Corentin POUSSET-BOUGERE

21403100

Unité 3

Diplôme Universitaire European School of Law

Université Toulouse 1 Capitole

Dissertation sur un sujet de droit comparé :

Quelle Législation pour un cyberespace en constante expansion ?

AVANT-PROPOS

Aux Etats-Unis, une récente affaire criminelle a fait couler beaucoup d'encre en raison d'une demande insolite du F.B.I. (Federal Bureau of Investigation) au cours de son enquête : la victime étant en possession d'une enceinte assistant vocal Echo vendu par Amazon, les agents exigeaient de la compagnie que lui soient remis les potentiels enregistrements qu'un tel appareil connecté aurait pu produire au moment du meurtre[1].

Cette anecdote est un criant témoin des progrès effectués par Internet et le cyberespace, depuis ses balbutiements jusqu'au très en vogue « internet des objets », mais également de son indéniable lien avec le domaine légal ; Internet étant devenu, au fil des années et des évolutions technologiques, un réseau aussi incontournable que tentaculaire dans tous les aspects de la vie courante, l'importance du législateur pour réguler un tel foisonnement d'activité est alors une évidence.

Internet est en effet devenu un réseau de réseaux[2], sans centre névralgique notoire, permettant l'échange de données par un ensemble de protocoles standardisés comme l'email, le peer-to-peer, et surtout le World Wide Web, plateforme ultra populaire de sites privés, publics, universitaires, commerciaux… dont le nombre avoisine aujourd'hui les deux milliards[3]. Il permet également l'envoi quotidien de 400 milliards de courriers électroniques, et connecte entre eux plus de 3 milliards d'êtres humains. Des chiffres faramineux, mais également en croissance constante à un rythme effréné, que l'on peut observer en direct sur le site Internetlivestats.com, sans toutefois parvenir à en prendre la pleine mesure.

Face à un tel déferlement, on peut comprendre la volonté du législateur de rapidement s'emparer de ce nouvel espace d'échange et de communication ; il souhaiterait alors y appliquer un modèle de gouvernance, cette notion définie par Marc Hufty comme « le processus d'interaction et de prise de décision entre les acteurs d'un problème collectif, encadré par la création, la reproduction ou le renforcement de normes sociales et d'institutions légales »[4]. Le problème devient alors qu'Internet, du fait de ses spécificités techniques, sa taille, sa globalité, ne peut que difficilement voir appliquer les modèles déjà connus et appliqués par les états-nations.

Il devient dès lors nécessaire de poser la question suivante : **Quelle législation appliquer à un cyberespace en constante expansion ?**

[1] Christopher Mele, "Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns", The New York Times, 28 Décembre 2016
[2] Bill Stewart (ed), « The Living Internet », Janvier 2000.
[3] internetlivestats.com, Real Time Statistics Project, (Worldometers / 7 Billion World)
[4] Marc Hufty, "Investigating Policy Processes: The Governance Analytical Framework (GAF)" In: Wiesmann, U., Hurni, H., et al. eds. Research for Sustainable Development: Foundations, Experiences, and Perspectives." (2011) Bern: Geographica Bernensia: 403–424.

Pour tenter d'apporter des éléments de réponse à cette question, il convient d'abord d'examiner l'histoire d'Internet et des modèles théoriques qui y sont attachés (I), avant de s'attarder sur les différentes facettes du cyberespace moderne, les challenges qu'il présente et les solutions que le droit peut y apporter : l'équilibre entre Données personnelles et sécurité (II), la régulation de l'usage de ces même données par les entreprises privées (III), la controversée question de la neutralité du réseau (IV), et enfin le contrôle de l'extraordinaire essor des parties commerciales et criminelles (V) de l'internet. Si une attention particulière sera bien entendu apportée au primordial aspect juridique de ces problématiques, ne pas mentionner les importantes influences sociales, politiques et techniques reviendrait à n'y répondre que partiellement.

I / La complexe application du droit au cyberespace : quelques modèles de gouvernance

Il est aujourd'hui facilement démontrable qu'Internet ne saurait être gouverné par la simple application des lois existantes (1) ; tout au long de son histoire, la doctrine a proposé des solutions pour combler ce vide et permettre cette gouvernance, d'abord par une approche très libertaire (2) puis, confrontée aux limites de cette méthode, par un système plus encadré par le droit national (3).

1. Internet, ou l'échec du droit dans une juridiction inédite

L'histoire d'Internet est faite à la fois de recherche et de découvertes scientifiques, de la coopération entre les auteurs de ces découvertes, et de la fusion de nombreuses infrastructures et systèmes de télécommunication préexistants. Comme le dit l'un de ses pères fondateurs, Vinton Cerf, « L'effort de développement d'Internet fut international dès ses débuts »[5], une globalité évidemment reflétée dans le réseau actuel. Après sa création et ses premiers balbutiements, il est possible de constater deux vagues majeures d'expansion du « réseau de réseaux » qu'est devenu Internet : les années 60-70, ou les infrastructures sont mises en place et des innovations comme le protocole TCP/IP de Mr Cerf permettent l'échange de données ; puis, l'explosion des années 1990 et du World Wide Web, qui provoque l'enthousiasme du grand public et mène à la prolifération de sites qui se poursuit encore aujourd'hui[6].

C'est bien cette prolifération, et l'usage de plus en plus standardisé d'internet dans tous les aspects de la vie courante, qui a pu inquiéter le législateur et le pousser à vouloir réguler ce nouvel espace de communication et d'échange. Quel que soit sa nation d'origine, il se heurta dès lors a une réalité simple : il est impossible de simplement transposer à Internet l'ensemble des lois existantes, du fait de sa spécificité.

Un exemple simple de ce problème est l'application du concept de juridiction : l'ensemble des critères qui, inscrits dans les textes légaux, résulte en la compétence d'un tribunal pour connaître certains faits. Cette compétence peut donc être basée sur une variété de critères, les plus communs étant matériels (comme celle du tribunal de

[5] Vinton Cerf, « How the Internet Came to Be », pour "The Online User's Encyclopedia," Bernard Aboba, Addison-Wesley, Novembre 1993, ISBN 0-201-62214-9

[6] Ronda Hauben, « The Internet: On its International Origins and Collaborative Vision », 1 mai 2004

commerce, en France[7]) ou territoriaux (un critère souvent retenu en matière de droit du travail, comme au Royaume-Uni qui applique sur ce sujet un test objectif[8]).

C'est l'application de ces critères qui pose un problème lorsqu'on les confronte à un nouveau réseau comme Internet, qui bien souvent les transcende. La notion de territorialité, en particulier, devient obsolète dans le contexte d'un espace mondial interconnecté. Une violation de la loi française, réalisée via un site américain, par un contrevenant résidant en Corée est non seulement tout à fait possible, mais dans les faits relativement courante. Dan Svantesson, de l'université de Bond, résume bien le cauchemar juridictionnel qui résulte d'un tel imbroglio : « la plupart Etats possèdent des règles de Droit International Privé qui leur confère une compétence sur n'importe quel site qui peut être accessible depuis leur territoire – similairement, [ils] disposent également de législations les autorisant à appliquer leur propre droit dans ces cas. »[9]

Ensuite, si Internet a rapidement démontré sa capacité à devenir un facteur important dans la commission de nombreuses infractions (trafics, harcèlements, etc), il introduit également de nouveaux délits qui lui sont propres, et doivent dès lors se voir encadrées par le législateur. En France, le récent cas Blue Touffe pose ainsi la question du téléchargement : s'étant introduit sans manipulation complexe ou logiciel pirate, et ayant simplement copié des données, n'empêchant donc pas leur propriétaire d'en jouir normalement, peut-on simplement se contenter d'accuser le prévenu de vol ? L'avocat général de la Cour de Cassation expose le problème ainsi : « L'article 311-1 du Code pénal définissant le vol comme la soustraction frauduleuse de la chose d'autrui pose deux conditions qui s'avèrent aujourd'hui inadaptées au vol de données ; d'une part, une donnée n'est pas une chose, mais un élément immatériel distinct de tout support de stockage ; d'autre part, une donnée extraite d'un STA à la suite d'un accès ou d'un maintien frauduleux n'est pas nécessairement soustraite de celui-ci mais seulement extraite par sa reproduction sur un autre support. »[10]

Ces problèmes démontrent bien la nécessité d'une forme de régulation sur le cyberespace ; si la doctrine l'avait rapidement compris, la solution de l'Etat comme pourvoyeur de cette régulation ne fait absolument pas l'unanimité, et demeure l'objet d'un débat animé entre deux groupes.

[7] Art L721-3, Code de Commerce français

[8] Green v SIG Trading Ltd., Employment Appeal Tribunal, 2017

[9] Dan Jerker B. Svantesson, « An introduction to jurisdictional issues in cyberspace », 2004, Journal of law, information and science, 15(1), 50-74.

[10] Olivier X. contre Cour d'Appel de Paris, Cour de Cassation, Chambre Criminelle, 20 mai 2015, N° de pourvoi: 14-81336

2. Un Internet auto-régulé : L'idéologie cyber libertaire et ses principaux représentants

D'un côté se trouvent les cyber libertaires, groupe doctrinal qui doit son nom à la journaliste Paulina Borsook[11]. Ce dernier vise à préserver l'aspect unique d'Internet, l'approche collaborative qui a mené à sa naissance et qui aujourd'hui encore fait le succès des forums d'entraides, programmes open source, plateformes de financement participatifs et autres projets partagés. Pour eux, Internet est bien trop différent de la juridiction habituelle du législateur, et devrait être traité par lui comme un Etat indépendant, auto-régulé par ses propres habitants. Cette idéologie est donc basée sur une forte confiance envers les internautes, la capacité qu'ils auront à se modérer mais aussi à se hiérarchiser selon leurs mérites dans la communauté et leur compréhension de l'aspect technique du réseau.

Elle repose sur l'idée que les dirigeants, qu'ils soient politiques ou législatifs, sont incapables d'appréhender et de comprendre ce nouveau réseau et la culture propre qui s'y est formée. Une idée qui par moments ne semble pas sans fondement, lorsqu'on observe la réaction du gouvernement anglais à une plaisanterie sur Twitter dans le cas Paul Chambers, dont la condamnation fera grande polémique et sera finalement reconnue comme une erreur judiciaire[12].

Parmi les membres les plus célèbres de cette doctrine, on trouve Julian Assange, dont le site WikiLeaks a maintes fois prouvé le peu de confiance qu'il accorde aux gouvernements étatiques et l'importance à ses yeux de la justice populaire, en se faisant une spécialité de la fuite d'informations confidentielles au grand public[13] ; mais également John Perry Barlow, auteur qui résume parfaitement sa philosophie dans sa *Déclaration d'indépendance du Cyberespace : « Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Au nom du futur, je vous demande à vous du passé de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté où nous nous rassemblons. »*[14]

Il est possible de dénoter dans ces théories, et la manière dont elles sont formulées, un certain idéalisme ainsi que même pour certains un certain extrémisme. Reposant entièrement sur une confiance absolue en les internautes et leur capacité à s'auto-réguler, afin de soutenir le rejet d'un exercice des formes de pouvoir habituelles, la doctrine cyber libertaire a fait l'objet de nombreuses critiques qui commencent généralement en constatant l'échec de son paradigme : sur Internet, la criminalité existe et se trouve même extrêmement répandue, et il est dorénavant admis que l'internaute ne saurait y faire barrage de lui-même.

---

[11] Paulina Borsook, « Cyberselfish: A Critical Romp Through the Terribly Libertarian Culture of High Tech », Public Affairs, 2000, ISBN 1891620789

[12] Clive Coleman, « Robin Hood Airport tweet bomb joke man wins case », BBC News, 27 Juillet 2012

[13] Helene Gully, « Les dix plus grosses révélations de Wikileaks », Les Echos, 4 octobre 201

[14] John P. Barlow, « Déclaration d'Indépendance du Cyberespace », Traduit et édité par Hache, février 1996

3. Le modèle cyber paternaliste en exercice aujourd'hui, inspiré par les théories déterministes

De l'autre côté du débat se trouve le groupe des cyber paternalistes, selon lequel le cyberespace ne peut être laissé sans surveillance ou régulation extérieure. S'il demeure un réseau effectivement trop novateur et spécifique pour la législation préexistante, son impact sur les juridictions traditionnelles est trop grand pour ne pas attirer l'attention et le contrôle du législateur.

L'auteur Lawrence Lessig décrit d'ailleurs le droit national comme l'un des quatre forces qui doivent réguler le comportement de l'internaute, en lui infligeant une peine en cas de contravention[15]. Le droit s'imposerait donc comme un outil de régulation important du cyberespace, à la fois répressif dans ses usages illégaux (lutte contre la cybercriminalité) mais aussi protecteur des libertés des usagers (comme son droit à la vie privée[16]).

La difficulté, et principale critique faite alors à ce principe réside donc dans la rédaction d'un droit adapté à ce domaine nouveau, aux considérations souvent hautement techniques, et soumis à la perpétuelle évolution des technologies dont il dépend. Un bon exemple de l'accord parfois difficile entre ces deux univers est la récente audition par le Sénat américain du dirigeant de Facebook Mark Zuckerberg. Ce qui devait être un interrogatoire difficile dans le cadre d'un scandale sur l'exploitation de données personnelles s'est vite avéré être un dialogue de sourds, entre un technicien expert et ses interlocuteurs qui n'entendent visiblement que très peu de choses à son champ d'expertise. S'il ne devait rester qu'un seul échange emblématique de cette audition, ce serait probablement le suivant, entamé par la question du Sénateur de l'Utah Orrin Hatch : « Comment maintenez-vous un modèle économique rentable, si les utilisateurs ne payent pas pour votre service ? », et conclu par la réponse incrédule de Zuckerberg : « mais, sénateur, grâce aux publicités »[17]…

C'est face à ces difficultés et limites du droit comme seul régulateur de l'Internet que Lessig en proposera d'autres : notamment l'économie de marché (régulation par le prix, la concurrence), la norme sociale (régulation par l'éducation et la sanction sociale), et surtout, en premier lieu, l'infrastructure du réseau elle-même, qui fixe les limites de ce que l'utilisateur peut accomplir via son interface.

Comme le dit Lessig lui-même, « ce régulateur, c'est le code : le logiciel et le matériel qui font du cyberespace ce qu'il est. Ce code, ou cette architecture, définit la manière dont nous vivons le cyberespace. Il détermine s'il est facile ou non de protéger sa vie privée, ou de censurer la parole. Il détermine si l'accès à l'information est global ou sectorisé. Il a un

[15] Lawrence Lessig, « Codes and Other laws of Cyberspace », 1999, Basic Books
[16] Article 8, Convention Européenne des Droits de l'Homme, 1953
[17] Shara Tikben, « Questions to Mark Zuckerberg show many senators don't get Facebook », Cnet magazine, 11 avril 2018

impact sur qui peut voir quoi, ou sur ce qui est surveillé. Lorsqu'on commence à comprendre la nature de ce code, on se rend compte que, d'une myriade de manières, le code du cyberespace régule. »[18]

Lessig rejoint ici la théorie du déterminisme technologique, selon laquelle « on suppose que le changement technique est un facteur indépendant de la société. D'une part, le changement technique est autonome [...]. D'autre part, un changement technique provoque un changement social »[19]. L'évolution de la société, et par corollaire du droit qui la gouverne, ne serait ainsi que la conséquence des nouvelles possibilités offertes par la technique.

Une théorie qui a pris de plus en plus de recul dans l'histoire récente, du fait de l'application en réalité de son exact opposé. Le code ne fait plus aujourd'hui loi (le fameux « code is law » de Lessig) ; c'est plutôt la loi qui fait le code, imposant des cahiers des charges et des règles infrastructurelles précises qui forcent développeurs et programmeurs à orienter leur code dans une direction choisie par le législateur. En exemple d'une telle tendance, le très récent Règlement Général pour la Protection des Données (RGPD) de l'Union Européenne est incontournable ; il impose aux entreprises de prendre, dès la phase de conception de leur produit, les mesures nécessaires à assurer la confidentialité des données de l'utilisateur[20].

Le droit s'est donc imposé, dans la théorie comme la pratique comme une influence majeure dans la régulation d'Internet. Nombre des critiques quant à son exécution de cette régulation, qu'elles aient été proférées par libertariens, paternalistes ou déterministes, restent valides et d'actualité. Dans différents domaines, ces critiques et l'application de modèles théoriques ont modifié l'approche de différents acteurs comme les Etats-Unis, la France ou l'Union Européenne dans leur législation.

Cette influence se retrouve par exemple dans le souvent polémique droit des données personnelles.

[18] « Le code fait loi – De la liberté dans le cyberespace », Framablog, 22 mai 2010 ; traduction en français de l'article de Lawrence Lessig : « Code Is Law : On Liberty in Cyberspace », Harvard Magazine, 2000.
[19] Dominique Vinck, « Sociologie des sciences », 1995, Armand Colin, p. 232.
[20] Article 25, Reglement Général sur La Protection des Données, Reglement Union Européenne 2016/679, 14 avril 2016

II / Législation sur les données personnelles et surveillance d'état dans le contexte terroriste moderne

En parallèle avec la diffusion de l'usage d'internet dans tous les aspects de la vie quotidienne du grand public, celui-ci a également développé une acuité croissante quant aux traces qu'il laisse dans cet usage. Ces données personnelles, définies dans le droit français comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »[21], regroupent tous les courriers envoyés, les photos, les préférences, les mentions « j'aime » … Dans le monde hyperconnecté moderne, il permet non seulement de cerner l'identité et la personnalité d'une personne, mais aussi ses habitudes et sa position géographique.

On peut dès lors comprendre que ces données et leur traitement revêtent un aspect important pour leurs propriétaires ; ces derniers ne sont toutefois pas les seuls à y avoir accès, les gouvernements et forces de police ayant tôt compris l'intérêt d'Internet comme outil de renseignement.

Si les gouvernements ont toujours réalisé le potentiel stratégique d'internet, qui était dès le stade de projet soutenu par les fonds publics de la Défense américaine par exemple[22], il est devenu au 21e siècle le premier outil de surveillance mondial. L'interception de communications, le profilage, sont autant de choses facilitées par ce réseau à l'usage massif et ou l'anonymat n'est souvent qu'une illusion. Et si le public est aujourd'hui plus conscient de cette surveillance, la législation demeure à ce sujet très permissive, au nom de la sécurité nationale et de sa protection.

1. Aux Etats-Unis, un droit façonné par les crises politiques

Le traumatisme des attentats du 11 septembre 2001 aura été la cause d'une refonte totale du renseignement américain : il était hors de question de subir une nouvelle attaque, de se laisser surprendre à nouveau. C'est dans cet esprit que sera élaboré et voté par les 2 chambres du Congrès le désormais célèbre Patriot Act : « Providing appropriate tools required to intercept and obstruct terrorism »[23], après sa proposition le 26 octobre par le président George W. Bush. Ce nouveau texte fournit de vastes nouveaux pouvoirs aux

[21] Article 2, Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, 6 janvier 1978
[22] Katie Hafner et Matthew Lyon, « Les sorciers du Net : les origines de l'Internet », Calmann-Levy, 1999, ISBN : 270212951X
[23] PATRIOT ACT, 107th Congress of the USA, Government Publishing Office, 2001

agences gouvernementales dans la surveillance et le recueil de données, notamment sur Internet.

La section 215, la plus célèbre, fait déjà parler d'elle en 2005, lorsque le *New York Times* révèle un vaste programme d'écoutes téléphoniques des citoyens américains[24]. Ce dernier montre plusieurs points alarmants, notamment via son mépris des *checks and balances* et de l'influence du judiciaire sur l'exécutif si chère au modèle américain ; mais également la taille de l'opération « le nombre de citoyens américains dont les conversations vers l'international ont été écoutées se chiffre en millions », du fait de « la collaboration entre la NSA (*National Security Agency)* et trois des grandes sociétés de télécommunications, Verizon, AT&T et South Bell, qui ont fourni le fichier de leurs usagers, ainsi que les appels passés par ces derniers et leur durée, de façon à créer une base de données »[25]. Le ton est donné : les données personnelles sont devenues un outil de surveillance, jouant dangereusement avec la notion de droit à la vie privée, et ce sans contrôle de la branche judiciaire du pouvoir.

La réelle prise de conscience a cependant lieu en 2013, lorsque le programme PRISM de cette même NSA est révélé au grand public par l'un de ses employés, Edward Snowden, dans les colonnes du Guardian[26] et du Washington Post. Il s'agit d'une immense expansion du programme précèdent, impliquant davantage de compagnies (AOL, Yahoo!, Facebook, Google…) et visant désormais bien davantage les métadonnées informatiques que les conversations téléphoniques. Pire, le programme s'étant sur toutes les communications transitant par ces compagnies, et recueillait donc également les données de citoyens étrangers, notamment européens. Classé secret, il a également le défaut de n'être pas soumis à la branche judiciaire, et constitue pour de nombreux citoyens une violation des fonctions constitutionnelles de leur Etat : les représenter, les protéger et les servir.

Le programme PRISM sera par la suite fermé, et sa base légale, le Patriot Act de 2001, reformé lors de l'expiration de certaines de ses mesures en 2015. Le nouveau USA Freedom Act (Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act)[27] met notamment fin à la collecte de données autorisée par la section 215, qui n'est ainsi pas renouvelée. Cela ne signifie pas pour autant la fin de toute surveillance de masse : l'écoute des communications, notamment, continue sous le couvert d'autres textes comme le Foreign Intelligence Surveillance Act. Mais elle est désormais mieux encadrée, et surtout n'est plus dissimulée au regard des juges, en particulier de la Cour Suprême.

La législation américaine, quant à la gestion gouvernementale de la question des données personnelles, s'est donc vue grandement influencer par des crises a priori éloignées de la sphère juridique : une attaque terroriste, suivie d'un scandale politique lié aux questions de Défense. Il est possible de voir ici un échec pratique de la doctrine libertaire : le

[24] James Risen et Eric Lichtblaudec, « Bush Lets U.S. Spy on Callers Without Courts », New York Times, 16 décembre 2005

[25] Sébastien Mort, « Surveillance des correspondances privées dans le cyberespace aux États-Unis : un contrôle marqué au sceau du secret », extrait de Revue Française d'études Américaines, N°123, p. 33-53, Belin, 2010

[26] Glenn Greenwald and Ewen MacAskill, « NSA Prism program taps in to user data of Apple, Google and others », The Guardian, 7 juin 2013

[27] USA FREEDOM Act, 114th Congress of the USA, Government Publishing Office, 2015

cyberespace ne peut être laissé de côté par les gouvernements et le législateur, il n'est pas une juridiction autarcique mais a au contraire de réelles conséquences sur d'autres domaines d'importance, comme la sécurité nationale. Mais cette hégémonie des agences gouvernementales américaines peut-elle être perçue comme une limite de la pensée paternaliste, où laisser la régulation du cyberespace aux gouvernements n'a résulté qu'en un abus de ce pouvoir.

Cette histoire récente de la réglementation des données aux Etats-Unis a marqué des esprits, notamment au sein des autres nations démocratiques.

2. En France, les leçons tirées de l'expérience américaine ?

L'Europe, et en particulier la France, ont en effet été frappées ces dernières années par une vague d'attentats qui ne sont pas sans rappeler les attaques sur le sol américain en 2001. L'histoire semble alors se répéter lorsque, 4 mois après les attentats de novembre 2015, l'Assemblée Nationale voit soumise à son examen le projet de loi relative au Renseignement.

On y retrouve certaines mesures qui rappellent le Patriot Act : collecte des métadonnées, écoutes téléphoniques, interception de courriers électroniques… Des mesures qui existaient *de facto* mais se voient pour la première fois attribuer une base légale[28]. S'y retrouve également, à l'article 2 du texte[29] un nouveau système permettant de recueillir les informations des personnes considérées comme menaces potentielles… via une collaboration étroite avec les opérateurs téléphoniques et les fournisseurs d'accès à Internet (FAI). Le parallèle avec le Patriot Act, le programme PRISM et ses polémiques est alors évident.

Le législateur français marque cependant son intention de se démarquer de ses homologues outre-Atlantique en établissant un organisme de contrôle de la mise en application de ces mesures par les forces de police. La Commission nationale de contrôle des techniques de renseignement (CNCTR) regroupe des représentants des 2 autres grands pouvoirs (des magistrats et des parlementaires), ainsi qu'un expert en télécommunications, pour contrebalancer ces nouveaux pouvoirs détenus par l'exécutif. Néanmoins, cette Commission n'a qu'un rôle consultatif, et elle peut être ignorée dans les cas « d'urgence absolue ».

Promulguée en 2015, la loi sera ensuite modifiée en 2016 lors de la prolongation de l'Etat d'Urgence suite à l'attentat de Nice, et attirera l'attention du Conseil Constitutionnel. En effet, suite à cette modification, « l'article L. 852-1 du code de la sécurité intérieure

[28] Félix Tréguer, "Intelligence Reform and the Snowden Paradox: The Case of France", Media and Communication Volume 5, Issue 1, Pages 17–28, 2017,
[29] Article 2, Loi n° 2015-912 du 24 juillet 2015 relative au renseignement

autorise les interceptions administratives de correspondances émises par […] les personnes appartenant à l'entourage d'une personne concernée par l'autorisation d'interception.»[30]

Voyant en cet élargissement à l'entourage des personnes cibles une porte ouverte à l'abus de libertés, l'association de défense des droits numériques la Quadrature du Net rédigera une Question Prioritaire de Constitutionnalité, à laquelle le Conseil répondra par une non-conformité partielle. Pour les sages, « le législateur a permis que fasse l'objet de cette technique de renseignement un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit. Ainsi, […] le législateur n'a pas opéré une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le droit au respect de la vie privée. » Il ressort de cette décision, et de la loi renseignement en elle-même, une volonté de la France de retenir les leçons du Patriot Act américain, en garantissant un contrôle judiciaire sur le pouvoir exécutif.

Dans cet objectif, les Etats du vieux continent dispose d'avantages de taille, comme l'Union Européenne ou la Convention Européennes des Droits de l'Homme

3. La législation britannique sur les données personnelles soumise au cadre européen

Ainsi, le Royaume-Uni, victime de nombreuses attaques terroristes au cours de son histoire récente (Londres en 2005, Londres et Manchester en 2017…), a lui aussi prévu de se doter d'une législation regardant la surveillance sur le cyberespace et la collecte de données personnelles au nom de la sécurité nationale.

L'Investigatory Powers Act, validé par les deux chambres du Parlement Britannique, est entré en vigueur le 29 novembre 2016[31], après une phase de projet longue et controversée, notamment suite aux critiques dues à son manque de réalisme vis-à-vis des pratiques modernes du cyberespace[32]. Il contient des mesures qui devraient sembler désormais familières : pouvoirs accrus des forces de police, nouveaux moyens de surveillance et d'écoute, collection de métadonnées avec la collaboration des FAI…

L'acte prévoit, comme l'avait fait la France l'année précédente, la mise en place d'un organisme de contrôle pour superviser l'usage de ces nouveaux pouvoirs : l'Investigatory Powers Commission (IPC). Contrairement à la Commission française, elle n'est composée que de juges ; le pouvoir législatif sera représenté par un comité parlementaire déjà existant, l'Intelligence and Security Committee of Parliament. Un « double-verrou » est mis en place,

[30] Conseil Constitutionnel, Décision n° 2017-648 QPC du 4 août 2017
[31] « Investigatory Powers Act 2016 c.25 », 29 novembre 2016, www.parliament.uk
[32] Andrew Griffin, « Uk Spying Law: government introduces law requiring Whatsapp and iMessage to break their own security », The Independant, 1er Mars 2016

supposant l'autorisation d'à la fois un secrétaire d'Etat et un des juges de la commission pour l'autorisation de mandats d'écoute et autres mesures très intrusives.

Il ressort de ce renforcement des mesures de supervision une volonté de s'affranchir au maximum de la possibilité d'un nouveau Patriot Act. Les critiques faites à l'organisme de contrôle français, considéré comme trop timide, résultent en ce second niveau d'autorisation et le raffermissement du contrôle.

Cela ne suffira toutefois pas à assurer la pérennité du texte. En 2018, le groupe Liberty pose à la High Court britannique la question de la conformité du texte avec le droit européen. Les juges décideront alors que le texte n'est pas conforme avec les standards établis par la jurisprudence de la Cour de Justice de l'Union Européenne (CJUE), suivant les droits fondamentaux comme le droit à la vie privée contenu à l'art 8 de la Convention Européenne des Droits de l'Homme (CEDH)[33]. Pour les Lord Justices Singh et Holgate, la loi ne cible pas explicitement la lutte contre les « crimes graves » comme cible de ses mesures ; et l'accès aux données collectées n'est pas suffisamment subordonné à une cour ou un organisme indépendant.

Cet exemple démontre l'avantage considérable que représente le droit Européen dans ces problématiques venant remettre en cause l'exercice de droits fondamentaux. Il offre un cadre, des limitations dont ne disposaient par exemple pas les Etats-Unis en 2001.

Il ressort de ce comparatif une claire progression, au fil du temps, des réformes mais aussi des crises politiques, de concilier au mieux les notions de protection de la vie privée et de sécurité nationale. Il s'agit à l'évidence d'un équilibre difficile à atteindre, qui fait face à une cybercriminalité et surtout un terrorisme toujours mieux dissimulé, sans cesse en quête de nouveaux canaux de communication ; En 2015, le Ministre de l'Intérieur Belge expliquait que « les communications entre terroristes les plus difficiles à traquer, […] pour tous les services de renseignement, sont celles passant par la PlayStation 4 »[34], impliquant que même les consoles de jeux n'étaient plus à l'abri de la surveillance.

De l'autre côté de la balance se trouve des citoyens plus conscients de leurs droits et libertés, et demandant plus que jamais à leurs représentants de les protéger. Quelle que soit le degré de surveillance adopté, la domination d'une approche paternaliste est ici indéniable, les questions d'espionnage, de surveillance et de sécurité nationale demeurant des domaines régaliens que les états-nations se refusent à laisser à d'autres, au nom de leur autorité représentative, mais aussi de leurs infrastructures et moyens largement supérieurs.

Lorsque la législation concerne plutôt l'usage privé d'Internet, les droits de l'utilisateur semblent dès lors prendre une place plus importante dans les considérations des gouvernants.

[33] « Liberty v Home Office », High Court of Justice, Queen's Bench Division, 27 avril 2018, Case No: CO/1052/2017

[34] Citation du Ministre de l'Interieur Belge Jan Jambon, dans « Why Terrorists Love PlayStation 4 », Kate Day, Politico, 15 novembre 2015.

III / La législation sur les données personnelles à l'épreuve du secteur privé

Le cyberespace contemporain est en effet majoritairement à usage privé. Réseaux Sociaux, e-commerce, forums, sites informatifs, ludiques ou éducatifs, foisonnent sur le web et sont libres de fournir différents services aux usagers. Dans de nombreux cas, utiliser ces sites revient à y déposer des données ; adresses mail ou IP, ou même numéros de carte bancaire, mots de passe et autres informations plus confidentielles.

Cette avalanche de données, accélérée par un accès à Internet sans cesse plus aisé, notamment grâce aux phénomène smartphone, en fait un bien précieux pour de nombreux domaines, dont le marketing, la recherche technologique, et bien d'autres. A tel point que l'on parle à présent des données comme « la ressource la plus lucrative du monde »[35], devant le pétrole. Les données personnelles deviennent un moyen sans précèdent pour le domaine de l'entreprise de connaître sa clientèle, de cibler ses besoins, ses envies et ses réactions. Un outil marketing, donc, mais aussi logistique : pour un géant de la livraison comme Amazon, comment rêver mieux pour implanter de nouveaux sites qu'une clientèle prête à obligeamment fournir son adresse ?

Emergent alors certains risques, comme le décrit la vice-présidente de l'Internet Society, l'une des plus importantes Organisations Non Gouvernementales à militer sur le terrain du cyberespace : « Si nos données peuvent maintenant se revendre pour des millions, cela crée une forte incitation à collecter tout ce qui est possible, le conserver aussi longtemps que faire se peut, l'utiliser dans tous les contextes imaginables »[36].

Le législateur a choisi de prévenir ces risques, notamment au nom du droit à la vie Privée, même si la sévérité des mesures varie grandement d'une juridiction à l'autre. Ainsi, si le droit américain se montre dans ce domaine très permissif (1), le récent Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne comporte de nombreuses mesures novatrices dans des domaines variés (2) et restreint davantage la marge de manœuvre des entreprises.

1. Un régime américain aux insuffisances notables

Ainsi, si en Europe, le droit à la vie privée reste une valeur fondamentale, la Constitution américaine a également choisi de le protéger… Mais d'une façon bien différente. Le

[35] The Economist, « The world's most valuable resource is no longer oil, but data », The economist, 6 mai 2017
[36] Sally Shipman Wentworth, « My Data. Your Business. », Internet Society, pour Better Business Bureau (bbb.com)

quatrième amendement garantit cette protection, mais uniquement à l'égard du gouvernement[37]; vestige de la guerre d'indépendance et des perquisitions britanniques, il sera par la suite étendu au-delà du domicile, notamment jusqu'aux conversations téléphoniques[38]. Néanmoins, il demeure impuissant face aux incursions d'acteurs privés dans la vie privée des citoyens, et cela est reflété dans l'absence de législation globale à ce sujet dans le droit américain.

Pour pallier à ce manque, une variété de lois fédérales ont été créés pour protéger les données sensibles dans certains domaines précis : les données de santé (HIPAA, Health Insurance Portability and Accountability Act), bancaires (GLBA, Gramm-Leach-Bliley Act) ou encore télécommunications (ECPA, Electronic Communications Privacy Act). Ce dernier texte en particulier cristallise l'ensemble des problèmes sur cette législation : entré en vigueur en 1986, il est maintenant largement dépassé, concerne encore une fois principalement la surveillance et la collection de données par l'état, et ses mesures au regard du secteur privé se concentrent sur la relation employeur/employé. Il est généralement considéré comme dépassé et en grand besoin d'une mise à jour[39].

Le système fédéral américain a toutefois permis aux 50 Etats de pallier à ce manque. Selon Winston Maxwell, avocat spécialiste au cabinet Hogan Lovells, « L'État de Californie a notamment adopté une loi protégeant les données à caractère personnel dans le cadre de sites Internet, ainsi qu'une loi accordant un droit à l'effacement à des utilisateurs mineurs de réseaux sociaux. Presque tous les États ont adopté des lois définissant les conditions dans lesquelles les violations de sécurité de données à caractère personnel doivent être déclarées aux autorités et aux victimes. »[40]

Une nouvelle mesure générale, plus insidieuse, est toutefois venue limiter l'usage des données personnelles par les grandes entreprises : « une loi générale sur la protection du consommateur, qui interdit toute pratique déloyale dans le commerce[41] ». Aujourd'hui, ces pratiques déloyales englobent « inclure tout traitement de données à caractère personnel incompatible avec les attentes légitimes du consommateur ». En exercice depuis 1914, ce texte donne ses pouvoir à la Federal Trade Commission, un organisme qui au fil des années, des sanctions et recommandations, a pu établir un véritable jeu de règles législatives quant à la vie privée des utilisateurs, à tel point que le professeur Daniel Solove, de l'université de Columbia, le décrit en ces termes : « en pratique, la jurisprudence en matière de vie privée de la FTC est devenu le plus large et le plus influent outil de régulation des données aux Etats-Unis »[42] ; pour lui, il s'agit réellement là d'un corps de « common law » semblable à la

[37] « Quatrième amendement », Constitution des Etats Unis d'Amérique, 1791
[38] « Katz v. United States », Cour Supreme des Etats-Unis, 389 U.S. 347 (1967)
[39] Miguel Heft et Claire Cain Miller, « 1986 Privacy Law Is Outrun by the Web », The New York Times, 9 Janvier 2011
[40] Winston J. Maxwell, « La Protection des données à caractère personnel aux Etats-Unis : Convergences et divergences avec l'approche Européenne », dans « Le Cloud Computing, L'informatique en nuage », p. 71 à 78, 2013
[41] « Section 5 : Unfair or Deceptive Acts or Practices », Federal Trade Commission Act,
[42] Daniel J. Solove & Woodrow Hartzog, « The FTC and the new common law of privacy », Columbia Law Review, 20 août 2013

jurisprudence de la cour suprême ou au système législatif anglo-saxon, où les décisions prises sur un sujet font loi pour les litiges suivants.

Finalement, la législation étatsunienne sur la question semble lacunaire, opaque aux yeux du grand public ; le simple fait que sa majorité provienne d'une autorité destinée à la régulation des activités commerciales démontre une vision extrêmement libérale, ou la protection n'est au final qu'une conséquence de la prévention de la concurrence déloyale. Cette libéralité s'explique d'abord par l'étroite collaboration, connue depuis les révélations d'Edward Snowden, entre les compagnies américaines et les agences gouvernementales : en imposant des limites légales à ces entreprises, ce sont les meilleurs agents de ces agences qui s'en trouveraient alors moins efficaces.

Cette libéralité se constate toutefois dans d'autres directions : Me Maxwell décrit en effet également le processus selon lequel « l'agence américaine de télécommunications et d'information, la NTIA, invite les acteurs du secteur privé à développer des codes de conduite relatifs à certains secteurs de l'Internet. La NTIA organise des réunions entre acteurs, facilite l'échange d'informations et brandit la menace d'une mesure de régulation contraignante si les acteurs n'arrivent pas à trouver un accord. »[40] Ce dialogue s'explique par la réalisation de l'importance du secteur privé dans la régularisation ; il est après tout à l'origine de la plus grande partie de la recherche, de l'innovation, et donc des nouveaux outils qui s'incluront dans cette régulation. Fusion moderne des visions paternalistes et libertaires, qui voit la collaboration des législateurs et des ingénieurs, cette collaboration, appelée *multistake-holderism*, est le plus grand point commun entre le régime américain et la réglementation européenne.

2. Le RGPD, représentant d'une législation européenne basée sur la communication entre tous les acteurs du cyberespace

Le dernier-né en matière de législation européenne sur les données personnelles, le fameux RGPD, reflète en effet également cette doctrine du *multistake-holderism*, mais va plus loin que le modèle américain en incluant également l'utilisateur et en montrant une claire volonté de transparence et d'information, ce que l'opaque et multiple législation outre-Atlantique a clairement échoué à accomplir.

Cette transparence passe d'abord par l'institutionnalisation du consentement de l'internaute. Si par le passé, la collecte de données a pu se faire de manière confidentielle, notamment pour les compagnies par un obscur lien vers les conditions d'utilisation de leur site, le RGPD introduit des règles claires quant au consentement de l'internaute. Selon l'article 7 du règlement, « la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. »[43] Cette demande de consentement

[43] Article 7, RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL

doit par ailleurs être précise ; l'internaute doit savoir quel genre de données sont collectées, dans quel objectif, et peut accepter individuellement chacune de ces collectes. Enfin, il lui est possible de retracter à tout moment ce consentement.

Impossible donc, du moins en théorie, pour l'utilisateur d'ignorer que ses données sont collectées, possiblement contre son gré, ce qui devrait lui permettre de faire des choix de navigation plus éclairés selon ses vœux. Toutefois, le consentement n'est qu'une des bases légales nécessaires à la collecte de données par le propriétaire du site. Si ce dernier a la possibilité d'en choisir une autre (exécution d'une obligation légale ou d'un contrat, intérêt légitime du responsable du traitement…) cette obligation de consentement disparaît totalement. Par ailleurs, des difficultés ont émergé quant à l'interprétation pratique des critères de validité de la demande de consentement ; ainsi, la plupart du temps, seul un bouton permettant de tout accepter est proposé à l'internaute, pressé de consulter son contenu et de se débarrasser de cette importune fenêtre, au point que pour réellement parvenir à réduire la collecte de données au minimum, l'utilisation de logiciels tiers est devenue nécessaire afin de s'épargner le fastidieux processus, à chaque visite, de refus des différentes collectes[44] .

L'utilisateur dispose par ailleurs d'un contrôle accru de ces données, même une fois collectées. Le RGPD poursuit par cette voie sa quête de transparence : l'utilisateur est non seulement à même de connaître l'usage destiné à ses données, mais il en demeure également le propriétaire, et peu en demander le transfert ou l'effacement. Le premier grâce à l'article 20, qui consacre le droit à la portabilité des données : la possibilité de transférer toutes ses informations vers un autre service ou site, y compris concurrent. Une mesure qui s'inscrit également dans un effort de protection de la concurrence, les grandes firmes ayant jusqu'à présent pris un malin plaisir à rendre la transition de l'utilisateur vers leur adversaire aussi fastidieuse que possible. Quant au second, le droit à l'effacement contenu à l'article 17 permet à tout particulier de demander la suppression de toute donnée à son nom, y compris chez de potentiels sous-traitants, et tant que ces données ne sont pas nécessaires pour un motif légitime (santé publique, obligation légale ou contractuelle…). Ce droit, déjà mis en place en 2014 par un arrêt de la Cour Européenne de Justice contre le géant Google, marquait déjà la volonté des institutions européennes de protéger leurs citoyens d'éventuels abus : « l'effet de l'ingérence dans les droits de la personne se trouve démultiplié en raison du rôle important que jouent Internet et les moteurs de recherche dans la société moderne, ces derniers conférant un caractère ubiquitaire aux informations contenues dans les listes de résultats »[45].

L'article 5 détermine quant à lui les conditions de traitement de ces données : en résumé, « licéité, loyauté, transparence, finalités limitées, données minimisées, exactes,

---

du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal Officiel de l'Union Européenne, 4 mai 2016

[44] David Legrand, « RGPD : une extension ajoute un refus global sur les sites utilisant le module Quantcast Choice », Nextinpact, 2 août 2018

[45] Google Spain SL / Google Inc. V Agencia Española de Protección de Datos (AEPD) / Mario Costeja González, Cour de Justice de l'Union Européenne (grande chambre), 13 mai 2014, C-131/12

dont la conservation est réduite dans le temps, et dont sont assurées l'intégrité et la confidentialité. »[46] Le plus important demeure le dernier alinéa de l'article, selon lequel il revient au responsable du traitement des données de démontrer que ces critères ont été respectés, résultant en une inversion de la charge de la preuve en cas de litige.

Ces mesures semblent faire peser un poids certain, très contraignant, sur les entreprises et les responsables du recueil et du traitement des données. C'est ici cependant que la doctrine du *multistake-holderism,* déjà en place aux Etats-Unis, refait son apparition : 2 des piliers majeurs du RGPD sont liés au travail en amont avec ces sociétés, afin que leurs produits soient dès le départ en conformité avec la vision du législateur. Contenus à l'article 25, « Protection des données dès la conception et protection des données par défaut », ils prévoient, d'abord, que tout produit prévoyant la personnalisation de la collecte des données devra être réglé par défaut sur les paramètres les plus restrictifs à cet égard (*privacy by default*).

Mais, plus important encore, que le respect des principes énoncés dans le règlement devrait modifier la mentalité d'ingénieurs, développeurs et autres créateurs dès le stade de la création du produit (*privacy by design*). Cet article suppose une réelle responsabilisation des entreprises, liée à la création du poste du Data Protection Officer, censé sensibiliser et prévenir les cas d'abus, de piratage ou de violation de vie privée. Le concept, popularisé en 2012 par le professeur Ann Cavoukian, était alors résumé en ces termes : « La notion selon laquelle les standards de protection de la vie privée doivent être délaissés au profit d'autres aspects (par exemple sécurité contre vie privée, ou performance contre vie privée) est abandonnée comme une vision dépassée. Des solutions innovantes doivent prévaloir »[47]. La démarche entamée par l'Union Européenne avec le RGPD se veut donc aussi constructive que restrictive, et, comme le système mis en place par NTIA américaine, repose sur un constant dialogue avec les acteurs privés du cyberespace.

La question des données laissées par les utilisateurs derrière eux et leur traitement est donc régi par un ensemble de textes à la sévérité variable. Il ne faut toutefois pas oublier que la nature elle-même des contenus consultés par les internautes peut également être sujet de régulation. Hormis les sites illégaux de par leur participation à des activités criminelles (piratage, trafics, terrorisme…), la question se pose : est-il légal, ou non, de restreindre l'accès des internautes à certaines régions du cyberespace ?

[46] Marc Rees, « Le RGPD expliqué ligne par ligne (articles 1 à 23) », Nextinpact, 21 février 2018
[47] Ann Cavoukian, « Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices », Information and Privacy Commissioner, Ontario, Canada, Décembre 2012

IV / Internet, un espace a la neutralité disputée

La question de la neutralité du net n'est pas des plus récentes. Popularisé par le professeur de droit Tim Wu en 2003, ce concept est décrit par lui comme l'absence de discrimination, positive ou négative, quant au traitement des différents flux de données, et ce à tous les niveaux : source, contenu et destinataire[48]. Selon Wu, « le cadre idéal pour assurer la neutralité du net […] se désintéressera des solutions structurelles pour se concentrer directement sur la discrimination d'accès aux bandes passantes ».

Selon le pays, ces recommandations ont été plus ou moins prises à cœur. En Chine, par exemple, les considérations politiques ont pris le pas sur la neutralité ; de nombreux sites ne sont tout simplement pas accessibles (1). Aux Etats-Unis, la réglementation imposant la neutralité du net vient d'être abolie, au nom de la concurrence qu'elle entraverait (2). Enfin, l'Europe maintient elle la neutralité du net comme principe fondamental, et la défend par sa législation (3).

1. La censure du cyberespace en Chine, ou l'antithèse d'un Internet neutre

Selon un rapport de l'organisation non gouvernementale Freedom House, la Chine serait le troisième pays le plus restrictif quant à l'usage du cyberespace par ses citoyens, derrière l'Iran et Cuba, et sans compter les états ou cet usage est tout simplement interdit, comme la Corée du Nord[49] .

Cela est dû à la progressive mise en place d'une censure extrêmement efficace de pans entiers du cyberespace, au nom de la protection des institutions politiques. La République Populaire de Chine (RPC) se justifie de cette censure dans un livre blanc publié à l'intention du reste du monde, et notamment de ses partenaires commerciaux, en 2010 : « au sein du territoire chinois, Internet est placé sous la juridiction de la souveraineté chinoise. Cette souveraineté doit être respectée et protégée. Si les citoyens de la RPC, les citoyens étrangers, les personnes légales et autres organisations sur le territoire chinois disposent du droit et de la liberté d'utiliser Internet, ils doivent en parallèle obéir les lois et régulations de la Chine et consciencieusement protéger la sécurité d'Internet. » La RPC utilise donc le

[48]Tim Wu, « Network Neutrality, Broadband Discrimination », Journal of Telecommunications and High Technology Law, vol. 2, p. 141, 2003

[49] « Freedom on the Net 2012 », Freedom House, 2012

principe de souveraineté nationale, ici basée sur le critère de territorialité, pour justifier sa législation.

Cette réglementation, basée sur plus de 60 textes législatifs selon le rapport Freedom House, voit ses objectifs résumés dans la Réglementations sur la sécurité, la protection et la gestion du réseau d'information informatique :

« Aucun groupe ou individu ne peut utiliser Internet pour créer, répliquer, récupérer ou transmettre les types d'informations suivantes :

1.Incitation à s'opposer ou violation de la Constitution ou les lois ou l'exécution des réglementations administratives ;

2. Incitation au renversement du gouvernement ou du système socialiste ;
3. Incitation à la division du pays, nuisance à l'unification nationale ;
4. Incitation à la haine ou la discrimination envers les ethnies ou nuisance à l'unité des ethnies ;
5. Fabrication de mensonges ou déformation de la vérité, propagation de rumeurs, destruction de l'ordre de la société ;
6. Promotion de superstitions féodales, de matériel sexuellement suggestif, de paris, de la violence, du meurtre ;
7. Terrorisme ou incitation de tiers à mener des activités criminelles ; insultes ouvertes envers d'autres personnes ou distorsion de la vérité pour calomnier une personne ;
8. Attaque de la réputation des organisations d'État ;
9. Toute activité contraire à la Constitution, aux lois ou réglementations administratives »[50]

Si cet article contient des mesures communes dans la législation des contenus autorisés sur le web (incitation à la haine, activités criminelles…) il va bien plus loin en se faisant le bouclier du pouvoir en place, toute remise en question du « système socialiste » ou « de la Constitution et des lois » se voyant frappée d'illégalité et censurée.

Cette censure fait de l'Internet chinois l'un des plus éloignés du concept de neutralité du net : l'usager n'a absolument pas accès à tous les contenus de manière égale, il est tenu à l'écart de certains, et ne pourra pas lui-même publier tout ce qu'il désire. Elle repose sur deux outils, le *Great Firewall* ou Grande Muraille Numérique, et le *Golden Shield,* bouclier doré.

Le premier, comme son homologue de pierre, vise à empêcher les invasions étrangères. Il constitue en un blocage systématique des sites établis ailleurs qu'en Chine qui diffuseraient les fameuses idées contraires à la section 5 de la règlementation de 97 : organisations de défense des droits de l'homme, presse internationale, réseaux sociaux, etc. Selon une étude du journal the Economist, les filtres se sont sophistiqués avec le temps, et

[50] Section 5, Réglementations sur la sécurité, la protection et la gestion du réseau d'information informatique, 11 décembre 1997

sont désormais à même de bloquer « des pages spécifiques de sites étrangers, plutôt que de les rendre entièrement inaccessibles »[51]. Plus important encore, « il est désormais possible de détecter et censurer certains termes lorsqu'ils sont utilisés dans un moteur de recherche ou un service de messagerie instantanée ».

Le Golden Shield, quant à lui, sert à la surveillance des réseaux domestiques, selon les mêmes critères et utilisant des outils similaires. Il est intéressant de noter que, tout comme les américains et européens dans leurs programmes de surveillance, ce système n'est rendu possible que par une étroite collaboration avec les fournisseurs d'accès. En Chine, il n'en existe qu'un nombre limité, sous réserve d'une licence fournie par l'Etat, et qui peut être retirée à tout moment, d'où une obéissance sans faille. A eux de repérer et de supprimer les commentaires, articles et contenus sensibles, selon « des listes de mots-clés régulièrement fournies par le gouvernement ». Si la plupart se prêtent au jeu avec zèle, certains ont tendance à laisser les contenus trainer un peu trop longtemps en ligne, ce qui peut leur permettre d'être très largement diffusés avant leur suppression. Par exemple, lors de l'explosion d'une école en 2001, un certain article[52] sujet de ces « lenteurs administratives » avait rendu de notoriété publique l'information interdite selon laquelle les feux d'artifices responsables avaient été fabriqués par des enfants…

Pour résumer, si la Chine a compris les bienfaits d'Internet pour notamment le commerce, les loisirs, ou l'éducation, et entend bien laisser ses citoyens en bénéficier, elle a par ailleurs fait le choix d'y tuer dans l'œuf toute forme de débat ou activisme politique qui pourrait remettre en cause le pouvoir en place. Si la Chine a depuis 2004 inclus dans sa Constitution que « l'Etat respecte et protège les droits de l'homme »[53], cette gestion du cyberespace démontre les limites de cette promesse, au vu des strictes limites qu'elle impose à la liberté d'expression et d'opinion[54].

Si la législation américaine, depuis peu, a également choisi de ne pas garantir la neutralité du net, les raisons en sont différentes : plus que politiques, elles sont économiques. L'union Européenne, confrontée aux mêmes questions, a quant à elle choisi d'inscrire la neutralité dans son droit.

[51] E.H., « How Does China Censor the Internet ? », The Economist, 22 Avril 2013

[52] « 万载爆炸事件：新闻大战功与过 », people.com.cn, 10 mars 2001

[53] Article 33, Constitution de la République Populaire de Chine, 2004

[54] Article 19, Déclaration Universelle des Droits de l'Homme, 1948

2. Etats-Unis et Union Européenne, deux visions de la neutralité divergeant sur la question de la concurrence

Il n'a en effet jamais été question, pour le droit américain, d'une restriction d'accès basée sur les contenus publiés. Bien davantage que les habitants de l'Empire du Milieu, les citoyens américains sont extrêmement attachés à une liberté d'expression historiquement très permissive et largement interprétée, et inscrite au sein même de leur Constitution, au premier amendement du Bill of Rights[55]. Bien plus que dans une République Populaire de Chine soumise depuis 1949 à la propagande et la répression d'un Etat communiste autoritaire, le débat et la contestation politique font partie intégrante de l'identité étatsunienne, construite sur l'idéal de liberté et d'auto-détermination ayant mené à l'éviction du colonisateur anglais.

Le point de vue européen est sur ce point extrêmement proche de celui du voisin outre-Atlantique. Ces idéologies similaires ne sont pas dues au hasard, mais à des influences communes, au sommet desquelles on trouvera les philosophes des Lumières, moteurs idéologiques des révolutions américaines et françaises chronologiquement très proches, et premières inspirations de textes fondateurs comme la Déclaration d'Indépendance et la Constitution Américaine, mais également la Déclaration des Droits de l'Homme et du Citoyen de 1789, qui consacre également la liberté d'expression comme un droit inaliénable[56].

Les Etats-Unis, tout comme les nations Européennes, n'ont donc pas ressenti le besoin de s'affranchir de la neutralité du net pour des raisons politiques. Les Etats-Nations ne sont cependant pas les seuls acteurs du cyberespace à pouvoir trouver un intérêt dans ces questions. Ces dernières années, ce sont les fournisseurs d'accès à Internet qui étudient la possibilité d'un Internet à vitesse variable. Le président d'un de ces FAI, Alain Weill, exprimait ainsi ses raisons : « « À certaines heures de la journée, Netflix et Google représentent 80 % des flux qui circulent sur notre réseau. Est-il normal que les conditions d'accès au réseau soient les mêmes pour des acteurs qui pèsent aussi lourd que pour d'autres plus petits ? On peut se poser la question, […] L'autoroute doit-elle être gratuite pour tout le monde ? Un 10 tonnes doit-il payer le même prix qu'une voiture électrique ? »[57]

Cette critique, une des plus importante vis-à-vis de la neutralité du net, cristallise son principal problème : en obligeant la fourniture des mêmes services aux géants du web (les fameux GAFAM : Google, Apple, Facebook, Amazon et Microsoft) comme aux acteurs plus modestes, impossible de demander une contribution sur l'investissement des réseaux plus importante à ces mastodontes, ce qui leur permet alors de faire circuler des flux gigantesques (notamment dû à l'hébergement de vidéos) à des coûts modiques. Cette inégalité d'utilisation est à l'origine d'un second problème, difficile à résoudre dans un

[55] Premier Amendement, Bill of Rights, Constitution des Etats-Unis d'Amérique, 1791
[56] Art. 11, Déclaration des Droits de l'Homme et du Citoyen, 26 août 1789
[57] Alain Weill, Altice Europe CEO, SFR-Groupe Altice, dans « Où est la démocratie Numérique ? », Conférence des Rencontres Economiques d'Aix-en-Provence, juillet 2018

Internet neutre, tel que souligné par l'ONG dnsBelgium, responsable de la gestion du domaine .be : « les gros consommateurs accaparent la bande passante, de sorte que les fournisseurs qui souhaitent desservir tous les utilisateurs pourraient être tentés de ralentir les services qui consomment beaucoup de bande passante »[58]. En bref, les fournisseurs d'accès taxent la neutralité du net d'archaïsme ; un principe dépassé, qui désormais n'agit plus que comme gêne, les empêchant de délivrer une offre plus adaptée à leur marché et personnalisée.

Ces fournisseurs d'accès se heurtent toutefois à une féroce résistance de la part des défenseurs de la neutralité, qui n'est pas dépourvue d'arguments. Leur principale crainte face à cet internet dérégularisé, c'est la mise en place par les FAI de restrictions dans leur utilisation du réseau, afin de maximiser leur profit. Ces potentielles restrictions sont détaillées par Axelle Lemaire, ancienne secrétaire d'Etat française chargée du Numérique, dans une intervention radio de France Culture : ce qui effraie, c'est d'abord la mise en place d'un Internet « à deux vitesses », ou le fournisseur d'accès prioritise certains services et en ralentit d'autres ; par exemple, « il aurait été très tentant de fermer le robinet de services de discussion par la voix comme Skype », finalement « directement concurrents » de ceux fournis « par un opérateur également téléphonique »[59]. L'autre grande peur, c'est celle d'un Internet dit « à la carte », où « l'accès à certains contenus dépendrait de l'offre souscrite auprès de votre FAI ». Un tel paradigme pourrait résulter en des moments probablement frustrants pour l'internaute, contraint de souscrire à l'offre « streaming et musique » pour profiter de sites comme Netflix ou Spotify, mais en des marchés d'exclusivité extrêmement profitables pour les opérateurs.

Ces débats ont amené les législateurs, européens comme américains, à inclure la question de la neutralité du net dans le droit positif. Pour l'Union Européenne, elle est désormais inscrite au corpus législatif en ces termes : « Dans le cadre de la fourniture de services d'accès à l'internet, les fournisseurs de services d'accès à l'internet traitent tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés. »[60]

Le cas des Etats-Unis est plus complexe ; la question y tombe sous l'autorité d'un conseil de 5 commissaires nommés par le Président et confirmés par le Sénat, la Federal Communications Commission ou FCC. Si, depuis 2005, cette dernière inclut dans ses principes la défense de la neutralité du net, « pour protéger le caractère ouvert

[58] « La neutralité du Net : le pour et le contre », dnsBelgium, 9 février 2018

[59] « Faut-il sauver la Neutralité du Net ? », Du Grain à Moudre (France Culture), émission d'Hervé Gavette avec Michel Combot, directeur général de la fédération française de télécoms ; Axelle Lemaire, ancienne secrétaire d'Etat chargée du numérique et de l'innovation ; Valérie Nicolas, Maître de conférences en droit public à l'Université Paris Ouest-Nanterre-La Défense, spécialiste du droit des TIC, 13 décembre 2017

[60] Article 3, §3, « Règlement établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union », 25 novembre 2015, 2015/2120

d'Internet »[61], toute tentative d'inscrire cette protection dans les textes s'est confrontée à l'opposition du Congrès. Ce n'est qu'en 2015 qu'un ensemble de règles instaurées par la FCC installe désormais la neutralité du net comme principe protégé par le droit[62]. C'est ce faisceau réglementaire, qui interdisait des pratiques comme le blocage de sites par les FAI, qui sera en 2017 rendu caduque par cette même FCC[63], suite notamment à un changement de ligne politique, dû à la nomination du nouveau président de la Commission, Ajit Pai, opposant notoire à la neutralité du Net.

Pour Pai, le principe de neutralité était avant tout une entrave au développement d'Internet, étant donné les restrictions qu'il imposait à la libre concurrence entre les FAI, et donc l'innovation. Le jour du vote, il s'exprimait en ces termes : « Il est temps pour Internet d'être à nouveau piloté par les ingénieurs, les entrepreneurs et les consommateurs, plutôt que par les avocats, les comptables et les bureaucrates »[64].

Les législations Européennes et américaines se trouvent donc désormais en totale opposition, la première ayant choisi un droit positif restrictif pour éviter tout débordement, tandis que la seconde fait le pari de déréguler. Si l'approche européenne semble suivre un cyber-paternalisme dominant dans le cyberespace contemporain, la décision américaine peut être assimilée à un retour aux doctrines libertaires ; en effet, comme le rappelle Axelle Lemaire, si l'Etat vient à se retirer de la problématique, « le meilleur des équilibres entre consommateurs et entreprises passe par la recherche du profit ». Les internautes se verraient alors en possession d'un pouvoir direct sur la neutralité de leur réseau, à même de sanctionner toute incartade en tant que consommateurs et clients de FAI dépendant d'eux pour la réalisation de leurs bénéfices. Comme préconisé par Lessig, l'économie concurrente de marché deviendrait alors un outil de régulation majeur. Ce raisonnement reste toutefois à vérifier sur le long terme, un tel équilibre ne restant possible que sur un marché stable où la neutralité est la norme, et l'Internet à deux vitesses ou à la carte l'exception.

Ce rapport commercial est extrêmement présent sur Internet. En permettant des communications instantanées, faciles d'accès et à coût modique, le cyberespace a été l'un des principaux instruments de la mondialisation de l'économie. Par corollaire, et souvent pour les mêmes raisons, il est également devenu un haut lieu de la criminalité.

[61] « New Principles to Preserve and Promote the Open and Interconnected Nature of Public Internet », FCC Press Release, 5 aout 2005
[62] « FCC Adopts Strong, Sustainable rules to protect the open Internet », FCC Press Release, 26 février 2015
[63] « Restoring Internet Freedom Order », FCC, 14 décembre 2017
[64] Citation d'Ajit Pai dans « Les Etats-Unis abrogent la neutralité du Net, un principe fondateur d'Internet », Le Monde, 14 décembre 2017

V / Le Cyberespace, moteur d'un commerce accéléré et d'une criminalité débridée en besoin de régulation

Dans ces 2 domaines, l'arrivée d'Internet a agi comme le carburant d'une croissance exponentielle.

Il a résulté en la naissance d'une nouvelle branche du commerce, le commerce électronique ou e-commerce dans la langue de Shakespeare, qui regroupe toutes les transactions effectuées sur le réseau. De la même manière, la notion de cybercriminalité englobe, selon le rapport remis par un groupe de travail interministériel en 2014, « toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet »[65]. Au sein de ces 2 classifications, une distinction pratique s'est par la suite naturellement faite entre les pratiques facilitées et accélérées par le cyberespace, et celles qui sont nées de cette technologie et étaient tout simplement impossible auparavant (par exemple, la vente par correspondance a connu une véritable révolution, tandis que des infractions comme le piratage sont nées avec Internet).

Devant une telle ruée vers l'or, il était nécessaire d'établir un cadre juridique pour encadrer et réprimer ces nouveaux comportements, que ce soit dans le domaine commercial (1) ou criminel (2).

1. E-commerce et régulation : une difficile balance entre marché libéral et protection juridique du consommateur

La croissance du commerce sur Internet s'est montrée aussi phénoménale que soudaine, et ne montre aucun signe de ralentissement. Selon une infographie réalisée pour le journal les Echos, le nombre de sites marchands est passé entre 2005 et 2015, « de 14 500 à 182 000 »[66]. Un marché donc en pleine explosion, mais très inégal, puisque 5% des sites totalisent 85% des ventes réalisées. La facilitation constante du processus d'achat, notamment via de nouveaux produits comme l'Amazon Echo ou le Google Home, ou

[65] « Protéger les Internautes – Rapport sur la Cybercriminalité », Groupe de Travail Interministériel de lutte contre la Cybercriminalité présidé par le procureur général près la cour d'appel de Riom, Marc Robert, Institut national des hautes études de la sécurité et de la justice, juillet 2015, ISSN 2265-447X

[66] « E-commerce : 10 ans de croissance ininterrompue en France », Elsa Dicharry, Geneviève Thibaud, Michaël Mastrangelo, Les Echos, 2 mai 2016

simplement une ergonomie toujours plus importante des sites, devrait encourager la poursuite de cette croissance.

Ces transactions se heurtent cependant régulièrement à des problèmes majeurs, liés notamment à la distance qu'elles créent entre vendeur et acheteur. Produits défectueux ou n'arrivant jamais, refus de remboursements, et bien sûr les risques encourus suite à l'abondante transmission de données personnelles par l'utilisateur.

L'établissement d'un cadre juridique pour ce nouveau marché devenait ainsi nécessaire afin d'en protéger les usagers.

A cette fin, l'Organisation de Coopération et de Développement Economique (OCDE) a publié en 2016 un ensemble de recommandations sur la bonne législation de l'e-commerce. Ces recommandations demandent avant tout que l'e-commerce ne reçoive pas un traitement différent des autres marchés : « Les consommateurs qui prennent part au commerce électronique devraient bénéficier d'une protection transparente et efficace d'un niveau au moins équivalent à celui de la protection assurée dans d'autres formes de commerce »[67]. Elles insistent par ailleurs sur la nécessité de prohiber les pratiques déloyales, l'importance de la transparence et de la bonne foi tout au long du processus de vente, et surtout « une réparation du préjudice subi du fait de biens ou de services dont il s'avère, par exemple, qu'ils sont défectueux ou dommageables pour leurs appareils ou qu'ils ne répondent pas aux critères de qualité annoncés ou encore en cas de problèmes de fourniture de ces biens ou services. »

Pour de nombreux pays, notamment les émergents, ces recommandations ne sont pas encore en application. Pris de cours par l'explosion du commerce électronique, de nombreux Etats comme l'Inde doivent se contenter d'appliquer au cyberespace le droit conçu pour le commerce traditionnel. Comme précisé par le journal indien Amie legal, « les intérêts du consommateur sont protégés par le Consumer Protection Act de 1968. […] et les protège même en l'absence de législation spécifiquement dédiée aux transactions électroniques »[68]. Cette solution ne peut être que transitoire, car comme on l'a vu précédemment, le droit commun ne peut indéfiniment s'adapter au cyberespace et ses spécificités. Comme le dénote l'article, « avec l'apparition de nouvelles pratiques et technologies, la loi se doit de se mettre à jour […]. Des problèmes comme la juridiction des transactions électroniques internationales dans les forums locaux, l'absence de protection pour les services annoncés comme gratuits […] se doivent d'être adressés immédiatement ».

Des pays comme les Etats-Unis ont déjà entamé cette transition, dans le droit de chaque état et, tout comme pour la neutralité du net, via les règlements édictés par la FTC[69].

[67] OCDE (2016), La protection du consommateur dans le commerce électronique : Recommandation de l'OCDE, Éditions OCDE, Paris

[68] Aditi Lahiri, « Consumer Protection in E-commerce in India », AMIE Legal, 15 mars 2018

[69] Gerald Spindler & Fritjof Börner, « E-Commerce Law in Europe and the USA », Springer, 8 avril 2002, ISBN : 3540431845

Mais c'est véritablement l'Union Européenne qui actuellement se dote des outils les plus imposants pour la législation du commerce électronique.

L'UE travaille en effet actuellement à la mise en place du Marché Commun numérique, l'alter ego sur Internet de la zone de libre échange qui fait de l'Union un acteur économique si important. La Commission de Jean-Claude Juncker a entamé un travail de longue haleine afin de créer une zone similaire sur Internet pour les commerçants et consommateurs européens, ou un droit commun s'applique à tous afin de faciliter les transactions internationales. L'enjeu est de taille : selon un rapport publié par l'agence irlandaise Wolfgang Digital, si les dépenses en ligne européennes sont déjà estimées aux alentours de 500 milliards d'euros, ce chiffre devrait doubler d'ici 2020 avec la mise en place du Digital Single Market (DSM)[70].

Les caractéristiques de ce nouveau marché sont expliquées par la Commission comme reposant sur trois piliers, qui font écho à ceux des Communautés Economiques Européennes : l'accès aux biens et services en ligne, les bonnes conditions pour le développement et la croissance des réseaux et services en ligne, et la croissance de l'économie digitale européenne[71]. L'absence de droit commun crée en effets de nombreux freins au développement de cette économie, en créant pour consommateurs et vendeurs incertitudes, frais supplémentaires, et un manque de protection quant aux droits du consommateur dans les transactions internationales. La mise en application de ces piliers passe par des mesures législatives visant à abolir les frontières numériques entre pays européens tout comme leur pendant physique. Ainsi, la suppression des coûts des données mobiles itinérantes[72] a permis aux Européens de jouir plus facilement du cyberespace en dehors de leur nation d'origine.

D'autres mesures majeures existent par ailleurs, comme l'actuelle proposition de directive au regard du commerce des biens et services entièrement digitaux, jusqu'alors non couvert par le droit communautaire[73] ; En prévoyant un cadre et des solutions strictes à ce marché (par exemple, la rupture immédiate du contrat par le consommateur, assortie d'un remboursement sous quinzaine, en cas de non-performance), l'Union Européenne renforce la confiance de ses citoyens et favorise les échanges. De la même manière, l'UE lutte contre le geoblocking, cette pratique qui consiste à restreindre l'accès aux services d'une entreprise en

[70] Wolfgang Digital, « Irish Online Economy Report 2016 », 2017

[71] Commission Européenne, « COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS : Stratégie pour un marché unique numérique en Europe », 6 mai 2015, COM(2015) 192 final

[72] Règlement 2017/920 modifiant le règlement (UE) no 531/2012 en ce qui concerne les règles applicables aux marchés de gros de l'itinérance, 32017R0920, adopté le 17 mai 2017, JO du 9 juin 2017, p. 1-8, entré en vigueur le 15 juin 2017

[73] Commission Européenne, « Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content » COM (2015) 634, 9 décembre 2015

fonction de la position géographique de l'utilisateur, en l'interdisant quand elle est pratiquée sans le consentement de l'utilisateur.[74]

Ces différents textes législatifs et les mesures qu'ils contiennent obéissent aux principes de subsidiarité et de proportionnalité de l'Union Européenne ; ce qui signifie qu'ils ne pouvaient être rendus possible que par cette entité supranationale, du fait du très haut niveau de coopération interétatique qu'ils supposent. De fait, la régularisation de l'e-commerce demeure un domaine encore soumis à la doctrine paternaliste, l'impact sur la souveraineté des Etats étant trop grand pour qu'ils acceptent de la concéder à d'autres acteurs.

Une approche différente a été adoptée pour la lutte contre les cyber délits, ou le secteur privé joue un rôle essentiel.

2. La complexe lutte de tous les acteurs majeurs d'Internet contre une cybercriminalité croissante

Tel un écho de l'essor du commerce sur Internet, l'arrivée du cyberespace a provoqué une véritable explosion de la criminalité sur ce nouveau réseau ; escroqueries, rançonnement, trafics, vols, piratages, sont devenus monnaie courante. Le phénomène est tel que selon le rapport annuel publié par l'entreprise de cybersécurité Norton-Symantec, plus de 19 millions de Français, c'est-à-dire 42 % de la population connectée, en ont été victimes en 2017. Au total, le préjudice s'évaluerait à 6,1 milliards d'euros en 2017, contre 1,8 milliard en 2016.[75]

Cette croissance est due en grande partie aux difficultés que posent la répression d'une telle délinquance. Le rapport Robert de 2015 identifie 3 problèmes majeurs dans cette action : le manque d'information menant à une quasi-impossibilité de la prévention des infractions, la grande clandestinité des acteurs, et la volatilité de la preuve, qui en se cumulant et s'entremêlant compliquent grandement la tâche du législateur et des forces de police.

Le premier est majoritairement dû aux espaces sur lesquels cette criminalité prend place : le darkweb ou darknet, cet Internet seulement accessible via des programmes et applications spécifiques, invisibles aux yeux des utilisateurs et moteurs de recherche traditionnels, et devenu un haut lieu de villégiature pour la délinquance Internet. Le rapport le décrit comme « un lieu de commercialisation de produits illégaux (drogues, armes,) mais aussi de services illégaux (prestations de piratage de messagerie, vente de numéros de

[74] « RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur », 28 février 2018, 2018/302

[75] Norton-Symantec, « Rapport Norton sur les Cyber risques – Edition 2017 », Symantec Corporation, 2018

cartes bancaires, location de botnet pouvant permettre le lancement d'attaques par déni de service) »[76].

Pour les Etats, la lutte contre cette partie pervertie du deep web est incroyablement complexe. Si la plupart des droits ne se focalisent pas sur le support de la vente de marchandises illégales (en France, les articles 222-34 à 222- 43-1 du code pénal punissent ainsi le trafic de stupéfiants peu importe la plate-forme de vente[77]) il s'agit là sans contexte de l'espace le plus sûr pour les trafiquants en tout genre. Dans la répression sur ce domaine, les forces américaines emmenées par le FBI sont assurément les plus performantes, comptant a leur tableau de chasse des réussites comme la condamnation des créateurs de l'« eBay de la drogue » SilkRoad[78].

Le dark web permet également un anonymat quasi absolu de ses utilisateurs, notamment en évitant le recours à des adresses IP si utiles à l'identification des délinquants sur le web « de surface ». Cet anonymat est renforcé par l'usage de monnaies virtuelles comme le désormais célèbre Bitcoin, qui rend impossible le traçage par le biais des paiements. Comme le précise le rapport Robert, « le caractère transnational des atteintes cyber, leur anonymat, la volatilité de la preuve numérique nécessite d'agir le plus en amont possible. L'action judiciaire est illusoire si elle est exercée seule, sans l'appui préalable de l'action administrative : le renseignement ». Un mouvement général de lutte s'est donc mis en place, qui voit à la fois l'union des Etats mais aussi l'intervention d'acteurs privés.

Cette coopération passe avant tout par un partage des méthodes, au sein d'agences comme Interpol ou Europol, ou bilatéralement entre services d'investigation. Pour Jean-Paul Pinte, docteur en information scientifique et technique et expert en cybersécurité, « L'État se trouve impuissant à lui-seul pour garantir sa sécurité nationale. La coopération internationale constitue donc une composante indispensable à la mise en œuvre d'une réponse qui se voudrait efficace. Une telle coopération doit cependant faire face à un certain nombre d'enjeux. Aucun progrès ne peut être accompli dans le monde au niveau des attaques sans un travail de coopération entre les pays et Europol en est le principal coordonnateur avec le FBI. »[79]

Cette coopération entre les services exécutifs doit cependant s'assortir d'une évolution des outils législatifs mis à leur disposition. Le problème de l'anonymat mettait ici par exemple les enquêteurs français dans une situation difficile : les investigations sous pseudonymes sont en effet prohibées, ne pouvant servir que dans certaines situations

[76] « Protéger les Internautes – Rapport sur la Cybercriminalité », Groupe de Travail Interministériel de lutte contre la Cybercriminalité présidé par le procureur général près la cour d'appel de Riom, Marc Robert, Institut national des hautes études de la sécurité et de la justice, juillet 2015, ISSN 2265-447X

[77] articles 222-34 à 222- 43-1, Code Pénal Français, Titre II, Livre II, Chapitre II.

[78] Laurent Lequien, « Affaire Silk Road : le créateur de "l'eBay de la drogue" condamné (encore une fois) à perpétuité », La tribune, 2 juin 2017

[79] Jean-Paul Pinte, « La guerre contre le deep web et les hors la loi en ligne peut-elle être gagnée ? », Atlantico, 10 Novembre 2014

exceptionnelles. Il a fallu attendre un arrêté de 2015[80] pour remédier à cette situation et permettre une meilleure présence policière sur le dark web.

Les organisations supranationales ne sont pas en reste : notamment en Europe, elles favorisent la coopération entre Etats par la création d'autorités à cet effet, et dotent ces derniers des outils législatifs nécessaires à la lutte ; ainsi, la directive de l'UE sur le sujet en 2016[81] a notamment permis la création d'un « groupe de coopération » entre les Etats. L'Europe est ici avantagée par l'Union, qui lui évite les enjeux, rivalités et luttes internes qu'ont pu entraîner ailleurs ces tentatives de coopération[82].

Enfin, les services publics se sont vu dans l'obligation de solliciter l'assistance du secteur privé, et de ses connaissances techniques, afin de lutter au mieux contre la cybercriminalité. Les fournisseurs d'accès à Internet demeurent des alliés privilégiés, fournissant données personnelles et journaux de connexion. Les sociétés de recherche et développement sont parfois également à l'origine d'innovations techniques qui pourraient permettre un meilleur contrôle du cyberespace ; parmi ceux-ci, on peut notamment citer la compagnie d'Eugene Karpersky, inventeur d'une véritable « carte d'identité numérique » qui mettrait fin à l'anonymat absolu procuré par le dark web[83].

En rassemblant tous les acteurs d'Internet contre un ennemi commun, le cybercriminel, le domaine pénal est devenu une application quasi-parfaite de la doctrine du *« multistake-holderism »*. La guerre contre les délinquants du web demeure ainsi quasiment l'unique représentant d'une telle union entre gouvernements, organisations internationales, internautes et acteurs du secteur privé.

Elle se heurte cependant toujours à des infractions de plus en plus complexes et difficiles à réprimer, aussi variées que les opérations de rançonnages à grande échelle façon *WannaCry,* responsable en 2016 de la paralysie de milliers de foyers, entreprises ou encore hôpitaux[84], ou encore opérations de cyberactivisme comme le ver *Stuxnet*, attaque d'un genre révolutionnaire sur le programme nucléaire iranien[85].

[80] Arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme, JORF n°0251 du 29 octobre 2015 page 20121 texte n° 38

[81] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union , Journal Officiel de l'Union Européenne, 19 juillet 2016

[82] Alix Desforges, « La coopération Internationale et bilatérale en matière de cybersécurité : enjeux et rivalités », Laboratoire de L'Institut de Recherche Stratégique de l'Ecole Militaire (IRSEM) n°16, Ministère de la Défense

[83] Ryan Huang, "'Internet passport' will benefit security, and e-commerce", ZD Net, 12 Novembre 2013

[84] Damien Leloup, « Cyberattaque : ce que l'on sait de WannaCry, le logiciel de racket qui a touché des dizaines de pays », Le Monde, 13 mai 2017

[85] Nicolas Falliere, Liam O Murchu, et Eric Chien, « W32.Stuxnet Dossier », Symantec Security Response, 11 février 2011.

Conclusion

En conclusion, il ressort de cette analyse que les modèles adoptés pour réguler le cyberespace diffèrent largement d'un domaine à l'autre, s'adaptant aux besoins spécifiques de chacun. Des domaines théoriques étudiés, qu'il s'agisse des cyberlibertaires ou paternalisme, ou encore du *multistake-holderism*, il semble impossible d'en dégager un qui pourrait être efficacement appliqué à toutes ces problématiques. La régulation d'Internet demeure donc à l'image du cyberespace lui-même : ses facettes sont multiples, ses enjeux en perpétuel changement, et son évolution extrêmement rapide du fait du progrès technique.

Bibliographie

- Aditi Lahiri, « Consumer Protection in E-commerce in India », AMIE Legal, 15 mars 2018

- Alain Weill, Altice Europe CEO, SFR-Groupe Altice, dans « Où est la démocratie Numérique ? », Conférence des Rencontres Economiques d'Aix-en-Provence, juillet 2018

- Alix Desforges, « La coopération Internationale et bilatérale en matière de cybersécurité : enjeux et rivalités », Laboratoire de L'Institut de Recherche Stratégique de l'Ecole Militaire (IRSEM) n°16, Ministère de la Défense

- Andrew Griffin, « Uk Spying Law: government introduces law requiring Whatsapp and iMessage to break their own security », The Independant, 1er Mars 2016

- Ann Cavoukian, « Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices », Information and Privacy Commissioner, Ontario, Canada, Décembre 2012

- Arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme, JORF n°0251 du 29 octobre 2015 page 20121
  texte n° 38

- Art L721-3, Code de Commerce français

- Art. 11, Déclaration des Droits de l'Homme et du Citoyen, 26 août 1789

- Article 19, Déclaration Universelle des Droits de l'Homme, 1948

- Article 2, Loi n° 2015-912 du 24 juillet 2015 relative au renseignement

- Article 2, Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, 6 janvier 1978

- Article 25, Règlement Général sur La Protection des Données, Règlement Union Européenne 2016/679, 14 avril 2016

- Article 3, §3, « Règlement établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les

réseaux publics de communications mobiles à l'intérieur de l'Union », 25 novembre 2015, 2015/2120

- Article 33, Constitution de la République Populaire de Chine, 2004
- Article 7, RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL
- Article 8, Convention Européenne des Droits de l'Homme, 1953
- articles 222-34 à 222- 43-1, Code Pénal Français, Titre II, Livre II, Chapitre II.
- Bill Stewart (ed), « The Living Internet », Janvier 2000.
- Christopher Mele, "Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns", The New York Times, 28 Décembre 2016
- Citation d'Ajit Pai dans « Les Etats-Unis abrogent la neutralité du Net, un principe fondateur d'Internet », Le Monde, 14 décembre 2017
- Citation du Ministre de l'Interieur Belge Jan Jambon, dans « Why Terrorists Love PlayStation 4 », Kate Day, Politico, 15 novembre 2015.
- Clive Coleman, « Robin Hood Airport tweet bomb joke man wins case », BBC News, 27 Juillet 2012
- Commission Européenne, « COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS : Stratégie pour un marché unique numérique en Europe », 6 mai 2015, COM(2015) 192 final
- Commission Européenne, « Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content » COM (2015) 634, 9 décembre 2015
- Conseil Constitutionnel, Décision n° 2017-648 QPC du 4 août 2017
- Damien Leloup, « Cyberattaque : ce que l'on sait de WannaCry, le logiciel de racket qui a touché des dizaines de pays », Le Monde, 13 mai 2017
- Dan Jerker B. Svantesson, « An introduction to jurisdictional issues in cyberspace », 2004, Journal of law, information and science, 15(1), 50-74.
- Daniel J. Solove & Woodrow Hartzog, « The FTC and the new common law of privacy », Columbia Law Review, 20 août 2013
- David Legrand, « RGPD : une extension ajoute un refus global sur les sites utilisant le module Quantcast Choice », Nextinpact, 2 août 2018

- Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union , Journal Officiel de l'Union Européenne, 19 juillet 2016

- Dominique Vinck, « Sociologie des sciences », 1995, Armand Colin, p. 232.

- E.H., « How Does China Censor the Internet ? », The Economist, 22 Avril 2013

- Elsa Dicharry, Geneviève Thibaud, Michaël Mastrangelo, « E-commerce : 10 ans de croissance ininterrompue en France », Les Echos, 2 mai 2016

- « Faut-il sauver la Neutralité du Net ? », Du Grain à Moudre (France Culture), émission d'Hervé Gavette avec Michel Combot, directeur général de la fédération française de télécoms ; Axelle Lemaire, ancienne secrétaire d'Etat chargée du numérique et de l'innovation ; Valérie Nicolas, Maître de conférences en droit public à l'Université Paris Ouest-Nanterre-La Défense, spécialiste du droit des TIC, 13 décembre 2017

- « FCC Adopts Strong, Sustainable rules to protect the open Internet », FCC Press Release, 26 février 2015

- Félix Tréguer, "Intelligence Reform and the Snowden Paradox: The Case of France", Media and Communication Volume 5, Issue 1, Pages 17–28, 2017,

- « Freedom on the Net 2012 », FreedomHouse, 2012

- Gerald Spindler & Fritjof Börner, « E-Commerce Law in Europe and the USA », Springer, 8 avril 2002, ISBN : 3540431845

- Glenn Greenwald and Ewen MacAskill, « NSA Prism program taps in to user data of Apple, Google and others », The Guardian, 7 juin 2013

- Google Spain SL / Google Inc. V Agencia Española de Protección de Datos (AEPD) / Mario Costeja González, Cour de Justice de l'Union Européenne (grande chambre), 13 mai 2014, C-131/12

- Green v SIG Trading Ltd., Employment Appeal Tribunal, 2017

- Helene Gully, « Les dix plus grosses révélations de Wikileaks », Les Echos, 4 octobre 201

- internetlivestats.com, Real Time Statistics Project, (Worldometers / 7 Billion World)

- « Investigatory Powers Act 2016 c.25 », 29 novembre 2016, www.parliament.uk
- James Risen et Eric Lichtblaudec, « Bush Lets U.S. Spy on Callers Without Courts », New York Times, 16 décembre 2005
- Jean-Paul Pinte, « La guerre contre le deep web et les hors la loi en ligne peut-elle être gagnée ? », Atlantico, 10 Novembre 2014
- John P. Barlow, « Déclaration d'Indépendance du Cyberespace », Traduit et édité par Hache, février 1996
- Katie Hafner et Matthew Lyon, « Les sorciers du Net : les origines de l'Internet », Calmann-Levy, 1999, ISBN : 270212951X
- « Katz v. United States », Cour Supreme des Etats-Unis, 389 U.S. 347 (1967)
- « La neutralité du Net : le pour et le contre », dnsBelgium, 9 février 2018
- Laurent Lequien, « Affaire Silk Road : le créateur de "l'eBay de la drogue" condamné (encore une fois) à perpétuité », La tribune, 2 juin 2017
- Lawrence Lessig, « Codes and Other laws of Cyberspace », 1999, Basic Books
- « Le code fait loi – De la liberté dans le cyberespace », Framablog, 22 mai 2010 ; traduction en français de l'article de Lawrence Lessig : « Code Is Law : On Liberty in Cyberspace », Harvard Magazine, 2000.
- « Liberty v Home Office », High Court of Justice, Queen's Bench Division, 27 avril 2018, Case No: CO/1052/2017
- Marc Hufty, "Investigating Policy Processes: The Governance Analytical Framework (GAF)" In: Wiesmann, U., Hurni, H., et al. eds. Research for Sustainable Development: Foundations, Experiences, and Perspectives." (2011) Bern: Geographica Bernensia: 403–424.
- Marc Rees, « Le RGPD expliqué ligne par ligne (articles 1 à 23) », Nextinpact, 21 février 2018
- Miguel Heft et Claire Cain Miller, « 1986 Privacy Law Is Outrun by the Web », The New York Times, 9 Janvier 2011
- « New Principles to Preserve and Promote the Open and Interconnected Nature of Public Internet », FCC Press Release, 5 aout 2005
- Nicolas Falliere, Liam O Murchu, et Eric Chien, « W32.Stuxnet Dossier », Symantec Security Response, 11 février 2011.

- Norton-Symantec, « Rapport Norton sur les Cyber risques – Edition 2017 », Symantec Corporation, 2018

- OCDE (2016), La protection du consommateur dans le commerce électronique : Recommandation de l'OCDE, Éditions OCDE, Paris

- Olivier X. contre Cour d'Appel de Paris, Cour de Cassation, Chambre Criminelle, 20 mai 2015, N° de pourvoi: 14-81336

- PATRIOT ACT, 107th Congress of the USA, Government Publishing Office, 2001

- Paulina Borsook, « Cyberselfish: A Critical Romp Through the Terribly Libertarian Culture of High Tech », Public Affairs, 2000, ISBN 1891620789

- Premier Amendement, Bill of Rights, Constitution des Etats-Unis d'Amérique, 1791

- « Protéger les Internautes – Rapport sur la Cybercriminalité », Groupe de Travail Interministériel de lutte contre la Cybercriminalité présidé par le procureur général près la cour d'appel de Riom, Marc Robert, Institut national des hautes études de la sécurité et de la justice, juillet 2015, ISSN 2265-447X

- « Quatrième amendement », Constitution des Etats Unis d'Amérique, 1791

- « RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur », 28 février 2018, 2018/302

- Règlement du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal Officiel de l'Union Européenne, 4 mai 2016
- Règlement 2017/920 modifiant le règlement (UE) no 531/2012 en ce qui concerne les règles applicables aux marchés de gros de l'itinérance, 32017R0920, adopté le 17 mai 2017, JO du 9 juin 2017, p. 1-8, entré en vigueur le 15 juin 2017

- « Restoring Internet Freedom Order », FCC, 14 décembre 2017

- Ronda Hauben, « The Internet: On its International Origins and Collaborative Vision », 1 mai 2004

- Ryan Huang, "'Internet passport' will benefit security, and e-commerce", ZD Net, 12 Novembre 2013

- Sally Shipman Wentworth, « My Data. Your Business. », Internet Society, pour Better Business Bureau (bbb.com)

- Sébastien Mort, « Surveillance des correspondances privées dans le cyberespace aux États-Unis : un contrôle marqué au sceau du secret », extrait de Revue Française d'études Américaines, N°123, p. 33-53, Belin, 2010

- Section 5, Réglementations sur la sécurité, la protection et la gestion du réseau d'information informatique, 11 décembre 1997

- « Section 5 : Unfair or Deceptive Acts or Practices », Federal Trade Commission Act

- Shara Tikben, « Questions to Mark Zuckerberg show many senators don't get Facebook », Cnet magazine, 11 avril 2018

- Tim Wu, «Network Neutrality, Broadband Discrimination », Journal of Telecommunications and High Technology Law, vol. 2, p. 141, 2003

- The Economist, « The world's most valuable resource is no longer oil, but data », The economist, 6 mai 2017

- USA FREEDOM Act, 114th Congress of the USA, Government Publishing Office, 2015

- Vinton Cerf, « How the Internet Came to Be », pour "The Online User's Encyclopedia", Bernard Aboba, Addison-Wesley, Novembre 1993, ISBN 0-201-622149

- Wolfgang Digital, « Irish Online Economy Report 2016 », 2017

- Winston J. Maxwell, « La Protection des données à caractère personnel aux Etats-Unis : Convergences et divergences avec l'approche Européenne », dans « Le Cloud Computing, L'informatique en nuage », p. 71 à 78, 2013

- « 万载爆炸事件：新闻大战功与过 », people.com.cn, 10 mars 2001