

Le *MoU* devait expirer le 30 septembre 2006. Cependant, le 26 septembre 2006, l'*ICANN* a conclu un nouvel accord avec le département du commerce américain modifiant une nouvelle fois les accords passés précédemment. Loin d'être un nouvel accord accordant une plus grande indépendance à l'*ICANN,* le *« Joint Project Agreement »* (*JPA*) semble constituer un « septième amendement »[72] du *MoU,* et pour Michael Froomkin, « la relation légale entre l'ICANN et les États-Unis n'était pas différente de ce qu'elle avait été »[73]. Toutefois, certains auteurs notent que le *JPA « succède au MOU »*[74]. La dernière modification rappelait que le *DoC* continuerait à superviser les activités conduites par l'*ICANN*[75]. Cette modification ne permit pas d'éteindre les critiques quant à l'indépendance de l'*ICANN.* Ainsi, par une réponse à une question parlementaire en date du 23 mars 2010 provenant de Mr le député Bernard Carayon, Mr le ministre de la culture et de la

71 Rapport annuel de l'*ICANN, 2011,* p. 3.

72 FAUSETT (B.), « What is the JPA ? », www.netpolicy.com, mis en ligne le 8 février 2008, consulté le 16 février 2014, disponible à l'adresse : <http://www.netpolicy.com/archives/003909.html>

73 FROOMKIN (M.), « Almost Free : An Analysis of ICANN's ″affirmation of Commitments″ », *9 J. on Telecomm. & High Tech. L. 187, op. cit.*, p. 193.

74 DREYFUS (N.), « La gouvernance de l'Internet L'Icann : entre régulation et gouvernance », *RLDI, op. cit.*, p. 119.

75 *« The Department agrees to perform the following activities : […] 4. Monitoring : Continue to monitor the performance of the activities conducted to this agreement », Joint Project Agreement between the U. S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers,* 29 septembre 2006, p. 1-2.

communication avait notamment indiqué que le *Joint Project Agreement* « donnait à ce dernier [au département du commerce américain] une véritable supervision de l'ICANN »[76]. Cependant, l'*Affirmation of Responsabilities*, approuvé par le conseil d'administration de l'*ICANN* le 25 septembre 2006 et annexé au *JAP* prévoyait, en son point 6, une amélioration du modèle « *multi-stakeholder* ».

Le *Joint Project Agreement* a expiré le 30 septembre 2009. Les espoirs des autres puissances mondiales quant à la gouvernance d'internet, et tendant vers une véritable gouvernance multilatérale et indépendante du département du commerce américain, ne furent pas concrétisés. En effet, le 30 septembre 2009, l'*ICANN* conclu un nouvel accord avec le département du commerce. Cet accord est connu sous le nom d'« *Affirmation of Commitments* » (*AoC)* ou « Affirmation d'engagements ». Toutefois, ce nouvel accord a parfois été présenté comme une amélioration quant à la prépondérance du gouvernement américain. Ainsi, pour Mme Françoise Massit-Folléa, « les accords successifs avec le DoC (successions de *Memorandum of Understanding* et actuel *Affirmation of Commitments*) sont toujours présentés comme un progrès vers la ″privatisation″ de l'organisme »[77]. Pour d'autres auteurs, l'*ICANN* « est à l'origine sous tutelle américaine »[78], mais « cette ″mainmise″ a pris fin en octobre 2009 », et donc avec l'expiration du *MoU,* et « jouit aujourd'hui d'une plus grande indépendance »[79]. Effectivement, l'article 1er des *AoC* ambitionne « d'institutionnaliser et d'immortaliser la coordination technique du système de noms de domaine et d'adressage d'internet (DNS), à l'échelle mondiale par une organisation du secteur privé ». D'autre part, le département du commerce américain affirme, par l'article 4, son « engagement » pour un modèle *multi-stakeholders,* et « mené par le secteur privé ». Enfin, le département du commerce « affirme également l'engagement du gouvernement des États-Unis envers la participation continue au comité consultatif gouvernemental », et « reconnaît le rôle important du GAC par rapport à la prise de décisions et l'exécution des tâches de l'ICANN et la prise en compte réelle par l'ICANN de la contribution du GAC *(Governmental Advisory Committee)* aux aspects de politique publique de la coordination technique du DNS de l'Internet ». Les États-Unis sont donc toujours représentés au comité consultatif gouvernemental, même si leur place est équivalente à celle reconnue aux autres États.

Cependant, même si l'influence américaine semble avoir reculé avec l'affirmation

76 Rép. min. à la QE n°65605 du 1er décembre 2009, *J.O. déb. parl. A.N.* (Q.) du 23 mars 2010, p. 3451.
77 MASSIT-FOLLÉA (F.), « La gouvernance de l'Internet. Une internationalisation inachevée », *Le Temps des médias, op. cit.*, p. 34.
78 TARDIEU-GUIGUES (E.), « Attribution et contentieux des noms de domaine », *J.-Cl. Commercial,* Fasc. 805, mis à jour le 23 mars 2011.
79 DREYFUS (N.), « La gouvernance de l'Internet - L'Icann : entre régulation et gouvernance », *RLDI, op. cit.*, n°81, p. 120.

d'engagements, il est judicieux de préciser que ce sont les États-Unis eux-mêmes qui ont accepté cela. Sans la décision du département du commerce américaine, le *MoU* aurait pu perdurer. Ainsi, même si les États-Unis ont fait l'objet de pressions de la part des autres pays, seule leur acceptation est à l'origine de cette perte d'influence. De même, il apparaît que cette « perte d'influence » semble relative, les États-Unis n'étant pas disposés à renoncer à leur domination. En effet, l'*ICANN*, même si elle plus ouverte aux autres pays grâce au modèle *multi-stakeholders,* demeure une société régie par le droit américain.

Au vu de la composition du conseil d'administration de *l'ICANN*, il est légitime de noter que l'influence américaine demeure. En effet, le journal *Les Échos* a dressé une infographie le 15 novembre 2013 : ainsi, il apparaît que sur les seize membres du conseil d'administration, quatre sont originaires des États-Unis. De plus, il convient de noter que l'actuel président du conseil d'administration, M. le docteur Stephen D. Crocker, a été un directeur de programme à la *DARPA*. Si la plupart des membres du conseil d'administration de l'*ICANN* ont été – partiellement ou en totalité – formés par des universités américaines, il est intéressant de noter qu'une membre du conseil d'administration, originaire d'Amérique du Sud, a travaillé dans une société de satellites américain, mais également à la *U. S. FCC (United States Federal Communications Commission).* Il convient toutefois de noter que l'étude présentée par Mme Nathalie Chiche mentionne que lors des auditions, M. Bertrand de la Chapelle, directeur des programmes de l'Académie diplomatique internationale et membre du Board des directeurs de l'*ICANN*, « a fait remarquer que la présence de ressortissants américains au Conseil d'Administration était très minoritaire »[80].

Malgré la signature de l'affirmation d'engagements, une autre question demeure : les États-Unis peuvent-ils continuer à influencer l'*ICANN* par le biais de la fonction *IANA ?* L'*IANA* est aujourd'hui une composante de l'*ICANN,* et « affecte et gère des codes uniques et des systèmes de numérotation qui sont utilisés dans les normes techniques (« protocoles ») permettant aux ordinateurs et autres périphériques de communiquer entre eux via Internet »[81]. La gestion de la fonction *IANA* est attribuée à l'*ICANN* en vertu d'un contrat conclu avec « le gouvernement des États-Unis ». Le dernier contrat a été signé le 2 juillet 2012 et expirera la 30 septembre 2015. Il était peu probable qu'un tel accord soit remis en cause à l'expiration du présent accord. En effet, le premier « *IANA Functions Contrats* » date du 9 février 2000. D'autres contrats similaires, bien que comportant certaines modifications, ont été conclus le 21 mars 2001, le 13 mars 2003 ou encore le

80 CHICHE (N.), *Internet : pour une gouvernance ouverte et équitable*, rapport au Conseil économique, social et environnemental, *op. cit.*, p. 14.

81 DAVIES (K.), « Présentation de l'IANA », www.iana.org, mis en ligne le 29 septembre 2008, consulté le 18 février 2014, disponible à l'adresse <https://www.iana.org/about/presentations/davies-atlarge-iana101-paper-080929-fr.pdf>, p. 1.

11 août 2006. La *NTIA* prend soin de préciser, dans un communiqué de presse publié le 2 juillet 2012, qu'elle avait consulté en 2011 les parties prenantes, « nationales et internationales »[82]. Cependant, la prédominance américaine est patente : en effet, l'*ICANN* est tenue de transmettre tous les mois des rapports « sur la gestion des demandes liées aux différents aspects du contrat de l'IANA »[83], comme l'impose la clause C.4.2 du contrat signé le 2 juillet 2012 et entré en vigueur le 1er octobre 2012 (p. 11). Enfin, il est nécessaire de souligner que « le gouvernement des États-Unis […] donne son aval à toute implémentation de modification »[84]. Le nouveau contrat a été conclu pour une durée de sept ans, et arrivera à expiration en septembre 2019. Enfin, il convient de noter que l'*IGP (Internet Governance Project)* a, le 3 mars 2014, publié une proposition visant à « déposséder » l'*ICANN* de la fonction IANA en créant une nouvel acteur « indépendant »[85].

De même, et nous abordons une des parties les plus techniques, M. Michael Froomkin démontre que l'empreinte américaine demeure, malgré l'*AoC*. Le *DNS* ne peut fonctionner qu'avec des serveurs racines. Ainsi, treize serveurs racines sont gérés par l'*ICANN*. Or, ces serveurs racines ne peuvent fonctionner qu'avec un fichier racine, dénommé « *root zone file* ». Ce fichier, d'une taille minime, « définit quels domaines de premier niveau sont visibles pour la plupart des utilisateurs d'internet et définit quel registre de nom de domaine contrôle chaque enregistrement dans chacun des domaines visés »[86]. Or, ce fichier est installé sur un ordinateur appartenant à Verisign, qui demeure un partenaire « fiable » du département du commerce américain. En effet, un accord a été conclu entre Verisign et le *DoC* (No. NCR 92-18742). Verisign a ainsi la responsabilité « d'éditer le fichier pour adapter celui-ci aux changements recommandés, de publier le fichier, et de le distribuer aux opérateurs du serveur racine »[87]. Le dernier amendement date du 29 novembre 2012, donc après l'*Affirmation of Commitments*. Pour M. Michael Froomkin, « avant l'*Affirmation* [*AoC*], si l'ICANN souhaitait ajouter, modifier ou supprimer un domaine de premier niveau, cela nécessitait l'autorisation du département du commerce, ou au moins son approbation. Rien dans l'Affirmation ne change cela, et cela reste vrai à moins que les États-Unis amendent le contrat avec Verisign, ou si les moyens techniques par lesquelles le fichier root zone est authentifié change de manière à ce que

82 ANONYME, « Commerce Department Awards Contract for Management of Key Internet Functions to ICANN », www.ntia.doc.gov, mis en ligne le 2 juillet 2012, consulté le 18 février 2014, disponible à l'adresse <http://www.ntia.doc.gov/press-release/2012/commerce-department-awards-contract-management-key-Internet-functions-icann>.

83 DAVIES (K.), « Présentation de l'IANA », www.iana.org, *op. cit.*, p. 6.

84 *Ibid.*, p. 6.

85 KUERBIS (B.), « A roadmap for globalizing IANA », www.Internetgovernance.net, mis en ligne le 3 mars 2014, consulté le 3 mars 2014, disponible à l'adresse <http://www.Internetgovernance.org/2014/03/03/a-roadmap-for-globalizing-iana/>

86 FROOMKIN (M.), « Almost Free : An Analysis of ICANN's ″affirmation of Commitments″ », *9 J. on Telecomm. & High Tech. L. 187, op. cit.*, p. 203.

87 http://www.ntia.doc.gov/page/verisign-cooperative-agreement

l'ICANN soit la seule partie à contrôler le processus de certification cryptographique »[88].

Le contrat conclu entre *l'ICANN* et Verisign ne semble pas être remis en question : ainsi, le 29 novembre 2012, ce contrat fut renouvelé par le département du commerce : « grâce à cet accord, Verisign gérera le registre pour le domaine de premier niveau .com pour six années de plus »[89]. Le département du commerce a fait part de sa satisfaction[90]. Il est nécessaire de rappeler que le contrat conclu entre l'*ICANN* et Verisign laisse une grande marge de manœuvre au département du commerce. Ainsi, un document intitulé *« Commerce, ICANN and Verisign agreement in principle »*, disponible sur le site de la *NTIA*, rappelle les principes ajoutés au contrat initial : le département du commerce conserve de nombreuses facultés, notamment celle d'approuver le potentiel successeur du registre gérant le .com, le .net, ou le .org « durant la période de transition »[91].

De plus, il est légitime de penser que la *NTIA* exerce toujours une influence sur l'*ICANN*. En effet, des lettres adressées à cette dernière démontrent que l'administration américaine dispense toujours des conseils à l'*ICANN*. Ainsi, dans une lettre en date du 4 octobre 2012, la *NTIA* reconnaissait que des « progrès avaient été fait dans plusieurs domaines »[92], mais restait « préoccupée des progrès limités sur le *Trademark Clearinghouse* et du *Uniform Rapid Suspension system (URS)* ». De surcroît, si la *NTIA* « encourage les parties prenantes à participer activement au modèle multistakeholder », elle rappelle également qu'elle « continuera à être un membre actif du comité consultatif gouvernemental, travaillant avec les autres parties, afin d'assurer un DNS stable, sécurisé et interopérable »[93]. Cette lettre n'est pas isolée, une autre lettre ayant été adressée à l'*ICANN* le 3 janvier 2012.

L'affaire « *red light district domain* » constitue une autre illustration de l'influence américaine sur l'*ICANN*. Cette affaire est relative au nom de domaine de premier niveau .xxx. L'*ICANN* avait prévu une période pour recueillir les commentaires quant à l'éventuel création de nouveau nom de domaine de premier niveau. Cependant, le département du commerce américain envoya une lettre le 11 août 2005, en réclamant l'extension de cette période[94]. Les puissantes

88 FROOMKIN (M.), « Almost Free : An Analysis of ICANN's ″affirmation of Commitments″ », *9 J. on Telecomm. & High Tech. L. 187, op. cit.*, p. 204.

89 ANONYME, « Department of Commerce Approves Verisign-ICANN .com Registry Renewal Agreement », www.ntia.doc.gov, mis en ligne le 30 novembre 2012, consulté le 27 février 2014, disponible à l'adresse <http://www.ntia.doc.gov/press-release/2012/department-commerce-approves-verisign-icann-com-registry-renewal-agreement>

90 *Ibid.*

91 ANONYME, « Commerce, ICANN and Verisign agreement in principle », www.ntia.doc.gouv, date de mise en ligne inconnue, consutlé le 27 février 2014, disponible à l'adresse <http://www.ntia.doc.gov/files/ntia/publications/doc_icann_verisign_agreement_05182001.pdf>.

92 STRICKLING (L. E.), lettre adressée au Dr. Stephen D. Crocker le 4 octobre 2012, p.1.

93 *Ibid.*, p. 2.

94 KRUGER (L. G.), *Internet Governance and the Domain Name System : Issues for Congress*, Congressional

associations familiales américaines s'étaient en effet érigées contre une telle éventualité. Le .xxx deviendra par la suite un nom de domaine de premier niveau, mais après un premier refus en date du 30 mars 2007. Certains commentateurs y virent l'influence du département du commerce. Ainsi, le site *foxnews.com*, dans un article du 24 mai 2006, mentionne des courriers électroniques émanant de fonctionnaires du département du commerce, et révèle que la société *ICM Registry*, qui avait proposé le .xxx, avait rendu public ces courriers électroniques[95]. Cette affaire avait été très largement relayée sur le web[96]. Cependant, tout comme M. Lennard G. Kruger, il convient de noter que d'autres gouvernements s'inquiétaient d'une possible introduction du .xxx. Cet auteur relève également que « la NTIA a indiqué qu'elle n'interférera pas (et elle ne le fit pas), pour l'acceptation du .xxx »[97].

Enfin, les relations « particulières » que le département du commerce américain entretient avec l'*ICANN* peuvent être illustrées par la volonté de l'*ICANN* de s'émanciper de son « cocontractant » : en effet, les récentes révélations de M. Edward Snowden ont encouragé l'Union européenne à promouvoir un modèle multi-parties prenantes (*multistakeholder model*), position appréciée par l'*ICANN*[98]. De même, M. Fadi Chehadé, président de l'*ICANN*, a reconnu, dans un entretien accordé au site web *Les Echos*, que la dépendance « envers les États-Unis est historique. On doit reconnaître le rôle qu'ont joué les États-Unis dans le développement d'Internet »[99]. Enfin, dans un rapport intitulé « *Internet Governance and the Domain Name System : Issues for Congress* », M. Lennard Kruger note que « le Congrès a un impact sur le sujet de la gouvernance d'internet, à la fois à travers la supervision sur la NTIA et le DNS, et au travers de ses actions sur d'autres domaines plus spécifiques du processus de décision relatif à Internet »[100].

Si les États-Unis souhaitent privilégier le modèle pluripartite, la Chambre des représentants

---

Research Service, 13 novembre 2013, p. 8.

95 ANONYME, « E-Mails Suggest Bush Administration Pressured ICANN to Nix'.Xxx Domain », www.foxnews.com, mis en ligne le 24 mai 2006, consulté le 27 février 2014, disponible à l'adresse <http://www.foxnews.com/story/2006/05/24/e-mails-suggest-bush-administration-pressured-icann-to-nix-xxx-domain/>

96 PULLAR-STRECKER (T.), « Once again, IS blocks porno domain », www.smh.com.au, mis en ligne le 28 mars 2006, consulté le 27 février 2014, disponible à l'adresse <http://www.smh.com.au/articles/2006/03/28/1143441122717.html>

97 KRUGER (L. G.), *Internet Governance and the Domain Name System : Issues for Congress*, Congressional Research Service, *op. cit.*, p. 8.

98 BAKER (J.), « ICANN's cozy relationship with the U.S. must end, says European Union », www.pcworld.com, mis en ligne le 12 février 2014, consulté le 27 février 2014, disponible à l'adresse <http://www.pcworld.com/article/2097120/icanns-cosy-relationship-with-the-us-must-end-says-eu.html>

99 RAULINE (N.), « Fadi Chehade : "La gouvernance d'Internet doit s'inspirer de ce qu'est Internet", entretien avec M. Fadi Chehade, président de l'*ICANN*, www.lesechos.fr, mis en ligne le 21 février 2014, consulté le 27 février 2014, disponible à l'adresse <http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0203332569914-fadi-chehade-la-gouvernance-d-Internet-doit-s-inspirer-de-ce-qu-est-Internet-652224.php>

100 KRUGER (L. G.), *Internet Governance and the Domain Name System : Issues for Congress*, Congressional Research Service, *op. cit.*, p. 19.

a adopté, le 5 décembre 2012 « une résolution s'opposant à la gouvernance de l'Internet par les Nations-Unies »[101].

Les États-Unis, par la voix de la *NTIA*, ont annoncé renoncer au contrôle sur la racine *DNS*, en partie à cause de la contestation internationale encouragée par les révélations relatives aux programmes de surveillance américains. La gestion par une institution internationale semble être envisagée, ce qui accorderait à l'*ICANN* une plus grande indépendance. De nombreux commentateurs ont perçu une véritable internationalisation de la gouvernance d'internet. Cependant, les États-Unis détiennent toujours le « pouvoir physique » sur l'internet, comme en témoigne la cérémonie des sept clés. Cette cérémonie, qui semble appartenir au domaine conspirationniste, est bien réelle. Ressemblant à un rite religieux, elle a eu lieu sur le territoire des États-Unis, et a pour but l'élaboration d'une « clé » permettant l'accès à la base de données de l'*ICANN*. Les deux premières cérémonies se sont déroulées sur le sol américain, et les sept clés nécessaires sont détenues par des membres de l'*ICANN*. Les sources sur ce sujet sont rares : deux articles fiables peuvent être consultées, sur le site de l'*ICANN*[102] et du *Guardian*[103].

§3 – L'influence américaine sur l'IETF/ISOC, un groupe informel au cœur de la gouvernance d'internet

L'*IETF/ISOC* est également l'un des acteurs majeurs de la gouvernance d'internet (A). Ce rôle majeur explique l'intérêt porté par les États-Unis (B).

A – Le rôle central de l'IETF/ISOC dans la gouvernance d'internet

L'*IETF (Internet Engineering Task Force)* est l'un des acteurs majeurs de la gouvernance d'internet, et remplit une mission cruciale, puisque cette mission est « faire fonctionner l'internet en produisant des documents techniques pertinents de haute qualité qui influencent la manière dont les gens conçoivent et gèrent l'Internet[104] ». L'*IETF* est ouverte à toute personne souhaitant y participer, conformément à ses principes. Si la communauté est particulièrement active, le groupe reste informel : aucune cotisation n'est réclamée, et il n'y a « rien à signer »[105]. Les personnes souhaitant contribuer aux travaux de l'*IETF* peuvent rejoindre un des huit groupes de travail qui existent

101 VIVANT (M.) et *alii*, *Lamy Droit du numérique*, Lamy, encyclopédie annuelle, 2013, 1984, p. 1274.
102 ANONYME, « ICANN's First DNSSEC Key Ceremony for the Root Zone », www.icann.org, mis en ligne le 7 juin 2010, consulté le 10 août 2014, disponible à l'adresse <https://www.icann.org/news/announcement-2-2010-06-07-en>
103 BALL (J.), « Meet the seven people who hold the keys to worldwide Internet security », www.theguardian.com, mis en ligne le 28 février 2014, consulté le 10 août 2014, disponible à l'adresse <http://www.theguardian.com/technology/2014/feb/28/seven-people-keys-worldwide-Internet-security-web>
104 ANONYME, « Participez à l'Internet Engineering Task Force », www.ietf.org, date de mise en ligne inconnue, consulté le 11 mars 2014, disponible à l'adresse <http://www.ietf.org/about/about-the-ietf-fr.pdf>
105 http://www.ietf.org/newcomers.html#participation

actuellement.

B – L'influence américaine sur l'IETF/ISOC

L'IETF est ouverte à tous, et la participation à ses travaux n'est donc pas soumise à un quelconque agrément. La communauté qui compose l'*IETF* oriente ses travaux vers les protocoles, et « tente d'éviter les questions relatives à la politique et aux affaires ». La personne intéressée par les problématiques politiques et économiques de l'internet sont encouragés à rejoindre *l'Internet Society.* L'*IETF* jouit d'une certaine indépendance, et il semble que l'influence des États-Unis, importante aux débuts de la communauté, soit moindre. L'*IETF* est par ailleurs un cosignataire de la Déclaration de Montevideo.

Une fois de plus, les États-Unis ont joué un rôle historique. En effet, la première réunion de l'*IETF* avait réuni des chercheurs sous contrat avec le gouvernement des États-Unis, et ce dernier finançait l'organisation jusqu'en 1997[106]. Il est possible de délimiter une influence actuelle sur l'*IETF* ou sur l'organisation parallèle, l'*IRTF (Internet Research Task Force)*. D'une part, le travail accompli par l'*IETF* relatif aux alphabets latins a été mené sur la demande de l'*ICANN*[107]. Il convient de noter que l'*ICANN* a conclu avec l'*IETF* un *« Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority »* le 1er mars 2000. D'autre part, et l'exemple est sans aucun doute plus pertinent, le co-directeur du groupe CFRG *(Crypto Forum Research Group)* de *l'IRTF* est un employé de la *NSA (National Security Agency).* Cette relation privilégiée avec une agence gouvernementale américaine a déclenché une polémique au sein de l'*IRTF,* qui entend protéger son indépendance et la vision communautaire de sa mission. Ainsi, cet employé est notamment accusé par des membres de l'*IETF* « d'avoir encouragé l'adoption d'une version affaiblie du protocole d'échange des clés *Dragon Fly* »[108], et son éviction a été réclamée[109]. La tentative a échoué, et cet employé demeure le co-directeur du *CFRG.*

Section 2 – Les tentatives de limitation de l'influence américaine sur la gouvernance d'internet

L'influence américaine est de plus en plus limitée par des initiatives provenant de l'*ICANN*

106 BRADNER (S.), « IETF Structure and Internet Standards Process », réunion de l'*IETF* des 24-29 juillet 2011, 81ème réunion de l'*IETF,* Quebec City, Canada, <http://www.ietf.org/meeting/81/documents/81newcomers.pdf>.

107 GAVALDA (Ch.) et SIRINELLI (P.), *Lamy droit des médias et de la communication,* tome 2, Lamy, *op. cit.*, 465-21.

108 LEYDEN (J.), « Campaign to kick NSA man from crypto standards group fails », www.theregister.co.uk, mis en ligne le 8 janvier 2014, consulté le 11 mars 2014, disponible à l'adresse <http://www.theregister.co.uk/2014/01/08/nsa_bod_crypto_standard_co_chair_controversy/>

109 La demande d'éviction peut être consultée à l'adresse <http://www.ietf.org/mail-archive/web/cfrg/current/msg03554.html>

ou de l'UIT (§1). De même, certaines puissances régionales souhaitent une gouvernance internationale. Les États-Unis n'étant pas disposé à abandonner le contrôle qu'ils exercent, certaines puissances régionales tentent de développer un réseau national (§2).

§1 – Les initiatives institutionnelles visant à limiter l'influence américaine

L'*ICANN* (A) et l'UIT (B) réclament une gouvernance internationale.

A – Les appels de l'ICANN à une plus grande indépendance

Malgré la dépendance « historique » de l'*ICANN* vis-à-vis des États-Unis, l'association souhaite acquérir une véritable indépendance. Les récentes révélations relatives au programme de surveillance ont démontré que l'influence des États-Unis demeurait. Ainsi, plusieurs puissances régionales, dont l'Union européenne, souhaitent une plus grande indépendance de l'*ICANN*.

Le 17 novembre 2013, un « panel sur l'avenir de la coopération mondiale dans le domaine de l'Internet » a été constitué. Celui-ci regroupe notamment « différentes parties prenantes représentant les gouvernements, la société civile, le secteur privé, la communauté technique et différentes organisations »[110]. L'*ICANN* occupe un rôle important, puisqu'elle a « servi de catalyseur pour la création de ce panel ». La première réunion s'est tenue le 13 décembre 2013. Lors de celle-ci, les membres du panel ont réaffirmé leur support pour une approche pluripartite.

La volonté d'une plus grande indépendance n'est pas uniquement reliée à la révélation d'interceptions massives de données numériques : par exemple, l'*ICANN* avait tenté, avant la conclusion du *Joint Project Agreement*, d'obtenir une plus grande indépendance. Par ailleurs, ce *JPA* avait été considéré comme une limitation de l'influence américaine.

Lors de son séjour à Paris, M. Fadi Chehadé s'est exprimé sur le sujet, en accordant un entretien au journal *Les Échos*. Le président de l'*ICANN* a souhaité une évolution, afin que l'organisme devienne une « société internationale » pouvant être basée à Genève. Le président rappelle également que le conseil d'administration a adopté un « plan de globalisation » comportant cinq étapes[111]. La consultation de la « version préliminaire de la vision, la mission et les domaines prioritaires de l'ICANN en vue de l'élaboration d'un plan stratégique sur cinq ans » révèle ainsi la véritable volonté d'indépendance. Ce document rappelle notamment que « la vision de l'ICANN est

110 ANONYME, « Constitution d'un panel de haut niveau pour étudier l'avenir de la gouvernance de l'Internet », www.icann.org, mis en ligne le 17 novembre 2013, consulté le 27 février 2014, disponible à l'adresse <http://www.icann.org/fr/news/announcements/announcement-2-17nov13-fr.htm>

111 RAULINE (N.), « Fadi Chehade : "La gouvernance d'Internet doit s'inspirer de ce qu'est Internet", entretien avec M. Fadi Chehade, président de l'*ICANN*, www.lesechos.fr, *op. cit.*

celle d'une organisation mondiale indépendante »[112].

De même, l'*ICANN* a signé la Déclaration de Montevideo « sur l'avenir de la coopération pour l'Internet ». Cette déclaration constitue un document majeur, notamment car les signataires sont d'éminents acteurs de l'internet, comme M. John Curran (directeur exécutif de l'ARIN – *American Registry for Internet Numbers*), M. Jari Arkko (président de l'*IETF*), Mme Lynn St-Amour (présidente et directrice exécutif de l'*ISOC*), ou encore M. Jeff Jaffe (directeur exécutif du *W3C*). La déclaration liste quatre points : les signataires ont en premier lieu souligné « l'importance d'une gestion cohérente de l'Internet au niveau mondial et mis en garde contre la fragmentation de l'Internet au niveau national ». D'autre part, ils « ont convenu de catalyser les efforts à l'échelle de la communauté globale en vue de l'évolution de la coopération multipartite de l'Internet mondial ». Les signataires ont également lancé un appel afin que la « mondialisation des fonctions de l'IANA et de l'ICANN » s'accélère. Enfin, la transition vers l'IPv6 a été abordée. Cette déclaration constitue ainsi un véritable appel à une plus grande indépendance de l'*ICANN*. Elle incarne également la volonté d'une « mondialisation » des « fonctions » *ICANN* et *IANA*, « afin que toutes les parties prenantes, en incluant les gouvernements participent sur un pied d'égalité ». Ainsi, dans un discours prononcé à la conférence sur le cyberespace 2013 (qui s'est déroulée à Séoul), madame Lynn St. Amour rappelle que « nous [IETF] avons appelé à l'accélération de la globalisation des fonctions ICANN et IANA, dans un environnement dans lequel toutes les parties, en incluant les gouvernements, participeraient dans leurs rôles respectifs ″d'experts″ »[113].

Les velléités d'indépendance ne sont donc pas récentes, mais « l'affaire Snowden » semble avoir encouragé l'*ICANN* à réclamer avec plus de force son indépendance.

B – Les initiatives de l'Union internationale des télécommunications

Les relations entre l'*ICANN* et l'Union internationale des télécommunications (UIT) ne sont pas empreintes de cordialité. Les deux organisations sont ainsi en « rivalité permanente »[114]. En effet, l'UIT souhaiterait devenir le gestionnaire du système *DNS*, et donc priver l'*ICANN* de l'une de ses principales missions. Certains auteurs ont ainsi pu noter que « pour l'Organisation, la réglementation de certaines questions techniques de l'Internet représente une évolution naturelle de

112 Version préliminaire de la vision, la mission et les domaines prioritaires de l'ICANN en vue de l'élaboration d'un plan stratégique sur cinq ans, 28 octobre 2013.

113 ST. AMOUR (L.), discours prononcé le 17 octobre 2013 lors de la conférence sur le cyberespace de 2013, à Séoul, consulté le 27 février 2014, disponible à l'adresse : <http://www.Internetsociety.org/sites/default/files/Seoul%20Conference%20on%20Cyberspace%202013%20Final%20Remarks.pdf>.

114 MASSIT-FOLLÉA (F.), « La gouvernance de l'Internet. Une internationalisation inachevée », *Le Temps des médias*, *op. cit.*, p. 34.

ses activités [...] »[115]. Le « conflit » entre les deux organismes n'est pas nouveau, celui-ci étant apparu avant même la fondation de l'*ICANN*. L'UIT, souhaitant maximiser l'internationalisation de la gouvernance d'internet, avait en effet estimé qu'elle pouvait remplir les rôles dévolus à l'*ICANN*. Plus d'une décennie après, le « conflit » perdure. Il convient de noter que l'UIT, en 1997, avait « servi de déposant pour un *"Memorandum of Understanding on Generic Top Level Domains"* alternatif, qui avait été élaboré avec l'IANA et l'Internet Society (ISOC), mais sans la participation du gouvernement américain »[116]. Ce document, allant à l'encontre des intérêts américains, fut retiré peu après, « en raison de lourdes pressions provenant des États-Unis […]. En échange, les États-Unis ne s'opposèrent pas à la proposition de l'UIT d'héberger le WSIS »[117]. Le *WSIS (World Summit on the Information Society)* est le Sommet sur l'Information qui s'est déroulé du 10 au 12 décembre 2003 (première phase) et du 16 au 18 novembre 2005 (seconde phase).

La récente manifestation du conflit opposant les deux conceptions distinctes de la gouvernance d'internet est le *WCIT-12 (World Conference on International Telecommunications).* La conférence mondiale des télécommunications internationales s'est déroulée du 3 au 14 décembre 2012, à Dubaï. Cette conférence internationale a donné lieu à de nombreux débats. Un texte a été adopté le 14 décembre 2012. Si cent quarante-quatre États ont participé à cette conférence, seulement quatre-vingt-neuf ont accepté de signer le document. Ce dernier est connu sous le nom d'*«Actes Finals (sic) de la Conférence Mondiale des Télécommunications Internationales* ». Il semble que l'adoption *in extremis* d'une résolution (résolution n°3, « *To foster an enabling environment for the grater growth of the Internet* ») a eu pour conséquence de scinder les participants à la conférence en deux groupes : l'un mené par la Fédération de Russie, et l'autre par les États-Unis. Il convient de noter que « l'UIT avait pris le soin de préciser que la résolution, au contraire du RTI, n'a pas force de traité. Les États-Unis ont malgré tout rejeté le RTI [Règlement des télécommunications internationales] »[118]. La France a suivi le *leadership* des États-Unis, en refusant également de signer le document. La résolution n°3, responsable en partie de l'échec des négociations et de la conférence de Dubaï, chargeait notamment le secrétaire général « de continuer de prendre les mesures nécessaires pour que l'UIT joue un rôle actif et constructif dans le développement du « large bande » et dans le modèle multi-parties prenantes de l'Internet »[119].

115 ACHILLEAS (P)., « Droit international des télécommunications (communications électroniques) », Fasc. 7350, *J.-C. Communication,* 1er décembre 2013.
116 POHLE (J.), MORGANTI (L.), « The Internet Corporation for Assigned Names and Numbers (ICANN) : Origins, Stakes and Tensions », *Revue française d'études américaines,* 2012-4 n°134, p. 40.
117 *Ibid.,* p.40.
118 ACHILLEAS (P)., « Droit international des télécommunications (communications électroniques), Fasc. 7350, *J.-C. Communication, op. cit.*
119 *Actes Finals de la Conférence Mondiale des Télécommunications Internationales (Dubaï, 2012)* : UIT, Genève,

L'UIT est cependant membre du *GAC* de l'*ICANN*. Toutefois, l'UIT est, pour le moment, contrainte de conserver ses positions actuelles. Il est à noter qu'en 2002, M. Houlin Zhao, alors directeur du *TSB* (*Telecommunications Standardization Bureau* – Bureau de la normalisation des télécommunications), avait, dans un document non officiel, affirmé qu'il « doit être clair que l'UIT ne propose pas de reprendre les fonctions de l'ICANN »[120], mais que « l'UIT pourrait aider l'ICANN à reformuler et à définir avec les détails appropriés, les limites de la mission d'élaboration de politiques de l'ICANN qui, à présent, apparaît insuffisamment claire »[121].

§2 – Les initiatives régionales et nationales

Plusieurs puissances régionales, comme l'Union européenne et le Brésil, réclament une gouvernance globalisée (A). D'autres puissances développent un réseau national (B).

A – L'appel de puissances régionales pour une gouvernance d'internet globale

1 – La position européenne et française

Alliée de longue date avec les États-Unis, la France semble réticente à remettre en cause l'influence exercée par les États-Unis sur l'*ICANN*, et, de manière générale, sur la gouvernance d'internet.

Le système *NSI* avait fait l'objet de nombreuses contestations. Le Conseil d'État, tout en remettant en cause ce système, avait privilégié « la solution d'une organisation internationale disposant d'une autorité même indirecte sur la répartition des noms de domaine »[122]. La fin du système *NSI* n'a pourtant pas remis en cause l'influence américaine. Ainsi, plusieurs parlementaires se sont inquiétés de cette influence. Les réponses adressées soulignent notamment la volonté de la France d'internationaliser l'*ICANN*. Pour le ministre de la culture et de la communication d'alors, un « premier pas a été franchi en septembre dernier, avec la fin du "Joint Project Agreement" (JPA) qui liait l'ICANN au département du commerce américain et donnait à ce dernier une véritable supervision de l'ICANN »[123]. Dans une autre question parlementaire, le député Lionel Tardy soulignait la nécessité d'une position française adoptée en adéquation avec l'Union européenne, et ce « quel que soit le représentant du Gouvernement français »[124]. Le sujet implique plusieurs ministères : la première question parlementaire citée était adressée à monsieur le ministre de la

2012, p. 115.

120 HOULIN (Z.), « L'UIT-T et la réforme de l'ICANN », document disponible sur le site de l'UIT, 17 avril 2002, p. 9.

121 *Ibid.*, p.9.

122 GAVALDA (Ch.) et SIRINELLI (P.), *Lamy droit des médias et de la communication*, tome 2, Lamy, encyclopédie annuelle, *op. cit.*, étude 465-31.

123 Rép. min. à la QE n°65605 du 1er décembre 2009, *J.O. déb. parl. A.N.* (Q.) du 23 mars 2010, p. 3451.

124 Rép. min. à la QU n°102688 du 15 mars 2011, *J.O. déb. parl. A.N.* (Q.) du 16 août 2011, p. 8742.

culture et de la communication, tandis que la seconde était adressée à monsieur le ministre des affaires étrangères et européennes. Les réponses à ces questions peuvent parfois rappeler l'intervention de la France à des événements mondiaux relatifs à la gouvernance d'internet. Ainsi, la réponse à la question parlementaire en date du 1er décembre 2009 rappelait la participation du ministre des Affaires étrangères et européennes au Forum des Nations Unies sur la gouvernance d'internet. Malgré la volonté affichée de la France de soutenir une internationalisation de l'*ICANN*, il apparaît que la position française est souvent en adéquation avec la position américaine. Par exemple, la France a refusé de signer les « Actes Finals » du 14 décembre 2012.

Il est nécessaire que la France adopte la même position que l'Union européenne. Cette nécessité est admise, comme en témoigne la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet » créée par le Sénat et dont les membres ont été désignés le 20 novembre 2013. La conclusion de l'*AoC* a réjoui l'Union européenne : la Commission européenne a en effet salué l'expiration du *JPA* et qui a eu pour conséquence la fin de la soumission de l'*ICANN* « au contrôle unilatéral du ministère américain du commerce »[125]. La préoccupation de l'Union européenne sur ce sujet n'est pas récente. Par exemple, dans une « communication de la commission au Conseil et au Parlement européen – L'organisation et la gestion de l'Internet – Enjeux internationaux et européens 1998-2000 », la Commission « invite le Conseil et le Parlement européen à confirmer l'Union dans ses missions de participant, de coordinateur et, au besoin, de négociateur dans ce domaine. Ces missions supposent la concertation avec les organisations internationales, dont l'OMPI et l'UIT, l'organisation de relations bilatérales avec plusieurs gouvernements, notamment avec les États-Unis, et la présence active de l'Union européenne et des États membres dans le comité consultatif des gouvernements (GAC) »[126].

L'Union européenne est en faveur du modèle multi-parties prenantes, et souhaite notamment internationaliser les fonctions de l'*ICANN* et de l'*IANA*. La gouvernance d'internet est une nouvelle fois influencée par les programmes de surveillance mis en place par les États-Unis. Un communiqué de presse en date du 12 février 2014 mentionne une confiance « dans le réseau mise à mal »[127]. De même, la Commission propose d'adopter des « mesures concrètes »[128], comme la fixation d'un

125 ANONYME, « La Commission européenne salue la décision américaine de rendre la gouvernance de l'Internet plus indépendante, plus démocratique et plus internationale », www.europa.eu, mis en ligne le 30 septembre 2009, consulté le 3 mars 2014, disponible à l'adresse <http://europa.eu/rapid/press-release_IP-09-1397_fr.htm>.

126 « Communication de la Commission au Conseil et au Parlement européen - L'organisation et la gestion de l'Internet - Enjeux internationaux et européens 1998 - 2000 », /* COM/2000/0202 final */, 52000DC0202, disponible à l'adresse : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0202:FR:HTML>.

127 ANONYME, « La Commission se propose comme médiateur dans les futures négociations mondiales sur la gouvernance de l'Internet », communiqué de presse mis en ligne le 12 février 2014, consulté le 3 mars 2014, disponible à l'adresse <http://europa.eu/rapid/press-release_IP-14-142_fr.htm>.

128 *Ibid.*

calendrier précis « pour la mondialisation des fonctions de l'ICANN et de l'IANA »[129], et le « renforcement du forum mondial sur la gouvernance de l'Internet »[130]. Enfin, la Commission européenne souhaite mondialiser « les principaux processus de prise de décision »[131]. La position de l'Union européenne est renforcée, et le modèle pluripartite est une nouvelle fois considéré comme la solution la plus adéquate. Cependant, le manque d'influence de l'Union européenne sur ce sujet est très régulièrement relevé.

2 – La place du Brésil dans le débat sur la gouvernance d'internet

Le Brésil, sous l'impulsion de madame la Présidente Dilma Rousseff, est devenu, en quelques mois seulement, le « porte-voix » pour un internet plus indépendant vis-à-vis des États-Unis. En effet, le président de l'*ICANN*, Fadi Chehadé, a très récemment rencontré la présidente du Brésil. La puissance régionale d'Amérique du Sud a accueilli un sommet relatif à la gouvernance d'internet. Cette décision fait suite à la réaction courroucée de la présidente du Brésil qui a violemment critiqué les actions des États-Unis. Le Brésil entend ainsi jouer un rôle majeur dans le débat sur la gouvernance d'internet. Le modèle privilégié reste le modèle multi-parties prenantes (« *multistakeholder model* »), cher à de nombreux acteurs de l'internet. La présidente du Brésil avait également « appelé devant l'Assemblée générale des Nations-Unies à la mise en place d'une solution multilatérale »[132]. Il convient de noter que cet appel a été vivement salué, notamment par le président de l'*ICANN*. De même, l'UIT a participé à ce sommet. Le secrétaire général de l'UIT, le docteur Hamadoun I. Touré a par ailleurs « félicité Mme Dilma Rousseff, Présidente du Brésil, de son initiative en faveur d'un dialogue ouvert et inclusif sur les efforts qu'il convient de fournir afin d'instaurer la confiance dans l'Internet [...] »[133]. Monsieur le secrétaire général de l'UIT siégera « au sein d'un Comité multi-parties prenantes de haut niveau »[134].

La Conférence Netmundial s'est déroulée le 23 et 24 avril 2014 à São Paulo. Cette conférence a abouti à une déclaration condamnant notamment la surveillance de l'internet par les agences de renseignements.

Le Mexique a également accueilli les « Dialogues sur la gouvernance de l'Internet », qui se

129 *Ibid.*
130 *Ibid.*
131 *Ibid.*
132 BACHOLLET (S.), « Gouvernance de l'Internet : au travail ! », www.afnic.fr, date de mise en ligne inconnue, consulté le 3 mars 2014, disponible à l'adresse : <http://www.afnic.fr/fr/ressources/blog/gouvernance-de-l-Internet-au-travail.html>.
133 PARKES (S.), « LUIT participera à la réunion organisée au Brésil sur la gouvernance de l'Internet », www.itu.int, mis en ligne le 20 février 2014, consulté le 3 mars 2014, disponible à l'adresse : <http://www.itu.int/net/pressoffice/press_releases/2014/05-fr.aspx>.
134 *Ibid.*

sont déroulés du 4 au 5 novembre 2013. Cette puissance régionale cherche à renforcer sa position sur la scène internationale. Le Mexique avait signé les « Actes Finals » du 14 décembre 2012 tout en formulant certaines réserves.

B – Les initiatives de création de réseaux internet régionaux : les exemples chinois et russe

1 – Le « Great Firewall » chinois, muraille contre « l'impérialisme américain »

Tout comme la Russie, la République populaire de Chine souhaite réduire l'influence américaine. La situation en Chine est très particulière, notamment parce que ce pays tente de contrôler les DNS et opère une censure de l'internet. La construction de l'internet chinois est allée dans ce sens : David Kurt Herold note ainsi que « dès le début, l'Internet chinois a été construit de manière très différente »[135]. De plus, si les initiatives provenant du secteur privé ont été déterminantes pour le développement de l'internet mondial, c'est le gouvernement chinois qui est le principal acteur de l'internet chinois. Ainsi, « le contrôle du gouvernement chinois sur l'internet en Chine a mené à une quasi-séparation du reste de l'internet mondial »[136]. Le gouvernement chinois a de ce fait tenté de construire un Internet chinois, notamment en tentant de créer son propre système de *DSN*. Ce nouveau système *DNS* offre la faculté aux internautes situés en Chine de ne plus utiliser le système *DNS* de l'*ICANN* afin d'atteindre les sites qu'ils souhaitent. Ce nouveau système a pu être qualifié de nouvelle architecture : « avec cette nouvelle architecture, il s'agit de faire en sorte que ceux qui utilisent un navigateur avec des caractères chinois ne puissent utiliser qu'une partie contrôlée des sites internationaux, et que ceux qui utilisent un navigateur classique ne puissent pas accéder à l'autre partie. On a donc l'équivalent de deux systèmes de noms de domaines dont une large partie est inaccessible à l'autre »[137]. Les appels de la Chine à son indépendance sont également lancés lors des conférences internationales. Ainsi, lors de la CMTI de 2012, la Chine avait suivi la Russie, en demandant une modification de la gouvernance d'internet. Ce bloc, soutenu par d'autres pays, était alors rentré en confrontation avec le bloc mené par les États-Unis.

La Chine est également régulièrement accusée d'opérer une véritable censure, comme le montre le projet *« Golden Shield »* (communément dénommé le *« Great Firewall of China »*). Ce

135 HEROLD (D.K.), « An inter-*nation*-al Internet : China's contribution to global Internet governance ? », note présentée lors du colloque « A decade in Internet Time: Symposium on the Dynamics of the Internet and Society », 21-24 septembre 2011, Oxford Internet Institute, Oxford University, Royaume-Uni, p 4. Cet article est consultable à l'adresse <http://hdl.handle.net/10397/5782>.

136 *Ibid.*, p. 5.

137 GUILLAUD (H)., « Chine : vers un grand schisme de l'Internet ? », www.lemonde.fr, mis en ligne le 19 février 2010, consulté le 10 mars 2014, disponible à l'adresse <http://www.lemonde.fr/technologies/article/2010/02/19/chine-vers-un-grand-schisme-de-l-Internet_1308660_651865.html>.

système permet notamment de filtrer et de bloquer des contenus jugés immoraux (sites pornographiques) ou attentatoires à la sécurité de l'État (par exemple, tous les articles relatifs à Tian'anmen). Ce système, régulièrement contesté, aurait été renforcé en décembre 2012 et permettrait également de contourner les *VPN (Virtual Private Network)* installés par les internautes chinois.

La Chine s'oppose donc aux États-Unis sur le sujet de la gouvernance d'internet, et tente de contrer cette hégémonie, par exemple en réclamant l'intervention de l'UIT dans la gouvernance d'internet. De même, la Chine, en 2011, avait réclamé auprès de l'ONU un code de conduite mondial « mettant en avant le primat de l'autorité politique des États sur les questions d'intérêt public liées à l'Internet »[138], et s'est opposé au modèle multi-parties qui ne garantit pas « une représentation équitable entre les différentes composantes et les différentes parties du monde »[139].

2 – L'internet russe, un outil au service de la censure

La Chine adopte régulièrement les positions tenues par la Russie. Les différentes initiatives portées par ces deux puissances économiques tendent vers ce que certains auteurs ont appelé « une balkanisation » ou une « dislocation » de l'internet. Pour autant, cette « balkanisation de l'internet » pourrait également être la conséquence des programmes de surveillances opérées par les services de renseignement occidentaux. Ainsi, à côté d'un internet « mondial », des internets nationaux pourraient naître, des puissances comme la Russie « tentant de créer un réseau fermé et contrôlé en marge du réseau Internet »[140]. Lors de la Conférence mondiale des télécommunications internationales de 2012, la Russie s'était opposée avec véhémence aux États-Unis, et avait proposé une internationalisation tout en soulignant le rôle majeur que pouvait endosser l'UIT en matière de gouvernance d'internet. Les États favorables à la position défendue par les États-Unis « considéraient l'intervention de l'UIT dans ce domaine comme une dérive pouvant à terme remettre en cause le caractère libre et ouvert de l'Internet »[141]. La conférence de Dubaï ayant été un échec, la Russie et les États-Unis s'opposent toujours sur ce sujet.

138 CHICHE (N.), *Internet : pour une gouvernance ouverte et équitable*, rapport au Conseil économique, social et environnemental, *op. cit.*, p. 35.
139 *Ibid.*, p. 35.
140 RAULINE (N.), « Gouvernance d'Internet : la France appelle à de nouvelles règles », mis en ligne le 14 janvier 2014, consulté le 10 mars 2014, disponible à l'adresse <http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0203243031717-gouvernance-d-Internet-la-france-appelle-a-de-nouvelles-regles-642831.php>.
141 ACHILLEAS (P)., « Droit international des télécommunications (communications électroniques) », Fasc. 7350, *J.-C. Communication*, 1er décembre 2013.

Ainsi, l'influence américaine est limitée sur les infrastructures physiques, et notamment sur les câbles sous-marins. De même, la gouvernance américaine d'internet est de plus en plus contestée par les puissances régionales. Peu à peu, cette emprise diminue. En revanche, les États-Unis ne souhaitent pas abandonner leur maîtrise et leur influence. De ce fait, la première puissance mondiale a su élaborer une législation adéquate afin de conserver cette influence. Celle-ci se redéploie en effet grâce au web et grâce à une législation qui constitue parfois une source pour des législations étrangères. De plus, les États-Unis mettent en œuvre des programmes de surveillance extrêmement avancés.

PARTIE II

Le renforcement de l'influence américaine sur l'internet *via* des moyens juridiques et extra-juridiques

Les États-Unis tentent de renforcer leur influence grâce à plusieurs initiatives juridiques, comme la légalisation des interceptions électroniques. Ainsi, la première puissance mondiale a réussi à légaliser – sur son territoire – les interceptions de communications de citoyens non-américains. Toutefois, ces initiatives sont parfois limitées, par exemple par l'Union européenne. De même, les États-Unis, ou des sociétés américaines, mènent de grandes campagnes de lobbying (Chapitre I). Les moyens extra-juridiques utilisés par les États-Unis pour renforcer leur influence sont très fortement contestés. Le programme PRISM est devenu ainsi le symbole d'une société de surveillance, dominée par les sociétés américaines qui tentent d'imposer un modèle purement américain (Chapitre II).

CHAPITRE I

Les initiatives juridiques tendant au renforcement de l'influence américaine sur internet

Les initiatives juridiques menées par les États-Unis sont diverses. Leur influence sur le réseau est renforcée par la légalisation des interceptions électroniques, mais également par les campagnes de lobbying (Section 1). Cependant, des puissances régionales, et notamment l'Union européenne, tentent de limiter cette influence (Section 2).

Section 1 – La légalisation des interceptions électroniques au cœur de la stratégie américaine

La législation américaine est complexe, et de nombreuses lois leur permettent de renforcer leur contrôle (§1). Cette législation a eu une forte influence sur plusieurs législations européennes (§2).

§1 – La législation américaine

La législation américaine nous intéressant a été élaborée dans les années 1970 (A). Celle-ci a été considérablement renforcée après les attentats du 11 septembre 2001 (B).

A – La construction d'un droit dédié aux interceptions électroniques

L'interception des communications n'est pas une problématique apparue avec l'avènement de l'âge de l'informatique. Cependant, la diffusion de l'internet auprès du grand public a permis de démultiplier les opportunités liées à l'interception des communications. Si le « cassage » des codes semble être de plus en plus compliqué, il apparaît toutefois qu'une infime minorité d'utilisateurs de l'internet se préoccupe de la sécurisation de leurs communications, ce qui permet des interceptions plus efficaces. En effet, les *VPN (Virtual Private Networks)* sont relativement peu connus du grand public. Les américains, pionniers du réseau internet, ont très vite pris conscience des opportunités militaires, politiques, diplomatiques et commerciales offertes par ce nouveau mode de transmission des informations. Si 1978 reste, pour la France, une année charnière pour la protection des données personnelles (loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), 1978 est également l'année *« FISA » (Foreign Intelligence Surveillance Act).*

Cette loi fédérale est la première pierre d'un édifice entièrement dédié aux interceptions de communications électroniques, et vise l'obtention d'informations détenues par des « puissances étrangères ». Certes, si cette expression englobe notamment les nations qui ne sont pas reconnues par la diplomatie américaine ou les organisations terroristes, elle englobe tous les pays étrangers[142]. Le champ d'application de cette loi fédérale est donc particulièrement large. Conçue pour assurer l'efficience des services de renseignements américains tout en limitant les violations du quatrième amendement de la Constitution[143], cette loi donne la possibilité au Président, à travers le ministre de la Justice et avec son autorisation, d'ordonner « la surveillance électronique sans autorisation judiciaire » afin de pouvoir récolter des informations détenues par une puissance étrangère. Certes, en 1978, l'internet n'était pas encore déployé dans les foyers. Cependant, cette loi a permis d'introduire très tôt un régime juridique qui sera modifié au cours des années 2000 (cf. *infra*).

Dans de nombreuses hypothèses, la délivrance d'une autorisation judiciaire est requise. Ainsi, une Cour spéciale est créée par la loi de 1978 : en effet, la section 103 prévoit notamment que « le Président de la Cour suprême des États-Unis désigne publiquement sept juges de cours fédérales provenant de sept circuits judiciaires qui constitueront une cour qui aura pour juridiction l'entente des demandes et la délivrance des ordres autorisant la surveillance électronique n'importe où sur le territoire américain ». Si le nombre de juges a été modifié après les attentats du 11 septembre 2001 *(USA PATRIOT ACT – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001),* cette Cour demeure au centre des interceptions électroniques.

B – Le renforcement des lois antiterroristes : le traumatisme du 11 septembre 2001

Si les interceptions d'informations étaient largement répandues durant la période de la Guerre froide (notamment par la « Peur Rouge » du maccarthysme), celles-ci visaient explicitement des personnes suspectées – à tort à ou à raison – d'espionner pour le compte de puissances étrangères. Or, le 11 septembre 2001 va permettre aux États-Unis de déployer des moyens juridiques autorisant l'interception massive de communications électroniques. L'interception de communications électroniques émises par des citoyens américains est, en théorie, soumise à une

142 « *A faction of a foreign nation or nations, not substantially composed of United States persons ; », Foreign Intelligence Surveillance Act of 1978,* Titre 1, section 101, (a), (2).

143 « Le droit des citoyens d'être garantis dans leur personne, leur domicile, leurs papiers et leurs effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou déclaration, ni sans que le mandat décrive particulièrement le lieu à perquisitionner et les personnes ou les choses à saisir », MELIN-SOUCRAMANIEN (F.), *Les grandes démocraties – Constitutions des États-Unis, de l'Allemagne, de l'Espagne et de l'Italie – Textes présentés par Ferdinand Mélin-Soucramanien,* Éd. Armand Colin, 2005, p. 16.

procédure stricte. En revanche, les communications émanant d'un territoire étranger ne font pas l'objet d'une procédure aussi stricte. La convergence opérée par le déploiement d'internet (voix sur IP, courrier électronique, transmission de fichiers, etc.) a permis d'améliorer l'efficacité des dispositions relatives aux interceptions. Ainsi, comme le note Claudine Guerrier, « les technologies existent depuis longtemps pour contrôler le corps social aux États-Unis et à l'étranger. Les attentats du 11 septembre 2001, très largement médiatisés, ont permis de faire avancer l'exploitation desdites technologies »[144].

Les attentats de 2001 sont à l'origine d'un durcissement de la législation relative aux interceptions de communications électroniques. Le texte le plus important est sans aucun doute le *USA PATRIOT ACT,* signé par Georges W. Bush le 26 octobre 2001. La lutte contre le terrorisme a en effet permis l'émergence de nouvelles dispositions juridiques renforçant les dispositions déjà existantes en matière de communications électroniques. Le *USA PATRIOT ACT* a une portée qui « ne s'arrête pas aux frontières américaines »[145]. L'impact sur l'internet est réel : « certaines de ses dispositions peuvent affecter l'usage d'internet, la sécurité informatique, et la protection des infrastructures essentielles »[146]. De nombreux acteurs économiques sont impactés par les dispositions du *USA PATRIOT ACT*, comme les sociétés de câbles ou les *ISP (Internet Service Providers).* Ces derniers, situés au centre du circuit d'interception de données échangées sur l'internet sont en effet particulièrement concernés. La section 216 du *USA PATRIOT ACT* autorise en effet les *ISP* à délivrer des informations, si ceux-ci estiment « qu'il y a un danger immédiat de mort ou de graves blessures physiques »[147]. Cependant, l'autorisation devient une obligation lorsque ces informations doivent être transmises à une « entité gouvernementale, sous certaines conditions »[148].

Le *FISA* fut également modifié : quelques années après les attentats du 11 septembre 2001, ses dispositions furent renforcées. En 2007, le Congrès des États-Unis a adopté le *PAA (Protect America Act).* Celui-ci amenda certaines dispositions du *FISA* afin de pouvoir viser spécifiquement les communications de toute personne ne se situant pas sur le territoire américain. Si la durée de vie du *PAA* était limitée, comme les différents contrats *(Memorandum Of Understanding)* conclus avec

144 GUERRIER (C.), « PRISM est-il conforme au droit ? », *RLDI,* 2013, 97, pp. 66-67.

145 LORNA (S.), « L'externalisation et la circulation transfrontalière des données : Défi de la protection des renseignements personnels dans le cadre du USA PATRIOT ACT », *Revue Internationale des Sciences Administratives,* 2007/4 Vol. 73, p. 584.

146 SMITH (M. S.), SEIFERT (J. W.), MCLOUGHLIN (G. J.), MOTEFF (J. D.), « The Internet and the USA PATRIOT ACT : Potential Implications for Electronic Privacy, Security, Commerce, and Governement », *Congressional Research Service, The Library of Congress,* RL31289, 2002, deuxième de couverture.

147 *Ibid.*, p. 17.

148 *Ibid.*, p. 17.

le *Department of Commerce*, il fut décidé de conserver cette faculté stratégique. Le *FISAA (Foreign Intelligence Surveillance Amendment Act of 2008)* fut adopté en 2008. L'objectif était alors de mettre en place, de manière légale, une surveillance de masse « spécifiquement orientée vers les données de citoyens non-américains localisés en dehors des États-Unis »[149]. Selon l'auteur de l'étude citée, M. Caspar Bowden, les nouvelles dispositions introduites sont particulièrement importantes, et leur impact sur les droits et libertés fondamentaux des citoyens excessivement larges : « […] FISAA permet à la NSA (National Security Agency) de demander aux grands fournisseurs cloud d'installer des dispositifs permanents pour scanner toutes données qu'elles gèrent en dehors des États-Unis »[150]. Un article de madame Jennifer Granick, directrice du Centre des libertés civiles de l'Université américaine de Stanford, précise que les modalités de surveillances introduites par le *FAA* sont particulièrement étendues, et présentent un réel danger, et ce tant pour les citoyens non-américains que pour les citoyens américains[151]. En effet, en s'appliquant aux entités étrangères, aux personnes physiques non-américaines ou encore aux citoyens américains, le champ d'application du *FAA* est particulièrement large, d'autant plus que cette « captation » de données s'opère tant sur les appels téléphoniques que sur le réseau internet. En effet, si le *FAA* se concentre sur les services basés sur le *cloud*, la captation de données touche à l'un des nouveaux usages de l'internet. En décembre 2012, le *FAA* fut prolongé pour une nouvelle période de cinq ans.

§2 – L'influence de la législation et de la jurisprudence américaines sur les législations européennes

La législation américaine a pu constituer une source directe pour l'élaboration de lois nationales (A). De même, les actualités font craindre l'élaboration d'une législation européenne dont les dispositions pourraient être similaires aux dispositions américaines (B).

A – La législation américaine, source pour les législations des États membres de l'Union européenne

La législation américaine peut également constituer une source importante pour l'élaboration de lois de pays européens. L'exemple le plus pertinent est sans aucun doute l'exemple celui du Royaume-Uni. Allié indéfectible des États-Unis, le Royaume-Uni s'est doté d'un véritable « arsenal

149 BOWDEN (C.) *et alii*, « The US surveillance programmes and their impact on EU citizens' fundamental rights », note au Parlement européen, septembre 2013, p. 12.

150 KALLENBORN (G.), « Comment les États-Unis légitiment la cybersurveillance mondiale, entretien avec Caspar Bowden », www.01net.fr, mis en ligne le 21 janvier 2013, consulté le 25 mai 2014, disponible à l'adresse <http://www.01net.com/editorial/584637/comment-les-etats-unis-legitiment-la-cybersurveillance-mondiale/>

151 GRANICK (J.), « The FISA amendments act authorizes warrantless spying on americans », https://cyberlaw.standford.edu/blog, mis en ligne le 5 novembre 2012, consulté le 25 mai 2014, disponible à l'adresse <https://cyberlaw.stanford.edu/blog/2012/11/fisa-amendments-act-authorizes-warrantless-spying-americans>

juridique » permettant aux États-Unis de déployer efficacement une influence sur les utilisateurs européens d'internet. Au cours de cette étude, nous n'aborderons pas l'aspect extra-juridique (liens entre le *GCHQ* et les agences de renseignement américaines). Les liens existants entre les agences américaines et le *GCHQ* ne sont pas une problématique récente. Ainsi, un parlementaire européen avait déjà fait le lien, en 1998, entre le Royaume-Uni et les États-Unis[152]. La préoccupation du Royaume-Uni pour l'interception de communications n'est pas nouvelle, comme en atteste le *Interception of Communications Act 1985.*

Les États-Unis peuvent légalement intercepter des communications électroniques en utilisant le réseau mondial. Le Royaume-Uni dispose du *Regulation of Investigatory Powers Act 2000 (RIPA).* Cette loi traite de la surveillance électronique, et a été révisée en 2003, et donc après le traumatisme du 11 septembre 2001. Ainsi, de nombreuses dispositions s'appliquent aux données (contenus, fichiers, métadonnées, *etc.*) transitant *via* l'internet. Cette loi est particulièrement importante, puisqu'elle autorise une obtention aisée de données par les agences gouvernementales. De nombreuses hypothèses autorisent en effet l'obtention de données : l'intérêt de la sécurité nationale, la prévention d'un crime, la sécurité publique, la protection de la santé publique, la prévention d'une mort immédiate, ou tout simplement la collecte des impôts[153]. *RIPA* est une loi permettant l'interception massive de communications électroniques. Les données échangées *via* l'internet sont particulièrement impactées :

« RIPA 2000 is of concern to UK Internet Service Providers that may be required to install interception 'black box' devices as part of the UK's government interception framework »[154].

Ainsi, les organisations visées par la loi peuvent obtenir très aisément les communications d'une personne spécifique.

Les opérateurs de communications (postales ou électroniques) peuvent également être tenus de maintenir une « capacité d'interception » (section 12 du *RIPA*). De surcroît, les agences gouvernementales ont la possibilité de « requérir d'un opérateur postal ou de télécommunications de divulguer les données liées aux communications […] »[155]. Si l'opérateur ne coopère pas, une injonction peut rendre exécutoire la demande[156].

Le *RIPA* avait été contesté au niveau européen, notamment parce qu'il permettait – sous

152 Rép. du 12 novembre 1998 de la Commission à la QE E-2966/98 du 8 octobre 1998 (question posée par Esko Seppänen à la Commission européenne).
153 Sect. 22, (2), *Regulation of Investigatory Powers Act 2000*, version en vigueur au mois de juin 2014.
154 CHESHER (M.), KAURA (R.), LINTON (P.), *Electronic Business & Commerce*, Ed. Springer London Ltd, Londres, 2003, p. 328.
155 SMITH (G. J. H.), *Internet Law and Regulation*, Ed. Sweet & Maxwell, Londres, 4ème éd., 2007, p. 1014.
156 Sect. 22, (8), *Regulation of Investigatory Powers Act 2000.*

certaines conditions – l'obtention par l'employeur des informations disponibles sur le matériel mis à la disposition du salarié pour l'exécution de la prestation de travail. Finalement, les poursuites furent abandonnées, le Royaume-Uni ayant accepté de renforcer la protection de ses propres citoyens. Cependant, le « cœur » de la loi demeure : ainsi, l'obligation des opérateurs de télécommunications à maintenir une « capacité d'interception » est maintenue.

Cette loi fut particulièrement critiquée. Au-delà des atteintes à plusieurs droits et libertés fondamentaux, ses détracteurs soulignent également qu'elle constitue une sorte de « brèche » dans les libertés. En effet, il apparaît que l'adoption de cette loi, au cours de l'année 2000 (sanction royale du 28 juillet 2000) a permis l'adoption de nouvelles dispositions par la suite. Le *Guardian*, journal britannique constituant une source importante d'informations sur les révélations d'Edward Snowden », note que « quand la loi entra en vigueur en 2000, seulement neuf organisations, en incluant la police et les services de sécurité, étaient autorisées à accéder aux enregistrements, mais les militants de la vie privée disent qu'il y a dorénavant trop d'organisations publiques qui y ont accès. En 2007, il y eut 519 260 réquisitions relatives aux données détenues par les opérateurs téléphoniques ou les fournisseurs d'accès à Internet »[157]. En 2008, la *RIPA* fut renforcée : la liste des organisations pouvant obtenir des communications privées fut élargie. Malgré les révélations d'Edward Snowden, le Gouvernement du Royaume-Uni ne semble toujours pas disposé à réformer le *Regulation of Investogatory Powers Act 2000.*

Il est également nécessaire de mentionner la Loi pour la programmation militaire française adoptée en 2013. En effet, le programme *PRISM* dispose d'une légalité relative en vertu des dispositions du *FAA* de 2008 qui autorise les agences de renseignements à accéder librement aux données des utilisateurs du réseau internet. L'article 20 de la loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale dispose notamment que :

« Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de

157 ANONYME, « Regulation of Investigatory Powers Act 2000 », www.theguardian.com, mis en ligne le 19 janvier 2009, consulté le 24 mai 2014, disponible à l'adresse <http://www.theguardian.com/commentisfree/libertycentral/2009/jan/14/regulation-investigatory-powers-act>

communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ».

La comparaison entre la LPM et le *FAA*, qui enjoint aux opérateurs et aux acteurs tels que Yahoo, Facebook, Apple ou Microsoft démontre ainsi que les deux lois sont relativement proches. Même si les dispositions du *FAA* sont utilisées pour intercepter les communications de citoyens américains, ces dispositions ont pour objectif la captation de données appartenant à des personnes non-américaines. Or, la LPM s'applique aux citoyens français.

B – L'influence de l'élaboration législative et de la jurisprudence

La volonté des États-Unis de conserver leur influence sur le réseau internet peut être illustrée par de nombreuses propositions d'*« Acts »* américains, comme *SOPA (Stop Online Privacy Act)* et *PIPA (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011).* Ces propositions de lois ont été sévèrement critiquées en raison de dispositions susceptibles de protéger les intérêts des entreprises américaines tout en mettant en péril de nombreux droits et libertés fondamentaux. Si ces propositions de lois sont purement américaines, les contestations ont été mondiales, eu égard aux dispositions pouvant impacter des sites non-américains. Par exemple, certaines dispositions du *SOPA* prévoyaient un « blocage » des sites non-américains accessibles au public américain. De même, la section 105 accordait l'immunité aux fournisseurs de services, fournisseurs de systèmes de paiement, opérateurs publicitaires, moteurs de recherche, et à un bureau ou office d'enregistrement « agissant de bonne foi et sur la base de preuves crédibles, qui stopperaient de fournir ou refuseraient de fournir des services à un site Internet mettant en danger la santé publique »[158].

Cependant, les nombreuses propositions de loi américaines ne sont pas les seules à heurter profondément l'opinion publique mondiale. Par exemple, le traité *ACTA (Anti-Counterfeiting Trade Agreement* – ou ACAC – Accord Commercial Anti-Contrefaçon) a également fait l'objet d'une campagne mondiale visant à suspendre la ratification dudit traité par de nombreux Parlements européens en raison de l'opacité des débats lors de son élaboration.

L'autre exemple pertinent est l'exemple relatif à la neutralité du net. Les récentes actualités

158 La proposition de loi *SOPA* peut être consultée librement sur le site de la Librairie du Congrès, à l'adresse <http://thomas.loc.gov/cgi-bin/query/C?c112:./temp/~c112ZugAln>

américaines relatives à la remise en cause totale du principe de neutralité du net illustrent bien le fait que le réseau internet est dans son intégralité lié aux États-Unis : ainsi, lorsqu'une juridiction américaine remet en cause ce principe pourtant fondateur du net et donc de l'internet, l'ensemble des acteurs mondiaux affirment qu'il s'agit d'une remise en cause totale du réseau et de ses principes fondamentaux. Il est ainsi légitime de penser que le modèle souhaité par les États-Unis s'impose à l'ensemble du réseau. Si cette étude se concentre sur l'internet, il convient de remarquer que l'influence américaine sur l'internet s'exerce pleinement sur le web. Le net étant l'une des composantes de l'internet, la problématique de la neutralité du net doit également être abordée.

En effet, le principe de la neutralité du net a été fortement remis en cause par une décision en date du 14 janvier 2014[159]. Cependant, la volonté de certains opérateurs de remettre en cause ce principe fondamental est ancienne. La première victoire de ces opérateurs se situe en avril 2010, lorsque le câblo-opérateur COMCAST réussit à remettre en cause l'autorité de la *FCC*. Cette dernière avait rappelé, par un communiqué de presse, sa volonté de conserver le principe de la neutralité du net. La *FCC* avait cependant estimé que ce principe n'avait pas été remis en cause par la décision *Comcast v. FCC*[160].

Outre les nombreuses réactions de personnalités politiques américaines ou européennes, cette décision a eu un impact extrêmement important sur les internautes. En effet, depuis 2010, le principe de neutralité du net, s'il n'est pas fondamentalement remis en cause, fait l'objet de menaces de plus en plus réelles, et sa disparition est dorénavant ouvertement envisagée. Or, une remise en cause de ce principe aux États-Unis pourrait avoir pour conséquence une remise en cause au niveau mondial. De ce fait, l'Union européenne doit adopter une position forte. Or, les opérateurs et acteurs du numérique américains disposent de nombreux moyens afin d'empêcher l'adoption d'une position unique européenne. Ceux-ci mettent en œuvre de nombreuses campagnes de lobbying. La meilleure illustration constitue sans doute la campagne de lobbying menée lors de l'élaboration du projet de règlement européen relatif aux données personnelles.

Section 2 – Les tentatives internationales et européennes visant à limiter l'influence américaine

Plusieurs pays et puissances régionales tentent de limiter l'influence américaine, qui est

159 *United States Court of Appeals for the District of Columbia Circuit,* 14 janvier 2014, n°11-1355, *Verizon v. Federal Communications Commission.*

160 « Mais la Cour n'a en aucun cas désapprouvé l'importance de la préservation d'un Internet ouvert et libre ; elle n'a également pas fermé la porte aux autres méthodes permettant d'atteindre ce but important », communiqué de presse de la *Federal Communications Commission,* 6 avril 2010, *« FCC statement on Comcast v. FCC decision »,* disponible sur le site http://www.fcc.gov.

source d'inquiétude (§1). Le Brésil se distingue ainsi dans la lutte contre cette influence (§2).

§1 – L'influence américaine, source d'inquiétude pour l'Union européenne

Les interceptions de communications électroniques sont une source de préoccupations pour l'Union européenne. En effet, si nous n'abordons pas dans notre étude l'analyse politique, il convient de noter toutefois que les interceptions opérées par les États-Unis doivent être traitées en fonction des relations commerciales et diplomatiques fortes qui unissent les deux puissances. Les révélations d'Edward Snowden ont soulevé une vague d'inquiétude chez des citoyens habitués à une sécurité virtuelle garantie par des certificats de sécurité ou autres mesures techniques, comme les techniques de cryptage. Les actualités des deux dernières années ont profondément remis en cause le sentiment d'une sécurité garantie par les mesures techniques : vols de données personnelles, usurpation numérique, faille *Heartbleed*, et surtout les révélations d'Edward Snowden, notamment publiées par le *Guardian*. Or, si cette forte remise en cause est récente, il apparaît que l'Union européenne s'est souciée relativement tôt du problème des interceptions électroniques. Ainsi, dans l'arrêt Klass et autres c. Allemagne, la Cour européenne des droits de l'homme note que « […] les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée »[161].

De même, un rapport de 2001 est relatif au système d'interception ECHELON[162]. Ce rapport, intervenant avant les lois post-11 septembre 2001, est d'une grande richesse. Ce rapport permet – ou plutôt, permettait – de minimiser les inquiétudes liées aux interceptions de données transitant *via* l'internet : accroissement de la quantité de données, difficultés techniques pour mettre en place un système d'interception massif, *etc.* Pour autant, le système ECHELON constitue un système d'interception massif. Ce système est constitué par un réseau de bases d'interception dispersées sur la surface du globe et implantées dans des territoires que les États-Unis estiment « sûrs » : Royaume-Uni, Australie, Nouvelle-Zélande, *etc.* Le rôle des alliés des États-Unis dans le déploiement de l'influence américaine sur l'internet sera analysé *infra*. Ce rapport, s'il est lui-même la conséquence d'autres rapports, avait d'ores et déjà attiré l'attention du Parlement européen sur la problématique de l'interception de communications électroniques. Ainsi, le rapport note que « Ce

161 CEDH, 6 septembre 1978, Klass et autres c. Allemagne.

162 SCHMID (G.) et commission sur le système d'interception ECHELON, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI))*, rapport au Parlement européen, 11 juillet 2001, RR\445698FR.

qui compte, c'est qu'il est utilisé pour intercepter des communications privées et économiques mais non militaires »[163]. L'insuffisance de la protection des citoyens contre ces atteintes à leurs droits et libertés fondamentaux avait également pu être soulignée. Au vu de la puissance américaine, seule une réponse européenne avait pu être envisagée. Cette nécessité ne peut être que renforcée après la publication des révélations d'Edward Snowden. Le rapport de 2001 envisageait comme réponse européenne diverses mesures : adoption d'un protocole additionnel « permettant à l'Union d'adhérer à la Convention relative aux droits de l'homme [...] »[164], l'adoption par les États membres de la « Charte des droits fondamentaux en tant qu'instrument contraignant et pouvant faire l'objet de recours afin d'améliorer le niveau de protection des droits fondamentaux [...] »[165], ou encore la conclusion d'une convention entre les États-Unis et l'Union européenne. De même, et il est intéressant de le noter, le rapport envisageait la création d'un « système de contrôle démocratique de la capacité de renseignement européenne autonome ainsi que des autres activités de renseignement connexes au niveau européen, étant entendu que le Parlement européen doit jouer un rôle important dans ce système de contrôle »[166]. Enfin, le rapport préconisait la généralisation de la formation des personnels des institutions, notamment aux mesures de cryptage.

L'inquiétude de l'Union européenne peut également être illustrée par une note réclamée par la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen[167]. Cette note formule plusieurs recommandations à l'attention du Parlement européen. Le rapport souligne que les citoyens européens disposent d'une protection juridique insuffisante et inefficace en la matière. Par exemple, le *Safe Harbor* ne peut protéger efficacement les citoyens européens face aux dispositifs – légaux, donc – utilisés par les agences de renseignements américains. Le rapport recommande notamment un renforcement de l'information des utilisateurs, une renégociation avec les États-Unis des textes relatifs à l'utilisation des données, et une réponse européenne en matière de *cloud*, mais également une politique européenne forte en matière de données personnelles[168].

Enfin, il convient de noter que l'inquiétude de l'Union européenne est également perceptible à travers des résolutions : par exemple, la résolution en date du 4 juillet 2013 est relative aux programmes de surveillance américains[169]. Par cette résolution, le Parlement européen a fait part

163 *Ibid.*, p. 145.
164 *Ibid,* p. 149.
165 *Ibid.*, p. 149.
166 *Ibid.*, p. 150.
167 BOWDEN (C.) *et alii,* « The US surveillance programmes and their impact on EU citizens' fundamental rights », note au Parlement européen, *op. cit.*
168 *Ibid.*, p. 28.
169 Résolution du Parlement européenne du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union, 2013/2682(RSP).

« tout en confirmant son soutien sans faille aux efforts transatlantiques déployés en matière de lutte contre le terrorisme et la criminalité organisée », des « graves inquiétudes que lui inspirent tant le programme *Prism* que les autres programmes similaires, dès lors que, si les informations actuellement disponibles venaient à être confirmées, ces programmes pourraient constituer une grave violation du droit fondamental à la vie privée et à la protection des données dont peuvent se prévaloir les citoyens et les résidents de l'Union, ainsi qu'une violation de la vie privée et familiale, de la confidentialité des communications, de la présomption d'innocence, de la liberté d'expression, de la liberté d'information et de la liberté d'entreprise; [...] ». Une fois de plus, l'importance stratégique d'une politique européenne est soulignée.

L'Union européenne, dont plusieurs membres sont des alliés militaires, diplomatiques, commerciaux et culturels historiques, est au centre de toutes les attentions. L'appui de l'Union est est effet nécessaire pour l'évolution du débat sur la gouvernance d'internet ainsi que sur la limitation de l'influence américaine. Le règlement européen relatif à la protection des données personnelles a ainsi fait l'objet d'une intense campagne de lobbying, dans laquelle modèles européen et américain ont été confrontés.

§2 – Les initiatives internationales visant à limiter l'influence américaine sur l'internet : l'exemple du Brésil

Plusieurs pays tentent de limiter l'influence exercée par les États-Unis sur l'internet. Ainsi, la Chine et la Russie tentent de promouvoir des réseaux plus « nationaux » afin de pouvoir déployer leur propre influence sur l'internet. Les initiatives de ces deux pays sont, de manière générale, contraire aux idéaux démocratiques qui animent – ou qui devraient – animer la gouvernance d'internet. En revanche, d'autres pays privilégient une approche plus protectrice des droits de leurs citoyens. Une fois de plus, le Brésil se distingue particulièrement des autres pays. Sous l'impulsion de sa présidente Dilma Rousseff et des révélations relatives aux programmes de surveillance électronique, le Brésil s'est doté d'une loi particulièrement innovante. Cette dernière est la *« Marco Civil da Internet »*[170]. Si cette loi a été érigée par ses partisans comme une réponse efficace à l'influence américaine, il convient de noter que l'élaboration de cette loi a débuté en 2010. Présentée comme la « Constitution de l'Internet », cette loi contient de nombreux principes assurant une meilleure protection des citoyens.

L'article 3 de la *« Marco Civil »* dispose notamment que l'utilisation de l'internet est guidée

170 Brazilian Civil Rights Framework for the Internet, loi n°12.965 du 23 avril 2014 établissant « les principes, les garanties, les droits et les obligations pour l'utilisation d'Internet au Brésil ». Une version anglaise peut être trouvée sur le site <http://direitorio.fgv.br>. Les traductions libres réalisées dans cette étude sont tirées de cette version anglaise.

par plusieurs principes : la liberté d'expression, de communication et de pensée, la protection de la vie privée, la protection des données personnelles, tout comme la préservation « de la stabilité, de la sécurité et du fonctionnement du réseau [...] ». Le chapitre 2, relatif aux « droits et garanties des utilisateurs » est particulièrement innovant. Ainsi, l'article 7 dispose notamment que « l'accès à l'Internet est essentiel pour l'exercice de la citoyenneté ». Le rapprochement avec la décision n°2009-580 DC du 10 juin 2009, relative à la « Loi favorisant la diffusion et la protection de la création sur Internet » est nécessaire. Dans cette décision, le Conseil constitutionnel notait notamment « qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services ». Le Brésil a donc inscrit ce principe dans une loi. Un autre rapprochement peut être opéré avec la situation juridique française en ce que l'article 7, IV°, prévoit la non-suspension de la connexion à l'internet, « excepté si cela est la conséquence d'une dette résultant de son utilisation ». L'article 7 est également innovant en ce qu'il consacre « l'inviolabilité de l'intimité et de la vie privée, protégées par le droit à la protection et la réparation des préjudices moraux et matériels résultant de leur violation ». De même, la *« Marco Civil »* réutilise le terme « inviolabilité » afin de protéger les données des utilisateurs :

« II- inviolability and secrecy of the flow of user's communications thought the Internet, except upon a court order, as provided by law ;

III. Inviolability and secrecy of user's stored private communications, except upon a court order ».

Les dispositions relatives aux données personnelles sont similaires – mais non identiques – en certains points aux dispositions françaises contenues dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, comme l'information des utilisateurs sur l'utilisation de leurs données personnelles ou l'interdiction de communication desdites données à des tierces parties (« excepté en cas de consentement exprès, libre et éclairé ou en accord avec les dispositions légales », article 7, VII°). De même, la loi consacre le principe de neutralité de l'internet (section I du chapitre III).

La *« Marco Civil »* tente également de limiter l'influence américaine en imposant aux entreprises récoltant des données *via* l'internet des dispositions contraignantes. Ainsi, ces entreprises sont tenues de respecter la loi brésilienne pour les opérations « de collection, de stockage, de rétention et de traitement de données ou de communications personnelles lorsque au moins une de ces opérations est réalisée sur le territoire national » (article 11). De même, la nationalité de

l'entreprise réalisant ces opérations importe peu, si les utilisateurs brésiliens peuvent avoir accès à ses services ou si un « membre de son groupe économique est établi au Brésil » (article 11, §2). Malgré la volonté forte du Brésil de limiter l'influence américaine et la consécration de principes forts comme celui de la neutralité du net et de la protection stricte des données personnelles, certaines dispositions n'ont pu être maintenues, suite à un intense lobbying effectué par les « grands » du secteur. Ainsi, une disposition prévoyait l'obligation de disposer de centres de stockage sur le territoire brésilien pour conserver la copie des données personnelles des citoyens brésiliens[171]. Cette disposition innovante et particulièrement protectrice des droits des utilisateurs n'a pas été maintenue dans la version finale.

De la gouvernance d'internet à la protection des données personnelles en passant par la création de nouvelles « routes câblières », le Brésil est dorénavant sur tous les fronts afin de limiter l'influence américaine. La *« Marco Civil »* a été largement approuvée par de nombreuses associations de défense des libertés numériques, comme la Quadrature du Net, qui a qualifié le projet de loi de « remarquablement progressiste »[172]. Ces associations réclament aujourd'hui l'adoption de lois similaires à la *« Marco Civil »*.

171 SEIBT (S.), « L'offensive anti-NSA du Brésil fait des remous », www.france24.com, mis en ligne le 13 novembre 2013, consulté le 31 mai 2014, disponible à l'adresse <http://www.france24.com/fr/20131113-rousseff-bresil-nsa-espionnage-marco-civil-Internet-polemique-data-center-snowden-ecoute/>

172 ANONYME, « Internet a besoin d'une « Marco Civil » sans compromis au Brésil ! », www.laquadrature.net, mis en ligne le 28 octobre 2013, consulté le 31 mai 2014, disponible à l'adresse <https://www.laquadrature.net/fr/Internet-a-besoin-dune-marco-civil-sans-compromis-au-bresil>

CHAPITRE II

Le renforcement de l'influence américaine *via* des moyens extra-juridiques

Les États-Unis renforcent leur influence en utilisant des moyens extra-juridiques. Ceux-ci peuvent d'une part consister en des moyens *« hardware »* : la première puissance mondiale a ainsi les capacités techniques pour intercepter de manière massive les données transitant sur le réseau (Section 1). Ces moyens peuvent aussi être *« software »* (Section 2).

Section 1 – Le renforcement de l'influence américaine *via* des moyens « hardware »

Les données transitant *via* les câbles sous-marins peuvent aisément être interceptées (§1). Les États-Unis ont également la possibilité d'introduire des « portes dérobées » *(« backdoors »)* sur plusieurs systèmes informatiques reliés au réseau (§2).

§1 – L'interception des données transitant *via i*nternet grâce aux câbles sous-marins

Les câbles sous-marins constituent la « colonne vertébrale » des télécommunications modernes. Entre 95 % et 99 % des communications mondiales sont acheminées par ces câbles (cf. *supra)*. Si les États-Unis ne peuvent influencer que faiblement l'installation, la maintenance et la gestion des câbles, ils peuvent en revanche opérer des interceptions électroniques grâce à ceux-ci. La première puissance mondiale peut opérer de telles interceptions grâce à des moyens légaux, *via* des lois autorisant l'interception de données (cf. *supra*), mais également par des moyens extra-juridiques. Les documents publiés grâce à Edward Snowden permettent de mesurer l'ampleur du phénomène.

Les États-Unis disposent d'une expérience certaine dans l'installation de boîtiers d'interception sur les câbles sous-marins. Ils ont notamment à leur disposition des sous-marins spécialement aménagés pour la « guerre électronique », et donc pour l'installation de tels boîtiers. Cette pratique est ancienne, puisqu'elle permettait de pouvoir réaliser des opérations d'espionnage contre l'URSS à l'époque de la Guerre froide. Ces techniques ont été perfectionnées, et, aujourd'hui, ces opérations sont parfaitement maîtrisées et permettent l'interception d'une somme extrêmement

importante de données, que celles-ci soient téléphoniques ou bien liées à l'internet.

Ces opérations ont récemment été exposées au su du grand public français, en raison de la révélation du « piratage » d'un câble sous-marin appartenant à un consortium dont fait partie l'opérateur français Orange. Ce câble est le SEA-ME-WE-4. Si tous les câbles sous-marins sont d'une importance stratégique élevée, celui-ci est particulièrement important, puisqu'il relie Marseille à Singapour. Ses « branches » atterrissent dans plusieurs pays, et notamment l'Algérie, la Tunisie, l'Arabie Saoudite, le Pakistan, l'Inde, le Sri Lanka, le Bangladesh ou encore la Malaisie. La longueur de ce câble est de plus de vingt mille kilomètres[173]. À la suite de ces révélations, Orange s'est constituée partie civile[174].

Les boîtiers d'interception peuvent être installés directement sur les câbles sous-marins, ce qui requiert une expertise que très peu de pays possèdent. Il est également possible d'installer un système d'interception dans les stations ou atterrissent les câbles sous-marins. Le Royaume-Uni, où atterrissent plusieurs câbles vitaux, collabore avec les agences de surveillance américaines. Le Royaume-Uni a de ce fait adapté une partie de sa législation afin de pouvoir intercepter en toute légalité les données transitant par les câbles sous-marins. Comme le note *Le Monde*, « grâce à une disposition obscure d'une loi datant de 2000, les opérateurs télécom sollicités par le gouvernement britannique sont forcés de coopérer à la surveillance – et empêchés d'en parler publiquement »[175].

Ces pratiques ne sont pas marginales. Au contraire, celles-ci semblent être usitées et maîtrisées : M. Francesco Ragazzi [176] note ainsi que « l'*upstraming* », qui est la pratique consistant à intercepter les données directement à partir des câbles sous-marins, est « le fait des États-Unis, *via* la NSA, mais aussi du Royaume-Uni, qui a placé quelque deux cents de ces dispositifs sur les câbles »[177]. Cependant, il convient de noter que cette pratique ne s'avère nécessaire que dans certains cas, par exemple lorsque le pays souhaitant intercepter des données liées à l'internet ne dispose pas d'un accès direct au câble visé. Le Royaume-Uni dispose en effet de bases d'interceptions à proximité directe des sites « d'atterrissement » des câbles sous-marins, et a mis en

173 GUEUGNEAU (R.), « NSA ; Orange se porte partie civile après le piratage d'un câble sous-marin », www.m.lesechos.fr, date de mise en ligne inconnue, consulté le 11 mai 2014, disponible à l'adresse <http://m.lesechos.fr/redirect_article.php?id=0203214421104>

174 *Ibid.*

175 VAUDANO (M.), « Les câbles sous-marins, clé de voûte de la cybersurveillance », www.lemonde.fr, mis en ligne le 23 août 2013, consulté le 11 mai 2014, disponible à l'adresse <http://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html>

176 Selon le site web du Sénat, M. Francesco Ragazzi est « chercheur associé au centre d'études et de recherches internationales (CERI) de Sciences Po Paris et maître de conférences à l'université de Leiden (Pays-Bas) ».

177 RAGAZZI (F.), « Comptes rendus de la MCI sur la gouvernance mondiale de l'Internet », table ronde, audition du 15 avril 2014. Le texte peut être consulté à l'adresse <http://www.senat.fr/compte-rendu-commissions/20131209/mci_gouvernance.html>

œuvre le programme *« TEMPORA »*. Ce dernier repose sur « l'aspiration massive » de données, par exemple relatives aux appels téléphoniques, aux contenus des courriels ou aux données *Facebook*[178]. Or, ces données sont partagées avec les agences de renseignements américaines : « un total de 850 000 employés de la NSA et les contractuels privés américains disposant de l'autorisation secret défense ont accès aux bases de données du GCHQ »[179]. La quantité de données traitées est toujours plus grande, la construction de nouveaux serveurs étant continuelle.

En 2001, la commission sur le système d'interception sur le système ECHELON notait que « dans la pratique, cela signifie que les États UKUSA *(United Kingdom – United States Communications Intelligence Agreement)* ne peuvent avoir accès qu'à une **partie très limitée** des communications Internet tributaires du câble »[180]. Or, nous nous apercevons que les États-Unis disposent des technologies adéquates pour l'interception de données transitant *via* les câbles sous-marins et qu'ils contrôlent plusieurs sites d'atterrissement des câbles.

§2 – La vulnérabilité des terminaux fixes ou mobiles aux agences de renseignement américaines, vecteur de déploiement de l'influence américaine

L'influence américaine se déploie également *via* d'autres moyens *hardware.* Nous pouvons distinguer les pratiques visant à l'introduction de *devices* dans les terminaux mobiles offrant la possibilité à leur utilisateur d'accéder au réseau, mais également le contrôle d'autres ressources, tels que les satellites, contrôlés par des sociétés américaines.

L'influence américaine est perceptible autant dans la captation de données à la source (c'est-à-dire au niveau des câbles sous-marins) que dans les terminaux se connectant à l'internet. En effet, de nombreuses révélations ont permis d'établir le fait que les États-Unis avaient inséré des *« devices »* dans les terminaux fixes ou mobiles, mais avaient également su exploiter les failles des terminaux.

Les États-Unis disposent des capacités techniques pour opérer une captation massive de données à partir des terminaux fixes ou mobiles. Cette captation peut être réalisée de plusieurs façons : d'une part, en installant des *« devices »* – ou « mouchards » – sur les terminaux, et d'autre part en exploitant des failles ou en créant des *« backdoors »*.

178 MACASKILL (E.), BORGER (J.), HOPKINS (N.), DAVIES (N.), BALL (J.), « GCHQ taps fibre-optic cables for secret access to world's communications », www.theguardian.com, mis en ligne le 21 juin 2013, consulté le 24 mai 2014, disponible à l'adresse <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

179 *Ibid.*

180 SCHMID (G.) et commission sur le système d'interception ECHELON, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI))*, rapport au Parlement européen, *op. cit.*, p. 35.

Les documents publiés grâce au concours d'Edward Snowden ont en effet démontré que les États-Unis avaient mis en place un circuit leur permettant d'installer des « mouchards » sur des ordinateurs avant que ceux-ci soient livrés. Ainsi, les données envoyées et reçues par l'utilisateur de l'ordinateur pouvaient être retransmises immédiatement à la *NSA.*

De même, si le Gouvernement fédéral américain ne peut contrôler seul le *« hardware »,* l'influence des sociétés de droit américain ou contrôlées par des acteurs américains peut lui offrir une réelle assistance en la matière. Nous citerons à titre d'exemple le projet mené par Google dans les satellites.

Google souhaite permettre à des zones défavorisées, comme certaines régions d'Afrique, de se connecter au réseau mondial. Ce projet est basé sur le lancement, pour environ un milliard de dollars, de cent quatre-vingts satellites[181], et sera mené par une société détenue en partie par Google, O3b Networks *(« Other 3 billions »).* Malheureusement, peu d'informations ont été données par Google ou O3b Networks. En revanche, l'Afrique étant un continent stratégique dont le marché des télécommunications est en pleine expansion, il est probable que Google souhaite s'imposer avant la prise de contrôle du marché par les sociétés chinoises, qui investissent massivement en Afrique (cf. l'arrivée de la société Huawei). Or, le modèle porté par Google est le modèle américain. Ce modèle est très régulièrement critiqué, notamment pour la gestion des données personnelles. Ce projet permettrait ainsi à Google d'investir massivement le marché africain en proposant des services basés sur une exploitation massive des données personnelles. Ainsi, ces données pourraient être stockées sur le territoire américain, ce qui aurait pour effet de grandement faciliter leur « traitement ». Il convient par ailleurs de noter que si les grandes sociétés du numérique tentent de remettre en cause leurs liens avec la *NSA* et réclament une réforme de son régime juridique, elles n'ont jamais remis en cause leur propre modèle de gestion des données personnelles. Or, il est certain que les États-Unis ne remettront pas en cause un modèle d'espionnage de cette envergure, comme le montre la récente réforme menée par Barack Obama.

Section 2 – Le renforcement de l'influence américaine *via* des moyens « software »

Le programme *PRISM* démontre que les États-Unis, s'il semblent disposer à accroître l'indépendance de l'*ICANN,* ne souhaitent pas pour autant renoncer à leur maîtrise du réseau (§1). Le contrôle du réseau par les États-Unis est ainsi garanti par ses alliés (§2) ou par les sociétés de

181 TALBOT (D.), « How Google Could Disrupt Global Internet Delivery by Satellite », www.technologyreview.com, mis en ligne le 4 juin 2014, consulté le 15 juin 2014, disponible à l'adresse <http://www.technologyreview.com/news/527831/how-google-could-disrupt-global-Internet-delivery-by-satellite/>

droit américain (§3).

§1 – Le programme « Prism »

Le programme *PRISM* est un programme de surveillance électronique massive mis en œuvre par la *NSA* et le *GCHQ*. Son existence a été révélée par Edward Snowden grâce à la collaboration de plusieurs journaux, comme le *Washington Post* ou le *Gardian*. Ce programme se démarque des autres programmes de surveillance par sa légalité – relative. En effet, il apparaît que l'arsenal juridique mis en place par les États-Unis autorise la captation de données en vue d'une surveillance massive. Le *FAA* autorise les services de renseignements américains à réclamer aux fournisseurs d'accès à l'internet et aux grands acteurs du numérique (Facebook, Microsoft, Apple, *etc.*) les données liées aux utilisateurs, et l'article 215 du *PATRIOT ACT* constituerait la base légale de la captation massive de données téléphoniques[182]. De même, *PRISM* a été autorisé par la *FISC*[183]. Malgré l'existence de nombreux autres programmes de surveillance utilisant le réseau internet, *PRISM* a été le plus commenté. L'ampleur et l'exploitation des nouveaux usages de l'internet permettent en effet d'ériger *PRISM* comme le symbole de la société de surveillance. Ainsi, ce programme a fait l'objet de nombreuses questions parlementaires. Par exemple, la députée Isabelle Attard rappelait que ce programme « permet au gouvernement américain d'accéder aux données des serveurs des géants de l'informatique : Google, Facebook et d'autres lui fourniraient, sur simple demande, tous les renseignements personnels, mails ou photos des internautes non américains. La réponse de ces entreprises est que seuls ceux qui ont quelque chose à cacher devraient être inquiets. Le caractère privé des opinions personnelles est pourtant la base de notre démocratie »[184]. *PRISM* constitue un programme *« downstream »* (au contraire des programmes *« upstream »*, qui ont pour objectif la captation des données à partir des câbles ou des satellites). Enfin, l'ampleur du programme PRISM est telle que la *NSA* aurait collecté quatre-vingt-dix-sept milliards d'informations pour le seul mois de mars 2013[185]. Ce programme aurait pu demeurer secret durant plusieurs années. En effet, et comme le note Anne Debet, « le FISA interdit par ailleurs toute

182 MEDINE (D.), COOK (E.C.), DEMPSEY (J.), WALD (P.), *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT ACT and on the Operations of the Foreign Intelligence Surveillance Court*, rapport du Privacy and Civil Liberties Oversight Board, 23 janvier 2014.

183 ROSEN (J.) – professeur de droit à l'Université Georges Washington, « Prism, un défi pour le droit », www.lemonde.fr, mis en ligne 27 octobre 2013, mis à jour le 29 octobre 2013, consulté le 1er juin 2014, disponible à l'adresse <http://www.lemonde.fr/technologies/article/2013/10/27/espionnage-de-la-nsa-quels-recours-juridiques-pour-les-citoyens-francais_3503775_651865.html>

184 Rép. Min. à la QE n°952 du 12 juin 2013, *J.O. déb. parl. A.N.* (Q.) du 12 juin 2013, n°6251.

185 ANONYME, « Comprendre le programme "Prism" », www.lemonde.fr, mis en ligne le 11 juin 2013, consulté le 1er juin 2014, disponible à l'adresse <http://www.lemonde.fr/international/infographie/2013/06/11/le-programme-prism-en-une-infographie_3427774_3210.html>

communication publique sur les demandes faites à ces opérateurs »[186].

La réaction de l'opinion publique peut aisément être expliquée par l'ampleur du programme. *PRISM* permet à la *NSA* – et au *GCHQ* – de capter plusieurs types de données : courriels, appels téléphoniques (*via* la *VoIP*) fichiers divers, photos, *etc.* De même, ces données proviennent de plusieurs sociétés qui réunissent plusieurs millions d'utilisateurs : Yahoo, Facebook, Apple, Microsoft (qui fut le premier à collaborer avec la *NSA*), Skype, Aol, ou encore Youtube. De même, *PRISM* donne la faculté à la *NSA* « d'obtenir des communications visées sans les réclamer aux fournisseurs de service et sans obtenir de décisions judiciaires individuelles »[187].

Si *PRISM* a eu un impact conséquent sur l'opinion publique, il apparaît que ce programme n'a pas été le seul. Ainsi, le programme *Xkeystone* mérite également une attention particulière. En effet, ce programme « collecte et suit en temps réel presque tout ce qu'un utilisateur y fait[...]. La sophistication du système est telle qu'elle lui permet de remonter à une personne en partant d'une simple recherche sur Internet suspecte »[188]. De même, l'influence américaine a pu se déployer sur le réseau internet grâce à la mise en œuvre d'autres programmes (comme *Bullrun*), parfois opérés grâce à la collaboration active de pays alliés.

Au-delà d'une crise diplomatique majeure, le programme *PRISM* a également eu un fort impact sur l'opinion publique. De nombreuses entreprises, dont certaines avaient pourtant transmis de nombreuses données à l'agence américaine, ont tenté d'utiliser le programme afin de renforcer leurs liens avec leurs utilisateurs – ou consommateurs. Ainsi, ces entreprises ont affirmé à de nombreuses reprises que leur collaboration constituait une collaboration imposée par la loi. De ce fait, elles auraient transmis les données d'utilisateurs en raison de leur obligation de se conformer à la loi. Le programme *PRISM* aurait du avoir pour conséquence une remise en cause fondamentale des usages de l'internet et *a fortiori* de l'emprise américaine sur le réseau. Or, il n'y a pas eu de désaffectation de la part des utilisateurs. Les sites les plus consommateurs de données (Facebook, services Google, *etc.*) ont en revanche appréhendé la révélation du programme avec une certaine appréhension. Plusieurs sociétés ont ainsi constitué un groupe réclamant une réforme profonde de la *NSA.* Il semble peu probable que les États-Unis, dorénavant favorable à une plus grande gouvernance mondiale du réseau, remettent en cause leurs capacités de captation des données. Les

186 DEBET (A.), « Programme Prism : les citoyens européens sur écoute », *Rec. Dalloz*, 2013, p. 1736.

187 GREENWALD (G.), MACASKILL (E.), « NSA Prism program taps in to user data of Apple, Google and others », www.theguardian.com, mis en ligne le 7 juin 2013, consulté le 1er juin 2014, disponible à l'adresse <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

188 KOCH (S.), « Petit guide des scandales de la NSA », La Tribune de Genève, 31 octobre 2013 (référence trouvée *in* DELEAGE (J-P), « Avec Edward Snowden, l'homme sorti de l'ombre qui voulait éclairer le monde! », Ecologie & politique 1/ 2014, N°48, p. 6).

récentes réformes opérées par Barack Obama n'ont pas permis d'apaiser l'opinion publique. En revanche, il convient de mentionner des volontés de réformes de la part de certains parlementaires américains. Ainsi, l'auteur du *USA PATRIOT ACT,* le député F. James Sensenbrenner Jr., a proposé à la Chambre des députés l'ambitieux *USA FREEDOM ACT (Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring).* Introduite à la Chambre des Représentants le 29 octobre 2013, la proposition de loi avait pour objectif de réformer le *USA PATRIOT Improvements and Reauthorization Act of 2005,* et le *FISA.* La volonté de ses promoteurs était d'instaurer des mesures rendant plus difficiles les écoutes électroniques. Votée par la Chambre des Représentants le 22 mai 2014 à une large majorité, la réforme n'a cependant pas été celle escomptée lors du dépôt de la proposition de loi. En effet, plusieurs dispositions importantes ont été supprimées ou modifiées peu de temps avant le vote, notamment celles relatives à la transparence des sociétés visées par les requêtes émanant de la NSA : « les auteurs de la loi concèdent que celle-ci a été fortement diminuée »[189].

§2 – Les alliés au service de l'influence nord-américaine

Si l'Union européenne, alliée des États-Unis, a fait part à de nombreuses reprises de son inquiétude vis-à-vis des agences de renseignement américaines et de leurs programmes, il apparaît que certains de ces membres sont particulièrement impliqués dans ces programmes. De nombreux pays européens sont en effet également membres de l'OTAN (Organisation du Traité Atlantique Nord). Ainsi, outre les liens diplomatiques basés sur une coopération militaire renforcée (par exemple, la Pologne), des liens basés sur une culture du renseignement émergent. Allié indéfectible des États-Unis, le Royaume-Uni entretient ainsi avec la première puissance mondiale des liens particuliers, notamment basés sur les échanges entre leurs agences de renseignement. Cependant, le Royaume-Uni ne constitue qu'un maillon du système de captation des données. Ce système est doté de plusieurs branches.

La principale branche est constituée par le réseau ECHELON, dont l'existence, maintes fois démentie, est dorénavant avérée. Le réseau ECHELON possède, selon le rapport sur l'existence d'un système d'interception mondial des communications privées et économiques deux caractéristiques principales : premièrement, une capacité de surveillance totale, puisque les données peuvent être captées à partir d'un réseau de satellites-espions ; et, deuxièmement, une implantation mondiale[190].

189 ROBERTS (D.), MCVEIGH (K.), « NSA surveillance reform bill passes House by 303 votes to 121 », www.theguardian.com, mis en ligne le 22 mai 2014, consulté le 7 juin 2014, disponible à l'adresse <http://www.theguardian.com/world/2014/may/22/nsa-reform-bill-usa-freedom-act-passes-house>

190 SCHMID (G.) et commission sur le système d'interception ECHELON, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)*

Le réseau repose en effet sur des bases disséminées sur l'ensemble de la planète et implantées dans des territoires loyaux aux États-Unis : Australie, Canada, Nouvelle-Zélande, Royaume-Uni. Ces pays sont les pays adhérents au traité *UKUSA.*

L'échange entre ces pays est total. Les États-Unis disposent ainsi d'un réseau mondial permettant d'intercepter n'importe quelle donnée : contenu d'un message téléphonique, contenu d'un courriel, données transitant *via* l'internet, *etc.* Or, ce rapport note que le réseau ECHELON « fonctionne dans un espace qui échappe, pour l'essentiel, à toute règle juridique »[191]. Un rapport d'information émanant de la Commission de la défense nationale et des forces armées, présenté par monsieur le député Arthur Paecht, souligne en effet que :

« le développement du réseau Echelon a été multiforme. Tout d'abord, le système n'a pas été conçu pour intercepter seulement certains types de communications comme les messages à caractère militaire lors de la guerre froide, mais il a eu vocation à intercepter de manière indistincte tous les messages dans le monde, quels que soient la nature de leur support et leur contenu, c'est-à-dire y compris les communications privées. Sont donc concernés tous les messages transmis par écrit (télex, fax, plus récemment courrier électronique) et par ondes hertziennes. Depuis le développement des téléphonies mobiles et le recours aux satellites, ce sont également les communications « vocales » qui sont susceptibles d'être interceptées »[192].

Ainsi, toute communication est susceptible d'être captée par les États-Unis. Ces derniers possédant les technologies adéquates afin de briser toute mesure technique de protection (par exemple, des programmes de cryptage), il apparaît qu'aucune donnée n'est sécurisée. Il est intéressant de noter que si l'internet est le fruit de la rencontre entre l'armée et la science *(DARPA)*, celle-ci donne également les moyens aux États-Unis de briser tout cryptage, notamment *via* les technologies quantiques, et donc de mettre en péril les libertés individuelles.

§4 – Les acteurs du numérique, alliés des États-Unis

Les États-Unis tentent également de conserver leur maîtrise du réseau internet *via* des moyens légaux grâce à la pratique du lobbying que la première puissance mondiale exerce auprès de diverses institutions, notamment européennes et internationales. L'exemple susceptible d'illustrer pertinemment cette pratique maintes fois critiquée est la campagne américaine de lobbying exercée auprès des institutions européennes travaillant sur le règlement européen relatif aux données

(2001/2098(INI)), rapport au Parlement européen, *op. cit.*, p. 27.

191 *Ibid.*, p. 26.

192 PAECHT (A.), Rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, rapport à l'Assemblée nationale, 11 octobre 2000, pp. 14-15.

personnelles. Au-delà des agissements du Gouvernement fédéral américain, c'est la campagne menée par les entreprises américaines qui doit être au centre de notre attention. En effet, ces sociétés promeuvent un modèle de l'internet qui garantit la conservation de l'influence américaine. Ainsi, ces grands acteurs du numérique exercent le lobbying auprès d'institutions internationales afin de garantir la conservation du modèle américain relatif aux données personnelles ou de permettre l'élaboration d'un modèle européen beaucoup moins exigeant. Cette campagne a été menée par les sociétés qui ont basé leur modèle sur une exploitation massive des données personnelles : Facebook, Google, Yahoo, *etc.*

La protection de ce modèle implique l'absence de toute contrainte juridique sur cette exploitation de données : les sociétés qui dominent le numérique – la plupart étant américaines – tentent de protéger leur modèle d'un protectionnisme européen : « Selon eux, ces mesures bureaucratiques sont en fait un nouveau type de « barrières non tarifaires » – une forme sournoise de protectionnisme commercial »[193]. Si le lobbying des grandes sociétés américaines auprès des institutions européennes n'est pas une pratique récente ou limitée à la sphère du numérique, il semble que ces entreprises sont particulièrement actives.

Par exemple, la consultation du registre de transparence européen[194] illustre l'importance de Google. En effet, la célèbre firme, dont le siège social est au Delaware, a dépensé (« estimation des coûts liés aux activités directes de représentation ») entre un million deux cent cinquante mille et un million cinq cent mille euros entre janvier 2013 et décembre 2013. De même, Facebook – *Facebook Ireland Limited* – a, entre les mois de janvier 2012 et janvier 2013, dépensé une somme comprise entre quatre cent mille et quatre cent cinquante mille euros. Microsoft, qui a été, semble-t-il, la première entreprise à collaborer avec la *NSA*, dispose d'une équipe de 16 personnes « participant aux activités qui relèvent du champ d'application du registre de transparence », et a dépensé une somme comprise entre quatre millions cinq cent mille et quatre millions soixante-quinze mille euros, sur une période d'un an (entre juillet 2012 et juin 2013). Enfin, Apple a dépensé entre deux cent cinquante mille et trois cent mille euros. Il convient également de noter que certaines sociétés, comme Microsoft, dispose d'une équipe accréditée « pour accéder aux bâtiments du Parlement européen ». Toutefois, il est impossible de déterminer le montant exact investi pour la campagne de lobbying relative au nouveau règlement européen.

193 EUDES (Y.), « Très chères données personnelles », www.lemonde.fr, mis en ligne le 2 juin 2013, consulté le 8 juin 2014, disponible à l'adresse <http://www.lemonde.fr/a-la-une/article/2013/06/02/tres-cheres-donnees-personnelles_3422477_3208.html>

194 Le registre de transparence européen peut être librement consulté à l'adresse <http://ec.europa.eu/transparencyregister/info/homePage.do?locale=fr>

Le modèle économique des puissants acteurs du numérique constitue donc un vecteur de renforcement du modèle américain. L'influence de ce modèle est ainsi « diffusé » par plusieurs moyens. Nous en distinguerons deux. D'une part, ces sociétés innovent fortement en proposant aux internautes des services basés sur le traitement des données personnelles en les diffusant mondialement. Par leur innovation et leur adaptabilité aux « besoins » des utilisateurs, ces services s'imposent progressivement et permettent de développer de nouveaux usages impliquant l'acceptation de conditions générales d'utilisation prévoyant l'utilisation de données personnelles. Ce modèle deviendra ainsi le modèle de référence. D'autre part, les campagnes de lobbying vont permettre d'élaborer des traités internationaux ou des textes nationaux ne remettant pas en cause le modèle économique.

La France prend conscience de cet état de fait. Ainsi, un rapport d'information du Sénat précise que « **L'Europe, ″colonie du monde numérique″, se trouve largement distancée dans cette redistribution des pouvoirs. Sa place est même en recul :** seul 8 groupes européens figurent désormais dans les 100 premiers groupes high-tech dans le monde, contre 12 il y a deux ans »[195].

195 MORIN-DESAILLY (C.), Rapport d'information fait au nom de la mission commune d'information « Nouveau Rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », enregistré à la Présidence du Sénat le 8 juillet 2014, tome 1, p. 10.

CONCLUSION

Malgré les contestations internationales, l'influence des États-Unis sur le droit du réseau internet demeure. Les puissances régionales qui tentent de limiter cette influence sont elles-mêmes soumises à celle-ci. En effet, les intenses campagnes de lobbying réalisées par les grandes sociétés américaines sur les institutions nationales et plus particulièrement européennes ne peuvent que retarder la mise en place d'une législation fondée sur le modèle européen.

Si les programmes d'espionnage sont de plus en plus contestés, il semble que les données réclamées grâce à une législation adéquate aux sociétés de droit américain dans le cadre desdits programmes ne peuvent que permettre la continuation d'une politique attentatoire aux droits et libertés fondamentaux.

Construit selon un modèle américain, l'internet doit dorénavant se développer grâce à une gouvernance internationale. La récente volonté des États-Unis d'accorder à l'*ICANN* une plus grande indépendance ne peut suffire à donner à l'internet un caractère d'indépendance. Comme le montre les actualités jurisprudentielles américaines, le monde scrute la moindre évolution juridique. Ainsi, la neutralité du Net est au centre des préoccupations. Cependant, ces évolutions ne doivent pas occulter la nécessaire réforme en profondeur de la gouvernance d'internet.

L'internationalisation de la gouvernance d'internet et les débats qui en découlent soulignent le risque d'une parcellisation du réseau. En effet, la Russie et la Chine souhaitent posséder leur propre réseau.

Ainsi, la France, et plus particulièrement l'Union européenne, doivent impérativement construire un modèle plus respectueux des idéaux européens. Les nombreux rapports récemment rédigés et remis à l'Assemblé nationale, au Sénat, et aux institutions européennes témoignent de cette prise de conscience. Si celle-ci est tardive, l'opposition de l'Europe aux programmes de surveillance américains et aux propositions de lois américaines démontre une volonté qu'il est nécessaire de maintenir.

En revanche, l'Union européenne doit également tenter de limiter l'influence américaine exercée *via* les grandes sociétés américaines du numérique. Celles-ci, par leur puissance économique, tendent à l'augmentation de l'influence de la première puissance mondiale.

L'Union européenne doit ainsi élaborer un modèle de l'internet basé sur l'internationalisation du réseau.

BIBLIOGRAPHIE

I. Ouvrages généraux et spécialisés

-ACHILLEAS (P)., « Droit international des télécommunications (communications électroniques) », Fasc. 7350, *J.-C. Communication,* 1er décembre 2013.

-*Actes Finals de la Conférence Mondiale des Télécommunications Internationales (Dubaï, 2012)* : UIT, Genève, 2012, 132 p.

-ANONYME, Rapport annuel 2011 de l'*ICANN*, 42 p.

-BOWDEN (C.) *et alii,* « The US surveillance programmes and their impact on EU citizens' fundamental rights », note au Parlement européen, septembre 2013, 40 p.

-CARTER (L.), BURNETT (D.) *et alii,* « Submarine cables and the oceans : connecting the world », rapport de l'*ICPC (International Cable Protection Committee)*, décembre 2009, 68 p.

-CHESHER (M.), KAURA (R.), LINTON (P.), *Electronic Business & Commerce*, Ed. Springer London Ltd, Londres, 2003, 455 p.

-CHICHE (N.), *Internet : pour une gouvernance ouverte et équitable*, rapport au Conseil économique, social et environnemental, 11 décembre 2013, 61 p.

-FÉRAL-SCHUHL (C.), *Cyberdroit, le droit à l'épreuve de l'Internet*, Dalloz, collection Praxis Dalloz, 2008, 997 p.

-GAO *(Government Accountability Office),* « Intelsat Privatization and the implementation of the ORBIT Act », *Report to Congressional Requesters,* septembre 2004, 27 p.

-GAVALDA (Ch.) et SIRINELLI (P.), *Lamy droit des médias et de la communication*, tome 2, Lamy, encyclopédie annuelle, 2013.

-KRUGER (L. G.), *Internet Governance and the Domain Name System : Issues for Congress*, Congressional Research Service, 13 novembre 2013, 26 p.

-MEDINE (D.), COOK (E.C.), DEMPSEY (J.), WALD (P.), *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT ACT and on the Operations of the Foreign Intelligence Surveillance Court*, rapport du Privacy and Civil Liberties Oversight Board, 23 janvier 2014, 238 p.

-MELIN-SOUCRAMANIEN (F.), *Les grandes démocraties – Constitutions des États-Unis, de*

l'Allemagne, de l'Espagne et de l'Italie – Textes présentés par Ferdinand Mélin-Soucramanien, Éd. Armand Colin, 2005, 237 p.

-MORIN-DESAILLY (C.), Rapport d'information fait au nom de la mission commune d'information « Nouveau Rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », enregistré à la Présidence du Sénat le 8 juillet 2014, tome 1, 398 p.

-PAECHT (A.), Rapport d'information sur les système de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, rapport à l'Assemblée nationale, 11 octobre 2000, 89 p.

-SCHMID (G.) et commission sur le système d'interception ECHELON, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI)),* rapport au Parlement européen, 11 juillet 2001, RR\445698FR, 210 p.

-SMITH (M. S.), SEIFERT (J. W.), MCLOUGHLIN (G. J.), MOTEFF (J. D.), « The Internet and the USA PATRIOT ACT : Potential Implications for Electronic Privacy, Security, Commerce, and Governement », *Congressional Research Service, The Library of Congress,* RL31289, 2002, 22 p.

-SMITH (G. J. H.), *Internet Law and Regulation,* Ed. Sweet & Maxwell, Londres, 4ème éd., 2007, 780p.

-VIVANT (M.) et *alii, Lamy Droit du numérique,* Lamy, encyclopédie annuelle, 2013.

II. Articles, contributions, interventions

-ANONYME, « France Télécom Marine devient Orange Marine », communiqué de presse, 16 juillet 2013, disponible à l'adresse <http://www.orange.com/fr/presse/communiques/communiques-2013/France-Telecom-Marine-devient-Orange-Marine>

-ANONYME, « présentation », marine.orange.fr, date de mise en ligne inconnue, mis à jour le 25 février 2014, disponible à l'adresse <http://marine.orange.com/fr/qui-sommes-nous/presentation>

-ANONYME, « Communications sous-marines », www.ifremer.fr, date de mise en ligne inconnue, mis à jour le 24 février 2012, consulté le 13 mars 2014, disponible à l'adresse <http://wwz.ifremer.fr/grands_fonds/Les-enjeux/Les-applications/Communications>

-ANONYME, « Les câbles télégraphiques sous-marins », www.cite-telecoms.com, date de mise en ligne inconnue, consulté le 13 mars 2014, disponible à l'adresse <http://www.cite-telecoms.com/histoire/200-ans-de-telecoms/lage-classique-des-annees-1790-aux-annees-1950/les-

cables-telegraphiques-marins/>

-ANONYME, « Alcatel-Lucent and Sea-Me-We 5 consortium to strengthen ultra-broadband undersea connectivity between Singapore and France », www.alcatel-lucent.com, mis en ligne le 7 mars 2014, consulté le 4 mai 2014, disponible à l'adresse <http://www.alcatel-lucent.com/press/2014/alcatel-lucent-and-sea-me-we-5-consortium-strengthen-ultra-broadband-undersea-connectivity-between>

-ANONYME, « About the National Science Foundation », http://nsf.gov, date de mise en ligne inconnue, consulté le 7 février 2014, disponible sur : <http://nsf.gov/about/>

-ANONYME, « Commerce Department Awards Contract for Management of Key Internet Functions to ICANN », www.ntia.doc.gov, mis en ligne le 2 juillet 2012, consulté le 18 février 2014, disponible à l'adresse <http://www.ntia.doc.gov/press-release/2012/commerce-department-awards-contract-management-key-Internet-functions-icann>

ANONYME, « Department of Commerce Approves Verisign-ICANN .com Registry Renewal Agreement », www.ntia.doc.gov, mis en ligne le 30 novembre 2012, consulté le 27 février 2014, disponible à l'adresse <http://www.ntia.doc.gov/press-release/2012/department-commerce-approves-verisign-icann-com-registry-renewal-agreement>

-ANONYME, « Commerce, ICANN and Verisign agreement in principle », www.ntia.doc.gouv, date de mise en ligne inconnue, consutlé le 27 février 2014, disponible à l'adresse <http://www.ntia.doc.gov/files/ntia/publications/doc_icann_verisign_agreement_05182001.pdf>.

-ANONYME, « E-Mails Suggest Bush Administration Pressured ICANN to Nix'.Xxx Domain », www.foxnews.com, mis en ligne le 24 mai 2006, consulté le 27 février 2014, disponible à l'adresse <http://www.foxnews.com/story/2006/05/24/e-mails-suggest-bush-administration-pressured-icann-to-nix-xxx-domain/>

-ANONYME, « ICANN's First DNSSEC Key Ceremony for the Root Zone », www.icann.org, mis en ligne le 7 juin 2010, consulté le 10 août 2014, disponible à l'adresse <https://www.icann.org/news/announcement-2-2010-06-07-en>

-ANONYME, « Participez à l'Internet Engineering Task Force », www.ietf.org, date de mise en ligne inconnue, consulté le 11 mars 2014, disponible à l'adresse <http://www.ietf.org/about/about-the-ietf-fr.pdf>

-ANONYME, « Constitution d'un panel de haut niveau pour étudier l'avenir de la gouvernance de l'Internet », www.icann.org, mis en ligne le 17 novembre 2013, consulté le 27 février 2014,

disponible à l'adresse <http://www.icann.org/fr/news/announcements/announcement-2-17nov13-fr.htm>

-ANONYME, « La Commission européenne salue la décision américaine de rendre la gouvernance de l'Internet plus indépendante, plus démocratique et plus internationale », www.europa.eu, mis en ligne le 30 septembre 2009, consulté le 3 mars 2014, disponible à l'adresse <http://europa.eu/rapid/press-release_IP-09-1397_fr.htm>.

-ANONYME, « La Commission se propose comme médiateur dans les futures négociations mondiale sur la gouvernance de l'Internet », communiqué de presse mis en ligne le 12 février 2014, consulté le 3 mars 2014, disponible à l'adresse <http://europa.eu/rapid/press-release_IP-14-142_fr.htm>.

-ANONYME, « Regulation of Investigatory Powers Act 2000 », www.theguardian.com, mis en ligne le 19 janvier 2009, consulté le 24 mai 2014, disponible à l'adresse <http://www.theguardian.com/commentisfree/libertycentral/2009/jan/14/regulation-investigatory-powers-act>

-ANONYME, « Internet a besoin d'une « Marco Civil » sans compromis au Brésil ! », www.laquadrature.net, mis en ligne le 28 octobre 2013, consulté le 31 mai 2014, disponible à l'adresse <https://www.laquadrature.net/fr/Internet-a-besoin-dune-marco-civil-sans-compromis-au-bresil>

-ANONYME, « Comprendre le programme "Prism" », www.lemonde.fr, mis en ligne le 11 juin 2013, consulté le 1er juin 2014, disponible à l'adresse <http://www.lemonde.fr/international/infographie/2013/06/11/le-programme-prism-en-une-infographie_3427774_3210.html>

-BACHOLLET (S.), « Gouvernance de l'Internet : au travail ! », www.afnic.fr, date de mise en ligne inconnue, consulté le 3 mars 2014, disponible à l'adresse : <http://www.afnic.fr/fr/ressources/blog/gouvernance-de-l-Internet-au-travail.html>.

-BALL (J.), « Meet the seven people who hold the keys to worldwide Internet security », www.theguardian.com, mis en ligne le 28 février 2014, consulté le 10 août 2014, disponible à l'adresse <http://www.theguardian.com/technology/2014/feb/28/seven-people-keys-worldwide-Internet-security-web>

-BAKER (J.), « ICANN's cozy relationship with the U.S. must end, says European Union », www.pcworld.com, mis en ligne le 12 février 2014, consulté le 27 février 2014, disponible à

l'adresse <http://www.pcworld.com/article/2097120/icanns-cosy-relationship-with-the-us-must-end-says-eu.html>

-BENHAMOU (B.), « Organiser l'architecture de l'Internet », www.diplomatie.gouv.fr, date de mise en ligne inconnue, consulté le 10 août 2014, disponible à l'adresse <http://www.diplomatie.gouv.fr/fr/IMG/pdf/OrganiserlarchitecturedelInternetBernardBenhamou-2.pdf>, publication initiale dans *Esprit*, mai 2006.

-BONVOISIN (G.), « Câbles Internet sous-marins : plusieurs pays affectés par une rupture », www.cnetfrance.fr, mis en ligne le 2 avril 2013, consulté le 13 mars 2014, disponible à l'adresse <http://www.cnetfrance.fr/news/cables-Internet-sous-marins-plusieurs-pays-affectes-par-une-rupture-39788887.htm>

-BRADNER (S.), « IETF Structure and Internet Standards Process », réunion de l'*IETF* des 24-29 juillet 2011, 81ème réunion de l'*IETF*, Quebec City, Canada, <http://www.ietf.org/meeting/81/documents/81newcomers.pdf>.

-CHAUBET (F.), « La mondialisation culturelle », P.U.F. « Que sais-je ? », 2013, p. 33-62.

-COL (P.), « Du mou dans le câble : conflit ouvert entre les USA et la Chine », www.zdnet.fr, mis en ligne le 16 février 2013, consulté le 8 mai 2014, disponible à l'adresse <http://www.zdnet.fr/actualites/du-mou-dans-le-cable-conflit-ouvert-entre-les-usa-et-la-chine-39787292.htm>

-DAVIES (K.), « Présentation de l'IANA », www.iana.org, mis en ligne le 29 septembre 2008, consulté le 18 février 2014, 6 p., disponible à l'adresse <https://www.iana.org/about/presentations/davies-atlarge-iana101-paper-080929-fr.pdf>

-DEBET (A.), « Programme Prism : les citoyens européens sur écoute », *Rec. Dalloz*, 2013, p. 1736.

-DREYFUS (N.), « La gouvernance de l'Internet L'Icann : entre régulation et gouvernance », *RLDI*, avril 2012, n°81, p.119-122.

-DU MARAIS (B.), « Le service public du nommage », *AJDA*, 2003, p. 1590.

-EFE (Agence), « Undersea Fiber-Optic Cable from Venezuela reaches Cuba », www.laht.com, date de mise en ligne inconnue, consulté le 4 mai 2014, disponible à l'adresse <http://www.laht.com/article.asp?ArticleId=386513&CategoryId=10718>

-EMMOTT (R.), « Brazil, Europe plan undersea cable to skirt U.S. spying », www.reuters.com, mis

en ligne le 24 février 2014, consulté le 8 mai 2014, diponible à l'adresse <http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224>

-ERIC (B.), « Internet et ses frontières en Afrique de l'Ouest », *Annales de géographie*, 2005/5, n°645, p. 557, pp. 550-563.

-EUDES (Y.), « Très chères données personnelles », www.lemonde.fr, mis en ligne le 2 juin 2013, consulté le 8 juin 2014, disponible à l'adresse <http://www.lemonde.fr/a-la-une/article/2013/06/02/tres-cheres-donnees-personnelles_3422477_3208.html>

-FAUSETT (B.), « What is the JPA ? », www.netpolicy.com, mis en ligne le 8 février 2008, consulté le 16 février 2014, disponible à l'adresse : <http://www.netpolicy.com/archives/003909.html>

-FROOMKIN (M.), « Almost Free : An Analysis of ICANN's ″affirmation of Commitments″ », *9 J. on Telecomm. & High Tech. L. 187*, 2011, pp. 187-234.

-GRANICK (J.), « The FISA amendments act authorizes warrantless spying on americans », https://cyberlaw.standford.edu/blog, mis en ligne le 5 novembre 2012, consulté le 25 mai 2014, disponible à l'adresse <https://cyberlaw.stanford.edu/blog/2012/11/fisa-amendments-act-authorizes-warrantless-spying-americans>

-GREENWALD (G.), MACASKILL (E.), « NSA Prism program taps in to user data of Apple, Google and others », www.theguardian.com, mis en ligne le 7 juin 2013, consulté le 1er juin 2014, disponible à l'adresse <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

-GRISET (P.), « Les câbles sous-marins : 150 ans de rebondissements », *La lettre de l'autorité de régulation des communications électroniques et des postes*, mai-juin 2008, n°61, 40 p.

-GRISET (P.), « Un fil de cuivre entre deux mondes : les premières liaisons télégraphiques transatlantiques », *in : Quaderni*, n. 27, Automne 1995, pp. 97-114.

-GUILLAUD (H)., « Chine : vers un grand schisme de l'Internet ? », www.lemonde.fr, mis en ligne le 19 février 2010, consulté le 10 mars 2014, disponible à l'adresse <http://www.lemonde.fr/technologies/article/2010/02/19/chine-vers-un-grand-schisme-de-l-Internet_1308660_651865.html>.

-GUERRIER (C.), « PRISM est-il conforme au droit ? », *RLDI*, 2013, 97, pp. 62-73.

-GUEUGNEAU (R.), « NSA ; Orange se porte partie civile après le piratage d'un câble sous-marin », www.m.lesechos.fr, date de mise en ligne inconnue, consulté le 11 mai 2014, disponible à l'adresse <http://m.lesechos.fr/redirect_article.php?id=0203214421104>

-HEROLD (D.K.), « An inter-*nation*-al Internet : China's contribution to global Internet governance ? », note présentée lors du colloque « A decade in Internet Time: Symposium on the Dynamics of the Internet and Society », 21-24 septembre 2011, Oxford Internet Institute, Oxford University, Royaume-Uni, p 4. Cet article est consultable à l'adresse <http://hdl.handle.net/10397/5782>.

-HOULIN (Z.), « L'UIT-T et la réforme de l'ICANN », document disponible sur le site de l'UIT, 17 avril 2002.

-HUBERT-RODIER (J.), « Satellites : les États-Unis cherchent à accélerer la privatisation d'Intelsat », www.lesechos.fr, mis en ligne le 30 avril 1996, consulté le 15 juin 2014, disponible à l'adresse <http://www.lesechos.fr/30/04/1996/LesEchos/17139-033-ECH_satellites--les-etats-unis-cherchent-a-accelerer-la-privatisation-d-intelsat.htm>

-KALLENBORN (G.), « Comment les États-Unis légitiment la cybersurveillance mondiale, entretien avec Caspar Bowden, www.01net.fr, mis en ligne le 21 janvier 2013, consulté le 25 mai 2014, disponible à l'adresse <http://www.01net.com/editorial/584637/comment-les-etats-unis-legitiment-la-cybersurveillance-mondiale/>

-KOCH (S.), « Petit guide des scandales de la NSA », La Tribune de Genève, 31 octobre 2013 (référence trouvée *in* DELEAGE (J-P), « Avec Edward Snowden, l'homme sorti de l'ombre qui voulait éclairer le monde ! », Ecologie & politique 1/ 2014, N°48, p. 6), pp. 5-12.

-KUERBIS (B.), « A roadmap for globalizing IANA », www.Internetgovernance.net, mis en ligne le 3 mars 2014, consulté le 3 mars 2014, disponible à l'adresse <http://www.Internetgovernance.org/2014/03/03/a-roadmap-for-globalizing-iana/>

-LE GALL (F.), « Les câbles sous-marins de fibre optique », www.ariase.com, date de mise en ligne inconnue, consulté le 4 mai 2014, disponible à l'adresse : <http://www.ariase.com/fr/reportages/navire-cablier-rene-descartes.html>

-LE GALL (J.), « Les trente ans de la Convention des Nations unies sur le droit de la mer (10 décembre 1982 – 10 décembre 2012) – Partie 2 », www.marine-oceans.com, mis en ligne le 8 octobre 2012, consulté le 10 mai 2014, disponible à l'adresse <http://www.marine-oceans.com/les-grands-dossiers-de-marine-et-oceans/3734-les-trente-ans-de-la-convention-des-nations-unies-sur-le-droit-de-la-mer-10-decembre-1982-10-decembre-2012-partie-2>

-LEYDEN (J.), « Campaign to kick NSA man from crypto standards group fails », www.theregister.co.uk, mis en ligne le 8 janvier 2014, consulté le 11 mars 2014, disponible à

l'adresse
<http://www.theregister.co.uk/2014/01/08/nsa_bod_crypto_standard_co_chair_controversy/>

-LORNA (S.), « L'externalisation et la circulation transfrontalière des données : Défi de la protection des renseignements personnels dans le cadre du USA PATRIOT ACT », *Revue Internationale des Sciences Administratives*, 2007/4 Vol. 73, pp. 583-606.

-MACASKILL (E.), BORGER (J.), HOPKINS (N.), DAVIES (N.), BALL (J.), « GCHQ taps fibre-optic cables for secret access to world's communications », www.theguardian.com, mis en ligne le 21 juin 2013, consulté le 24 mai 2014, disponible à l'adresse <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

-MASSIT-FOLLÉA (F.), « La gouvernance de l'Internet. Une internationalisation inachevée », *Le Temps des médias*, 2012/1 n°18. DOI : 10.3917/tdm.018.0029, p. 29-40.

-MOUNIER (P.), « L'ICANN : Internet à l'épreuve de la démocratie », *Mouvements*, 2001/5 no18, DOI : 10.3917/mouv.018.0081, p. 81-86.

-NGUYEN (A.-T.), « Les échanges technologiques entre la France et les États-Unis : les télécommunications spatiales (1960-1985 », *Flux*, 2001/1, n°43, pp. 17-24.

-PARKES (S.), « LUIT participera à la réunion organisée au Brésil sur la gouvernance de l'Internet », www.itu.int, mis en ligne le 20 février 2014, consulté le 3 mars 2014, disponible à l'adresse : <http://www.itu.int/net/pressoffice/press_releases/2014/05-fr.aspx>.

-POHLE (J.), MORGANTI (L.), « The Internet Corporation for Assigned Names and Numbers (ICANN) : Origins, Stakes and Tensions », *Revue française d'études américaines*, 2012-4 n°134, pp. 29-46.

-PULLAR-STRECKER (T.), « Once again, IS blocks porno domain », www.smh.com.au, mis en ligne le 28 mars 2006, consulté le 27 février 2014, disponible à l'adresse <http://www.smh.com.au/articles/2006/03/28/1143441122717.html>

-QIU (W.), « Why It Is China's Turn to Lead the Submarine Cable Industry », www.telecomramblings.com, mis en ligne le 11 février 2014, consulté le 8 mai 2014, disponible à l'adresse <http://www.telecomramblings.com/2014/02/chinas-turn-lead-submarine-cable-industry/>

-RAGAZZI (F.), « Comptes rendus de la MCI sur la gouvernance mondiale de l'Internet », table ronde, audition du 15 avril 2014.

-RAULINE (N.), « Fadi Chehade : ”La gouvernance d'Internet doit s'inspirer de ce qu'est Internet”,

entretien avec M. Fadi Chehade, président de l'*ICANN*, www.lesechos.fr, mis en ligne le 21 février 2014, consulté le 27 février 2014, disponible à l'adresse <http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0203332569914-fadi-chehade-la-gouvernance-d-Internet-doit-s-inspirer-de-ce-qu-est-Internet-652224.php>

-RAULINE (N.), « Gouvernance d'Internet : la France appelle à de nouvelles règles », mis en ligne le 14 janvier 2014, consulté le 10 mars 2014, disponible à l'adresse <http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0203243031717-gouvernance-d-Internet-la-france-appelle-a-de-nouvelles-regles-642831.php>.

-ROBERTS (D.), MCVEIGH (K.), « NSA surveillance reform bill passes House by 303 votes to 121 », www.theguardian.com, mis en ligne le 22 mai 2014, consulté le 7 juin 2014, disponible à l'adresse <http://www.theguardian.com/world/2014/may/22/nsa-reform-bill-usa-freedom-act-passes-house>

-ROSEN (J.) - professeur de droit à l'Université Georges Washington, « Prism, un défi pour le droit », www.lemonde.fr, mis en ligne 27 octobre 2013, mis à jour le 29 octobre 2013, consulté le 1er juin 2014, disponible à l'adresse <http://www.lemonde.fr/technologies/article/2013/10/27/espionnage-de-la-nsa-quels-recours-juridiques-pour-les-citoyens-francais_3503775_651865.html>

-ST. AMOUR (L.), discours prononcé le 17 octobre 2013 lors de la conférence sur le cyberespace de 2013, à Séoul, consulté le 27 février 2014, disponible à l'adresse : <http://www.Internetsociety.org/sites/default/files/Seoul%20Conference%20on%20Cyberspace%202013%20Final%20Remarks.pdf>.

-SEIBT (S.), « L'offensive anti-NSA du Brésil fait des remous », www.france21.com, mis en ligne le 13 novembre 2013, consulté le 31 mai 2014, disponible à l'adresse <http://www.france24.com/fr/20131113-rousseff-bresil-nsa-espionnage-marco-civil-Internet-polemique-data-center-snowden-ecoute/>

-STRICKLING (L. E.), lettre adressée au Dr. Stephen D. Crocker le 4 octobre 2012, p.1.

-TALBOT (D.), « How Google Could Disrupt Global Internet Delivery by Satellite », www.technologyreview.com, mis en ligne le 4 juin 2014, consulté le 15 juin 2014, disponible à l'adresse <http://www.technologyreview.com/news/527831/how-google-could-disrupt-global-Internet-delivery-by-satellite/>

-TARDIEU-GUIGUES (E.), « Attribution et contentieux des noms de domaine », *J.-Cl.*

Commercial, Fasc. 805, mis à jour le 23 mars 2011.

-TORRES (I.), « Dilma Rousseff défie le Big Brother américain », www.courrierinternational.com, mis en ligne le 12 mars 2014, disponible à l'adresse <http://www.courrierinternational.com/article/2014/03/12/dilma-rousseff-defie-le-big-brother-americain>

-VAUDANO (M.), « Les câbles sous-marins, clé de voûte de la cybersurveillance », www.lemonde.fr, mis en ligne le 23 août 2013, consulté le 11 mai 2014, disponible à l'adresse <http://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html>

III. Sites Internet

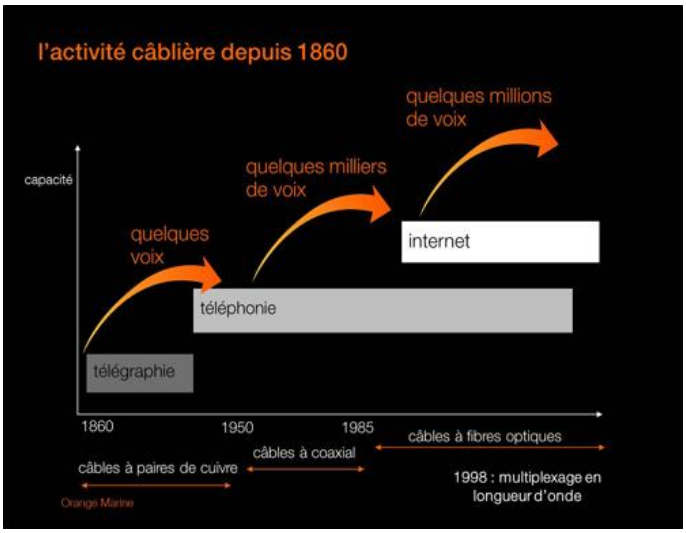
http://www.01net.fr
http://www.afnic.fr
http://www.alcatel-lucent.com
http://www.ariase.com
http://www.assemblee-nationale.fr
https://cyberlaw.standford.edu/blog
http://www.cite-telecoms.com
http://www.cnetfrance.fr
http://www.courrierinternational.com
http://www.diplomatie.gouv.fr
http://direitorio.fgv.br
http://www.foxnews.com
http://www.france24.com
http://www.kiplingsociety.co.uk
http://www.iana.org
http://www.icann.org
http://www.ietf.org
http://www.ifremer.fr
http://www.intelsat.com/services
http://www.Internetgovernance.net
http://www.Internetsociety.org
http://www.itu.int
http://www.lecese.fr
http://www.laht.com
http://www.laquadrature.net
http://www.law.nyu.edu
http://www.lemonde.fr
http://www.lesechos.fr
http://www.marine-oceans.com
http://marine.orange.fr
http://www.netpolicy.com
http://nsf.gov
http://www.ntia.doc.gov
http://www.reuters.com
http://www.senat.fr
http://www.smh.com.au
http://www.submarinecablemap.com
http://www.technologyreview.com

http://www.telecomramblings.com
http://www.theguardian.com
http://www.theregister.co.uk
http://thomas.loc.gov
http://www.zdnet.fr

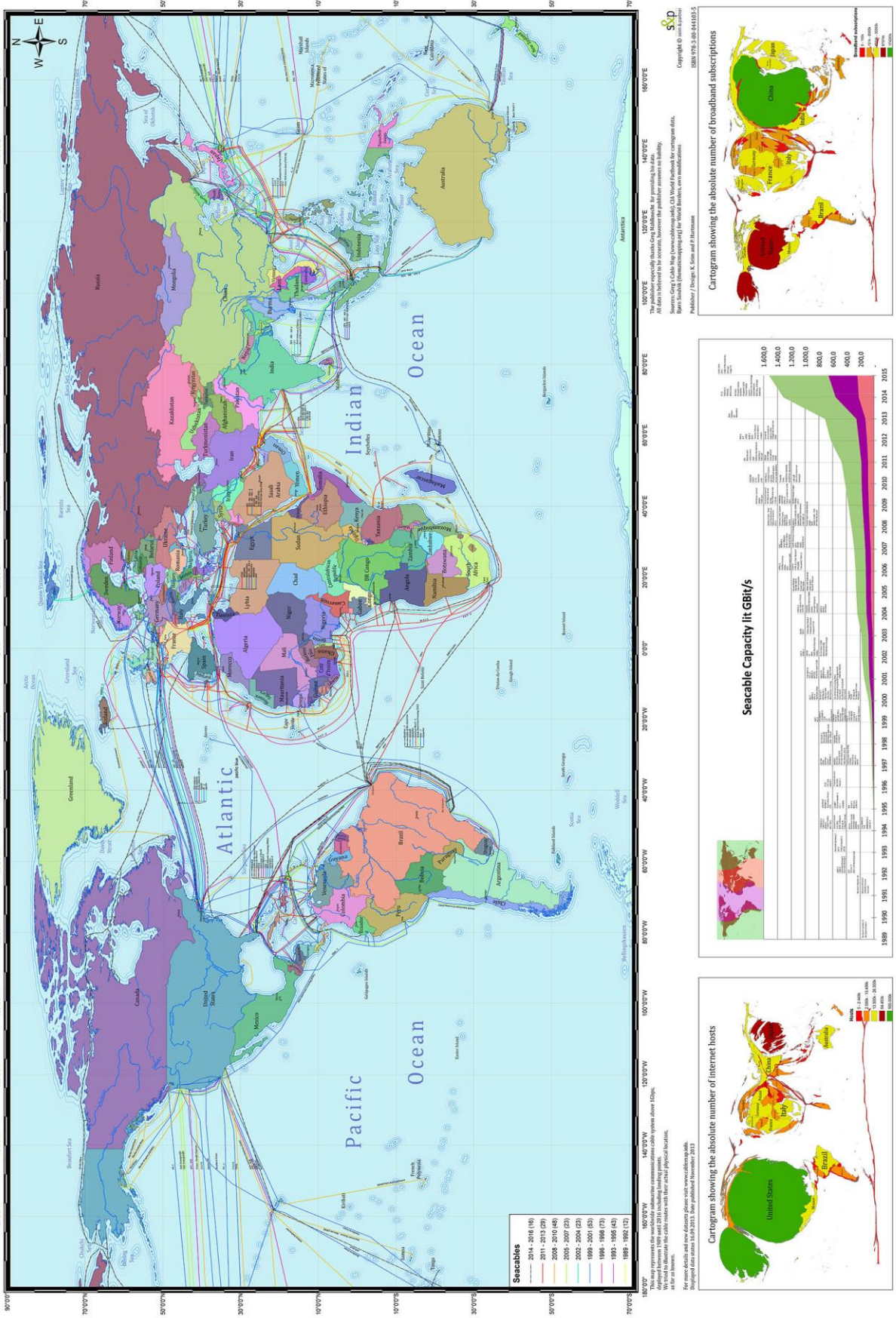
Bases de données

http://www.cairn.info
http://www.dalloz.fr
http://www.europa.eu
http://eur-lex.europa.eu
http://ec.europa.eu/transparencyregister
http://www.lamyline.fr
http://www.lexisnexis.fr

ANNEXES



Source : http://marine.orange.com/fr/qui-sommes-nous/presentation/historique, « évolution technologique depuis 1860 (source Orange Marine 2011)



Source : www.cablemap.info

Table des matières

REMERCIEMENTS **2**

TABLE DES ABRÉVIATIONS **3**

INTRODUCTION **7**

PARTIE I **10**

Les limites de l'influence américaine sur la gestion des infrastructures physiques et la gouvernance d'internet **10**

CHAPITRE I 11

L'influence américaine sur la gestion des infrastructures physiques de l'internet 11

Section 1 – Une influence historiquement limitée pour l'installation et la gestion des câbles sous-marins **11**

§1 – Les câbles sous-marins, des infrastructures au cœur des réseaux de données numériques *11*

A – Les câbles sous-marins, du télégraphe à l'internet 11

B – Les câbles sous-marins, colonne vertébrale stratégique des télécommunications modernes 13

§2 – Une influence américaine limitée *14*

A – Le régime juridique des câbles sous-marins 15

B – Les puissances régionales, frein à l'influence américaine 16

Section 2 – L'influence américaine sur les satellites **19**

§1 – La construction d'Intelsat *19*

§2 – La privatisation d'Intelsat *20*

CHAPITRE II 21

La contestation grandissante de l'influence américaine sur la gouvernance d'internet 21

Section 1 – Une influence américaine toujours très présente **21**

§1 – Le protocole TCP/IP, racine de l'internet *21*

A – L'internet, une construction américaine 21

B – Le protocole TCP/IP 21

§2 – L'ICANN, société de droit californien au cœur de la gouvernance d'internet *22*

A – L'ICANN au cœur de la géopolitique mondiale 22

1 – Les origines de l'ICANN 22
2 – La création de l'ICANN 23
3 – L'influence américaine lors de la création de l'ICANN 25
4 – Les missions de l'ICANN 26
5 – La structure de l'*ICANN* 27

B – L'influence de l'ICANN sur les offices et bureaux d'enregistrement 27

C – Les liens actuels de l'ICANN avec les institutions gouvernementales américaines 29

§3 – L'influence américaine sur l'IETF/ISOC, un groupe informel au cœur de la gouvernance

d'internet *35*
A – Le rôle central de l'IETF/ISOC dans la gouvernance d'internet 35
B – L'influence américaine sur l'IETF/ISOC 36
Section 2 – Les tentatives de limitation de l'influence américaine sur la gouvernance d'internet 36
§1 – Les initiatives institutionnelles visant à limiter l'influence américaine *37*
A – Les appels de l'ICANN à une plus grande indépendance 37
B – Les initiatives de l'Union internationale des télécommunications 38
§2 – Les initiatives régionales et nationales *40*
A – L'appel de puissances régionales pour une gouvernance d'internet globale 40
1 – La position européenne et française 40
2 – La place du Brésil dans le débat sur la gouvernance d'internet 42
B – Les initiatives de création de réseaux internet régionaux : les exemples chinois et russe 43
1 – Le « Great Firewall » chinois, muraille contre « l'impérialisme américain » 43
2 – L'internet russe, un outil au service de la censure 44
PARTIE II 46
Le renforcement de l'influence américaine sur l'internet *via* des moyens juridiques et extra-juridiques 46
CHAPITRE I 47
Les initiatives juridiques tendant au renforcement de l'influence américaine sur internet 47
Section 1 – La légalisation des interceptions électroniques au cœur de la stratégie américaine 47
§1 – La législation américaine *47*
A – La construction d'un droit dédié aux interceptions électroniques 47
B – Le renforcement des lois antiterroristes : le traumatisme du 11 septembre 2001 48
§2 – L'influence de la législation et de la jurisprudence américaines sur les législations européennes *50*
A – La législation américaine, source pour les législations des États membres de l'Union européenne 50
B – L'influence de l'élaboration législative et de la jurisprudence 53
Section 2 – Les tentatives internationales et européennes visant à limiter l'influence américaine 54
§1 – L'influence américaine, source d'inquiétude pour l'Union européenne 55
§2 – Les initiatives internationales visant à limiter l'influence américaine sur l'internet : l'exemple du Brésil 57
CHAPITRE II 60
Le renforcement de l'influence américaine *via* des moyens extra-juridiques 60
Section 1 – Le renforcement de l'influence américaine *via* des moyens « hardware » 60
§1 – L'interception des données transitant via internet grâce aux câbles sous-marins *60*

§2 – La vulnérabilité des terminaux fixes ou mobiles aux agences de renseignement américaines, vecteur de déploiement de l'influence américaine 62

Section 2 – Le renforcement de l'influence américaine *via* des moyens « software » 63

§1 – Le programme « Prism » 64

§2 – Les alliés au service de l'influence nord-américaine 66

§4 – Les acteurs du numérique, alliés des États-Unis 67

CONCLUSION 70

BIBLIOGRAPHIE 71

ANNEXES 82