UNIVERSITÉ DE NANTES

FACULTÉ DE DROIT ET SCIENCES POLITIQUES DE NANTES

& AGENCE UNIVERSITAIRE DE LA FRANCOPHONIE

ANNÉE UNIVERSITAIRE 2014-2015

Les intermédiaires de l'internet face aux droits de l'homme : de l'obligation de respecter à la responsabilité de protéger

MÉMOIRE DE RECHERCHE

MASTER 2 SPÉCIALITÉ DROIT INTERNATIONAL ET EUROPÉEN DES DROITS FONDAMENTAUX

Présenté par :

Guillaume CHAMPEAU

Tuteur :

Patrick CHAUMETTE

Directeur du Centre de Droit Maritime et Océanique (CDMO)

Responsable pédagogique du Master 2 Droit International et Européen des Droits Fondamentaux (MDIEDF)

NOTE OBTENUE : 32/40

REMERCIEMENTS

Toute ma reconnaissance va d'abord à **l'équipe pédagogique du Master 2** de droit international et européen des droits fondamentaux (M2DIEDF) qui en m'intégrant dans leur passionnante formation m'ont offert la possibilité de reprendre des études trop longtemps interrompues, ainsi qu'à **mon épouse**, qui a su trouver les mots pour m'y encourager, et la patience pour le supporter.

Je veux aussi remercier tout particulièrement le professeur Patrick **CHAUMETTE**, dont le tutorat m'aura été précieux par l'intérêt porté au sujet, la grande pertinence de ses conseils, la promptitude de ses réponses, et son regard à la fois neuf et expérimenté sur un sujet qu'il m'a permis de mieux cadrer. Ainsi que le professeur André **LUCAS**, dont l'amabilité et la bienveillance m'ont apporté la confiance nécessaire pour obéir à cette vieille envie de retrouver les chemins universitaires.

Enfin, que soient également remerciés :

Jérémie **ZIMMERMANN**, cofondateur de l'association La Quadrature du Net, et Benjamin **BAYART**, fondateur de la fédération de fournisseurs d'accès à internet associatifs French Data Network (FFDN), pour avoir si souvent expliqué avec brio comment les décisions techniques et juridiques altérant le fonctionnement d'internet avaient toujours un impact sur les droits et libertés des utilisateurs. Ils ont été et resteront d'importantes sources d'inspiration.

Eric **WALTER**, secrétaire général de la Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur internet (Hadopi), ancien conseiller technique au Secrétariat d'État aux affaires étrangères et aux droits de l'homme, pour avoir été un interlocuteur aussi ouvert au débat qu'intransigeant sur la solidité des arguments. Nos discussions et nos différences de vue ont toujours été sources d'enrichissement.

Ainsi que tous ceux qui par leur conduite exemplaire et leur droiture m'ont amené à la volonté de faire de la défense des droits de l'homme mon combat quotidien. Ce mémoire leur est dédié.

LISTE DES SIGLES ET ABRÉVIATIONS

ARCEP	Autorité de régulation des communications électroniques et des postes
CADH	Convention américaine des droits de l'homme
CADHP	Charte africaine des droits de l'homme et des peuples
CArDH	Charte arabe des droits de l'homme de 2004
Cass. civ	Chambre civile de la Cour de cassation française
CAUSE	Coalition against unlawful surveillance exports
CCE	Communication Commerce Électronique (LexisNexis Jurisclasseurs)
CDFUE	Charte des droits fondamentaux de l'Union européenne
CEDH	Convention européenne des droits de l'homme
CJUE	Cour de Justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
Cour EDH	Cour européenne des droits de l'homme
Cour IADH	Cour interaméricaine des droits de l'homme
DUDH	Déclaration universelle des droits de l'homme de 1948
EDRi	European Digital Rights
EPU	Examen Périodique Universel
FAI	Fournisseur d'accès à internet
FIDH	Fédération internationale des droits de l'homme
G29	Groupe de travail « article 29 » sur la protection des données
GNI	Global Network Initiative
HADOPI	Haute autorité pour la diffusion des œuvres et la protection des droits sur internet
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IETF	Internet Engineering Task Force
JCP	Juris-Classeur périodique (La Semaine Juridique), édition générale
LCEN	Loi pour la confiance dans l'économie numérique
NSA	National Security Agency
OCDE	Organisation de Coopération et de Développement Économiques
ONG	Organisation non gouvernementale
P2P	Peer-to-Peer (ou « pair à pair »)
PIDCP	Pacte international relatif aux droits civils et politiques
PIDESC	Pacte international relatif aux droits économiques, sociaux et culturels
RSF	Reporters Sans Frontières

RTD Eur.	Revue trimestrielle de droit européen (Dalloz)
RTDH	Revue trimestrielle des droits de l'homme
TDI	Telecommunications Industry Dialogue
TGI	Tribunal de grande instance
TIC	Technologies de l'information et de la communication
UIT	Union Internationale des Télécommunications
UNESCO	Organisation des Nations Unies pour l'éducation, la science et la culture
V.	Voir
W3C	World Wide Web Consortium

SOMMAIRE

« En utilisant son personnel et son équipement propres, IBM Allemagne a conçu et fourni l'assistance technologique dont le IIIe Reich avait besoin pour accomplir ce que personne n'avait accompli avant lui — l'automatisation de la destruction humaine ».[1]

« *L'informatique [...] ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». [2]

[1] Edwin BLACK, *IBM et l'Holocauste : l'alliance stratégique entre l'Allemagne nazie et la plus puissante multinationale américaine*, Robert Laffont, 2011, p.11.

[2] Art.1er de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

INTRODUCTION

L'agence spécialisée des Nations Unies pour les technologies de l'information et de la communication, l'Union Internationale des Télécommunications (UIT), estime qu'il y avait en 2014 près de 3 milliards d'utilisateurs d'internet dans le monde, soit 40 % de la population mondiale[3]. Près de la moitié d'entre eux sont inscrits en tant qu'utilisateurs d'un même service privé, Facebook. Parmi eux 900 millions d'internautes — soit 12,5 % de la population mondiale — reviennent chaque jour[4] utiliser les services du réseau social américain pour s'informer, partager des informations publiques ou privées, se réunir et discuter avec leurs amis ou leur famille, ou encore pour organiser des rencontres ou manifestations, en confiant au passage à l'entreprise commerciale une quantité insoupçonnée de données personnelles. S'il existait une citoyenneté Facebook, le pays virtuel serait le premier au monde devant la Chine et l'Inde. Et sans aucun doute, il serait de très loin le mieux informé sur les habitudes, les centres d'intérêt, les relations intimes et les opinions de chacun de ses concitoyens.

Mais l'homme peut-il jouir de la liberté qui devrait être la sienne dans un environnement social où tout ce qu'il fait et tout ce qu'il dit, se dit ou se fait par l'intermédiaire d'une tierce personne ? La question n'est pas que philosophique ; avec internet, elle est d'une grande actualité juridique, et elle devient fondamentalement politique. Elle concerne la place qu'occupent au côté des États ceux qu'il convient d'appeler les « intermédiaires de l'internet » dans l'effectivité du respect des droits des individus qui utilisent leurs services d'intermédiation sur les réseaux de communication électronique.

Dans un rapport qui étudie leur rôle pour la promotion des objectifs de politique publique, l'OCDE a défini ces « intermédiaires de l'internet » comme les personnes qui « *donnent accès, hébergent, transmettent ou indexent du contenu, des produits ou des services émis par des tiers sur l'internet, ou qui fournissent des services basés sur internet à des tiers* »[5]. Elle en avait ainsi identifié six grandes catégories : les fournisseurs d'accès à internet, les fournisseurs de traitements de données et d'hébergement sur le web, les portails et moteurs de recherche internet, les intermédiaires du commerce électronique, les systèmes de paiement

---

3 UIT, *The World in 2014: ICT Facts and Figures*, 2014, p.5. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf>

4 FACEBOOK, *Statistics*, Newsroom. [http://newsroom.fb.com/company-info/]

5 OCDE, *The Role of internet Intermediaries in Advancing Public Policy Objectives*, 2011, p.20. <http://dx.doi.org/10.1787/9789264115644-en>

sur internet, et les plate-formes participatives de mise en réseau (c'est-à-dire les « réseaux sociaux »). Pour l'UNESCO les intermédiaires de l'internet sont plus simplement les « *services et plate-formes qui hébergent, donnent accès à, indexent, ou facilitent la transmission et le partage de contenus créés par d'autres* »[6]. Or la place majeure acquise par certains de ces intermédiaires, et pas uniquement Facebook, impose de s'interroger sur le pouvoir dont ils disposent pour assurer ou au contraire miner l'effectivité du respect des droits de l'homme dans l'environnement numérique.

La question du rôle des intermédiaires en matière de droits de l'homme s'inscrit dans la continuité d'une réflexion déjà ancienne sur la responsabilité concurrente des États et des pouvoirs privés. Les prétendus droits naturels de l'homme furent mis en cause dès les formes primitives d'organisation sociale, qui se sont complexifiées jusqu'à concentrer d'importants pouvoirs dans les mains exclusives de l'État. C'est pourquoi s'est faite jour, d'abord au 18ème siècle puis surtout suite au traumatisme de la seconde guerre mondiale, la nécessité d'assurer une protection de l'individu contre les pouvoirs de l'État. Ce sont les États eux-mêmes, en créant les Nations Unies et en adoptant la Déclaration Universelle des Droits de l'Homme de 1948, qui ont manifesté leur prise de conscience des limites qu'ils se devaient d'imposer à leurs propres capacité de nuisance. Protéger l'homme contre l'État est toutefois apparu comme une condition nécessaire mais non suffisante à la protection des droits de l'homme, également menacés par les pouvoirs privés.

Souvent traitée comme secondaire, la question de la protection des droits fondamentaux des individus contre les pouvoirs privés fut soulevée rapidement après l'adoption des deux pactes de New York de 1966, qui n'engageaient que des États. Dès 1969, un professeur de droit public avait ainsi alerté la doctrine sur le fait que « *les pouvoirs privés sont parfois plus dangereux que les pouvoirs publics dans le monde contemporain* »[7]. L'auteur faisait remarquer qu'ils pouvaient porter atteinte non seulement aux droits de leurs propres membres, mais aussi à ceux des tiers avec lesquels ils entrent en rapport. C'est avec cette même préoccupation que l'UNESCO organisa donc à Alger en 1982 une réunion d'experts sur le rôle des pouvoirs privés comme facteurs de limitation des droits de l'homme. Ces experts regrettaient qu' « *alors qu'il existe des mécanismes internationaux de protection des droits de l'homme à l'encontre des pouvoirs étatiques, même s'ils ne sont pas toujours efficaces, rien*

---

6 UNESCO, *Fostering Freedom Online: the Role of internet Intermediaries*, 2014, p.21. <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>

7 Robert PELLOUX, « Réflexions sur les libertés collectives », *Revue des droits de l'homme*, Paris, Pédone, 1969 p.371, cité par Tran VAN MINH, « Droits de l'homme et pouvoirs privés : le problème de l'opposabilité », *Multinationales et droits de l'homme*, PUF, 1984, p. 97

n'existe à cet égard à l'encontre des pouvoirs privés non étatiques »[8]. En plein essor de la mondialisation, il s'agissait à l'époque essentiellement de s'inquiéter des risques que faisaient courir les puissantes sociétés commerciales transnationales sur les droits économiques, sociaux et culturels.

L'État s'étant toujours préoccupé de la défense des individus dans leurs rapports privés, y compris lorsqu'il s'agissait d'assurer l'effectivité de la doctrine libérale, il est apparu naturel qu'il cherche à limiter les potentielles violations des droits de l'homme par les sociétés privées, en établissant des règles législatives ou réglementaires qui s'imposent à elles. Mais cette protection est aussi le fruit d'une obligation faite aux États en vertu du droit international. Ratifié dans 168 pays, le Pacte international relatif aux droits civils et politiques (PIDCP) impose que les États parties « *s'engagent à respecter et à garantir à tous les individus se trouvant sur leur territoire et relevant de leur compétence les droits reconnus dans le présent Pacte* »[9]. Dès lors si une entreprise viole ou met en danger les droits d'un individu, il est de la responsabilité de l'État de prendre toutes les mesures proportionnées pour y mettre fin ou prévenir la violation. Le Comité des droits économiques, sociaux et culturels estime aussi que les États parties au Pacte international relatif aux droits économiques, sociaux et culturels (PIDESC) doivent non seulement « *respecter l'exercice* » des droits reconnus, mais aussi « *empêcher tout tiers de (les) violer dans d'autres pays s'ils sont à même d'influer sur ce tiers en usant de moyens d'ordre juridique ou politique compatibles avec la Charte des Nations Unies et le droit international applicable* »[10]. Enfin même si la Déclaration universelle des droits de l'homme (DUDH) de 1948 se concentre principalement sur les obligations qui incombent aux États, le préambule prévient que « *tous les organes de la société* », y compris les entreprises, doivent s'efforcer « *de développer le respect de ces droits et libertés* ».

---

8 UNESCO, *réunion d'experts sur le rôle des pouvoirs privés comme facteurs de limitation des droits de l'homme, Alger, 5-8 décembre 1982, Rapport final SS-82/CONF.610/10*. <http://unesdoc.unesco.org/images/0005/000575/057537FB.pdf>

9 Art. 2 du PIDCP

10 Comité des droits économiques, sociaux et culturels, *Observation générale n°14 sur le droit au meilleur santé susceptible d'être atteint (art. 12 du PIDESC)*, U.N. Doc. E/C.12/2000/4 (2000), $39. Voir aussi dans les mêmes termes, *Observation générale n°15 sur le droit à l'eau (art. 11 et 12)*, §33.

C'est donc pour donner corps à ces principes qu'au terme d'un long processus qui faillit ne jamais aboutir[11], le Conseil des droits de l'homme a enfin approuvé le 16 juin 2011[12] les « principes directeurs relatifs aux entreprises et aux droits de l'homme », élaborés par le Représentant spécial du Secrétaire général des Nations Unies chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises, John Ruggie[13]. Se fondant sur un cadre de référence « protéger, respecter et réparer », les « Principes de Ruggie » énoncent d'un côté « *les obligations existantes qui incombent aux États de respecter, protéger et mettre en œuvre les droits de l'homme et les libertés fondamentales* », et de l'autre « *le rôle dévolu aux entreprises (...) tenues de se conformer à toutes les lois applicables et de respecter les droits de l'homme* »[14].

Sont ainsi différenciés le rôle des États à qui incomberait l'obligation suprême de protéger les droits fondamentaux par des mesures actives, et le rôle des entreprises qui n'auraient que la responsabilité bienveillante de respecter les droits en s'abstenant d'y porter atteinte.

Il ne fait bien sûr aucun doute que sur internet aussi, les droits de la personne humaine doivent être protégés. Le principe a été rappelé s'il en était besoin par l'Assemblée générale des Nations unies dans une résolution du 18 décembre 2013, qui reprend les termes du Conseil des droits de l'homme[15] et « *affirme que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne* » [16]. En avril 2014, la réunion multi-partite mondiale sur la gouvernance de l'internet NETMundial, organisée au Brésil avec la participation de 87 pays, a abouti à une déclaration commune selon laquelle « *les droits que les personnes ont hors-ligne doivent aussi être protégés en ligne, conformément aux*

[11] *V.* Emmanuel DECAUX, « Présentation de la Journée d'étude du Centre de recherche sur les droits de l'homme et le droit humanitaire (CRDH) organisée à Paris le 9 février 2007 », *La responsabilité des entreprises multinationales en matière de droits de l'homme*, Emmanuel DECAUX (dir.), Bruylant, 2010, p.11-17.

[12] Conseil des droits de l'homme des Nations Unies, *résolution 17/4 sur les droits de l'homme et les sociétés transnationales et autres entreprises*, A/HRC/RES/17/4, 16 juin 2011.

[13] Conseil des droits de l'homme, 17ème session, « Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence «protéger, respecter et réparer» des Nations Unies », *Rapport du Représentant spécial du Secrétaire général chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises, John Ruggie*, A/HRC/17/31, 2011. <http://www.ohchr.org/Documents/Issues/Business/A.HRC.17.31_fr.pdf>

[14] *Idem*, « Principes généraux », p. 7.

[15] Conseil des Droits de l'Homme, 20ème session, résolution 20/8 sur « La promotion, la protection et l'exercice des droits de l'homme sur l'internet », A/HRC/RES/20/8, 5 juillet 2012. <http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20340>

[16] Assemblée Générale des Nations Unies, résolution 68/167 sur « le droit à la vie privée à l'ère du numérique », A/RES/68/167, 18 décembre 2013, §3. <http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167>

obligations légales internationales en matière de droits de l'homme, notamment les Pactes Internationaux sur les Droits Civils et Politiques et les Droits Économiques, Sociaux et Culturels, et la Convention sur les Droits des Personnes Handicapées »[17].

Par conséquent en vertu des Principes de Ruggie, les personnes morales qui proposent leurs services d'intermédiaire sur internet doivent elles-mêmes veiller à respecter les droits de l'homme lorsqu'elles sont en situation de pouvoir leur porter atteinte. C'est d'ailleurs cette obligation de respect qui occupe le plus la doctrine, légitimement préoccupée par les atteintes portées directement ou indirectement par les intermédiaires de l'internet au droit à la vie privée et à la protection des données personnelles[18], à la liberté d'expression[19], au droit de propriété intellectuelle[20], ou dans une moindre mesure à la liberté de réunion et d'association[21].

Mais n'a-t-on pas tort de continuer à n'envisager le rôle des intermédiaires de l'internet en matière de droits de l'homme que sous l'angle des menaces qu'ils représentent ? Leur fonction-même d'intermédiaire fait qu'ils peuvent tout à la fois entraver l'exercice de droits et de libertés s'ils font eux-mêmes acte d'intrusion ou imposent des restrictions, ou au contraire empêcher des intrusions et des restrictions de la part de tiers, en particulier des États, s'ils choisissent de faire efficacement écran et de protéger les utilisateurs de leurs services.

---

17 NETmundial Multistakeholder Statement, 24 avril 2014. <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>

18 *V.* par ex. Noémie WEINBAUM, « Les données personnelles confrontées aux objets connectés », *CCE* n°12, décembre 2014, étude 22 ; Emilie MOUCHARD, « La protection de la vie privée dès la conception ou l'intégration de la Privacy by Design comme mécanisme du régime général sur la protection des données en droit Européen », *Lex Electronica*, Vol. 18, n°2, automne 2013 ; Noémie WEINBAUM, « La protection des données personnelles à l'épreuve du nuage informatique », *La Semaine Juridique — Entreprise et Affaires*, n°46, 13 novembre 2014, 1578 ; Franck CONROY, sous la supervision de Laurent CYTERMANN, « L'encadrement du « big data » et la protection des droits fondamentaux », *Revue des Juristes de Sciences Po,* n° 10, Mars 2015, 118 ; Anne-Laure FALKMAN, « Les réseaux sociaux face à de nouvelles contraintes . - Impacts de la recommandation de la Commission des clauses abusives », *La Semaine Juridique Entreprise et Affaires*, n° 12, 19 Mars 2015, 1136.

19 *V.* par ex. Emmanuel DERIEUX, « Neutralité et responsabilité des intermédiaires de l'Internet . - Mythe ou réalité du principe de « neutralité » ? », *JCP* n° 13, 26 Mars 2012, doctr. 386 ; Nathalie MALLET-POUJOL, « La liberté d'expression sur l'internet : aspects de droit interne », D. 2007. 591 ; Emmanuelle ALLAIN, « Liberté d'expression : la nécessaire adaptation de l'arsenal répressif au Web 2.0 », AJ pénal 2015. 112.

20 *V.* par ex. Christophe CARON, « Contrefaire, c'est s'exprimer illicitement », *CCE* n° 6, Juin 2013, comm. 63 ; Frédéric POLLAUD-DULAIN, « Contrefaçon par internet », *RTD com.* 2008. 301 ; Michel VIVANT, « Internet, piratage et contrefaçon », D. 2009. 1808.

21 *V.* par ex. Katherine J. STRANDBURG, « Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance », Boston College Law Review, Vol. 49, No. 741, 2008 ; Julian CHIUNG-WEN HSU, Aurore MERLE, « Internet et les nouveaux mouvements sociaux à Taïwan », *Hermès, La Revue* 3/2009 (n° 55) , p. 97-105.

Il ne faut bien évidemment pas négliger la menace que représentent les intermédiaires de l'internet pour les droits et les libertés individuelles. Mais à la lumière des informations récentes sur l'existence de programmes de surveillance massive des communications privées dans des pays démocratiques, ou face aux restrictions croissantes à la liberté d'expression à travers le monde, il nous paraît tout aussi essentiel d'étudier comment les intermédiaires de l'internet peuvent apporter une protection effective des droits menacés par des États dont les pratiques sont parfois très éloignées des principes rappelés par la conférence NETMundial.

Tout comme les États ont pris conscience au siècle dernier de la nécessité de prendre entre eux des engagements pour reconnaître aux individus des droits universels et les protéger contre leur propre pouvoir de nuisance ou celui des tiers, les grandes sociétés transnationales qui fournissent des services sur internet prennent de plus en plus conscience de la possibilité et de la responsabilité qu'elles ont de protéger les droits des utilisateurs. Mais ne devrait-on pas parler d'une véritable obligation de protection des droits de l'homme par les intermédiaires de l'internet, et en tirer toutes les conséquences ?

La présente étude n'a pas pour ambition de détailler de façon exhaustive ou approfondie les atteintes aux droits fondamentaux qui sont ou pourraient être réalisées directement par les intermédiaires de l'internet, mais de brosser plus modestement le portrait d'une transition en cours — ou à tout le moins l'existence d'un rapport de force croissant — dans la politique de protection des droits de l'homme appliquée à internet, et d'en déceler les failles. Nous le ferons en nous appuyant principalement sur le droit international public, sur la pratique des multinationales de l'internet, et en faisant parfois quelques crochets vers le droit national, en particulier celui de la France qui nous est le plus familier.

Pour tordre le cou au langage binaire qui domine dans le numérique, c'est en trois temps que nous étudierons comment l'obligation faite aux intermédiaires de l'internet de respecter les droits de l'homme tend à se compléter d'une obligation de les protéger. Tout d'abord, nous verrons comment les intermédiaires appliquent l'obligation rappelée par les Principes de Ruggie de « se conformer à toutes les lois applicables et de respecter les droits de l'homme », ce qui peut être parfois antinomique (I). Puis, après avoir constaté que les États qui peinent à faire respecter leur droit national et les droits de l'homme sont eux-mêmes à l'origine directe ou indirecte de nombre d'atteintes portées aux droits fondamentaux sur internet (II), nous verrons comment se traduit chez certains prestataires le sentiment croissant d'une responsabilité, non plus seulement de respecter les droits des utilisateurs et des tiers, mais de les protéger lorsqu'ils sont menacés (III).

L'OBLIGATION DES INTERMÉDIAIRES DE L'INTERNET DE RESPECTER LES DROITS DE L'HOMME DANS LE CADRE DES LOIS NATIONALES

Selon les termes du Conseil d'État français, il faut désormais « *considérer comme un droit fondamental à part entière* » l'accès à internet[22], qui conditionne l'accès à d'autres droits (1.1). Mais le fait d'accéder sans entrave à internet n'est absolument pas une garantie suffisante du bénéfice effectif des droits fondamentaux auxquels les utilisateurs peuvent prétendre. Du fait de leur place incontournable, les intermédiaires qui fournissent l'accès à internet ou à des services en ligne doivent eux-mêmes veiller à respecter les droits des individus soumis à leur pouvoir privé, ce qui peut se heurter à la liberté contractuelle des entreprises (1.2). A cet égard, les États ressentent parfois des difficultés à imposer le rapport de force nécessaire pour faire respecter certains droits fondamentaux traduits dans leur droit national par des intermédiaires de l'internet soumis à d'autres droits nationaux (1.3).

1.1 – Le droit d'accès neutre à internet, nouvelle pierre angulaire des droits fondamentaux

Avant que les individus puissent prétendre au respect des droits de l'homme dans leurs activités en ligne et les opposer aux intermédiaires de l'internet, il faut d'abord établir le constat préliminaire que l'accès à internet est lui-même devenu une liberté fondamentale (1.1.1). Mais puisque les fournisseurs d'accès disposent du pouvoir technique d'opérer un traitement discriminatoire entre les services utilisés par leurs abonnés, voire entre leurs abonnés, il devient nécessaire de comprendre ce droit d'accéder à internet comme un droit à un accès neutre (1.1.2).

[22] Conseil d'État, *Étude annuelle 2014 : Le numérique et les droits fondamentaux*, août 2014, p.90.

1.1.1. La liberté fondamentale d'accéder à internet

C'est par la France que la question de la reconnaissance de l'accès à internet comme droit fondamental s'est présentée le plus concrètement, au moment où le gouvernement poussait à l'adoption de la loi « favorisant la diffusion et la protection de la création sur internet » (dite « loi Hadopi I »). Celle-ci prévoyait de confier à une autorité administrative indépendante le pouvoir d'ordonner la suspension de l'accès à internet d'un abonné accusé de n'avoir pas pris les mesures suffisantes pour empêcher la mise à disposition du public d'œuvres contrefaites. Par crainte que le modèle français ne fasse tâche d'huile, le Parlement européen s'était emparé du sujet pour tenter d'y faire obstacle au nom des droits fondamentaux. Avant l'adoption de la loi française, un amendement aux directives « Paquet Télécom » fut donc adopté en 2008 à une très large majorité[23] en première lecture, qui imposait qu' « *aucune restriction ne [puisse] être imposée aux droits et libertés fondamentaux des utilisateurs finaux [d'internet] sans décision préalable des autorités judiciaires, notamment conformément à l'article 11 de la charte des droits fondamentaux de l'Union européenne concernant la liberté d'expression et d'information, sauf lorsque la sécurité publique est menacée, auquel cas la décision peut intervenir ultérieurement* »[24]. La France rejeta publiquement l'interprétation selon laquelle l'amendement s'opposait aux sanctions administratives de coupure de l'accès à internet prévues par son projet de loi Hadopi[25], mais œuvrait tout de même en coulisses pour qu'il soit réécrit dans des termes plus permissifs. Un an plus tard lors de l'adoption définitive du Paquet Télécom révisé, le texte fut effectivement édulcoré, mais disposait toujours que « *les mesures nationales relatives à l'accès des utilisateurs finals aux services et applications, et à leur utilisation, via les réseaux de communications électroniques [doivent respecter] les libertés et droits fondamentaux des personnes physiques, y compris eu égard à la vie privée et au droit à un procès équitable, tel qu'il figure à l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* »[26].

---

23 573 voix contre 73.

24 *V.* Commission européenne, « Position de la Commission sur l'amendement 138 adopté par le Parlement européen lors de la session plénière du 24 septembre », 7 novembre 2008, MEMO/08/681. <http://europa.eu/rapid/press-release_MEMO-08-681_fr.htm?locale=fr>

25 *V.* « "Riposte graduée" rejetée à nouveau par le Parlement européen : quelles conséquences pour le projet de loi français ? », *CCE* n° 11, Novembre 2008, alerte 121.

26 Art. 1Er de la Directive 2009/136/CE du Parlement européen et du Conseil modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateur.

C'est dans ce contexte que le Conseil constitutionnel français eut à se prononcer sur l'existence d'un droit fondamental d'accéder à internet. Il jugea qu' « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions* », le droit à la liberté d'expression et de communication protégé par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 « *implique la liberté d'accéder à ces services* »[27]. Aussi, parce que la sanction de suspension de l'accès à internet aménagée par la loi Hadopi I pouvait « *conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile* »[28], le Conseil décidait de censurer la disposition qui confiait ce pouvoir à une autorité administrative. La loi fut en revanche validée lorsque cette prérogative — jamais appliquée et finalement supprimée[29] — fut confiée dans une loi Hadopi II à l'autorité judiciaire[30]. Le juge constitutionnel français venait ainsi de reconnaître le droit d'accès à internet en « *empruntant par capillarité la nature de son tuteur, la liberté d'expression* »[31], et en y transposant sa jurisprudence.

Au niveau universel également, le rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Franck La Rue, a considéré en 2011 que « *supprimer l'accès à l'internet et ce, quelle que soit la justification fournie, [...] est excessif et constitue une violation* » de l'article 19§3 du Pacte International relatif aux droits civils et politiques[32]. Quelques mois plus tard il précisera que *« bien que l'accès à internet ne soit pas encore un droit de l'homme en tant que tel* », il est « *indispensable non seulement à l'exercice du droit à la liberté d'expression mais aussi à celui d'autres droits, comme le droit à l'éducation, le droit de s'associer librement avec d'autres et le droit de réunion, le droit de participer pleinement à la vie sociale, culturelle et politique et le droit au développement économique ou social* »[33].

---

27 Conseil Constitutionnel, décision n° 2009-580 DC du 10 juin 2009, §12.

28 *Ibid.* §16

29 Un seul jugement ordonnant la suspension de l'accès a été prononcé, mais il n'a jamais été mis en œuvre. Le décret n° 2013-596 du 8 juillet 2013 est ensuite venu abroger le dispositif réglementaire. Ne reste plus qu'une amende de cinquième classe.

30 *V.* Christophe CARON, « La lutte contre la contrefaçon sur internet dans les lois HADOPI I et II », CCE n° 1, Janvier 2010, comm. 1.

31 Laure MARINO, « Le droit d'accès à internet, nouveau droit fondamental », D.2009, p.2045.

32 Frank LA RUE, *Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the internet*, A/HRC/17/27, 16 mai 2011, §78. <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>

Au niveau régional, la Cour européenne des droits de l'homme (Cour EDH) a eu l'occasion de « *déduire de l'ensemble des garanties générales protégeant la liberté d'expression qu'il y a lieu de reconnaître un droit d'accès sans entraves à Internet* »[34]. Avant elle, le Comité des ministres du Conseil de l'Europe avait reconnu que « *l'accès limité ou l'absence d'accès aux [technologies de l'information et de la communication] peut priver les individus de la capacité d'exercer pleinement leurs droits fondamentaux* »[35]. Dans l'Union européenne, la Commission a estimé que « *la sécurité, la stabilité et la résilience de l'internet et des autres technologies des communications électroniques constituent une des pierres angulaires de la démocratie* » et qu'il y a donc « *lieu de prévenir toute tentative arbitraire visant à empêcher les citoyens d'y accéder ou à en perturber l'accès* »[36].

Sans aller jusqu'à reconnaître un « droit à » qui générerait une obligation positive de fournir l'accès à internet, les États ont donc au minimum l'obligation de garantir la liberté d'accéder à internet en tant que « facilitateur » de l'exercice des droits de l'homme, ce qu'ils ne peuvent toutefois faire qu'avec le concours des fournisseurs d'accès à internet (FAI), qui font office d'intermédiaire entre l'internaute et internet. Or ces FAI n'offrent pas toujours le même internet, selon qu'ils décident ou non d'appliquer des restrictions.

1.1.2. La neutralité d'internet comme garantie fondamentale

Techniquement, avoir accès à internet c'est avoir la possibilité d'être à la fois « client » pour recevoir les données envoyées par les serveurs interconnectés qui forment le réseau mondial, et « serveur » pour envoyer soi-même des données vers d'autres clients. Avoir pleinement accès à internet nécessite donc, pour dire les choses plus simplement, de pouvoir communiquer librement avec l'ensemble des machines elles-mêmes connectées à internet, qu'il s'agisse des serveurs de grands sites internet mondialement connus ou du téléphone mobile de son voisin de pallier. Dès lors qu'une restriction empêche de recevoir ou d'envoyer correctement tout ou partie des informations, l'accès à internet devient vicié, et tous les droits fondamentaux qui dépendent de l'accès à internet s'en trouvent fragilisés.

---

33 Frank LA RUE, *Rapport établi par le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression* , A/66/290, 10 août 2011, §61. <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290>

34 Cour EDH, 18 décembre 2012, *Ahmet Yildirim c. Turquie* (req. N°3111/10), §31.

35 Conseil de l'Europe, « Déclaration du Comité des Ministres sur les droits de l'homme et l'état de droit dans la Société de l'information », 13 mai 2005, CM(2005)56 final. <https://wcd.coe.int/ViewDoc.jsp?id=849009>

36 Commission européenne, « Un partenariat pour la démocratie et une prospérité partagée avec le sud de la Méditarrenée », COM(2001) 200 final, 8 mars 2011, p. 12.

Lorsqu'internet a été conçu, les techniciens ont souhaité en faire un réseau sans intelligence, qui se contenterait de distribuer les paquets de données destinés aux uns et aux autres, sans appliquer aucune forme de traitement privilégié en fonction du contenu, de l'expéditeur ou du destinataire. L'intelligence serait reléguée à l'extérieur du réseau, sur les machines qui s'y connectent. C'est le principe dit du « end-to-end », qui a longtemps garanti par ce choix d'architecture technique le respect des droits et libertés par les FAI[37]. Mais c'est en constatant que les opérateurs commençaient à introduire de l'intelligence discriminatoire au sein du réseau que le professeur de droit américain Tim Wu a développé en 2003 le concept de la « neutralité du réseau»[38], devenu central dans tous les débats sur la régulation des télécommunications. Il existe une multitude de définitions du principe[39], dont l'une des plus claires et des plus efficaces est probablement celle retenue (pas encore définitivement) dans un rapport en cours d'adoption au Parlement européen. Elle dispose que la neutralité du réseau est « *le principe selon lequel l'ensemble du trafic internet est traité de façon égale, sans discrimination, limitation ni interférence, indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application* »[40].

Partout dans le monde, le débat porte sur la nécessité d'imposer ou non le respect strict de ce principe aux intermédiaires de l'internet, afin que les droits fondamentaux qui dépendent d'un accès sans entrave à internet soient respectés. Nombre d'opérateurs sont en effet tentés de porter atteinte au principe pour des motifs essentiellement commerciaux, souhaitant avoir la possibilité de favoriser sur leur réseau un service pour lequel ils reçoivent une rémunération complémentaire, ou au contraire de saper des communications qui font concurrence à leur propres intérêts[41]. Ce faisant, ils minent les droits reconnus aussi bien aux individus — au premier rang desquels la liberté d'expression et de communication — qu'aux personnes

---

37 *V.* David D. CLARK et Marjory S. BLUMENTHAL, « Rethinking the design of the internet. The end-to-end arguments vs. the brave new world », *ACM Transactions on internet Technology*, Vol. 1, No. 1, août 2001, p.70-109. <http://nms.lcs.mit.edu/6829-papers/bravenewworld.pdf>

38 Tim WU, « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863>

39 Pour un aperçu des différentes approches retenues par la doctrine, *V.* C. ERHEL, L. DE LA RAUDIERE, « Rapport d'information (...) sur la neutralité de l'internet et des réseaux », Assemblée Nationale, n° 3336, 13 avr. 2011, p, 69-71.

40 Pillar DEL CASTILLO VERA, « Rapport sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté (... », COM (2013) 627, Art. 2 (12 ter) tel qu'amendé par le Parlement européen le 3 avril 2014.

41 A titre d'exemple, les opérateurs de téléphonie mobile ont pendant longtemps interdit à leurs clients d'utiliser des applications comme Skype qui permettent de téléphoner à l'étranger en passant par le réseau internet, à des tarifs très inférieurs à ceux pratiqués par les opérateurs eux-mêmes.

morales, ces dernières étant par exemple privées de la liberté d'entreprendre[42] lorsque les services qu'elles développent subissent des restrictions qui les privent d'accès à la clientèle.

Aussi en dépit du débat qui persiste principalement sous l'effet de résistances économiques (qui ne sont pas dénuées de leur propre logique progressiste[43]), il serait singulier de soutenir l'idée qu'existerait une liberté d'accéder à internet, fondamentale parce qu'elle donne accès à l'exercice de droits fondamentaux, mais de considérer néanmoins que la neutralité de cet accès n'a pas à être garantie. Si l'on retient comme nous l'avons démontré qu'il existe un droit fondamental d'accéder à internet dérivé de la liberté d'expression et de communication, il est indispensable de reconnaître que cette liberté ne doit être pas être entravée en dehors de limitations légitimes reconnues classiquement par le droit international des droits de l'homme.

Une fois l'accès à internet proposé dans des conditions non discriminatoires par les FAI, le risque d'atteinte aux droits des individus se déplace alors vers les services eux-mêmes, qui ont eux aussi l'obligation de respecter les droits de l'homme.

1.2 – La liberté d'entreprendre des intermédiaires de l'internet confrontée à l'effet horizontal des droits fondamentaux

D'abord réservée aux opérateurs de télécommunications qui donnent accès aux services en ligne, la question de la neutralité des intermédiaires s'étend désormais aux services en ligne eux-mêmes, à travers des notions beaucoup plus discutées de « neutralité des plate-formes »[44] ou de « loyauté des plate-formes »[45]. Partant du constat que les intermédiaires de l'internet doivent respecter aussi bien les droits de leurs utilisateurs que les droits des tiers

---

42 Reconnue comme telle à l'article 16 de la Charte des droits fondamentaux de l'Union européenne.

43 L'idée étant que les opérateurs doivent pouvoir générer les revenus suffisants pour investir dans le déploiement des réseaux, et ainsi donner accès à internet à un nombre toujours plus importants d'individus, et participer à l'effectivité du droit au développement.

44 Conseil National du Numérique, « Neutralité des plateformes : Réunir les conditions d'un environnement numérique ouvert et soutenable », mai 2014. <http://www.cnnumerique.fr/wp-content/uploads/2014/06/CNNum_Rapport_Neutralite_des_plateformes.pdf>

45 Conseil d'État, *Op.cit* note 22, p. 217.

(1.2.1), ces concepts naissants visent à restreindre davantage la liberté contractuelle des entreprises qui fournissent leurs services d'intermédiation (1.2.2).

1.2.1. La responsabilité des intermédiaires de l'internet de respecter les droits de l'homme

Les Principes directeurs relatifs aux entreprises et aux droits de l'homme élaborés par le Représentant spécial du Secrétaire général des Nations Unies[46] disposent que « *les entreprises devraient respecter les droits de l'homme* », ce qui « *signifie qu'elles devraient éviter de porter atteinte aux droits de l'homme d'autrui et remédier aux incidences négatives sur les droits de l'homme dans lesquelles elles ont une part* »[47]. L'emploi du conditionnel plutôt que l'impératif peut surprendre alors que l'effet horizontal des droits fondamentaux n'est plus à démontrer[48], mais il s'agit pour l'essentiel d'une précaution oratoire due au fait que le document n'a pas vocation à être juridiquement contraignant. Le « guide interprétatif » élaboré par le Haut-Commissariat aux droits de l'homme[49] n'a d'ailleurs pas cette prudence, puisque s'il reconnaît que « *les traités internationaux relatifs aux droits de l'homme n'imposent pas d'obligations juridiques directes aux entreprises commerciales* »[50], il affirme néanmoins que « *la responsabilité de respecter les droits de l'homme [n'est pas] facultative* »[51] pour ces dernières. Approuvés à l'unanimité par le Conseil des droits de l'homme en 2011[52], les Principes directeurs « *s'appuient solidement sur le droit international des droits de l'homme existant* » et sur « *les normes et pratiques qui existaient déjà avant* », mais ils ne créent donc pas de nouvelles obligations juridiques[53]. Ils doivent être compris comme une aide à l'interprétation du droit, qui repose sur l'ensemble du corpus juridique international.

---

46 *Op.cit.* note 13.

47 *Idem*, principe directeur n°11.

48 *V.* Achim SEIFERT, « L'effet horizontal des droits fondamentaux », *RTD Eur.* 2012, p.801.

49 Haut-Commissariat aux droits de l'homme des Nations Unies, *La responsabilité des entreprises de respecter les droits de l'homme : guide interprétatif*, HR/PUB/12/02, 2012. <http://www.ohchr.org/Documents/Publications/HR_PUB_12_2_fr.pdf>

50 *Id.* p.12.

51 *Id.* p.15.

52 Conseil des droits de l'homme, résolution 17/4 du 16 juin 2011

53 Conseil des droits de l'homme, *Note d'information du secrétariat sur le Forum sur les entreprises et les droits de l'homme*, A/HRC/FBHR/2012/2, 25 septembre 2012, §4. <http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20860>

En premier lieu les entreprises se doivent de respecter le droit national, censé incarner la « courroie de transmission » entre les engagements de protection et de promotion des droits de l'homme pris au niveau international par les États, et les personnes privées placées sous leur juridiction. Mais les entreprises n'en ont pas moins l'obligation de respecter les droits fondamentaux en cas de défaillance de l'État. A cet égard le principe fondateur n°12 précise que « *la responsabilité des entreprises de respecter les droits de l'homme porte sur les droits de l'homme internationalement reconnus − à savoir, au minimum, ceux figurant dans la Charte internationale des droits de l'homme*[54]» et, ce qui intéresse moins directement notre sujet, « *les principes concernant les droits fondamentaux énoncés dans la Déclaration relative aux principes et droits fondamentaux au travail de l'Organisation internationale du Travail* ». Aussi en vertu de l'idée rappelée par la Déclaration et le programme d'action de Vienne selon laquelle « *tous les droits de l'homme sont universels, indissociables, interdépendants et intimement liés* »[55], c'est l'ensemble des droits reconnus à la personne humaine qui doivent être respectés par les entreprises susceptibles d'y porter directement ou indirectement atteinte ; y compris sur internet.

Or si l'on pense bien sûr immédiatement avec internet aux questions liées au respect du droit à la vie privée[56] menacé par la collecte et le traitement de données personnelles par de nombreux services en ligne, à la liberté d'opinion et d'expression[57] qui peut être fragilisée par ceux qui hébergent ou donnent accès aux publications, ou encore au droit de propriété (intellectuelle)[58] défié par le développement de la contrefaçon dématérialisée, les entreprises qui fournissent des services d'intermédiation sur internet sont aussi en position de porter atteinte à des droits qui — hélas — attirent moins l'attention.

Par exemple, les personnes souffrant de handicaps temporaires ou permanents, comme les aveugles, les malvoyants ou les malentendants doivent bénéficier sur internet de droits spécifiques reconnus par la convention relative aux droits des personnes handicapées, qui vise à favoriser à leur égard l'effectivité des droits universels. Ainsi c'est pour permettre aux

---

54 C'est-à-dire la Déclaration universelle des droits de l'homme de 1948 et les deux principaux instruments qui la codifient, le Pacte international relatif aux droits civils et politiques et le Pacte international relatif aux droits économiques, sociaux et culturels, de 1966.

55 ONU, *Déclaration et programme d'action de Vienne adoptés par la Conférence mondiale sur les droits de l'homme le 25 juin 1993*, A/Conf. 157/23, §5. <http://www.ohchr.org/Documents/Events/OHCHR20/VDPA_booklet_fr.pdf>

56 DUDH (art. 12), PIDCP (art. 17), CEDH (art. 8), CADH (art. 11).

57 DUDH (art.19), PIDCP (art.19), CEDH (art.10), CADH (art.13), CADHP (art. 9).

58 DUDH (art. 17), CEDH (art. 1Er du protocole additionnel n°1), CADHP (art. 14), CADH (art. 21), Convention pour l'élimination de toutes les formes de discrimination raciale (art. 5.d.v) .

personnes handicapées de « *vivre de façon indépendante et de participer pleinement à tous les aspects de la vie* » que les États signataires doivent faire en sorte d'assurer « *l'accès à la communication, y compris aux systèmes et technologies de l'information et de la communication* »[59]. Toutefois le World Wide Web Consortium (W3C), qui définit les standards techniques de création des pages des sites internet, n'avait pas attendu la convention signée en 2006 pour établir dès 1999 des « Web Content Accessibility Guidelines »[60], qui favorisent la création de contenus dans des formats accessibles pour chaque type de handicap. L'organisation avait déjà intégré sa responsabilité d'aider au respect des droits de l'homme sur internet, pour toutes les catégories d'utilisateurs.

Cependant en pratique, le respect des droits de l'homme sur internet se heurte aussi bien souvent aux propres intérêts commerciaux des intermédiaires, qu'ils défendent à travers des contrats imposés aux utilisateurs, qui leur font renoncer en partie au bénéfice de certains de leurs droits et libertés.

1.2.2. Les droits fondamentaux à l'épreuve du contrat d'adhésion

Encore parfois décrié à l'emporte-pièce comme une « zone de non-droit », internet est tout au contraire un espace d'omniprésence du droit. Non pas seulement par le corpus désormais imposant de règles juridiques spécifiques qui lui sont consacrées[61], mais plus encore parce que tout y est partout contrats. Il faut tout d'abord signer un premier contrat pour s'abonner à un fournisseur d'accès à internet, puis il faut ensuite signer virtuellement des contrats particuliers avec la quasi-totalité des services en ligne que l'on utilise, que ce soit pour y être actif en agissant sur le contenu, ou pour n'en bénéficier qu'en qualité de simple lecteur des informations affichées. Démuni du moindre pouvoir de négociation, avec pour seul choix alternatif de ne pas utiliser les services en cause, l'utilisateur d'internet se retrouve donc — souvent sans en avoir pleinement conscience — à signer un nombre considérable de contrats d'adhésion qui lui font accepter les clauses rédigées par les éditeurs des services.

Or en matière de contrats, le principe est le respect de l'autonomie de la volonté des parties, c'est-à-dire la liberté contractuelle. Les clauses réputées acceptées par l'utilisateur d'un

---

59 Convention relative aux droits des personnes handicapées du 13 décembre 2006, art. 9.

60 *V.* Web Content Accessibility Guidelines (WCAG) 2.0. <http://www.w3.org/TR/2008/REC-WCAG20-20081211/>

61 *V.* notamment Catherine FÉRAL-SCHUHL, *Cyberdroit : Le droit à l'épreuve d'internet*, 6ème éd., Dalloz, 2010, 997p. ; Vincent FAUCHOUX, Pierre DEPREZ, Jean-Michel BRUGUIERE, *Le droit de l'internet : Lois, contrats et usages*, 2ème éd., Lexis Nexis, 2014, 446p. ; Luc GRYNBAUM, Caroline Le Goffic, Lydia-Haidara MORLET, *Droit des activités numériques*, Dalloz, 2014, 1054p.

service sur internet lient ce dernier, et peuvent lui être opposées[62]. Mais cette liberté des cocontractants ne saurait être absolue et les États doivent veiller à ce que soit préservé entre les parties le respect d'un ordre public[63], et au dessus de lui le respect plus vaste des droits fondamentaux, qu'ils émanent du droit national ou du droit international. Lorsque la loi nationale ne prévoit pas explicitement la nullité de clauses qui seraient contraires aux droits fondamentaux, les tribunaux peuvent se référer aux traités qui lient les États. C'est ainsi que depuis un premier arrêt du genre en 1996 en matière de contrat de bail[64], la Cour de cassation française n'hésite plus à viser régulièrement la Convention européenne des droits de l'homme pour sanctionner de nullité les clauses contractuelles qui seraient contraires aux droits fondamentaux[65]. Et lorsque les tribunaux nationaux manquent à cette possibilité de convoquer le droit international pour annuler une clause contractuelle contraire aux droits de l'homme, les juridictions supra-nationales se font parfois un devoir d'y veiller. Ainsi la Cour européenne des droits de l'homme (Cour EDH) explique qu'elle « *ne saurait rester inerte* » lorsqu'une disposition d'un contrat privé est « *en flagrante contradiction* » avec les principes de la Convention[66].

Néanmoins, le respect des droits fondamentaux n'est pas non plus absolu entre les parties, ou plus exactement il fait l'objet de compromis entre les droits. Comme l'écrit le professeur Fages, « *même en contradiction avec un droit fondamental, une disposition contractuelle peut parfaitement produire ses effets si elle apparaît justifiée par un intérêt légitime, et proportionnée à ce qu'exige cet intérêt* »[67]. C'est donc comme souvent la mise en balance des intérêts qu'il convient d'effectuer, entre d'une part la liberté d'entreprendre qui s'exerce à travers le choix des clauses imposées aux clients, et d'autre part les différents droits des cocontractants qui peuvent être menacés dans leur exercice par l'application du contrat.

---

62 Cependant le simple affichage d'un lien menant aux conditions générales d'utilisation d'un site internet, en l'absence de leur acceptation expresse, ne suffit pas à leur opposabilité. Cf. *Cass. civ*, 1re, 31 octobre 2012, Métropole télévisions c. SBDS. <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3534>

63 En France, consacré par l'art. 6 du code civil : « *On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes moeurs.* »

64 *Cass. civ*, 3ème, 6 mars 1996, Mel Yedei (Bulletin 1996 III N° 60 p. 41). <http://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007035565>

65 Pour une liste d'exemples, *V.* Delphine COSTA, Anne PÉLISSIER, « Rapport introductif », *Contrats et droits fondamentaux*, Presses Universitaires d'Aix-Marseille, 2011, p. 14, note 10.

66 Cour EDH, 13 juillet 2004, *Pla et Puncernau c. Andorre* (req. n° 69492/01), §59. <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-66458>

67 Bertrand FAGES, *Droit des obligations*, LGDJ, 4ème éd., 2013, p. 141.

Sur ce principe, une clause attributive de compétence présente dans les conditions générales d'un réseau social sur internet a pu être jugée abusive car trop attentatoire au droit fondamental d'accès à la justice, en raison des « *difficultés pratiques et [du] coût d'accès aux juridictions californiennes* »[68]. Cependant la jurisprudence mettant en évidence la violation de droits fondamentaux par des dispositions contractuelles d'intermédiaires de l'internet est encore excessivement pauvre. L'essentiel des affaires concerne l'irrespect du droit à la vie privée et à la protection des données personnelles, à travers des clauses d'obtention du consentement souvent trop imprécises, ou des allégations de violation de droits de propriété intellectuelle, mais les actions reposent alors bien davantage sur le droit national que sur des instruments internationaux de protection des droits de l'homme.

A l'avenir, l'application de certaines dispositions contractuelles imposées par des intermédiaires difficilement contournables pourraient toutefois conduire à des recours appuyés sur l'effet direct des droits fondamentaux[69], les tribunaux prenant conscience qu'en présence d'une asymétrie de pouvoir entre personnes privées, « *une applicabilité horizontale des droits fondamentaux […] peut mettre la partie plus faible d'une relation contractuelle dans la position d'exercer son autonomie de volonté de manière effective* »[70]. Songeons à titre d'exemple à la clause présente dans les conditions de Facebook qui stipule que « *si vous enfreignez la lettre ou l'esprit [du contrat], ou créez autrement un risque de poursuites à notre encontre, nous pouvons arrêter de vous fournir tout ou partie de Facebook* »[71]. Dans quelle mesure un réseau social qui compte plus de 1,4 milliard de membres à travers le monde peut-il de façon discrétionnaire et sans préavis priver subitement l'un d'entre eux du droit de se réunir à distance avec les autres membres, du droit de s'exprimer librement sur la plate-forme, du droit de participer à la vie culturelle qui se manifeste sur le réseau social[72], ou encore du droit d'accéder aux informations qui y sont publiées[73] ? Et dans quelle mesure un individu est-il libre de refuser de participer à Facebook ou de risquer une telle exclusion de la

---

68 TGI de Paris, 4ème chambre, 2ème section, ordonnance du juge de la mise en état du 5 mars 2015, *Frédéric X. c. Facebook Inc*. <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4515>

69 *V.* Frédéric SUDRE, « Le juge national juge de droit commun de la Convention », in *Droit européen et international des droits de l'homme*, PUF, 12ème éd., 2015, §122.

70 Achim SEIFERT, *op.cit.* note 48, §I.B.1.

71 Facebook, « Déclaration des droits et responsabilités » telle que révisée au 30 janvier 2015, §14. <https://www.facebook.com/legal/terms?locale=fr_FR>

72 Selon le Comité des droits économiques, sociaux et culturels, la culture «*doit être considérée comme un processus interactif* », qui « *façonne et reflète les valeurs de bien-être ainsi que la vie économique, sociale et politique d'individus, de groupes d'individus et de communautés* ». Cf Observation n°21 sur le droit de chacun de participer à la vie culturelle (art.15, par.1a du PIDESC), §12-13. <http://www2.ohchr.org/english/bodies/cescr/docs/gc/E-C-12-GC-21_fr.doc>

73 Les pages du site Facebook n'étant pas visibles sans être inscrit.

vie sociale numérique (par exemple en ignorant les restrictions imposées contractuellement à sa liberté d'expression), alors qu'aujourd'hui l'accès à l'emploi semble facilité par la participation active aux principaux réseaux sociaux sur internet[74] , et que la vie privée et familiale se prolonge sur les espaces de discussion offerts aux proches ?

Il est vrai qu'en principe « *la responsabilité qui incombe aux entreprises de respecter les droits de l'homme s'applique à toutes les entreprises indépendamment de leur taille* » mais « *néanmoins, la portée et la complexité des moyens par lesquels les entreprises s'acquittent de cette responsabilité peuvent varier selon [ce] facteur*»[75]. Un intermédiaire de l'internet dont les services sont ainsi utilisés par des dizaines voire des centaines de millions d'internautes devra veiller tout particulièrement à l'incidence que peuvent avoir l'application de ses contrats sur les droits fondamentaux de ses clients. A cet égard, il est intéressant d'observer que Facebook propose une procédure d'appel en cas de désactivation d'un compte[76], ce qui est également le cas sur Twitter[77] ou encore YouTube[78]. Ces procédures privées de règlement des litiges visent à limiter les risques d'atteinte abusive aux droits fondamentaux de leurs utilisateurs, et expliquent peut-être en partie la pauvreté de la jurisprudence[79], ce qui peut être un signe de bon fonctionnement de l'auto-régulation. C'était aussi une préconisation du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, qui recommandait aux intermédiaires de l'internet d'instaurer « *des voies de recours effectives pour les utilisateurs concernés [...], y compris la possibilité d'un recours au travers des procédures prévues par l'intermédiaire et par une autorité judiciaire compétente* »[80].

Notons enfin que les contrats des intermédiaires reflètent également leur responsabilité de respecter non seulement les droits de leurs utilisateurs, mais aussi les droits des tiers.

---

74 V. Valérie CHARRIÈRE, Cécile DEJOUX, Françoise DUPUICH, « L'impact des réseaux sociaux et des compétences émotionnelles dans la recherche d'emploi : étude exploratoire », *Management & Avenir* 2/2014 (N° 68) , p. 137-163. <http://www.cairn.info/revue-management-et-avenir-2014-2-page-137.htm>

75 Principes directeurs, n°14, *op.cit* note 15

76 <https://www.facebook.com/help/185747581553788/>

77 <https://support.twitter.com/forms/general?subtopic=suspended>

78 <https://support.google.com/youtube/answer/2802168>

79 Aux Etats-Unis, Facebook a été poursuivi pour violation de la liberté d'expression par une utilisatrice dont le compte avait été suspendu, mais la justice a refusé de faire application du 1er amendement de la Constitution américaine à l'encontre d'une entreprise privée. Cf *Young v. Facebook, Inc.*, 790 F. Supp. 2D 1110 <http://docs.justia.com/cases/federal/district-courts/california/candce/5:2010cv03579/230726/34/0.pdf?ts=1288078449>

80 Nations Unies, *Conseil des droits de l'homme*, « Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue », A/HRC/17/27, §76. <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/17/27>

Comme d'autres, le contrat de Facebook intègre ainsi toute une section dédiée à la « protection des droits d'autrui »[81], qui interdit de façon générale d' « *enfreindre les droits d'autrui ou autrement enfreindre la loi* », et qui vise en particulier le droit de propriété intellectuelle ou le droit à la vie privée des tiers. Toutefois la volonté affichée par les intermédiaires de l'internet de respecter les droits fondamentaux n'est pas toujours ressentie comme telle par les États, qui peinent à protéger leur propre vision des droits de l'homme sur internet à travers leur droit national.

1.3 – L'universalité des droits de l'homme face à un internet traversé par une diversité d'ordres juridiques

Respecter les droits de l'homme, oui, mais lesquels ? Internet est par essence un réseau international dans lequel les communications entre les hommes ne connaissent aucune frontière, ce qui tend à favoriser une forme d'uniformisation du respect des droits de l'homme autour des seules obligations auxquelles les intermédiaires de l'internet se sentent soumis (1.3.1). Mais même sans frontières matérielles, les cultures et les ordres juridiques propres à chaque État demeurent et comme l'a indiqué la Cour EDH dans son arrêt *Lopez-Ostra*, les autorités nationales ont la responsabilité de prendre chacune les mesures nécessaires pour protéger sous leur juridiction les droits humains définis par les traités internationaux[82], ce qui peut passer par l'obligation positive de prendre des mesures législatives protectrices[83]. La globalisation des droits fondamentaux sur internet doit alors composer avec la diversité des ordres juridiques qu'il traverse (1.3.2).

1.3.1. Le risque d'uniformisation des droits fondamentaux appliqués à internet

Ce n'est pas parce qu'il existe une Déclaration universelle des droits de l'homme approuvée par la quasi-totalité des États du monde et qu'est ainsi soutenu le principe idéal d'une universalité des droits garantis à l'ensemble de la communauté humaine qu'il n'existe

81 *Op. cit.* note 71, §5.

82 *V.* Cour EDH, 9 décembre 1994, *López Ostra c. Espagne* (req. n°16798/90), §55.

83 *V.* Cour EDH, 13 août 1981, *Young, James et Webster c. Royaume-Uni* (req. n° 7601/76; 7806/77), §49.

qu'une et une seule vision, uniforme et absolue, des droits fondamentaux. En dehors (et encore) du « noyau dur » formé par les droits intangibles reconnus explicitement comme tels[84] par l'ensemble des textes internationaux à portée générale[85], il existe une pluralité d'interprétations et de sensibilités différentes selon les cultures.

Comme l'enseignait le professeur Gérard Cohen-Jonathan, « *il faut se convaincre que l'universalité des droits de l'homme ne correspond aucunement à un impérialisme culturel* », et accepter que « *le droit international des droits de l'homme est pluriel et doit prendre en compte le droit à la différence, la diversité des cultures* »[86]. Mais comment s'exprime cette nécessaire diversité sur un internet qui fait figure de paroxysme de la mondialisation ?

Lorsque l'on évoque la place qu'occupent les intermédiaires de l'internet dans la communication mondialisée et leur rôle dans la protection des droits de l'homme, on ne peut écarter la question de l'universalité des droits de l'homme de celle de l'impérialisme économique et culturel. Internet est en effet le règne de ce que les économistes surnomment le « Winners-Take-All ». Les leaders du marché tendent à en rafler très vite une part disproportionnée, plus encore sur internet que dans l'économie libérale traditionnelle[87]. Google fournit ainsi les réponses aux recherches de 90 % des internautes dans le monde, et même 95 % en France[88]. Facebook administre le réseau social que près d'un milliard d'internautes utilisent chaque jour pour communiquer ensemble, et a fait l'acquisition à prix d'or de WhatsApp, une messagerie en forte croissance qui comptait moins de 500 millions d'utilisateurs mensuels lors de son rachat début 2014[89], et plus de 800 millions d'utilisateurs un an plus tard[90]. YouTube (propriété de Google) délivre chaque jour 4 milliards de vidéos à plus d'un milliard de spectateurs chaque mois, et « *300 heures de vidéo sont mises en ligne chaque minute sur YouTube* »[91] par les utilisateurs du monde entier. Nous pourrions ainsi

84 Droit à la vie, droit de ne pas être torturé ni de subir de traitements inhumains ou dégradants, interdiction de l'esclavage ou de la servitude, et non-rétroactivité de la loi pénale plus dure.

85 A l'exception notable de la Charte africaine des droits de l'homme et des peuples.

86 Gérard COHEN-JONATHAN, « Universalité et singularité des droits de l'homme », Discours prononcé le 25 juillet 2002 lors de la séance de clôture de la 33e session d'enseignement de l'Institut international des droits de l'homme, *RTDH* 53/2003. En ligne : <http://www.rtdh.eu/pdf/20033.pdf>, p.10.

87 *V.* Edouard LAUGIER, « GAFTAM : 'Winner takes it all' », *Le nouvel économiste*, 17 juillet 2014. <http://www.lenouveleconomiste.fr/gaftam-winner-takes-it-all-23479/>

88 *V.* <http://www.blogdumoderateur.com/chiffres-google/>

89 Robert HOF, « In One Chart, Here's Why Facebook Is Blowing $19 Billion On WhatsApp », Forbes, 19 février 2014. <http://www.forbes.com/sites/roberthof/2014/02/19/in-one-chart-heres-why-facebook-is-blowing-19-billion-on-whatsapp/>

90 Nate RALPH, « WhatsApp touts 800M monthly active users », *CNET*, 18 avril 2015. <http://www.cnet.com/news/whatsapp-touts-800m-monthly-active-users/>

91 *V.* <http://www.youtube.com/yt/press/fr/statistics.html>

multiplier les exemples d'hégémonies d'intermédiaires de l'internet, qui obligent à s'interroger sur la verticalité de l'effet horizontal des droits fondamentaux dont ils se font ensuite les relais à l'endroit de l'ensemble des utilisateurs et des tiers placés sous leur responsabilité.

Sur les dix sites internet les plus visités au monde[92], trois sont originaires de Chine (le moteur de recherche Baidu, la plate-forme marchande Taobao et le portail QQ.com) et tous les trois ne sont toujours proposés pour le moment qu'exclusivement en langue chinoise, ce qui assure une certaine cohérence entre la « culture locale des droits de l'homme » et les pratiques des entreprises du pays sur internet — avec évidemment toutes les précautions oratoires qu'il convient d'ajouter concernant les droits de l'homme en Chine, en prenant garde toutefois à ne pas tomber dans la caricature occidentaliste vers laquelle peut justement conduire l'idée d'universalité[93]. Les sept autres (Google, Facebook, YouTube, Yahoo, Wikipedia, Amazon et Twitter) sont tous Américains et proposés au contraire dans une multitude de langues différentes[94], ce qui favorise la globalisation de la culture américaine des droits de l'homme à travers les politiques qu'ils appliquent à leurs services.

C'est ainsi qu'en voulant respecter l'orientation sexuelle et les choix de vie familiale de ses membres, Facebook a intégré en 2012 la possibilité pour l'ensemble de ses 1,5 milliard de membres de se déclarer marié(e) à une personne du même sexe[95], puis a introduit en 2014 la possibilité de décrire son genre, non plus seulement comme « homme » ou « femme », mais aussi comme « transsexuel » ou « intersexuel »[96]. En revanche Facebook n'offre pas aux utilisateurs la possibilité de déclarer plusieurs conjoints ou compagnons de vie. Il n'est pas question pour le réseau social américain de paraître encourager ou même reconnaître la polygamie, même si elle est reconnue légalement et pratiquée dans une cinquantaine de pays du monde, dont de nombreux pays africains dans lesquels Facebook est très utilisé. Le réseau social participe ainsi à la diffusion de ce que la Cour EDH avait décrit comme le choix d'une

---

92 *V.* Classement Alexa <http://www.alexa.com/topsites>

93 *V.* Geneviève MÉDEVIELLE, « La difficile question de l'universalité des droits de l'homme », *Transversalités* 3/2008 (N° 107) , p. 69-91. <http://www.cairn.info/revue-transversalites-2008-3-page-69.htm>

94 A titre d'exemples, Facebook est disponible en 92 langues, Google et YouTube en 97 langues, Twitter en 29 langues et Wikipedia propose des articles dans 280 langues.

95 Samantha MURPHY KELLY, « Facebook Adds Same-Sex Marriage Icons for Couples », *Mashable*, 2 juillet 2012. <http://mashable.com/2012/07/02/facebook-same-sex-marriage/>

96 Pour le moment uniquement dans la version américaine, la version francophone proposant un champ « autre » pour décrire librement son orientation sexuelle. *V.* Maximilien DE LESELEUC, « Facebook reconnaît les Transsexuels et Intersexuels », *Tom's Guide*, 14 février 2014. <http://www.tomsguide.fr/actualite/facebook-trans-intersexuels,40401.html>

société « *adhérant au principe de la monogamie* »[97], laquelle n'est pas universelle. Le refus de la prise en compte de la réalité polygame participe en outre à la confusion entre les régimes discriminatoires n'autorisant que la polygynie et les régimes libéraux (certes bien plus rares) autorisant la polygamie à égalité entre les sexes.

Entre autres exemples, évoquons aussi le choix de YouTube d'autoriser le partage d'un film critiquant durement l'islam et parodiant le prophète Mahomet. La plate-forme a estimé que le film qui a provoqué une vague de violences en Égypte et en Libye[98] n'était pas contraire à ses règles d'utilisation. Elle a appliqué à son bénéfice la jurisprudence très permissive de la Cour suprême des États-Unis concernant la liberté d'expression garantie par le premier amendement de la Constitution américaine[99], se contentant de bloquer l'accès à la vidéo depuis les deux pays précités, pour des raisons beaucoup plus diplomatiques que juridiques[100]. C'est bien la prééminence de la liberté d'expression sur le droit au respect des convictions religieuses qui a incité YouTube à appliquer cette politique, héritée de sa culture américaine. Sans doute sa vision de la hiérarchie des droits de l'homme (en principe inexistante mais en réalité très présente) aurait-elle été différente si la plate-forme avait été éditée depuis un pays adhérant à la Charte arabe des droits de l'homme de 2004 (CArDH)[101]. Non pas que l'article 32 de cette Charte consacré à la liberté d'opinion et d'expression soit très éloigné de l'article 19 du PIDCP — ils sont même en réalité très proches, mais plutôt que la culture sous-jacente à la CArDH invite à davantage prendre en compte le respect des croyances dans « l'ordre public » ou « la moralité publique » à sauvegarder.

Néanmoins, les États dont le système juridique n'a pas infusé jusque dans les pratiques des intermédiaires de l'internet ont aussi les moyens de faire respecter leur droit national, ce qu'ils font dans les limites du rapport de force qu'ils parviennent ou non à opposer.

---

97 CEDH, *Johnston et autres c/Royaume-Uni*, 18 décembre 1986, A.112, § 52.

98 *V.* Hélène SALLON, « "L'Innocence des musulmans", le film qui a mis le feu aux poudres », *Le Monde*, 12 septembre 2012. <http://www.lemonde.fr/afrique/article/2012/09/12/l-innocence-des-musulmans-le-film-qui-a-mis-le-feu-aux-poudres_1758964_3212.html>

99 Celle-ci estime qu'il ne suffit pas de prouver la simple potentialité d'un risque pour l'ordre public pour réprimer l'énoncé d'une opinion, fut-ce même un discours raciste. Il faut démontrer l'existence d'un risque « imminent », tel que l'appel explicite à commettre des crimes. *V.* Cour Suprême des Etats-Unis, *Brandenburg v. Ohio* : 395 US 444 [1969].

100 *V.* « YouTube bloque l'accès à "L'Innocence des musulmans" dans certains pays », *Le Monde*, 13 septembre 2012. <http://www.lemonde.fr/technologies/article/2012/09/13/youtube-bloque-l-acces-a-l-innocence-des-musulmans-dans-plusieurs-pays_1759947_651865.html>

101 Charte arabe des droits de l'homme de 2004. <http://www.acihl.org/texts.htm?article_id=16>

1.3.2. Le rapport de force opposé par le droit national dans un monde sans frontières

« *C'est où internet ?* », demandait Grégoire Loiseau. « *L'enthousiaste : partout ! Le sceptique : nulle part ! Le réaliste : quelque part* »[102]. La question est bien sûr de première importance puisque la réponse détermine le droit applicable et influe sur la responsabilité des États. Rappelons que le PIDCP leur impose de garantir les droits reconnus « *se trouvant sur leur territoire et relevant de leur compétence* »[103], tandis que les pays signataires de la CEDH « *reconnaissent à toute personne relevant de leur juridiction* »[104] les droits et libertés définis dans la Convention. On peut donc défendre l'idée que les États ont la responsabilité de garantir les droits de l'homme non seulement à leurs nationaux et aux étrangers présents sur leur territoire, mais aussi aux individus qui, sur internet, utiliseraient les services fournis par des intermédiaires de l'internet dont le siège social, un établissement secondaire ou même de simples serveurs essentiels au fonctionnement du service se trouveraient placés sous leur juridiction. Or à l'ère de « l'informatique en nuage » (ou « cloud computing ») dans laquelle les données concernant un même service sont sans cesse morcelées, reproduites et transportées à travers des centres de données localisés dans une multitude de pays différents, le nombre d'États susceptibles de revendiquer leur compétence pour la protection des droits sur internet semble plus élevé que jamais.

C'est pourquoi il paraît aujourd'hui surréaliste de relire les propos de l'un des pionniers de la défense des droits et libertés sur internet, qui dans une célèbre « Déclaration d'indépendance du cyberespace » proclamait en 1996, en s'adressant aux gouvernements des États : « *I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. […] We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders* »[105].

Vingt ans plus tard, que reste-t-il de cette déclaration ? Il n'est plus rare de voir des tribunaux ordonner aux fournisseurs d'accès à internet de bloquer l'accès à un site accusé de

---

[102] Grégoire LOISEAU, « La supra-territorialité du site internet », *CCE* n° 11, Novembre 2013, comm. 115.

[103] PIDCP, art. 2§1.

[104] CEDH, art. 1Er.

[105] John PERRY BARLOW, *A Cyberspace Independence Declaration,* 9 février 1996. <https://w2.eff.org/Censorship/internet_censorship_bills/barlow_0296.declaration>

porter atteinte à la propriété intellectuelle[106] ou d'ordonner à un moteur de recherche de déréférencer des informations portant atteinte à la vie privée[107], ou encore de voir des autorités nationales saisir des noms de domaine de sites contrefaisants[108]. Les lois qui visent à apporter un encadrement juridique national sur internet sont légion, avec par exemple près d'une loi par an en France depuis dix ans[109]. Les intermédiaires de l'internet sont loin d'avoir l'autonomie qui a pu être autrefois fantasmée.

Dans les pays représentant un marché important, la menace de coupure de l'accès au service est pour les États un moyen efficace de faire plier les intermédiaires qui, en principe, ne sont pas sous leur juridiction. L'on a ainsi vu la plate-forme américaine GitHub (principalement hébergeur de codes sources de logiciels et de documents) accepter de bloquer l'accès des Russes à un document détaillant des méthodes de suicide, après que les autorités russes ont bloqué pendant plusieurs jours l'accès à l'ensemble du site américain qu'utilisaient en Russie des développeurs de logiciels. « *Même si nous ne sommes pas toujours d'accord avec les choix du gouvernement russe, nous respectons la souveraineté du pays et nous reconnaissons que les Russes peuvent avoir des sensibilités culturelles différentes* », avait fini par admettre GitHub[110]. Avant lui d'autres intermédiaires de l'internet ont également mis en place un filtrage géographique pour appliquer une censure différenciée en fonction de l'État d'origine des demandes d'accès aux informations, comme Twitter, Facebook, Google ou YouTube. Cela permet à chaque État de faire respecter sa propre « marge nationale d'appréciation » en matière de restrictions à la liberté d'expression, sans que celles-ci n'aient d'impact direct sur les autres pays.

Reste cependant que les États peinent encore parfois à faire respecter sur internet leur droit national, en particulier lorsqu'autour de la question de la collecte et du traitement des

---

106 *V.* par ex. en France, TGI de Paris, 3ème ch. 1ère section, 4 décembre 2014 <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4386> ; en Italie <http://censura.bofh.it/elenchi.html> ; en Grande-Bretagne, *Cartier, Montblanc and Richemont v BskyB, BT, TalkTalk, EE and Virgin* [2014] EWHC 3354 (Ch) <http://www.pblegal.co.uk/news/13-news/163-cartier-montblanc-and-richemont-v-bskyb-bt-talktalk-ee-and-virgin-2014-ewhc-3354-ch> ; en Espagne <http://www.elmundo.es/tecnologia/2014/07/16/53c65dceca474155548b4588.html> ; en Finlande <http://torrentfreak.com/finnish-isp-ordered-to-block-the-pirate-bay-111026/>...

107 *V.* par ex. TGI de Paris, ordonnance de référé du 16 septembre 2014, *M. et Mme X et M. Y / Google France*. <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4291>

108 *V.* « La saisie de noms de domaine jugée non contraire à la liberté d'expression », Le Monde, 8 août 2011. <http://www.lemonde.fr/technologies/article/2011/08/08/la-saisie-de-noms-de-domaine-jugee-non-contraire-a-la-liberte-d-expression_1557223_651865.html>

109 « Huit lois en dix ans pour encadrer le Web français », Le Monde, 15 avril 2015. <http://www.lemonde.fr/les-decodeurs/article/2015/04/15/sept-lois-en-dix-ans-pour-encadrer-le-web-francais_4615841_4355770.html>

110 <https://github.com/github/roskomnadzor>

données personnelles, les enjeux commerciaux des intermédiaires de l'internet sont directement concernés. « *Les marchés, les pratiques et les acteurs sont désormais transnationaux. Certaines des grandes entreprises les plus concernées par les problématiques de vie privée comptent deux fois plus d'utilisateurs que l'Europe n'a d'habitants* », constatait ainsi le Premier ministre du gouvernement français Manuel Valls lors du discours introductif du European Data Governance Forum organisé à Paris à l'UNESCO, le 8 décembre 2014. « *Il faut disposer de la capacité à établir un rapport de force* »[111].

Au cours de ce même discours, il ajoutait : « *N'ayons pas peur de faire de la régulation. C'est le rôle des États, de la puissance publique, au niveau national, au niveau européen, comme au niveau mondial. Les gouvernements sont là pour répondre aux attentes des citoyens* ». Mais cette volonté de régulation des États sur internet ne se fait pas toujours avec la volonté de protéger les droits fondamentaux des citoyens, et peut même parfois témoigner d'un objectif contraire...

[111] Manuel VALLS, Discours inaugural de la conférence internationale « Protection des données, innovation et surveillance : quel cadre éthique pour l'Europe ? » 8 décembre 2014. <https://www.youtube.com/watch?v=9DmkpxYrg6s>

DES VIOLATIONS DES DROITS FONDAMENTAUX COMMISES PAR LES ÉTATS PAR L'INTERMÉDIAIRE D'INTERNET

Évoquant au sujet d'internet les principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, le Commissaire aux droits de l'homme du Conseil de l'Europe a regretté que « *ces principes portent toujours sur l'obligation faite aux pays d'accueil de lutter activement contre les violations des droits de l'homme commises par les entreprises, et ne traitent pas en détail de la situation inverse, dans laquelle les États imposent aux entreprises des exigences qui, si elles sont satisfaites, amènent ces dernières à commettre des violations du droit international en matière de droits de l'homme* »[112].

Le constat vaut aussi sur internet. Les États sont en effet eux-mêmes à l'origine de nombreuses violations des droits de l'homme sur internet, tout d'abord par leurs intrusions ou leurs restrictions qui peuvent porter directement atteinte au droit au respect de la vie privée ou à la liberté d'expression (2.1), mais aussi par leur passivité ou leur instrumentalisation des intermédiaires de l'internet, qui peuvent constituer de la part des États des atteintes indirectes aux droits de l'homme susceptibles d'engager leur responsabilité (2.2).

2.1. Des violations directes des droits fondamentaux commises par les États

Que ce soit par les législations et réglementations qu'ils choisissent de mettre en œuvre dans le droit national, ou par des pratiques de leurs organes qui débordent du cadre officiellement fixé, les États sont parfois ceux qui enfreignent directement leur propre obligation de respecter les droits de l'homme sur internet. On le voit en particulier par la surveillance massive des communications électroniques qui ne respecte pas le principe de proportionnalité des restrictions nécessaires dans une société démocratique (2.1.1), et par des atteintes répétées à la liberté d'expression et d'information (2.1.2).

[112] Conseil de l'Europe, *Commissaire aux droits de l'homme*, « La prééminence du droit sur l'internet et dans le monde numérique en général », 8 décembre 2014, CommDH/IssuePaper(2014)1. <https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2014)1&Language=lanFrench>

2.1.1. L'atteinte à la vie privée par la surveillance massive des communications

a. Le principe du secret de la correspondance

Le droit des individus au secret des correspondances émises par des moyens de télécommunication a été reconnu par les États comme droit autonome bien avant l'élaboration des premiers instruments internationaux de protection des droits de l'homme. Dès la Convention télégraphique de Paris de 1865 qui donnait naissance à ce qui allait devenir en 1932 l'Union Internationale des Télécommunications (UIT), une disposition imposait déjà que les dix-neuf parties contractantes « *s'engagent à prendre toutes les dispositions nécessaires pour assurer le secret des correspondances* »[113]. Cette garantie avait été comprise très tôt comme un corollaire indispensable d'un autre principe fondamental, celui de la liberté de correspondance, car sans protection de la confidentialité des messages échangés, les individus et les entreprises auraient montré bien plus d'hésitation à utiliser un moyen de communication qui ne présentait pas la sécurité apportée par le cachet d'une enveloppe.

Dans les textes relatifs aux droits de l'homme, le droit au secret des correspondances est explicitement couvert par les dispositions relatives au droit à la vie privée. Au niveau universel, l'article 12 de la DUDH affirme ainsi que « *nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, son domicile ou sa correspondance* », ce qui est repris dans des termes quasi identiques par l'article 17§1 du PIDCP. A l'échelle régionale, le secret des correspondances est un principe rappelé par l'article 8§1 de la CEDH[114], l'article 11§2 de la CADH[115], et l'article 21§a de la CArDH[116]. En Europe, la Cour EDH a eu l'occasion de préciser que le principe s'appliquait à toutes les télécommunications quelles que soient les technologies employées, qu'il s'agisse du téléphone[117] ou de courriers électroniques et journaux de connexions à des sites internet[118].

---

113 Convention télégraphique internationale de Paris (1865), art. 5. <http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000014002PDFF.pdf>

114 CEDH, art.8§1 : « Toute personne a droit au respect de sa vie privée et familiale,de son domicile et de sa correspondance ».

115 CADH, art. 11§2 : « Nul ne peut être l'objet d'ingérences arbitraires ou abusives dans sa vie privée, dans la vie de sa famille, dans son domicile ou sa correspondance, ni d'attaques illégales à son honneur et à sa réputation ».

116 CArDH, art. 21§a : « Nul ne fera l'objet d'immixtion arbitraire ou illégale dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteinte à son honneur ou à sa réputation ».

117 *V.* Cour EDH, 6 septembre 1978, *Klass et autres c. Allemagne* (req. n° 5029/71), §41.

118 *V.* Cour EDH, 3 juillet 2007, *Copland c. Royaume-Uni* (req. n°62617/00), §41-43.

Bien sûr, le secret de la correspondance n'est cependant pas un droit absolu. Aujourd'hui la Constitution de l'UIT précise en son article 37 que les États membres de l'organisation « *se réservent le droit de communiquer ces correspondances aux autorités compétentes, afin d'assurer l'application de leur législation nationale ou l'exécution des conventions internationales auxquelles ils sont parties* », ce qui est très vaste. S'il pose le principe du secret des correspondances, le PIDCP n'interdit que les immixtions « arbitraires ou illégales », ce qui autorise a contrario les immixtions prévues par la loi. C'est également le cas de la CEDH qui permet par son article 8§2 une « *ingérence d'une autorité publique [...] pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». Là aussi le champ des dérogations est tellement large que l'on se demandait bien quelle borne le législateur pouvait rencontrer dans ses velléités d'accroître les pouvoirs d'écoutes policières.

C'est ce qui a incité la Cour EDH à vérifier que les ingérences prévues par la loi l'étaient de façon accessible et prévisible, avec des règles précises et détaillées, et que le dispositif légal était effectivement « *nécessaire dans une société démocratique* »[119]. La Cour a donc sanctionné la France en 1990 pour violation de l'article 8 suite à la mise sur écoute de deux individus, qui n'avaient « *pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique* ». Suite à ces deux condamnations prononcées le même jour à l'unanimité des juges[120], la France adopta rapidement la loi du 10 juillet 1991 sur les écoutes téléphoniques pour mieux les encadrer, notamment avec un système de contrôle par une autorité administrative indépendante[121], qui fut cette fois-ci validé par la justice européenne. Mais celle-ci observe toujours avec beaucoup de prudence les mises sous surveillance, qu'il s'agisse d'écoutes téléphoniques ou de collecte de données sur des moyens de communication modernes.

« *Caractéristique de l'État policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* », avait prévenu dès 1978 la Cour EDH, « *consciente du*

---

119 *V.* par ex. Cour EDH, 24 août 1998, *Lambert c. France* (88/1997/872/1084), §23-28.

120 Cour EDH, 24 avril 1990, *Kruslin c. France* (req. n°11801/85) et *Huvig c. France* (req. n°11105/84).

121 *V.* Roger ERRERA, « Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques », *RTDH* 55/2003, pp.851-870. <http://www.rtdh.eu/pdf/2003851.pdf>

danger [...] de saper, voire de détruire, la démocratie au motif de la défendre »[122]. Or c'est toute la question posée ces dernières années par les systèmes de mises sous surveillance massive.

b. Des atteintes disproportionnées au secret des correspondances sur internet

Pour défendre ce qu'ils estiment être l'intérêt national, les États peuvent avoir tendance, soit à dissimuler l'étendue de pratiques illicites d'atteinte au secret des correspondances — ce qu'ont confirmé les révélations de l'ancien agent américain de la National Security Agency (NSA) Edward Snowden[123], soit à les passer à la blanchisserie d'une pseudo-légalisation par des mesures de droit national ou même régional qui ne sont pourtant pas toujours conformes aux droits de l'homme[124]. C'est ainsi que dans son arrêt *Digital Rights Ireland* d'avril 2014, la Cour de justice de l'Union européenne (CJUE) s'est fondée sur les articles 7 (relatif au respect de la vie privée et familiale) et 8 (relatif à la protection des données personnelles) de la Charte des droits fondamentaux de l'Union européenne (CDFUE) pour conclure à la nullité d'une directive européenne de 2006[125]. Celle-ci faisait obligation aux États membres de contraindre les FAI et les opérateurs téléphoniques à conserver toutes les données de connexion et celles relatives aux communications de leurs clients « *pour une durée minimale de six mois et maximale de deux ans à compter de la date de la communication* »[126]. La Cour a jugé que l'obligation que ces données soient conservées pour être accessibles aux autorités judiciaires ou administratives était une « *ingérence particulièrement grave dans les droits fondamentaux de la qualité-totalité de la population européenne* »[127]. Elle note que même si le contenu des correspondances n'est pas conservé, les « métadonnées »[128] conservées « *prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données*

122 *V. Klass et autres c. Allemagne*, *op.cit.* note 117, §42 et §49.

123 Pour une vue détaillée des révélations sur l'ampleur des programmes de surveillance américains et européens et de leurs implications juridiques, *V.* Pieter OMTZIGT, « Les opérations de surveillance massive », *Rapport de la commission des questions juridiques et des droits de l'homme*, Assemblée parlementaire du Conseil de l'Europe, 18 mars 2015, Doc. 13734. <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-fr.asp?fileid=21583&lang=fr>

124 *V.* Philippe HAYEZ, « L'effet Snowden », *Le Débat* 4/2014 (n°181), p. 93-102.

125 La directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

126 *Ibid.* art.6.

127 CJUE, grande ch., 8 avril 2014, *Digital Rights Ireland c. Irlande*, §56. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642>

128 C'est-à-dire les données de contexte telles que les numéros de téléphone appelés ou appelants, la durée des appels, les adresses IP utilisées pour se connecter, le type de terminal utilisé, la géolocalisation des antennes-relais « accrochées » par un téléphone mobile, etc.

ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci ». En conséquence, plusieurs États européens qui avaient transposé la directive invalidée ont révisé leur propre droit national, pour réduire les durées de conservation imposées ou ne plus imposer du tout la conservation des données[129].

Souvent perçues comme une nécessité par les autorités publiques dans leurs stratégies de lutte contre le terrorisme, les politiques de surveillance massive permises par les nouvelles technologies de communication ont pourtant une grande incidence négative sur nombre de droits fondamentaux. L'Assemblée parlementaire du Conseil de l'Europe l'a rappelé récemment au moment-même où les députés français examinaient un projet de loi très controversé sur le renseignement, devant mettre à jour la loi de 1991. « *Les opérations de surveillance révélées jusqu'ici mettent en danger les droits de l'homme fondamentaux, notamment le droit au respect de la vie privée (article 8 de la Convention européenne des droits de l'homme (STE n°5)), le droit à la liberté d'information et d'expression (article 10), ainsi que le droit à un procès équitable (article 6) et le droit à la liberté de religion (article 9)* », a prévenu l'Assemblée[130].

Dans un rapport sur le droit à la vie privée à l'ère du numérique publié à l'été 2014, le Haut-Commissariat aux droits de l'homme des Nations Unies avait aussi dénoncé le recours à la surveillance massive comme étant « *une dangereuse habitude plutôt qu'une mesure exceptionnelle* »[131]. La Haut-Commissaire Navi Pillai y décrivait une « *contrainte de fait sur les entreprises du secteur privé pour qu'elles fournissent un accès global aux informations et aux données liées à des particuliers, sans leur consentement et sans qu'ils en aient connaissance* », et rappelait que toute loi autorisant des mises sous surveillance devait être « *suffisamment accessible, claire et précise pour qu'un individu puisse s'y référer pour vérifier qui est autorisé à pratiquer la surveillance des données et en quelles circonstances* »[132].

---

129 L'Irlande, l'Autriche, la Bulgarie, la Roumanie, la Slovaquie, la Slovénie et les Pays-Bas. *V.* Quadrature du Net, « Surveillance : la conservation généralisée des données remise en cause partout en Europe », 12 mars 2015. <https://www.laquadrature.net/fr/conservation-des-donnees-la-retention-generalisee-remise-en-cause-partout-en-europe>

130 Assemblée parlementaire du Conseil de l'Europe, Résolution 2045 (2015) sur « les opérations de surveillance massive », §4. <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=fr>

131 « The right to privacy in the digital age », *Report of the Office of the United Nations High Commissioner for Human Rights*, 30 juin 2014, A/HRC/27/37, §3.

132 *Ibid.* §23.

« *Il ne suffit pas que les mesures soient ciblées pour trouver certaines aiguilles dans une botte de foin; ce qu'il convient d'examiner, c'est leur impact sur la botte de foin, au regard du risque de préjudice, c'est-à-dire déterminer si la mesure est nécessaire et proportionnée* »[133], résumait-elle.

Concernant l'effet sur la botte de foin de la recherche de l'aiguille, la Rapporteuse spéciale sur la liberté d'expression auprès de la Commission interaméricaine des droits de l'homme, Catalina Botero, avait parfaitement décrit le lien entre atteinte au secret des corresponsdances et fragilisation du droit à la liberté d'expression, lors d'une réunion-débat du Conseil des droits de l'homme. Elle a en effet expliqué que l'impact « *pouvait être soit direct, quand ce droit ne pouvait être exercé anonymement à cause d'une surveillance, soit indirect, quand la simple existence de mécanismes de surveillance pouvait avoir un effet paralysant, inspirer la crainte et inhiber les personnes concernées en les contraignant à la prudence dans leurs dires et leurs agissements* »[134].

A cet égard, on peut observer avec beaucoup de circonspection voire d'inquiétude le projet de loi relatif au renseignement présenté par le gouvernement français, tel que rédigé dans la version renvoyée au Sénat au moment où nous rédigeons ces lignes. Il n'est en effet pas certain que la France ait bien pris toute la mesure de la résolution 68/167 de l'Assemblée générale des Nations Unies, qui appelait les États à « *revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, notamment à grande échelle, afin de défendre le droit à la vie privée en veillant à respecter pleinement toutes leurs obligations au regard du droit international* »[135]. Entre autres dispositions contestées, l'Assemblée nationale a adopté un article qui prévoit que pour les besoins de la prévention du terrorisme, le Premier ministre peut ordonner aux FAI et aux hébergeurs d'installer sur leurs réseaux « *un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés* »[136]. Concrètement il s'agira d'algorithmes dont le degré de sophistication pourrait un jour conduire à parler d'une « intelligence artificielle », qui auront pour mission d'observer le comportement des

133 *Ibid.* §25.

134 « Résumé de la réunion-débat du Conseil des droits de l'homme sur le droit à la vie privée à l'ère du numérique », *Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme*, 19 décembre 2014, A/HRC/28/39, §21. <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Pages/ListReports.aspx>

135 Résolution de l'Assemblée générale des Nations Unies du 18 décembre 2013 sur le droit à la vie privée dans l'ère numérique, A/RES/68/167, §4c. <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=/english/&Lang=F>

136 Projet de loi sur le renseignement (texte résultant des délibérations de l'Assemblée nationale à l'issue de la séance du 16 avril 1015), art.2 al.14. <http://www.assemblee-nationale.fr/14/ta-pdf/2697-p.pdf>

internautes et de signaler aux services de renseignement les individus suspects de desseins terroristes. « *On sait quels sont leurs comportements et on sait, par conséquent que, par la mobilisation de techniques ciblées, il est possible de prévenir leurs actes en regardant sur internet la manière dont ils se comportent* », avait expliqué le ministre de l'Intérieur lors des débats parlementaires[137]. Or le dispositif paraît — pardonnez l'euphémisme — bien peu compatible avec la jurisprudence de Cour EDH[138]. En outre il sera classifié pour des raisons évidentes d'efficacité, et ce secret nourrira la crainte de ceux qui sans avoir pourtant la moindre intention terroriste, pourraient renoncer à des pratiques d'accès ou d'échanges d'informations dans leurs activités en ligne, par simple hypothèse et peur irrationnelle que celles-ci n'attirent sur eux l'attention.

Ce serait alors une autre forme d'atteinte à la liberté d'expression sur internet, dont les États même démocratiques sont hélas de plus en plus coutumiers.

2.1.2. L'atteinte à la liberté d'expression et d'information sur internet par la censure étatique

a. Le principe de la liberté d'expression et d'information appliqué à internet

Dès sa première session en 1946, l'Assemblée générale des Nations Unies a adopté une résolution qui stipulait que « *la liberté de l'information est un droit fondamental de l'homme et la pierre de touche de toutes les libertés à la défense desquelles se consacrent les Nations*

---

137 Assemblée nationale, XIVe législature, Session ordinaire de 2014-2015, *Compte rendu intégral, Première séance du lundi 13 avril 2015*. <http://www.assemblee-nationale.fr/14/cri/2014-2015/20150212.asp>

138 Au moins trois arrêts méritent l'attention à cet égard. Tout d'abord dans l'affaire *Klaas c. Allemagne*, la Cour EDH n'avait jugé conforme à l'article 8§2 la loi de l'Allemagne de l'ouest sur les écoutes administratives qu'après avoir constaté que celle-ci « *n'autorise pas une surveillance dite exploratoire ou générale* » notamment parce que « *la surveillance ne concerne que le suspect lui-même ou les personnes présumées avoir des contacts avec lui* » (op.cit. note 117, §51). Le dispositif de la loi française projetée est au contraire exploratoire par nature. Ensuite, dans l'affaire *Kruslin c. France* qui a déterminé le canevas à suivre pour toute législation sur le sujet, la Cour EDH a imposé de fixer une durée limitée renouvelable aux écoutes, pour que l'atteinte à la vie privée cesse lorsqu'elle n'apporte plus aucun élément intéressant la procédure. Une durée de 4 mois est certes prévue par le projet de loi français, mais elle n'a guère de sens s'agissant d'un dispositif sans cible prédéterminée. Le renouvellement devrait être automatique tant qu'au moins quelques suspects sont découverts par la surveillance élargie. Dans un sursaut de bon sens le gouvernement n'avait d'ailleurs pas jugé utile de prévoir un tel délai dans le texte initial soumis à l'Assemblée (*V. Kruslin c. France*, req. N°11801/85, 24 avril 1990, §35). Enfin dans l'affaire *Malone c. Royaume-Uni*, la Cour a rappelé « *l'exigence de prévisibilité* » de toute loi sur les écoutes, en demandant qu'elle use « *de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance* ». Un lecteur optimiste du projet de loi peut douter que « détecter une menace terroriste sur la base de traitements automatisés » soit d'une grande prévisibilité (*V. Malone c. Royaume-Uni*, req. N°8691/79, 2 août 1984, §67), en tout cas pas davantage que la loi epsagnole condamnée par la Cour EDH dans l'affaire *Bugallo c. Espagne* (req. N°58496, 18 février 2003).

Unies »[139]. Elle « *implique le droit de recueillir, de transmettre et de publier les nouvelles en tous lieux et sans entraves* ». C'est un principe essentiel pour la paix et donc pour la garantie du respect des droits de l'homme, car « *la compréhension et la collaboration entre les pays sont impossibles sans une opinion mondiale saine et vigilante, ce qui exige une entière liberté de l'information* »[140].

Le droit international des télécommunications relaie cette exigence lorsqu'il fait interdiction aux États de brouiller de façon préjudiciable les radiocommunications[141], non seulement pour des impératifs de sécurité civile ou militaire, mais aussi pour garantir la liberté d'information essentielle à la paix. Philippe Achilleas nous rappelle que « *le brouillage intentionnel des programmes de radiodiffusion a toujours fait partie des relations internationales* » et qu'il est une pratique « *couramment admise en période de conflit armé, utilisée pour empêcher la réception des programmes de propagande étrangère* »[142]. Mais l'ONU ayant mis la guerre hors-la-loi, il n'y a plus lieu d'admettre le brouillage des télécommunications. Le Règlement des radiocommunications impose donc aux États de s'abstenir de toute interférence et de protéger les émissions en prenant les mesures nécessaires lorsqu'ils ont connaissance d'un brouillage induit par une station relevant de leur juridiction[143], ce qui a permis à l'UIT d'exhorter l'Iran à « *poursuivre son effort pour localiser la source de l'interférence et à l'éliminer* » lorsque l'opérateur Eutelsat s'est plaint d'un brouillage qui affectait la BBC Persian, Voice Of America, Radio Free Europe/Radio Liberty, et la fourniture d'accès à internet par satellite[144].

L'ONU a réalisé la jointure entre les droits de l'homme et le droit international des télécommunications en adoptant en 1950 une résolution qui, citant côte à côte l'interdiction du brouillage imposée par la Convention Internationale des Télécommunications et la liberté d'expression affirmée dans la Déclaration universelle des droits de l'homme, a « *condamn[é]*

---

[139] Résolution 59(I) de l'Assemblée générale des Nations Unies, 14 décembre 1946, « Convocation d'une Conférence internationale sur la liberté de l'information ». < http://www.un.org/french/documents/view_doc.asp?symbol=A/RES/59%28I%29&Lang=F>

[140] *Idem*.

[141] Le n°1.169 du Règlement des radiocommunications définit le brouillage préjudiciable comme étant un « *brouillage qui compromet le fonctionnement d'un service de radionavigation ou d'autres services de sécurité ou qui dégrade sérieusement, interrompt de façon répétée ou empêche le fonctionnement d'un service de radiocommunication utilisé conformément au règlement des radicommunications* ».

[142] Philippe ACHILLEAS, « Droit international des télécommunications (communications électroniques) », *JurisClasseur Communication*, Fasc. 7350, 1er décembre 2013, §51.

[143] Règlement des radiocommunications, n°15.21.

[144] REUTERS, « L'UIT somme l'Iran de cesser de brouiller Eutelsat », 26 mars 2010. <http://fr.reuters.com/article/frEuroRpt/idFRLDE62P0XI20100326>

les mesures de cette nature en tant que négation du droit de toute personne à être pleinement informée eu égard aux nouvelles, opinions, et idées, sans considérations de frontières »[145]. Cela vaut aussi lorsque le brouillage affecte internet, en particulier lorsqu'il s'agit de coupures totales de l'accès à internet dont nous avons déjà vu qu'elles constituaient une violation des droits de l'homme[146].

Dans le droit international, le droit à l'information est garanti en tant que composante ou corollaire de la liberté d'expression. L'article 19 du PIDCP dispose ainsi que « *toute personne a droit à la liberté d'expression; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix* ». La CEDH (art. 10) utilise sensiblement les mêmes termes, tout comme la Charte européenne (art. 11) et la Convention américaine (art. 13). La Charte arabe (art. 32) et la Charte africaine (art. 9) présentent quant à elles le droit à l'information et la liberté d'expression comme deux droits autonomes, mais ils restent associés au sein d'un même article.

Cependant tout comme le droit à la vie privée étudié précédemment, le droit à la liberté d'expression et donc le droit à l'information ne sont pas des droits absolus. A l'exception de la Charte africaine qui formellement ne prévoit aucune restriction possible pour le droit à l'information (mais qui en autorise pour le droit d'exprimer et de diffuser ses opinions, ce qui revient sensiblement au même), et de la DUDH qui n'a pas de portée juridiquement contraignante, tous les textes internationaux relatifs aux droits de l'homme ouvrent grand la porte aux restrictions à la liberté d'expression et d'information, après avoir affirmé le principe de son respect. Le PIDCP permet ainsi aux États de soumettre ces libertés à des restrictions fixées par la loi et nécessaires au respect des droits ou de la réputation d'autrui, ou à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publique[147].

Ces aménagements du principe ne sont toutefois pas un blanc-seing qui permettrait aux États d'appliquer à volonté d'importantes restrictions au droit de s'exprimer et de s'informer, notamment sur internet.

---

145 Résolution 424(V) de l'Assemblée générale des Nations Unies, « Freedom of expression : interference with radio signals », 14 décembre 1950. <http://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/RES/424(V)&Lang=E&Area=RESOLUTION>

146 *V.* supra, section 1.1.1, p14.

147 *V.* PIDCP, art. 19§3.

Le Comité des droits de l'homme de l'ONU a ainsi fait observer que « *toute restriction imposée au fonctionnement des sites Web, des blogs et de tout autre système de diffusion de l'information par le biais de l'Internet, de moyens électroniques ou autres, y compris les systèmes d'appui connexes à ces moyens de communication, comme les fournisseurs d'accès à Internet ou les moteurs de recherche, n'est licite que dans la mesure où elle est compatible* » avec l'article 19§3 du PIDCP[148]. En tout état de cause, ajoutait-il, « *les restrictions licites devraient d'une manière générale viser un contenu spécifique; les interdictions générales de fonctionnement frappant certains sites et systèmes ne sont pas compatibles avec le paragraphe 3* »[149]. De même, « *interdire à un site ou à un système de diffusion de l'information de publier un contenu uniquement au motif qu'il peut être critique à l'égard du gouvernement ou du système politique et social épousé par le gouvernement est tout aussi incompatible avec le paragraphe 3* »[150].

b. Des restrictions abusives imposées par les États à la liberté d'expression et d'information sur internet

La compatibilité des restrictions imposées à l'accès à internet avec l'article 19§3 du PIDCP fait donc partie des points régulièrement vérifiés par le Comité des droits de l'homme lors de l'Examen périodique universel (EPU). C'est ainsi qu'à l'occasion du premier EPU concernant l'Égypte, la Suède a demandé en 2010 au pays alors dirigé par Hosni Moubarak de « *prendre les mesures pour veiller à ce que les droits de l'homme puissent aussi être exercés sur l'Internet* » et de « *libérer immédiatement toute personne détenue ou emprisonnée pour avoir exercé son droit à la liberté d'expression sur l'Internet* »[151]. Quatre ans plus tard, l'Égypte qui avait coupé totalement l'accès à internet lors de la révolution[152] fit remarquer lors de son nouvel EPU post-Moubarak que « *la Constitution et les lois n'imposaient pas de restrictions à l'accès des blogueurs ou du public à Internet* »[153]. De même à l'occasion de

---

148 Nations unies, Comité des droits de l'homme, « Observation générale n° 34 — Article 19 : Libertés d'opinion et d'expression », CCPR/C/GC/34, 21 juillet 2011, §34. <http://ohchr.org/english/bodies/hrc/docs/CCPR.C.GC.34_fr.doc>

149 *Idem*.

150 *Idem*.

151 Nations Unies, Conseil des droits de l'homme, « Rapport du groupe de travail sur l'Examen périodique universel — Égypte », A/HRC/14/17, 26 mars 2010. <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/14/17&Lang=F>

152 V. Tristan VEY, « L'Egypte coupe tous les accès à Internet », *Le Figaro*, 28 janvier 2011. <http://www.lefigaro.fr/international/2011/01/28/01003-20110128ARTFIG00505-l-egypte-coupe-tous-les-acces-a-internet.php>

153 Nations Unies, Conseil des droits de l'homme, « Rapport du groupe de travail sur l'Examen périodique universel — Égypte », A/HRC/28/16, 24 décembre 2014. <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/28/16&Lang=F>

l'EPU de la Tunisie réalisé en 2012, le nouveau régime a tenu à signaler aux Nations unies que « *la censure de l'Internet avait également été levée, un choix irréversible dicté notamment par le rôle des médias électroniques dans la révolution tunisienne* »[154]. Bien d'autres pays ont eu recours (ou ont encore recours) avec des fortunes diverses à la coupure à l'échelle nationale ou locale d'internet lors de soulèvements de leur population, tels la Syrie[155], la Libye[156], le Barheïn[157], la Chine[158], ou plus récemment, la République Démocratique du Congo[159].

La technique d'atteinte au droit d'accéder à internet est parfois plus subtile. Plutôt que d'interdire toute communication en ligne, ce qui paralyse aussi l'économie du pays, certains gouvernements comme la Syrie ou l'Iran agissent sur le niveau de bande passante disponible, pour limiter la vitesse de l'accès et donc la capacité à envoyer notamment des vidéos de témoignage, lors de périodes de crise.

Beaucoup plus souvent, les violations du droit à la liberté d'information sur internet se traduisent par des restrictions ciblées, et néanmoins très discutables au regard des droits de l'homme. Les exemples seraient ici bien trop nombreux pour approcher l'exhaustivité. Dans un rapport publié en 2012, Reporters Sans Frontières (RSF) avait identifié douze pays « ennemis d'internet » et quatorze « sous surveillance »[160], en raison principalement de mesures de blocage ou de filtrage de l'information. Citons simplement l'exemple le plus célèbre, le « Grand pare-feu de Chine », qui fait l'objet d'une vigilance importante de la part de l'ONG GreatFire.org[161]. « *Le système de filtrage et de surveillance chinois, l'un des plus aboutis au monde, a été utilisé pour éviter tout risque de contagion des mouvements de contestation, notamment en retirant la majeure partie des références au Printemps arabe et*

---

154 Nations Unies, Conseil des droits de l'homme, « Rapport du groupe de travail sur l'Examen périodique universel — Tunisie », A/HRC/21/5, 9 juillet 2012, §87. <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/21/5&Lang=F>

155 *V.* « Internet Coupé en Syrie », *L'Expansion*, 3 juin 2011. <http://lexpansion.lexpress.fr/high-tech/internet-coupe-en-syrie_1441930.html>

156 *V.* « Internet coupé en Libye », *Le Monde*, 4 mars 2011. <http://www.lemonde.fr/technologies/article/2011/03/04/internet-coupe-en-libye_1488285_651865.html>

157 *V.* « Autour du Bahreïn d'accentuer le filtrage d'Internet », *Numerama*, 18 février 2011. <http://www.numerama.com/magazine/18111-au-tour-du-bahreiumln-d-accentuer-le-filtrage-d-internet.html>

158 *V.* RSF, « Le Tibet toujours plus coupé du reste du monde », 1er mars 2012. <http://fr.rsf.org/chine-le-tibet-coupe-du-reste-du-monde-23-02-2012,41927.html>

159 *V.* « RDC : Internet coupé à Kinshasa sur ordre du pouvoir », *Le Monde*, 20 janvier 2015. <http://www.lemonde.fr/pixels/article/2015/01/20/rdc-internet-coupe-a-kinshasa-sur-ordre-du-pouvoir_4559720_4408996.html>

160 RSF, *Les ennemis d'Internet — Rapport 2012*, 12 mars 2012, 73p. <http://fr.rsf.org/IMG/pdf/rapport_ennemis_internet_2012.pdf>

161 <http://en.greatfire.org>

aux mouvements Occupy Wall Street de l'Internet chinois », constatait RSF dans son rapport. « *Des blogs et microblogs ont été fermés, des mots clés comme "jasmin" ou "Égypte" ont été interdits. Il est impossible de combiner le mot "occuper" suivi d'une ville chinoise (ex : "Occupy Beijing" (` ¬) pour effectuer une recherche web* ». Nombreux sont les pays à bloquer durablement l'accès à des sites internet populaires comme YouTube, Facebook ou Twitter, largement utilisés à travers le monde pour diffuser des informations, à l'image de la Chine, l'Iran, le Vietnam, le Pakistan, la Corée du Nord, ou l'Erytrhée. Parfois la levée d'un blocage est un simple leurre, comme en Syrie où la censure de Facebook a été abandonnée… au profit d'un espionnage des communications privées de ceux qui s'y connectent[162].

Le blocage de sites internet peut aussi avoir des objectifs insoupçonnés. Ainsi la République de Nauru, établie dans une petite île d'Océanie, a décidé de bloquer l'accès à Facebook et à plusieurs autres sites internet, officiellement pour empêcher la diffusion de contenus pédopornographiques, pourtant rarissimes sur la plateforme américaine. Officieusement, il s'agirait selon l'opposition de priver les quelques milliers d'habitants de l'accès à des informations indépendantes en l'absence de journal local, en particulier concernant les possibilités d'émigration en Australie[163].

Des pays adhérant à la Convention européenne des droits de l'homme se prêtent aussi à la censure d'internet. La Cour EDH a par exemple sanctionné comme étant une ingérence illicite d'autorités publiques dans le droit à la liberté d'expression le blocage par la Turquie d'un site internet (Google Sites) qui hébergeait lui-même de nombreux sites internet de tiers. « *L'effet limité de la restriction litigieuse n'amoindrit pas son importance, d'autant que l'Internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit à la liberté d'expression et d'information* », a expliqué la Cour[164].

Mais même au sein de l'Union européenne, la censure partielle d'internet est de mise. Y compris en France, qui a le triste privilège d'être le seul pays européen désigné par RSF parmi les pays sous surveillance[165]. A titre d'illustration, la France a adopté sans contrôle constitutionnel en novembre 2014 une loi contre le terrorisme[166] qui autorise l'autorité

[162] *V.* Peter ECKSERSLEY, « A Syrian Man-In-The-Middle Attack against Facebook », *Electronic Frontier Foundation*, 5 mai 2011. <https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook>

[163] *V.* Paul FARRELL, « Nauru says Facebook block a 'temporary restriction' to keep public safe from 'sexual perverts' », The Guardian, 11 mai 2015. <http://www.theguardian.com/weather/2015/may/11/facebook-block-in-nauru-a-temporary-restriction-says-government>

[164] Cour EDH, *Ahmet Yildirim c. Turquie*, *op.cit.* note 34, §54.

[165] *Op.cit.* note 160, p.50.

[166] Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

administrative à notifier aux FAI une liste de sites internet établie par elle-même, accusés de faire publiquement l'apologie du terrorisme ou de provoquer directement à la commission d'actes de terrorisme. Les FAI ont alors l'obligation d' « *empêcher sans délai l'accès à ces adresses* »[167], et les moteurs de recherche ont l'obligation de les déréférencer. Le public n'a plus la possibilité ni de consulter ces sites dont la qualification pénale (qui peut servir des intérêts politiques) n'est pas vérifiée par un juge, ni même la possibilité de savoir qu'ils existent. Or les premières mises en application de ce pouvoir de censure ne sont pas sans poser questions[168].

Les États totalitaires n'ont donc pas le monopole de la violation de la liberté de recevoir ou de communiquer des informations sur internet. Les démocraties occidentales tendent aussi à restreindre le droit pour les citoyens d'exprimer librement leurs opinions. Mais elle le font souvent de façon plus indirecte, en instrumentalisant la position clé des intermédiaires de l'internet.

2.2. Des violations indirectes des droits fondamentaux par l'instrumentalisation des intermédiaires de l'internet

Les atteintes aux droits de l'homme sur internet par les États ne sont pas toujours le résultat d'une action directe des administrations, mais peuvent aussi résulter de l'inaction complice d'un État face aux violations commises par des acteurs privés (2.2.1), voire être provoquées par eux par une forme d'instrumentalisation et de délégation du pouvoir judiciaire et législatif aux intermédiaires de l'internet (2.2.2).

2.2.1. L'ingérence passive des États devant des violations de droits fondamentaux par des intermédiaires de l'internet

a – l'obligation des États de prendre des mesures actives pour protéger les droits de l'homme

Les États n'ont pas seulement l'obligation négative de s'abstenir de porter atteinte aux droits garantis par les textes internationaux en matière de droit de l'homme, mais aussi

[167] *Ibid.*, art.12.

[168] *V.* « Moi, censuré par la France pour mes opinions politiques », *Numerama.com*, 18 mars 2015. <http://www.numerama.com/magazine/32516-moi-censure-par-la-france-pour-mes-opinions-politiques.html>

l'obligation positive de prendre des mesures concrètes pour promouvoir le respect des droits, que ce soit dans leurs propres actions ou dans celle des tiers. Lorsqu'ils en sont signataires, ce qui est le cas d'une très grande majorité des pays du monde, les États « *s'engagent à respecter et à garantir à tous les individus se trouvant sur leur territoire et relevant de leur compétence les droits reconnus* » par le PIDCP[169]. Le Comité des droits de l'homme prévient à cet égard que si l'État « *s'abstient de prendre des mesures appropriées ou d'exercer la diligence nécessaire pour prévenir et punir [des] actes [violant les droits de l'homme] commis par des personnes privées, physiques ou morales, enquêter à leur sujet ou réparer le préjudice qui en résulte, […] lesdits actes sont imputables à l'État partie concerné* »[170].

Au niveau régional aussi, même si la Cour EDH se refuse « *à élaborer une théorie générale des obligations positives de nature à découler de la Convention* »[171], ses arrêts sont désormais innombrables qui découvrent dans la CEDH une obligation positive des États d' « *adopter des mesures raisonnables et adéquates pour protéger les droits de l'individu* »[172]. Comme la Cour l'avait indiquée dans son arrêt *Airey*, « *l'exécution d'un engagement assumé en vertu de la Convention appelle parfois des mesures positives de l'État* » et donc « *celui-ci ne saurait se borner à demeurer passif* »[173].

L'État qui s'abstiendrait de prendre les mesures adéquates pour protéger les droits reconnus à l'individu risque donc d'être accusé d'une forme d' « abstention coupable » ou, pour reprendre l'expression de Frédéric Sudre, d' « ingérence passive »[174]. Celle-ci peut parfois résulter « *d'une défaillance du système de droit interne telle qu'elle a rendu possible ou toléré la violation par un particulier, ou un groupe de particuliers, d'un droit protégé par la Convention* »[175]. Comme l'avait jugé la Cour interaméricaine des droits de l'homme (Cour IADH), un tel comportement passif face à des violations des droits fondamentaux « *peut*

---

169 PIDCP, art. 2.

170 Nations Unies, *Comité des droits de l'homme*, « Observation générale N°31, La nature de l'obligation juridique générale imposée aux États parties au Pacte », HRI/GEN/1/Rev.7 (2004), §8. <http://www1.umn.edu/humanrts/gencomm/french/f-gencom31.html>

171 Cour EDH, 21 juin 1988, *Plattform "Ärzte für das Leben" c. Autriche* (req. n°10126/82), §31.

172 Cour EDH, 9 décembre 1994, *López Ostra c. Espagne* (req. N°16798/90), §51. Pour un aperçu de la grande richesse de la jurisprudence européenne en matière d'obligations positives des États, *V.* Frédric SUDRE, « La portée des obligations positives » in *Les grands arrêts de la Cour européenne des Droits de l'homme*, Thémis Droit, PUF, 7e éd., 2015, pp.23-29.

173 Cour EDH, 9 octobre 1979, *Airey c. Irlande* (req. N°6289/73), §25.

174 *V.* Frédric SUDRE, « Les "obligations positives" dans la jurisprudence européenne des droits de l'homme », *RTDH*, n°1995/23, §14, p.369. <http://www.rtdh.eu/pdf/1995363.pdf>

175 *Idem*., p.372.

conduire à la responsabilité internationale de l'État, non pas pour l'acte lui-même, mais en raison du manque de diligence raisonnable pour empêcher la violation ou y répondre »[176].

b – la passivité des États face aux violations commises sur internet par des entreprises nationales

Dès lors, peut être engagée la responsabilité internationale de l'État qui resterait passif devant la fourniture par des entreprises relevant de sa juridiction d'outils destinés à faciliter l'interception massive de télécommunications de la population, en particulier lorsque cette surveillance a des conséquences dramatiques. En France, deux entreprises nationales font l'objet d'informations judiciaires ouvertes à Paris pour complicité d'actes de torture, pour avoir fourni réciproquement aux services de renseignement syriens[177] et libyens[178] des moyens permettant d'intercepter les communications électroniques d'opposants au régime, et de découvrir leur identité. Mais leur cas est loin d'être isolé.

Ainsi par exemple, une société italienne s'est spécialisée dans la fourniture de « solutions offensives » pour enquêter à distance sur les utilisateurs des réseaux de télécommunications, et indique n'avoir que des gouvernements comme clients. Or en 2014, des traces de ses solutions qui permettent notamment de déchiffrer les communications ont été découvertes sur des serveurs connectés à internet depuis une vingtaine de pays[179] dont neuf étaient classés comme « autoritaires » par le magazine *The Economist*[180]: l'Arabie Saoudite, l'Éthiopie, l'Azerbaïdjan, le Kazakhstan, le Nigéria, Oman, le Soudan, les Émirats Arabes Unis, et l'Ouzbékistan. D'autres entreprises dont les services ont été exploités par des régimes

---

176 Cour IADH, 29 juillet 1988, *Velasquez Rodriguez c. Honduras* (Ser. C) n°4 (1988), §172. <http://www1.umn.edu/humanrts/iachr/b_11_12d.htm>

177 *V.* « France : Ouverture d'une information judiciaire visant la société Qosmos pour complicité d'actes de torture en Syrie », *FIDH*, 11 avril 2014 <https://www.fidh.org/La-Federation-internationale-des-ligues-des-droits-de-l-homme/europe/france/15115-france-ouverture-d-une-information-judiciaire-visant-la-societe-qosmos>

178 *V.* Anne VIDALIE, « France-Libye: information judiciaire contre Amesys », *L'Express*, 21 mai 2012 <http://www.lexpress.fr/actualite/societe/justice/france-libye-information-judiciaire-contre-amesys_1116962.html>

179 Bill MARCZAK *et al.*, « Mapping Hacking Team's "Untraceable" Spyware », Citizen Lab (Munk School of Global Affairs, University of Toronto), 17 février 2014. <https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/>

180 « Democracy Index 2013 », *The Economist*. <http://www.eiu.com/public/topical_report.aspx?campaignid=Democracy0814>

autoritaires pour espionner et arrêter des dissidents ont leur siège en Grande-Bretagne[181], en Allemagne[182] ou encore en Israël[183].

C'est donc pour faire pression sur les gouvernements et leur rappeler leur responsabilité de protéger les droits de l'homme en prenant des mesures positives à l'encontre de leurs propres nationaux que s'est formée en avril 2014 une fédération d'ONG, la Coalition Against Unlawful Surveillance Exports (CAUSE)[184], qui rassemble Amnesty International, Reporters Sans Frontières, Human Rights Watch, Privacy International, la Fédération internationale des droits de l'homme (FIDH), la Digitale Gesellschaft et l'Open Technology Institute. « *The proliferation of these technologies allows for mass surveillance of entire countries, via hacking computers or phones, mapping, profiling and analysing social networks, installing malware allowing for surreptitious extraction of data, and mass internet monitoring and filtering through the tapping of under-sea fibre-optics cables that carry all communications traffic in and out of countries. These technologies enable regimes to crush dissent or criticism, chill free speech and destroy the fundamental rights that underpin democratic societies* », écrivent-ils dans une lettre ouverte[185].

Annonçant leur intention d'actionner la responsabilité internationale des États qui y feraient défaut, l'organisation demande aux 41 États signataires de l'Arrangement de Wassenaar d'ajouter plus largement qu'ils ne l'ont fait[186] l'ensemble des technologies de surveillance à la liste des produits et services visés par l'accord relatif aux contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage : « *Any*

---

181 V. « Gamma International », *Les ennemis d'internet*, RSF. Extrait : « *Ses logiciels ont été retrouvés notamment au Bahreïn et aux Émirats arabes unis, des pays connus pour malmener les producteurs de l'information. La technologie FinFisher vendue par la société est capable de lire des fichiers encryptés, des emails, et d'enregistrer des appels passés en VoIP. Parmi les cibles de cette surveillance, Ala'a Shehabi, journaliste bahreïnie et maître de conférence à l'université, qui a dû fuir son pays et vit désormais au Royaume-Uni.* » <http://surveillance.rsf.org/gamma/>

182 *V.* à propos de la société Utimaco, « Post-Revolt Tunisia Can Alter E-Mail With `Big Brother' Software », *Bloomberg*, 13 décembre 2011. <www.bloomberg.com/news/articles/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software>

183 *V.* à propos des sociétés Verint Israel et NICE Systems, « Privacy International uncovers widespread surveillance throughout Central Asia, exposes role of Israeli companies », *Privacy International*, 20 novembre 2014. <https://www.privacyinternational.org/?q=node/429>

184 CAUSE. <http://www.globalcause.net/>

185 *Idem*.

186 Les « logiciels d'intrusion » et « systèmes de surveillance de réseau IP » ont déjà été ajoutés suite à la 19ème réunion plénière de l'Arrangement de Wassenaar en Autriche en décembre 2013, à l'initiative de la France et de la Grande-Bretagne.V. « Summary of changes — List of dual-use goods & technologies and munitions list as of 4 December 2013 », Wassenaar Arrangement, 4 décembre 2013. <http://www.wassenaar.org/controllists/2013/Summary%20of%20Changes%20to%20Control%20Lists%202013.pdf>

export policy relating to surveillance technologies should place human rights at its heart. Governments must exercise a strict policy of restraint and should refuse to grant export licenses for surveillance technology destined for end-users in countries where they are likely to be used in an unlawful manner »[187]. A cet effet la Commission européenne a d'ores-et-déjà pris des mesures en ajoutant l'an dernier à sa liste de contrôles à l'exportation toute une série de « matériels d'interception des télécommunications mobiles ou de brouillage, et équipements de surveillance »[188]. Par ailleurs la Suisse, qui a pu servir de passerelle pour contourner les régulations de l'Union[189], a engagé récemment des poursuites contre une entreprise ayant exporté illégalement du matériel de surveillance utilisé pour traquer des dissidents et les torturer[190]. Mais le cadre général de contrôle des exportations reste jugé insuffisant par les organisations de défense des droits de l'homme[191].

Sur des sujets sans doute moins graves mais non moins importants, l'on pourrait aussi s'interroger sur l'ingérence passive de l'État dans le respect des droits de l'homme lorsque le constat d'une violation massive et durable de la réglementation sur la protection de la vie privée par le géant Google n'aboutit qu'à une condamnation indolore à 150 000 euros d'amende[192], lorsque rien n'est fait pour mettre fin à une entente des intermédiaires de paiement en ligne qui refusent subitement de traiter les paiements destinés à un média sur internet[193], ou lorsque les États européens restent largement inactifs suite aux révélations de programmes secrets permettant aux services de renseignement américains d'accéder aux données personnelles d'Européens stockées sur des serveurs appartenant à des entreprises

---

187 « CAUSE: 2014 Open Letter to the Members of the Wassenaar Arrangement », CAUSE, 2 décembre 2014. <www.globalcause.net/resources/cause-2014-open-letter-members-wassenaar-arrangement>

188 *V.* Commission européenne, « *Annexe au règlement délégué de la Commission modifiant le règlement (CE) n°428/2009 du Conseil instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage* », 22 octobre 2014, C(2014) 7567 Final, §5A1.f, p.173. <http://ec.europa.eu/transparency/regdoc/rep/3/2014/FR/3-2014-7567-FR-F1-1-ANNEX-1.Pdf>

189 *V.* EDRi, « Has Switzerland Become A Center Of Spy Technology Exports? », 9 octobre 2013. <https://edri.org/has-switzerland-become-a-center-of-spy-technology-exports/>

190 *V.* à propos des poursuites contre la société zurichoise Neosoft accusée d'avoir voulu livrer au Bangladesh une technologie de surveillance des communications mobiles : 20 Minutes, « Le SECO porte plainte », 11 septembre 2014. <http://www.20min.ch/ro/news/suisse/story/19675000>

191 Pour un aperçu des limites de la régulation actuelle, *V.* FIDH, « Position paper — Surveillance technologies "made in Europe" : Regulation needed to prevent human rights abuses », décembre 2014, 40 p. <https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe-1-2.pdf>

192 *V.* Le Figaro, « La CNIL condamne Google à 150.000 euros d'amende », 8 janvier 2014. <http://www.lefigaro.fr/flash-eco/2014/01/08/97002-20140108FILWWW00523-amende-maximale-de-la-cnil-par-google.php>

193 V. Le Monde, « WikiLeaks : plainte à Bruxelles contre Visa et MasterCard », 13 juillet 2011. <http://www.lemonde.fr/technologies/article/2011/07/13/wikileaks-plainte-a-bruxelles-contre-visa-et-mastercard_1548164_651865.html>

américaines[194]. Dans ces exemples parmi d'autres, nombre d'États semblent avoir développé une certaine tolérance à l'égard de l'irrespect de droits fondamentaux par des intermédiaires de l'internet. Par ailleurs ils tirent eux-mêmes parfois profit de la place incontournable des intermédiaires pour porter atteinte aux droits de l'homme, non plus directement, mais indirectement.

2.2.2. L'instrumentalisation par les États de la position stratégique des intermédiaires de l'internet

a – la censure par procuration

Les intermédiaires de l'internet ont par définition une position clé en matière de liberté d'expression, puisque ce sont eux qui font le lien entre la personne qui exprime un message et la personne qui en prend connaissance. Ne serait-ce que parce qu'il y a toujours un fournisseur d'accès à internet entre eux, il n'est jamais possible pour deux internautes de communiquer directement l'un avec l'autre. Toutes leurs communications passent nécessairement par le truchement de tiers. Aussi, les États qui souhaitent porter atteinte à la liberté d'expression et d'information sont-ils tentés de ne pas s'attaquer directement à la personne qui parle ou à la personne susceptible d'écouter, mais plutôt à celui ou ceux que le professeur de droit américain Seth Kreimer a identifié comme le « maillon le plus faible » permettant aux États d'exercer une « censure par procuration »[195]. La stratégie est simple et se déploie en contradiction radicale avec l'obligation faite aux États parties au PIDCP de « *veiller à ce que les individus soient protégés de tout acte commis par des personnes privées, physiques ou morales, qui compromettrait l'exercice de la liberté d'opinion et de la liberté d'expression* »[196]. Elle consiste à inciter par divers procédés les intermédiaires de l'internet à restreindre eux-mêmes la liberté d'expression et de communication des utilisateurs, en évitant que l'État ne prenne directement et spécialement des mesures qui sont susceptibles de constituer une violation des droits fondamentaux.

---

[194] *V.* Ludwig GALLET, « PRISM : l'Irlande rejette les recours contre Apple et Facebook », *Clubic Pro*, 25 juillet 2013. <http://pro.clubic.com/legislation-loi-internet/donnees-personnelles/actualite-574902-prism-irlande-rejette-recours-europe-vs-facebook.html>. Sur ce sujet, il faut noter que le « Safe Harbor » qui autorise le transfert de données personnelles vers les Etats-Unis est officiellement en cours de renégociation depuis les révélations d'Edward Snowden, mais aucune poursuite n'a été ouverte contre les entreprises ayant participé au programme PRISM.

[195] *V.* Seth KREIMER, « Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link », *University of Pennsylvania Law Review*, Vol. 155, N°11, 2006. <http://ssrn.com/abstract=948226>

[196] Comité des droits de l'homme, *Observation générale n°34 sur l'article 19 du PIDCP*, juillet 2011, CCPR/C/GC/34, §7.

La méthode la plus efficace vise à provoquer l'auto-censure des intermédiaires de l'internet en les rendant pénalement ou civilement responsables de ce qu'ils contribuent par leurs services à rendre accessible. La Chine et la Thaïlande ont ainsi institué des régimes de responsabilité stricte qui obligent les intermédiaires à opérer une surveillance active des contenus publiés, et à censurer préventivement tout ce qui risque d'engager leur responsabilité[197]. Puisqu'il est généralement moins coûteux de censurer une information parmi des millions que de risquer une amende ou le retrait d'une autorisation d'exercer, les acteurs privés soumis à un tel régime ont tendance à user d'excès de zèle, le doute profitant alors davantage à l'auto-censure qu'à la liberté d'expression. Des définitions d'infractions imprécises suffisent pour que la censure s'étende d'autant plus[198].

Plus souvent, les États mettent cependant en place des régimes de responsabilité dérogatoire (ou « restreinte ») qui accordent l'immunité aux intermédiaires de l'internet à condition notamment qu'ils retirent les contenus illicites dès qu'ils leur sont notifiés. Généralement perçus comme un bon équilibre pour sauvegarder la liberté d'expression, ces mécanismes n'en sont pas moins contestés par ceux qui estiment qu'ils profitent trop à la violation de droits tels que la propriété intellectuelle[199], ou qu'ils profitent trop à la liberté d'expression de ceux que l'imprécision du droit autorise à appeler parfois hâtivement « terroristes ». Les régimes de responsabilité dérogatoire font l'objet ces dernières années de propositions d'aménagements plus stricts, y compris de la part du Conseil d'État français[200] ou de la Commission européenne. Dans le cadre de la communication de sa stratégie pour un marché unique numérique en Europe, celle-ci a annoncé récemment son souhait « *d'imposer aux intermédiaires une obligation de responsabilité et de vigilance accrues dans la gestion de leurs réseaux et systèmes, c'est-à- dire un devoir de diligence* »[201].

[197] *V.* Article 19, « Intermédiaires Internet : dilemme de la responsabilité », 2013, p. 8. <http://www.article19.org/data/files/WEB_French.pdf>

[198] La Chine a ainsi défini neuf catégories de contenus interdits, dont le fait de porter atteinte « aux principes fondamentaux déterminés par la Constitution », « saper l'unité nationale », ou encore « la propagation de rumeurs, perturber l'ordre social ou saper la stabilité sociale ». *V.* Conseil d'Etat de la République populaire de Chine (n° 292), « Internet Information Services », 25 septembre 2000. <http://www.net.cn/static/hosting/fa_xinxi.htm>. Traduction française : <http://tinyurl.com/M2DIEDF-Chine>

[199] *V.* par ex., « Quelle(s) responsabilité(s) pour les nouveaux acteurs de l'Internet ? . - 3 questions à Guillaume Leblanc, directeur général du SNEP », *CCE* 2015 n°1, entretien n°1, janvier 2015. Le représentant des producteurs de disques y déplore « *les faiblesses de notre cadre juridique actuel en matière de lutte contre la contrefaçon en ligne liées au régime d'hypo-responsabilité des intermédiaires techniques* ».

[200] *V.* à propos de sa proposition de créer une catégorie juridique des « plateformes » soumise à un principe de « loyauté », Conseil d'État, *op.cit.* note 22, p. 274.

[201] Commission européenne, « Stratégie pour un marché numérique en Europe », *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen, et au Comité des régions*, 6 mai 2015, COM(2015) 192 Final, p. 14. <http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_fr.pdf>

Par ailleurs ces régimes imposent des mécanismes de notification des contenus illicites, comme c'est le cas en France par l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). Celui-ci fait obligation aux intermédiaires de l'internet de « *mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance* »[202] un contenu illicite. En pratique, ces dispositifs sont les mêmes que ceux déployés pour notifier aux plateformes des contenus qui, s'ils ne contreviennent pas à la loi, contreviennent en revanche aux contrats privés imposés par les intermédiaires. Or la tentation existe de la part d'États démocratiques d'instrumentaliser ces contrats et ces mécanismes d'alerte pour obtenir une censure non prévue par la loi, donc en principe incompatible avec les textes internationaux des droits de l'homme[203], mais néanmoins voulue par des gouvernements et permise dans une plus large mesure par le droit contractuel[204]. Dans un rapport publié en 2014, l'UNESCO constatait « *une tendance de plus en plus marquée* » au fait que « *certains gouvernements s'appuient sur les entreprises du secteur privé pour réguler les contenus en ligne en dehors de toute procédure légale et de toute responsabilité électorale* » [205].

C'est ainsi que dans un rapport confidentiel révélé par l'association StateWatch, le coordinateur de la lutte anti-terrorisme de l'Union européenne a explicitement proposé aux Etats membres, entre d'innocentes parenthèses, de « *soumettre [aux intermédiaires] les contenus terroristes ou extrémistes qui violent les propres termes et conditions des plateformes (et pas nécessairement la législation nationale)* »[206]. Dans cet esprit, le gouvernement français a annoncé en avril 2015 avoir négocié avec « *les "géants" de l'internet mondial, comme Google, Facebook, Microsoft, Apple et Twitter, ainsi que l'Association française des fournisseurs d'accès et de services internet* », la création d'un « *label permettant le retrait plus rapide des contenus illicites sur Internet* »[207], qui passe par le droit souple (une « plateforme de bonnes pratiques »[208]) plutôt que par l'activation des voies

202 LCEN, art. 6.7.

203 *V. supra*, §2.1.2, p.38.

204 *V. supra*, §1.2.2., p.21.

205 UNESCO, *Tendances mondiales en matière de liberté d'expression et de développement des médias*, 2014, p. 38. <http://unesdoc.unesco.org/images/0022/002275/227515F.pdf>

206 Conseil de l'Union européenne, EU Counter-Terrorism Coordinator, « EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015 », DS 1035/15, 17 janvier 2015, p.3. <http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf>

207 *V.* « Lutte contre la propagande terroriste : le Gouvernement mobilise les dirigeants des grands opérateurs de l'internet », 23 avril 2015. <http://www.gouvernement.fr/lutte-contre-la-propagande-terroriste-le-gouvernement-mobilise-les-dirigeants-d-internet>

208 *V.* Communiqué de presse de M. Bernard CAZENEUVE, Ministre de l'Intérieur, « Rencontre avec les grands opérateurs de l'Internet », 22 avril 2015. <http://www.interieur.gouv.fr/Presse/Les-communiques/Rencontre-

judiciaires ordinaires. Les États se déchargent ainsi de leur responsabilité internationale de protection de la liberté d'expression, en délégant leur pouvoir de censure à des entreprises privées.

Un autre moyen pour les États de censurer par procuration sur internet est de saper ou orienter le référencement des informations sur les moteurs de recherche ou annuaires. Sur internet, la difficulté pour la personne qui souhaite s'exprimer n'est jamais de trouver un support sur lequel publier ce qu'il souhaite, puisqu'il est toujours possible soit d'utiliser des plateformes existantes, soit de créer son propre site internet. Il n'y a pas sur internet de régime d'autorisation préalable comme il peut en exister, conformément au droit international des droits de l'homme[209], sur certains vecteurs de diffusion de médias audiovisuels. Il y aurait ainsi actuellement plus d'un milliard de sites internet mis en ligne, soit environ un site pour trois personnes connectées au réseau mondial[210]. Mais la difficulté devient alors de trouver une audience pour que son propre discours émerge de la multitude. L'on comprend dès lors l'importance stratégique capitale des moteurs de recherche dont la mission est justement d'ordonner les informations publiées par des milliards d'internautes et d'y donner accès à travers les résultats affichés aux requêtes des utilisateurs. Il n'y a plus besoin pour censurer d'effacer l'information à la source ni d'interdire d'y avoir accès ; il suffit simplement de miner les chances qu'a une information d'être vue et partagée. Là aussi la méthode peut être radicale comme en Chine, où les moteurs de recherche et les réseaux sociaux ont l'obligation indirecte (par leur responsabilité stricte) de censurer des résultats et reçoivent directement des « listes noires » de contenus à écarter[211], ou même en France où existent désormais plusieurs lois permettant à l'État d'obtenir le déréférencement de sites internet, y compris sans procédure judiciaire[212]. Parfois la technique de censure est plus subtile et consiste à noyer l'information indésirée sous celles qui sont préférées. C'est bien sûr un instrument qu'emploient les moteurs

---

avec-les-grands-operateurs-de-l-Internet>

209 *V.* par ex. CEDH, art.10 (« Le présent article n'empêche pas les Etats de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisation »).

210 *V.* Le Monde, « Le Web a plus d'un milliard de sites », 17 septembre 2014. <http://www.lemonde.fr/pixels/breve/2014/09/17/internet-a-25-ans-et-desormais-plus-d-un-milliard-de-sites_4488678_4408996.html>

211 *V.* UNESCO, *Fostering freedom online : the rôle of intermediaries*, 2014, p.106 (« industry representatives interviewed for this report confirm that companies including Baidu receive regular instructions as well as "blacklists" from authorities specifying what content needs to be either removed or blocked by the service itself »). <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>

212 Avec le contrôle d'un juge pour les sites illégaux de jeux d'argent (Loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, art. 61 al. 3) ; par simple ordonnance administrative pour les sites de pornographie infantile et les sites d'apologie d'actes de terrorisme (Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, art.12.II al.5).

de recherche eux-mêmes à des fins commerciales lorsqu'ils privilégient leurs propres services au détriment de ceux de la concurrence[213], mais c'est aussi une tactique que peuvent imiter des États lorsqu'ils amorcent une tentative de régulation de l'algorithme des moteurs de recherche. « *Ce serait aller loin que de demander aux moteurs de recherche de surréférencer certains sites labellisés, cela constituerait une forme de censure* », avait ainsi protesté Google France, lorsqu'un amendement à la loi Hadopi proposait de mettre en avant des sites internet homologués par l'autorité administrative[214].

b – une certaine privatisation du pouvoir judiciaire et législatif

Parce qu'ils ont droit de vie ou de mort sur un contenu publié, les intermédiaires de l'internet disposent d'un pouvoir probablement inédit par son ampleur dans le choix des informations auxquelles les individus peuvent accéder. « *Jusqu'à récemment, la personne qui avait le plus de pouvoir pour déterminer qui peut parler et qui peut être écouté à travers le monde n'était pas un président ou un roi ou un juge de la Cour Suprême. C'était Nicole Wong, qui était avocat général adjointe chez Google jusqu'à sa démission récente* », racontait le professeur Jeffrey Rosen en 2012[215]. « *Ses collègues l'appelait "la Décideuse". Nicole Wong était la Décideuse, qui était réveillée au milieu de la nuit pour décider quel contenu monte ou disparaît* » sur les moteurs de recherche de Google ou sur YouTube, acquis par la firme en 2006. Au quotidien, le choix des contenus laissés en ligne ou censurés est confié à des centaines voire des milliers d'employés d'intermédiaires de l'internet, dont le travail à plein temps consiste à évaluer la conformité aux lois et aux contrats des contenus qui leur sont signalés par l'État ou par les utilisateurs des services en ligne. Les régimes de responsabilité dérogatoire mis en place pour provoquer l'autorégulation par les intermédiaires de l'internet imposent que chacun évalue la licéité ou l'illicéité des contenus qui leur sont signalés, et qu'ils enfilent donc un costume de juge privé. Mais comme dans les régimes de responsabilité stricte, le doute profite le plus souvent à la censure[216], pour des raisons d'abord économiques.

---

213 *V.* Commission européenne, « Abus de position dominante: la Commission adresse une communication des griefs à Google au sujet du service de comparaison de prix et ouvre une procédure formelle d'examen distincte concernant Android », 15 avril 2015, IP/15/4780. <http://europa.eu/rapid/press-release_IP-15-4780_fr.htm>

214 *V.* « Hadopi : Google redoute "une forme de censure" », *Numerama.com*, 5 mars 2009. <http://www.numerama.com/magazine/12212-hadopi-google-redoute-une-forme-de-censure.html>

215 Jeffrey ROSEN, « The Deciders : The future of privacy and free speech in the age of Facebook and Google », Fordham Law Review, Vol.80, Issue 4 (2012), p. 1536. <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4774&context=flr>

216 Pour tenter de limiter cet effet, en France le Conseil constitutionnel a émis une réserve d'interprétation à l'article 6 de la LCEN, qui stipule que « *ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge* »

Sur des services qui sont pour la plupart gratuits, il coûte bien moins cher de perdre un client fâché d'être censuré que de rémunérer juristes et avocats dans le cas où la responsabilité de l'hébergeur serait engagée devant les tribunaux. Et pour la personne censurée ou privée du droit de s'informer, le recours judiciaire apparaît lui-même comme une procédure trop fastidieuse pour être régulièrement employée.

Cette « *privatisation de la censure* » dénoncée par l'UNESCO, développée « *à la faveur de l'importance grandissante des entreprises technologiques et autres intermédiaires de l'écosystème des médias* »[217], génère une forme de privatisation du pouvoir judiciaire qui aurait pu apparaître comme une menace aux États partiellement dépossédés d'une prérogative régalienne. Et pourtant elle est au contraire régulièrement encouragée, car perçue comme permettant d'atteindre une efficacité que n'offre pas le système judiciaire étatique alourdi par des contraintes procédurales qui sont néanmoins autant de garanties apportées au respect des droits de l'homme. L'on peut ainsi s'étonner des applaudissements politiques qui ont accompagné la publication par la CJUE de son arrêt *Google Spain*[218], en se demandant avec Anne Debet si le juge européen s'est véritablement contenté de consacrer un « droit à l'oubli » sur internet en jugeant que les moteurs de recherche devaient censurer sur demande des résultats de recherches liées au nom d'un individu, ou s'il n'a pas commis au passage un « oubli du droit »[219]. Comme nous le verrons plus en détails dans la troisième partie de cette étude[220], le juge européen a en effet confié aux moteurs de recherche la lourde responsabilité d'arbitrer entre deux droits fondamentaux, celui du respect de la vie privée de l'individu dont des informations le concernant sont indexées et rendues accessibles, et celui du droit des internautes à l'information. Cette prérogative, qui était jusque là assumée par les tribunaux, permet d'y voir un « droit à l'oubli de la neutralité du moteur de recherche »[221], mais « *laisser à Google, au lieu et place de l'autorité judiciaire ou des autorités de protection des données, le soin de faire le tri n'apparaît pas très judicieux* »[222].

(Cons. const., déc. n° 2004-496 DC, 10 juin 2004, §9).

217 *Op.cit.* note 205, p. 9.

218 *V.* par ex. le commentaire du Commissaire européen Michel Barnier, se félicitant de ce que la CJUE aurait affirmé que l'Europe était « un continent de valeurs avec l'homme en son centre », Twitter, 13 mai 2014. <https://twitter.com/MichelBarnier/status/466216256933482496> ; ou le communiqué du ministre de l'industrie français Arnaud Montebourg, selon lequel « cet arrêt contribue à rétablir l'équilibre entre les pratiques des grandes plateformes numériques et les droits des utilisateurs d'internet, citoyens et entreprises » <http://www.economie.gouv.fr/donnees-personnelles-internet-arret-cjue>.

219 *V.* Anne DEBET, « Google Spain : Droit à l'oubli ou oubli du droit ? », CCE n°7-8, juillet 2014, étude 13.

220 *V. infra*, §3.2.2, p.73.

221 *V.* Guillaume BUSSUEIL, « Arrêt Google : du droit à l'oubli de la neutralité du moteur de recherche », *La Semaine Juridique — Entreprises et Affaires*, n°24, 12 juin 2014, 1327.

222 Anne DEBET, *op.cit.* note 219.

Dans le même esprit il faut remarquer la tendance forte, au moins en France et dans l'Union européenne, de s'en remettre de plus en plus souvent au droit souple pour réguler les activités sur internet, par la multiplication de chartes, guides, recommandations, engagements volontaires et autres codes de bonne conduite qui sont négociés avec les intermédiaires de l'internet, mais qui mettent à l'écart le législateur. Les utilisateurs des services en ligne concernés sont rarement représentés dans ces processus de création de droit alors que les engagements pris avec les États peuvent avoir d'importantes répercussions sur les droits fondamentaux des internautes. Les gouvernements y voient encore une méthode efficace, tandis que pour nombre d'entreprises, comme l'avait analysé le Conseil d'État, « *la réticence à l'intervention contraignante de l'État, et donc la préférence pour le droit souple, a fortiori lorsqu'il est d'origine privée, paraît inhérente au libéralisme économique* »[223]. Citons à titre d'exemple le principe de la neutralité du net, dont nous avons vu qu'il était indispensable au respect des droits fondamentaux sur internet[224], mais qui en France fait seulement l'objet de « recommandations » émises par l'Autorité de régulation des communications et des postes (ARCEP)[225]. Citons également les simples « recommandations » du groupe des CNIL européennes (G29) concernant la protection des données personnelles sur les smartphones et tablettes[226], qui engrangent quantités de données dans des conditions souvent opaques[227] et pourraient (devraient ?) faire l'objet de réglementations plus strictes et plus dissuasives par les États membres de l'Union européenne. Citons enfin les « chartes des bonnes pratiques » négociées sous l'égide du ministère de la Culture en France pour lutter contre la contrefaçon sur internet, l'une avec les régies publicitaires[228], l'autre avec les intermédiaires de paiement en ligne[229], qui confient à des représentants d'ayants droits le soin d'établir eux-mêmes des

---

223 Conseil d'État, *Étude annuelle 2013 — Le droit souple*, La documentation française, mai 2013, p.40.

224 *V. supra*, §1.1.2, p.16.

225 ARCEP, *Neutralité de l'Internet et des réseaux. Propositions et recommandations*, septembre 2010. <http://www.arcep.fr/uploads/tx_gspublication/net-neutralite-orientations-sept2010.pdf>

226 G29, « Avis 02/2013 sur les applications destinées aux dispositifs intelligents », adopté le 27 février 2013, p.33-37. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_fr.pdf>

227 *V.* Neil MCALLISTER, « How many mobile apps collect data on users? Oh ... nearly all of them », *The Register*, 21 février 2014. <http://www.theregister.co.uk/2014/02/21/appthority_app_privacy_study/>

228 Ministère de la Culture et de la Communication, « Charte des bonnes pratiques dans la publicité pour le respect du droit d'auteur et droits voisins ». <http://www.youscribe.com/catalogue/tous/actualite-et-debat-de-societe/actualite-evenements/charte-des-bonnes-pratiques-dans-la-publicite-pour-le-respect-du-2562094>

229 Encore en négociation au moment où nous écrivons ces lignes. *V.* Ministère de la Culture et de la Communication, « Lutte contre le piratage des œuvres sur internet : une mission conjointe IGF/CNC pour empêcher l'usage des moyens de paiement en ligne sur les sites Internet violant le droit d'auteur », 14 avril 2015. <http://culturecommunication.gouv.fr/Presse/Communiques-de-presse/Lutte-contre-le-piratage-des-aeuvres-sur-internet-une-mission-conjointe-IGF-CNC-pour-empecher-l-usage-des-moyens-de-paiement-en-ligne-sur-les-sites-Internet-violant-le-droit-d-auteur>

listes noires de sites internet réputés — mais non jugés par un tribunal — illicites, avec lesquels les entreprises concernées s'interdisent de faire affaire.

Or en « pseudo-légiférant » ainsi par la voie du droit souple négocié de gré à gré avec les intermédiaires de l'internet, les États contribuent consciemment ou non à traiter ces intermédiaires d'égal à égal. Peut-être est-ce l'une des raisons qui expliquent que ces acteurs privés se sentent parfois investis de la possibilité et de la responsabilité de ne plus simplement respecter le droit national, mais de s'opposer aux volontés des États lorsqu'ils portent atteinte aux droits de l'homme.

LA RESPONSABILITÉ CROISSANTE DES INTERMÉDIAIRES DE L'INTERNET DE PROTÉGER LES DROITS DE L'HOMME

En 2003, huit ans avant que les principes directeurs de Ruggie ne viennent affaiblir cette formulation[230], la Sous-Commission de la promotion et de la protection des droits de l'homme avait adopté des normes sur la responsabilité en matière de droits de l'homme des sociétés transnationales et autres entreprises, qui constataient que « *même si les États ont la responsabilité première de promouvoir, respecter, faire respecter et protéger les droits de l'homme et de veiller à leur réalisation, les sociétés transnationales et autres entreprises, en tant qu'organes de la société, ont, elles aussi, la responsabilité de promouvoir et de garantir les droits de l'homme énoncés dans la Déclaration universelle des droits de l'homme* »[231]. Chez les intermédiaires de l'internet, cette responsabilité fait l'objet d'une conscience relativement ancienne de la possibilité de protéger les droits de l'homme à travers les options technologiques retenues par les ingénieurs (3.1.1). Sans doute les atrocités facilitées par l'espionnage des réseaux électroniques lors des Printemps arabes, les révélations d'Edward Snowden sur les programmes de la NSA et les atteintes croissantes à la liberté d'expression ont-elles toutefois aidé à la naissance d'une véritable prise de conscience, non seulement de la possibilité qu'ont les intermédiaires de protéger les droits de l'homme sur internet, mais du devoir de le faire en opposant une véritable diplomatie parallèle aux États qui dérogent à leur responsabilité (3.2).

---

230 *V. supra*, p. 10.

231 Nations Unies, *Conseil économique et social, Sous-Commission de la promotion et la protection des droits de l'homme*, « Normes sur la responsabilité en matière de droits de l'homme des sociétés transnationales et autres entreprises », adoptées le 13 août 2003 (E/CN.4/Sub.2/2003/12/Rev.2), préambule. <http://www.humanrights.ch/upload/pdf/091127_NORMES_SUR_LA_RESPONSABILIT_EN_MATIRE_DE_DROITS.pdf>

3.1. La prise en compte des droits de l'homme dans la « *lex informatica* »

Comme d'autres champs d'activités humaines, internet n'est pas seulement régulé par le droit national ou international, mais aussi par ses règles propres. Dans l'univers numérique, celles-ci ont toutefois la particularité d'être d'abord des normes et des choix technologiques, qui forment leur propre ordre juridique (3.1.1), lequel a des conséquences sur la jouissance effective des droits de l'homme, ou la possibilité qu'il leur soit porté atteinte (3.1.2).

3.1.1. La *Lex Informatica*, ou quand « le code fait loi »

a – la technique, créature et créatrice d'un ordre juridique extra-légal

Lorsqu'ils signent des traités internationaux de protection des droits de l'homme, les États s'engagent à protéger les droits qui y sont garantis. Ces engagements se traduisent alors d'une part, par des pratiques étatiques plus conformes au respect des droits et libertés des individus, d'autre part, par l'adoption de lois et règlements qui apportent aux justiciables les traductions en droit interne des dispositions prévues par les textes internationaux, et enfin par l'acceptation par l'État du fait d'être placé sous l'observation de ses pairs, pour apporter les modifications nécessaires à ses comportements et à ses législations en cas de violation. Lorsque les États relaient ces droits de l'homme dans le droit national, les individus et les entreprises ont le sentiment d'être liés par le droit national du pays dont ils dépendent, et donc de ne pouvoir y déroger sans risquer de subir la « violence légitime » chère à Max Weber[232]. Dans cette dimension, le particulier comme l'entreprise n'est pas créateur de droit public, il n'en est que le sujet.

Mais sur internet règne un ordre juridique bien particulier qui interagit avec le droit international et la pluralité des droits nationaux. Joel R. Reidenberg l'avait appelé en 1998 la « Lex Informatica »[233], en référence à la fameuse *lex mercatoria* des marchands du moyen-âge. « *La Lex informatica désigne la régulation de l'Internet par la technique, c'est-à-dire*

---

[232] *V.* Max WEBER, *Le savant et le politique*, traduction de Julien Freund, Paris, Plon, collection « 10/18 », 1959 (édition 1963).

[233] V. Joel R. REIDENBERG, « Lex Informatica: The Formulation of Information Policy Rules Through Technology », *Texas Law Review*, Vol. 76, N°3, février 1998. <http://reidenberg.home.sprynet.com/lex_informatica.pdf>

l'ensemble des contraintes et des choix technologiques qui sont imposés sur les activités en ligne », résumera-t-il quelques années plus tard dans une contribution pour Sciences Po[234].

Sur internet existent en effet de nombreuses normes technologiques dont le respect est rendu quasiment obligatoire en pratique par la nécessité de communiquer avec les autres utilisateurs et d'interagir avec les autres services. Ces normes qui concernent aussi bien les protocoles de communication qui permettent aux ordinateurs de se parler ensemble, que la manière de formater des documents en ligne pour qu'ils soient visibles par tous, sont établies au gré d'un maillage de gouvernances complexes, très largement dominées par l'autorégulation entre acteurs privés (voir Annexe 1[235]). En quelque sorte, ces normes internationales correspondent aux traités internationaux. Il est possible d'y déroger ou de ne pas y adhérer, mais mieux vaut s'y conformer et rejoindre les plus importants si l'on ne veut pas se trouver au ban du « concert des nations », ou au ban du réseau.

Les normes techniques définies par les différentes instances de gouvernance offrent une multitude d'options possibles à ceux qui les implémentent. Chaque développeur de site internet ou d'application, chaque hébergeur, chaque fournisseur d'accès, chaque prestataire de messagerie, chaque moteur de recherche ou chaque fabricant d'équipement réseau va faire ses propres choix technologiques dans le cadre des normes internationales. Il va adhérer à certaines normes (à certains traités, pour filer la métaphore), en ignorer d'autres, et faire ses propres choix dans la manière d'interpréter les documentations de référence et de les traduire dans ses logiciels ou matériels destinés à communiquer sur internet. Ces choix correspondent, dans l'ordre juridique de la *Lex Informatica*, aux droits nationaux dans l'ordre juridique du droit international public.

Or ces normes internationales privées et ces choix technologiques sont eux-mêmes créateurs de droit public, au sens où ils fixent un cadre qui détermine la réalité ou non des droits auxquels peuvent prétendre les utilisateurs des services en ligne gouvernés par ces normes et choix techniques.

---

234 *V.* Joël R. REIDENBERG, « La régulation d'Internet par la technique et la Lex informatica », *Droit et économie de la régulation, Vol. 3*, Paris, Presses de Sciences Po, «Hors collection», 2005, p. 81.

235 Ou pour une version PDF en meilleure définition : <https://www.icann.org/en/system/files/files/governance-06feb13-fr.pdf>

Dans un livre qui a profondément marqué les esprits lors de sa publication[236], et à travers un article qui en offrait la synthèse[237], le professeur de droit constitutionnel américain Lawrence Lessig avait parfaitement analysé les enjeux de cet ordre juridique nouveau fait de « code », non plus légal, mais informatique. Et surtout, il avait mis en garde, il y a désormais quinze ans, sur les risques qu'il entrevoyait :

> « Nous sommes tellement obnubilés par l'idée que la liberté est intimement liée à celle de gouvernement que nous ne voyons pas la régulation qui s'opère dans ce nouvel espace, ni la menace qu'elle fait peser sur les libertés.
>
> 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 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. Cette régulation est en train de changer. Le code du cyberespace aussi. Et à mesure que ce code change, il en va de même pour la nature du cyberespace. Le cyberespace est un lieu qui protège l'anonymat, la liberté d'expression et l'autonomie des individus, il est en train de devenir un lieu qui rend l'anonymat plus difficile, l'expression moins libre et fait de l'autonomie individuelle l'apanage des seuls experts.
>
> […] Si nous ne comprenons pas en quoi le cyberespace peut intégrer, ou supplanter, certaines valeurs de nos traditions constitutionnelles, nous perdrons le contrôle de ces valeurs »[238]

Quinze ans après, la prophétie de Lessig semble hélas s'être en partie réalisée, comme nous l'avons démontré dans les deux premières parties de cette étude. Les violations des droits fondamentaux sont nombreuses qui se produisent à travers internet, que ce soit de la part des entreprises qui en ont fait leur lieu d'activité, ou de la part des États qui profitent de ce que les individus sont de plus en plus connectés pour mieux les surveiller, et qui exploitent la position

---

236 Lawrence LESSIG, *Code : and other laws of cyberspace*, Basic Books, 1999.

237 Lawrence LESSIG, « Code Is Law — On Libery In Cyberspace », *Harvard Magazine*, janvier-février 2000. <http://harvardmagazine.com/2000/01/code-is-law-html>

238 *Idem*. Traduction par Framablog : <http://framablog.org/2010/05/22/code-is-law-lessig/>

clé des intermédiaires de l'internet pour porter atteinte indirectement à la liberté d'expression. Or ces violations des droits de l'homme ont été facilitées par les choix technologiques opérés par les intermédiaires de l'internet, qui d'ailleurs sont en eux-mêmes une anomalie problématique de l'histoire.

Conçu en temps de guerre froide pour assurer la disponibilité des systèmes d'information même en cas d'attaque nucléaire, internet était à son origine un réseau égalitaire hautement déconcentré et décentralisé. Tout ordinateur qui se connectait au réseau hébergeait ses propres données, parfois dupliquées sur plusieurs machines, et tous participaient au routage des informations en communiquant constamment ensemble pour établir une cartographie dynamique. Il n'existait aucun point central, aucune possibilité d'interrompre internet en attaquant un point névralgique. Au pire, une attaque faisait disparaître quelques serveurs et les quelques informations qu'ils étaient les seuls à détenir, mais le réseau dans son ensemble restait résilient. Il n'existait pas ou peu d' « intermédiaire de l'internet » comme on l'entend aujourd'hui et donc il n'était pas possible de faire pression sur eux pour supprimer des informations publiées par des tiers, ou pour communiquer les données qu'ils détenaient sur ces derniers. Chacun était responsable de ses propres contenus et agissements. Mais le besoin d'accessibilité suscité par le développement d'internet auprès du grand public a accéléré la concentration des contenus sur quelques services en ligne, jusqu'à un stade où avec « l'informatique en nuage » (ou « cloud »), même ses propres contenus créés sur son propre ordinateur sont hébergés à distance sur des serveurs de prestataires privés[239].

L'on avait pourtant connu un sursaut de la logique décentralisée à partir de la fin des années 1990 et jusqu'au milieu des années 2000, avec le développement des protocoles dits de « Peer-to-Peer », ou P2P. Ceux-ci consistent à bannir tout serveur intermédiaire dans le partage des informations, qui se fait directement d'un internaute à un autre dans un réseau de pairs à pairs. Chaque ordinateur personnel qui reçoit une information la copie et en devient immédiatement le relais potentiel pour d'autres. La technologie a, il est vrai, surtout été utilisée pour porter atteinte à des droits en permettant le partage illicite d'œuvres protégées par le droit d'auteur, ce qui a pu engager la responsabilité de leurs concepteurs[240]. Mais dans le fond, si l'on veut bien sacrifier un peu de l'esprit pénaliste pour nourrir l'humaniste (au droit d'auteur de s'adapter ?[241]), le P2P repose sur un protocole technique formidablement libérateur. Chacun est libre de diffuser et de propager les messages de son choix, et nul — ni

[239] *V.* Hervé LE CROSNIER, « A l'ère de l' " informatique en nuages" », *Le Monde Diplomatique*, août 2008. <http://www.monde-diplomatique.fr/2008/08/LE_CROSNIER/16174>

[240] *V.* Yves GAUBIAC, « La responsabilité des fournisseurs de logiciels dans la diffusion illégale des oeuvres et autres prestations protégées », *CCE* n° 11, Novembre 2006, étude 34.

acteur privé ni acteur public — ne peut supprimer un contenu ou en bloquer l'accès. La liberté d'expression n'y est plus un droit mais un fait.

Dans une illustration évidemment choquante du point de vue européen mais qu'il faut prendre au sérieux du point de vue culturel américain, c'est à la technologie P2P qu'a eu recours une association qui souhaitait distribuer des plans de fabrication d'armes à feu au nom du second amendement à la Constitution des États-Unis, après que l'État fédéral a ordonné de fermer son site internet, portant selon elle atteinte à sa liberté d'expression[242]. « *Le Net interprète la censure comme un accident et le contourne* », avait expliqué un pionnier et activiste d'Internet[243]. Mais c'est aussi une option technologique, salutaire pour les uns puisqu'elle permet de poursuivre ceux qui participent à la diffusion de contenus illicites[244], dommageable pour les autres puisqu'elle facilite l'ingérence dans leur vie privée, qui fait que pour la plupart d'entre eux, les protocoles P2P rendent visibles publiquement toutes les adresses IP[245] de ceux qui partagent des informations. D'autres, au contraire, sont conçus spécifiquement pour garantir la confidentialité des échanges et permettre à des dissidents politiques — mais aussi, ne l'ignorons pas par excès de naïveté, à des criminels[246] — d'échapper à la censure et à des poursuites, grâce à des options technologiques différentes[247]. Ils participent, par le code informatique, à défendre les droits de l'homme.

3.1.2. La protection des droits de l'homme par la *Lex Informatica*

a – la protection de la vie privée par la fourniture de moyens de communication sécurisés

Il serait vain pour le juriste qui peut se sentir dépassé par des considérations techniques de tenter d'analyser les conséquences de la *Lex Informatica* sur les droits de l'homme sans comprendre comment fonctionne internet, donc sans s'intéresser aux normes et

---

241 *V* à propos de l'idée de l'instauration d'une « licence globale » pour rémunérer les auteurs, Christophe CARON, « Questions autour d'un serpent de mer », *CCE* n°11, Novembre 2009, repère 10.

242 V. *Defense Distributed v. U.S. Dep't of State*, plainte déposée le 5 juin 2015. <http://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2015/05/DefenseDistributed.pdf>

243 John Gilmore, cité par Philip ELMER-DEWITT, « First Nation in Cyberspace », *TIME International*, n°49, 6 décembre 1993. <http://www.chemie.fu-berlin.de/outerspace/internet-article.html>

244 *V.* « La Cnil autorise la mise en oeuvre de dispositifs de surveillance des réseaux P2P », *JCP*, n° 1, 2 Janvier 2008, act. 11.

245 C'est-à-dire les numéros d'identification de l'accès à internet utilisé par l'ordinateur.

246 V. Andy BECKETT, « The dark side of the internet », *The Guardian*, 26 novembre 2009. <http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet>

247 *V.* par ex. « Qu-est-ce que Freenet ? », <https://freenetproject.org/whatis.html>

aux choix technologiques qui font loi sur le réseau. Tentons néanmoins de garder nos explications au minimum nécessaire (et avouons-le, au maximum de nos capacités), le lecteur intéressé pouvant se rapporter aux ouvrages savants pour en savoir plus[248]. Sur internet, tous les échanges d'informations reposent sur un ensemble de protocoles empilés dans ce que l'on appelle les « couches TCP/IP »[249], dont le principe a été inventé en 1983. Ces protocoles couvrent les méthodes de communication entre appareils reliés au réseau, la manière dont les paquets de données doivent être distribués et ordonnés jusqu'au destinataire, et enfin, le fonctionnement des grands types d'applications qui reposent sur le réseau. Le Web est l'une d'entre elles, à travers le protocole HTTP (HyperText Transfer Protocol) qui détermine la manière dont les informations sont demandées ou envoyées à un serveur. Or lors de sa création en 1990, le protocole HTTP n'intégrait aucune méthode de chiffrement des informations circulant sur le réseau, certainement parce que la cryptographie était encore considérée dans de nombreuses législations comme un domaine réservé des militaires, et donc soumise à des déclarations ou autorisations spéciales pour les usages civils[250]. Le HTTP est encore aujourd'hui sur le Web le protocole le plus répandu. Pour effectuer une cryptographie des données et ainsi assurer la confidentialité, l'authenticité et l'intégrité des informations échangées, il est nécessaire de recourir à une couche supplémentaire de chiffrement, via le protocole HTTPS (HTTP Secure).

Pendant plus de deux décennies, le HTTPS qui est plus exigeant (et légèrement plus coûteux) à mettre en œuvre a été essentiellement réservé dans les faits aux transactions bancaires et à quelques applications sensibles. Mais depuis la fin des années 2000 et de façon exponentielle depuis les révélations sur les programmes étatiques de surveillance massive, les intermédiaires de l'internet qui utilisaient des moyens techniques facilitant l'interception des communications ont considérablement renforcé la protection de la vie privée des utilisateurs de leurs services, en recourant beaucoup plus largement qu'avant au HTTPS pour chiffrer les communications. Ainsi par exemple, Google propose le HTTPS sur sa messagerie Gmail depuis 2008[251], et l'a généralisé à l'ensemble de ses utilisateurs en 2010[252]. Quatre ans plus

---

248 Par ex., José DORDOIGNE, *Réseaux informatiques - Notions fondamentales*, 6e édition, Éditions ENI, 603 p.

249 *V.* « Suite des protocoles Internet », Wikipedia. <https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet>

250 *V.* « Loi et cryptographie », *La Recherche*, juin 1998, p. 22.

251 *V.* Google, « Making security easier », Official Gmail Blog, 24 juillet 2008. <http://gmailblog.blogspot.fr/2008/07/making-security-easier.html>

252 *V.* Google, « Default https access for Gmail », Official Gmail Blog, 12 janvier 2010. <http://gmailblog.blogspot.fr/2010/01/default-https-access-for-gmail.html>

tard, Google a été un cran plus loin en chiffrant également les communications entre ses propres serveurs, pour éviter toute interception des e-mails lorsqu'ils sont copiés d'un serveur à un autre[253]. C'est « *quelque chose dont nous avions fait la plus grande priorité depuis les révélations de l'an dernier* », avait expliqué la firme dans un communiqué[254], faisant allusion aux révélations du Washington Post[255] selon lequel la NSA aurait collecté secrètement des informations sur des clients de Google en interceptant les données au niveau des liens de réseau entre les infrastructures des géants du Web américains. Évidemment motivé avant tout par des considérations commerciales liées à la confiance que ses clients doivent avoir dans ses services, Google a ainsi adopté à l'encontre des États une véritable posture de « protection » de la vie privée des utilisateurs, comme nombre de ses concurrents qui ont mis en place ou annoncé des mesures de protection similaires.

Ce mouvement est soutenu par l'Assemblée parlementaire du Conseil de l'Europe qui a fait sien l'appel lancé par le Parlement européen le 12 mars 2014 visant à « *promouvoir l'utilisation généralisée du cryptage et résister à toute tentative de fragilisation du cryptage et des autres normes de sécurité d'internet, non seulement pour protéger la vie privée, mais également pour écarter les menaces que font peser sur la sécurité nationale les États voyous, les terroristes, les cyberterroristes et les criminels de droit commun* »[256]. Dans un rapport sur les implications de la surveillance des communications par les États, le Rapporteur spécial des Nations Unies sur la promotion et la protection de la liberté d'opinion et d'expression avait été jusqu'à dénoncer les acteurs privés qui « *ont souvent échoué à déployer des technologies améliorant la vie privée, ou les ont implémentées d'une manière moins sécurisée qui ne représente pas l'état de l'art* »[257]. Il recommandait que « *les individus [soient] libres d'utiliser n'importe quelle technologie de leur choix pour sécuriser leurs communications* », sans que l'État ne s'aménage la possibilité d'obtenir les clés de déchiffrement sur simple demande aux intermédiaires[258].

---

253 *V.* Google, « Staying at the forefront of email security and reliability: HTTPS-only and 99.978% availability », 20 mars 2014. <http://gmailblog.blogspot.fr/2014/03/staying-at-forefront-of-email-security.html>

254 *Idem.*

255 Barton GELLMAN et Ashkan SOLTANI, « NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say », *Washington Post*, 30 octobre 2013. <http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html>

256 *Op.cit*, note 130, §17.2.

257 Nations Unies, *Conseil des droits de l'homme*, « Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue », 17 avril 2013, A/HCR/23/40, §74. <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/23/40&Lang=E>

258 *Idem*, §89.

Certaines organisations d'autorégulation qui pèsent sur la *Lex Informatica* ont aussi soutenu une évolution permettant de passer d'une logique passive de simple respect des droits fondamentaux à une logique de protection active. C'est le cas en particulier de l'Internet Engineering Task Force (IETF), qui produit l'essentiel des normes techniques pour internet, et qui s'est préoccupée du sujet dès 1996. Ne manquant pas d'un certain humour, c'est par un document portant la cote orwellienne « RFC 1984 » que l'IETF avait demandé que les obstacles étatiques posés au chiffrement des communications soient levés[259]. En 2013, l'organisation a publié une recommandation RFC 6973[260] proposée notamment par des ingénieurs de Nokia et Microsoft, qui « *dit en substance que tout nouveau protocole de la famille TCP/IP devrait avoir, lors de sa conception, une réflexion sur les risques qu'il pose pour la vie privée et les moyens de les limiter* »[261]. Et lors des travaux préparatoires du protocole HTTP/2 qui remplacera à terme le protocole HTTP, il a été proposé d'y imposer le chiffrement intégral du Web[262], ce qui ne sera toutefois pas le cas dans la version finale.

En février 2014, le W3C, qui préside à l'adoption de toutes les normes technique de création des sites internet, a lui aussi appelé la communauté des ingénieurs à « *construire des protocoles et des formats Web qui permettent aux individus et aux groupes de communiquer avec ceux qu'ils essayent d'atteindre, et de protéger ces communications contre toute écoute par des tiers* »[263].

Le plus souvent cependant, les intermédiaires de l'internet qui ont un but lucratif n'appliquent des mesures protectrices de la vie privée qu'à l'encontre d'une intrusion par les tiers, se réservant pour eux un accès à la clé qui permet de déchiffrer et lire les messages qu'ils stockent. Un tel accès leur est indispensable notamment pour affiner la connaissance qu'ils ont des centres d'intérêts de l'utilisateur, et lui proposer des publicités ciblées. Mais l'on assiste aussi ces dernières années à un mouvement plus radical, où même l'intermédiaire se prive de la possibilité d'être mis sous pression par les États pour déchiffrer le contenu de communications, et se place en protecteur des droits de l'homme. Apple, par exemple, a décidé contre l'avis de la police américaine de chiffrer le contenu de ses smartphones avec une

---

259 *V.* IETF, Network Working Group, RFC 1984, août 1996. <http://www.rfc-editor.org/rfc/rfc1984.txt>

260 *V.* IETF, Network Working Group, RFC 6973. <http://www.rfc-editor.org/rfc/rfc6973.txt>

261 *V.* Stéphane BORTZMEYER, « RFC 6973: Privacy Considerations for Internet Protocols », 25 juillet 2013. <http://www.bortzmeyer.org/6973.html>

262 *V.* Dan GOODIN, « Internet architects propose encrypting all the world's Web traffic », *Ars Technica*, 14 novembre 2013. <http://arstechnica.com/security/2013/11/encrypt-all-the-worlds-web-traffic-internet-architects-propose/>

263 *V.* Wendy SELTZER, « Strengthen Web security on the day we fight back », *W3C*, 11 février 2014. <http://www.w3.org/blog/2014/02/strengthen-web-security-on-the-day-we-fight-back/>

clé unique à chaque téléphone, qu'il ne connaît pas[264]. Google a suivi le même mouvement. WhatsApp, utilisé bientôt par près d'un milliard d'individus, propose également depuis peu le chiffrement des communications, pour que même sa maison-mère Facebook n'ait pas accès au contenu des conversations[265]. L'ONG américaine Electronic Frontier Foundation (EFF) a analysé 40 services de messagerie instantanée, et la moitié d'entre elles[266] a intégré désormais un chiffrement intégral qui assure que personne ne peut lire les conversations en dehors du destinataire et de l'expéditeur[267]. Elles étaient rarissimes il y a encore quelques années.

Mais la volonté de passer du respect des droits de l'homme à la protection des droits de l'homme et de le faire par la technique incite parfois les intermédiaires de l'internet à croire que tout ou presque peut être automatisé par la technologie, ce qui peut représenter paradoxalement de nouvelles menaces sur les droits fondamentaux.

b – la menace de l'automatisation de la protection des droits

Les intermédiaires de l'internet n'ont pas seulement le souci de protéger les droits fondamentaux de leurs utilisateurs contre la menace que représentent les États, mais aussi de plus en plus la volonté (ou comme nous l'avons vu, la contrainte[268]) de respecter et protéger les droits des tiers, y compris contre les agissements de leurs clients. Il s'agit en particulier de protéger le droit de propriété en s'assurant que les droits de propriété intellectuelle ne soient pas enfreints via leurs services en ligne, ou encore de lutter contre toutes sortes de « discours de haine » qui — bien davantage du point de vue européen qu'américain — sont des abus de la liberté d'expression qui peuvent être analysés comme des provocations à la discrimination. Dans son arrêt *Willem c. France*, la Cour EDH a ainsi estimé que la diffusion par un maire sur internet d'un message d'appel au boycott des produits israéliens avait « *aggravé le caractère discriminatoire de la position du requérant, confortée par l'utilisation de termes polémiques* »[269], et donc que le droit des Israéliens à ne pas être discriminés justifiait la

---

264 *V.* Kevin POULSEN, « Apple's iPhone Encryption Is a Godsend, Even if Cops Hate It », *Wired*, 10 août 2014. <http://www.wired.com/2014/10/golden-key/>

265 *V.* Martin UNTERSINGER, « WhatsApp se met au chiffrement pour protéger ses utilisateurs », *Le Monde*, 18 novembre 2014. <http://www.lemonde.fr/pixels/article/2014/11/18/whatsapp-se-met-au-chiffrement-pour-proteger-ses-utilisateurs_4525423_4408996.html>

266 21 au moment où nous écrivons ces lignes.

267 Electronic Frontier Foundation, « Secure messaging scorecard — Which apps and tools actually keep your messages safe ? ». <https://www.eff.org/secure-messaging-scorecard#about>

268 *V. supra*, §2.2.1.a p.49.

269 *V.* Cour EDH, affaire *Willem c. France* (req. n°10883/05), 16 juillet 2009, §36.

restriction à la liberté d'expression sur internet. Mais lorsqu'ils protègent les droits des tiers, les intermédiaires de l'internet ont de plus en plus souvent recours à des outils automatisés.

Ainsi pour éviter la violation de droits d'auteurs par les utilisateurs qui hébergent des vidéos sur leurs services, YouTube[270], Dailymotion[271] ou encore Vimeo[272] ont mis en place des outils préventifs de détection de contenus dont les droits sont détenus par des tiers. Si un utilisateur exploite dans sa vidéo tout ou partie d'une œuvre qui ne lui appartient pas, les systèmes de contrôle automatisés empêchent que la vidéo soit mise en ligne sans l'autorisation des ayants droits[273]. Or la législation sur le droit d'auteur n'est pas binaire ; elle connaît tout un champ des possibles entre l'interdiction de principe d'exploiter une œuvre littéraire ou artistique, et l'autorisation donnée explicitement par le titulaire des droits. Il n'est pas ici le lieu de détailler les exceptions au droit d'auteur prévues par les traités internationaux ou le droit national[274], mais il est important de rappeler qu'elles existent. Elles visent par exemple à permettre les courtes citations, la parodie, ou le pastiche. « *La liberté d'expression est à la base des dérogations que l'on rencontre dans presque toutes les lois nationales* », explique le professeur André Lucas[275]. Plus largement, pour la Rapporteuse spéciale dans le domaine des droits culturels des Nations Unies, les exceptions au droit exclusif de l'auteur « *constituent une part essentielle de l'équilibre que le droit d'auteur doit maintenir entre les intérêts des titulaires de droits, s'agissant du contrôle exclusif, et les intérêts des tiers en ce qui concerne la participation à la vie culturelle* »[276]. Or les logiciels de filtrage mis en place par les plateformes de vidéos en ligne pour détecter les exploitations préjugées illicites des contenus de tiers sont bien incapables — et n'essayent pas — d'avoir le raisonnement juridique d'un juge humain, pour déterminer si telle exploitation relève de la contrefaçon, ou si telle autre relève du droit à la critique ou à la parodie. C'est ainsi que de nombreuses vidéos non contrefaisantes sont régulièrement bloquées avant-même d'être mises en ligne, privant les

---

270 *V.* « Fonctionnement de Content ID », YouTube. <https://support.google.com/youtube/answer/2797370?hl=fr>

271 *V.* « Pourquoi et comment Dailymotion supprime certaines vidéos », Dailymotion, 7 janvier 2011. <http://blog.dailymotion.com/2011/01/07/pourquoi-et-comment-dailymotion-supprime-certaines-videos/>

272 *V.* « Copyright Match on Vimeo », Vimeo, 21 mai 2014. <https://vimeo.com/blog/post:626>

273 Ceux-ci ont généralement la possibilité de pré-approuver toute utilisation de leurs œuvres, par le biais de contrats-types qui prévoient une rémunération par le partage des revenus publicitaires.

274 Sur ce sujet, *V.* par ex. André LUCAS, « Droits des auteurs – Droits patrimoniaux – Exceptions au droit exclusif (CPI, art. L. 122-5 et L. 331-4) », *JurisClasseur* Fasc. 1248, §19.

275 *Idem*. §19.

276 Nations Unies, *Conseil des droits de l'homme*, « Rapport de la Rapporteuse spéciale dans le domaine des droits culturels, Farida Shaheed — Politiques en matière de droit d'auteur et droit à la science et à la culture », 24 décembre 2014, A/HRC/28/57, §61. <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Pages/ListReports.aspx>

individus du droit de participer à la vie culturelle sur les plateformes où cette vie culturelle est la plus dynamique. Par goût pour l'ironie, citons simplement en exemple le retrait automatique par YouTube d'une vidéo… qui critiquait les retraits automatisés de vidéos[277].

La censure confiée à des machines consiste aussi parfois à interdire à un internaute de publier de nouveaux messages après qu'il ait fait l'objet de signalements traités par un algorithme, ou à filtrer automatiquement des expressions interdites. Récemment, des chercheurs de Yahoo ont annoncé le développement d'une intelligence artificielle qui détecte les nouvelles expressions racistes, xénophobes, homophobes ou autres, pour faciliter la suppression automatisée des messages et la désactivation des comptes[278], au risque de mal interpréter l'intention de celui qui s'exprime. De même, Facebook, Google et Microsoft mettent en place des technologies qui visent à détecter les comportements de délinquants sexuels potentiels sur leurs services en ligne, pour s'autoriser à lire ensuite leurs correspondances privées et rapporter leurs découvertes aux autorités compétentes si l'intrusion dans la vie privée confirme un risque[279].

Ces dérives, réelles ou potentielles, valent souvent aux entreprises concernées d'être critiquées au moins autant que les États par les associations spécialisées dans la protection des libertés publiques sur internet, qui expriment désormais à l'égard des intermédiaires de l'internet une véritable attente de protection des droits. Ceci a sans doute contribué à ce que les entreprises elle-mêmes prennent toute la mesure de leur responsabilité sociale, et se forgent une forme de diplomatie autonome, qui s'organise pour adopter les meilleures normes de protection des droits de l'homme, et rendre comptes aux individus.

---

277 *V.* « Les robots de la police privée du copyright attaquent "Robocopyright" », *La Quadrature du Net*, 19 septembre 2013. <https://www.laquadrature.net/fr/les-robots-de-la-police-privee-du-copyright-attaquent-robocopyright>

278 *V.* Nemanja DJURIC et autres, « Hate speech detection with comment embeddings », 18 mai 2015. <http://labs.yahoo.com/publication/hate-speech-detection-with-comment-embeddings/>

279 *V.* Nolwenn LE BLEVENNEC, « Jean-Luc Lahaye, qui a corrompu une mineure, s'en prend à Facebook », *Rue 89*, 18 mai 2015. <http://rue89.nouvelobs.com/2015/05/18/jean-luc-lahaye-a-corrompu-mineure-sen-prend-a-facebook-259211>

3.2. La naissance d'une diplomatie des multinationales de l'internet, prêtes à rendre comptes

Désormais conscientes qu'elles sont en position de porter atteinte aux droits fondamentaux de leurs utilisateurs mais aussi de protéger leurs droits et ceux de tiers, les entreprises évoluant dans les technologies de la communication s'organisent pour établir des principes communs permettant d'opposer un véritable rapport de force aux États, dans une forme de dialogue diplomatique (3.2.1). A l'égard du public, les initiatives se traduisent par des efforts de transparence sur les résultats obtenus et le respect des principes édictés, même si ces efforts sont encore insuffisants (3.2.2).

3.2.1. Des règles communes de protection des droits fondamentaux opposées aux États

a. la Global Network Initiative (GNI) et Telecommunications Industry Dialogue (TID)

Il est très fréquent que des entreprises privées ou des associations se réunissent dans des consortiums pour défendre des intérêts communs contre des gouvernements ou contre d'autres organisations. Il est beaucoup plus rares qu'elles le fassent prioritairement pour défendre les droits des tiers contre leur propre pouvoir de nuisance. C'est pourtant en partie la philosophie de la Global Network Initiative (GNI), une coalition d'entreprises des technologies de l'information et de la communication (TIC), d'organisations de la société civile, d'investisseurs privés et d'universitaires, qui s'est créée en 2008 pour « *fournir une direction à l'industrie des TIC et à ses parties prenantes sur la manière de protéger et promouvoir les droits de l'homme à la liberté d'expression et à la vie privée lorsqu'elle est confrontée à des pressions de gouvernements pour entreprendre des actions qui enfreignent ces droits* »[280].

Aux côtés d'institutions universitaires (dont le Berkman Center for Internet & Society de Harvard ou la George Washington University Law School) et d'associations de défense des

[280] Global Network Initiative, « What does the Global Network Initiative aim to accomplish ? », <https://globalnetworkinitiative.org/content/frequently-asked-questions>

droits de l'homme (dont Human Rights Watch), la GNI compte actuellement six entreprises multinationales membres qui offrent des services d'intermédiaire de l'internet, toutes d'origine américaine : Facebook, Google, LinkedIn, Microsoft, Procera Networks et Yahoo. Ses trois membres fondateurs étaient Google, Microsoft et Yahoo.

Souhaitant créer un véritable ordre juridique supérieur qui lie les membres entre eux, à l'instar de ce que peuvent être les traités internationaux entre les États, la GNI prévoit dans ses directives que les engagements pris par les entreprises participantes sont supérieurs à tout autre engagement. Elles stipulent en effet que « *les participants devront s'abstenir de conclure des accords volontaires les contraignant à limiter la liberté d'expression des utilisateurs ou portant atteinte au respect de la vie privée d'une manière incompatible avec les Principes* » énoncés dans les documents de base de l'organisation, et qu'ils doivent dénoncer dans les trois ans tout engagement préalable qui ne serait pas compatible[281]. Les Principes eux-mêmes stipulent que « *les Participants vont chercher à accroître dans le monde entier le nombre des organisations appuyant ces Principes pour qu'ils s'imposent comme la nouvelle norme mondiale* »[282].

La GNI offre également ses moyens logistiques à une autre organisation plus étroite, la Telecommunications Industry Dialogue (TID), qui s'est créée en 2013 pour établir des règles de conduite spécifiques aux opérateurs et fournisseurs d'outils de télécommunication. Contrairement à la GNI dont la gouvernance est multi-partite, TDI n'accueille en son sein que des entreprises qui discutent ensemble des règles qu'elles acceptent de s'imposer, selon un mode décisionnel qui semble être celui de l'unanimité[283]. L'organisation se décrit comme un « *groupe d'opérateurs et de fournisseurs de télécommunications qui abordent communément les droits à la liberté d'expression et à la vie privée dans le secteur des télécommunications dans le contexte des Principes Directeurs des Nations Unies sur les Entreprises et les Droits de l'Homme* ». TID compte actuellement neuf membres, principalement européens : Alcatel-Lucent, Orange, Nokia, Telefonica, Telenor, TeliaSonera, Millicom, Vodafone et AT&T.

Ensemble, ces deux organisations forment les deux principales structures d'auto-régulation visant à apporter aux individus une meilleure protection des droits de l'homme face

---

281 *V.* Global Network Initiative, « Directives de mise en œuvre des Principes de liberté d'expression et de respect de la vie privée », §5. <https://www.globalnetworkinitiative.org/sites/default/files/pdfs/FR_Implementation_Guidelines_FRA.pdf>

282 *V.* Global Network Initiative, « Principes de liberté d'expression et de respect de la vie privée », Préambule. <https://www.globalnetworkinitiative.org/sites/default/files/pdfs/FR_Principles_FRA.pdf>

283 Aucune forme de statuts n'est publiée sur le site officiel de l'organisation : <http://www.telecomindustrydialogue.org/>

aux menaces que représentent les ingérences de l'État. Il faudrait toutefois noter que même sans en être membres, de nombreux autres intermédiaires de l'internet agissent désormais selon les mêmes principes, en tout ou partie.

b. les principes communs de liberté d'expression et de respect de la vie privée, contre les États

Que ce soit la GNI ou TID, les deux organisations ont fait le choix de se concentrer exclusivement sur les problématiques liées à la liberté d'expression et au respect de la vie privée, qui sont les deux droits les plus menacés par l'action des États sur internet. Mais les principes de la GNI rappellent, dans une formule qui n'est pas sans évoquer la Déclaration et le programme d'action de Vienne[284], que « *les droits de l'homme sont indivisibles, interdépendants et étroitement liés* », que « *la restriction de l'un d'entre eux pénalise tous les autres* », et donc que la protection des deux droits précités « *facilit[e] une matérialisation constructive des autres droits de l'homme* »[285].

Alors que les Principes directeurs de Ruggie adoptés aux Nations Unies se contentent de faire état de la responsabilité des entreprises « *de se conformer à toutes les lois applicables et de respecter les droits de l'homme* »[286], les membres de la GNI vont plus loin. Ils choisissent d'ignorer cette quadrature du cercle qui consisterait à demander à la fois aux entreprises d'obéir à des lois nationales et de respecter les droits de l'homme, alors que ce sont parfois les droits nationaux qui sont à l'origine des violations des droits fondamentaux, et assument de chercher à imposer un rapport de force aux États pour la protection des droits, quelle que soit leur législation. Les adhérents à l'organisation reconnaissent ainsi explicitement que « *les entreprises du secteur du secteur des technologies de l'information et de la communication (TIC) sont responsables du respect et de la protection du droit à la liberté d'expression et au respect de la vie privée de leurs utilisateurs* », et disent vouloir « *assurer à l'échelle de la planète la protection et la promotion de la jouissance des droits de l'homme* »[287], ce qui est d'ordinaire perçu comme une prérogative et une obligation dévolue aux seuls États.

Aussi, non seulement les membres de la GNI « *respecteront et protégeront* » les droits visés, en « *cherchant à éviter ou à minimiser l'impact des restrictions gouvernementales* »,

[284] *V.* Nations Unies, « Déclaration et programme d'action de Vienne », *Conférence mondiale sur les droits de l'homme*, 12 juillet 1993, A/CONF.157/23, §5. (« Tous les droits de l'homme sont universels, indissociables, interdépendants et intimement liés »)

[285] Principes de la GNI, *op. cit.* note 281, §1.

[286] *V. op. cit.* note 13.

[287] Principes de la GNI, *op. cit. note 281, §1.*

mais en plus elles protégeront les droits des « *utilisateurs soumis à des exigences du gouvernement, des lois et des règlements* » contraires aux principes énoncés par l'organisation[288].

En pratique, selon les directives de mise en œuvre des principes, les membres de la GNI « *encourageront les gouvernements à être précis, transparents et cohérents dans leurs demandes, dispositions législatives et réglementaires concernant le respect de la vie privée en ligne* », « *exécuteront a minima les demandes gouvernementales compromettant le respect de la vie privée* », et même « *poursuivront le gouvernement devant les tribunaux nationaux [...] en cas de demandes gouvernementales semblant incompatibles [...] avec les lois internationales sur les droits de l'homme et les normes de liberté d'expression* »[289]. C'est ainsi par exemple que Microsoft, membre de la GNI, a déposé un recours aux États-Unis contre une ordonnance demandant l'accès à des données privées hébergées dans un centre de données en Irlande[290]. Cette protection des utilisateurs des services en ligne par la voie judiciaire ne sera toutefois pas systématique puisque les membres « *s'attacheront de préférence à sélectionner les cas sur la base d'une série de critères* », dont le coût de l'action, la gravité du cas, ou sa probabilité de succès[291].

Concernant TID, ses propres principes directeurs stipulent en introduction qu'ils « *visent à remédier à ces situations exceptionnelles* » dans lesquelles « *les technologies de télécommunications peuvent [...] être détournées par les gouvernements d'une manière qui peut affecter la liberté d'expression et la vie privée de leurs citoyens* »[292]. Les opérateurs de télécommunication sont néanmoins bien plus mesurés que les membres de la GNI dans leur opposition aux gouvernements, sans doute parce qu'ils n'ont aucune possibilité de déménager, puisqu'ils doivent par nature être présents dans le pays qui accueillent leurs infrastructures. Ainsi les membres de TID se disent « *conscients des responsabilités qui découlent de la fourniture de produits, de services et d'infrastructures de communication* », de la nécessité de s'appuyer « *sur des relations de long terme, stables* » avec les gouvernements, et n'édictent leurs principes que « *dans la mesure qui ne les place pas en violation des lois et règlements*

---

288 *Idem*, §2 et §3.

289 Global Network Initiative, *Directives*, *op. cit* note 280, §3 et §4.

290 *V.* Liam TUNG, « Microsoft files fresh appeal against handing over email in Irish datacentre », *ZDNet*, 9 décembre 2014. <http://www.zdnet.com/article/microsoft-files-fresh-appeal-against-handing-over-email-in-irish-datacentre/>

291 *Idem.*

292 Telecom Industry Dialog, « Principes directeurs en matière de liberté d'expression et de protection de la vie privée dans les télécommunications », 12 mars 2013, p. 2. <http://www.telecomindustrydialogue.org/wp-content/uploads/Telecoms_Industry_Dialogue_Principles_Version_1_-_FRENCH.pdf>

nationaux », ce qui relativise largement leur portée et leur sincérité. En revanche, on peut souligner une volonté implicite de leur donner un caractère contraignant, puisqu'il est précisé en toute fin que « *seule la version anglaise [des principes directeurs] prévaudra en cas de litige* ».

Là aussi, les principes de TID stipulent que les entreprises de télécommunication devront notamment « *s'assurer que les exigences du gouvernement sont réexaminées par du personnel dûment qualifié et expérimenté afin d'évaluer leur conformité juridique ainsi que la régularité de la procédure* »[293], « *rechercher des mesures de remplacement qui pourraient minimiser ou atténuer l'incidence des impacts négatifs sur la liberté d'expression et le respect de la vie privée* »[294], ou encore « *rechercher le contrôle judiciaire, dès lors qu'il est possible* »[295].

Enfin, les deux organisations prévoient de rendre compte de leurs engagements à travers la publication de rapports, qui doivent permettre au public de vérifier le respect effectif de leur responsabilité de protéger les droits de l'homme.

3.2.2. Des engagements de transparence perfectibles

a – la publication de rapports de transparence

Dans ses Directives de mise en œuvre, la GNI prévoit « *trois niveaux de rapports différents sur la progression de la mise en œuvre des Principes* »[296], qui semblent s'inspirer en partie de la pratique des EPU du Conseil des droits de l'homme des Nations Unies. Leur contenu est détaillé dans le Cadre de gouvernance, de responsabilisation et d'apprentissage[297]. Il s'agit tout d'abord pour chaque membre d'un rapport confidentiel destiné à la GNI, préparé par un expert indépendant, qui évalue la conformité des pratiques de l'entreprise avec les principes, les mesures correctives prévues, et les recommandations faites. Ensuite, après une phase de réponses, un rapport public commun à tous les membres résume les progrès réalisés, donne des exemples de cas pratiques étudiés, des informations sur les difficultés rencontrées sous différentes juridictions, et la décision de conformité ou de non-conformité prise pour

---

293 *Idem*. §3 a.

294 *Idem*, §4 iv.

295 *Idem*, §4 ii.

296 Global Network Initiative, *Directives*, *op. cit.* Note 280.

297 Global Network Initiative, « Accountability, Policy, and Learning Framework », février 2015. <https://globalnetworkinitiative.org/content/accountability-policy-and-learning-framework>

chacun des membres audités l'année du rapport[298]. Enfin, un troisième rapport est publié par les membres ayant fait l'objet d'une évaluation indépendante, pour rendre compte des conclusions au maximum dans les six mois suivant leur réception.

Pour le moment, sept ans après la création de la Global Network Initiative, un seul rapport public a été communiqué, en janvier 2014[299]. Il rend compte de l'évaluation des trois entreprises fondatrices de l'Initiative (Google, Microsoft et Yahoo), et conclut dans des termes dithyrambiques à leur conformité aux principes de l'organisation. Un esprit taquin notera peut-être que ce sont les entreprises évaluées qui choisissent et rémunèrent elles-mêmes leur « expert indépendant » dans une courte liste de cabinets d'audit accrédités sur candidature par la GNI[300]. Même si la Charte de gouvernance affirme que « *les individus et organisations qui évaluent la conformité d'une entreprise aux Principes de la GNI doivent maintenir l'indépendance à l'égard des entreprises qu'ils évaluent* », on a vu indépendance mieux garantie[301].

TID publie également des rapports, sans prétention d'apporter une évaluation sur le respect de ses principes par chaque membre. L'organisation composée exclusivement d'entreprises de télécommunication a publié très récemment un premier rapport commun qui couvre ses deux premières années, 2013 et 2014[302], tandis que ses neuf membres ont tous publié des rapports individuels, la plupart du temps dans le cadre de rapports plus globaux sur leur politique de responsabilité sociale d'entreprise ou de développement durable[303].

Trois membres de TID (AT&T, Vodafone et TeliaSonera) ont par ailleurs publié des « rapports de transparence », une pratique de plus en plus courante qui consiste, pour les intermédiaires de l'internet, à rendre compte en détails au public de l'ampleur de leur coopération — ou de leur refus de coopérer — avec les pouvoirs publics, en termes

298 Depuis une réforme adoptée en juin 2014, il est prévu que les entreprises s'auto-évaluent l'année de leur adhésion à la GNI, et soient ensuite auditées par un expert indépendant tous les deux ans. *V.* « Charte de gouvernance », *infra* note 300, §5.A.

299 Global Network Initiative, *Public report on the independant assessment process for Google, Microsoft, and Yahoo*, janvier 2014, 29 p. <http://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf>

300 Actuellement Deloitte, Foley Hoag, KPMG, PricewaterhouseCoopers, et SSP Blue.

301 Global Network Initiative, « Charte de gouvernance », §5.B. <https://globalnetworkinitiative.org/sites/default/files/GNI%20Governance%20Charter%20-%202015.pdf>

302 Telecommunications Industry Dialogue, *The Telecommunications Industry Dialogue at Two Years : advances in respecting freedom of expression and privacy in 2014*, mai 2015, 16 p. <http://www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Dialogue-Annual-Report-2015.pdf>

303 *V.* la liste des rapports sur <https://www.telecomindustrydialogue.org/about/implementing-the-guiding-principles/>

volumétriques. Ainsi par exemple, l'opérateur américain AT&T indique qu'il s'est opposé à 2 110 demandes de données privées au premier semestre 2014[304], tandis que Vodafone annonce un peu plus de 605 000 demandes de données de communications reçues de l'Italie sur une seule année, mais ne pas avoir le droit de communiquer de chiffres pour sa filiale en Égypte[305].

Google avait été le premier à publier un tel « rapport de transparence » en 2010. La firme le fait désormais chaque semestre[306], avec des informations détaillées par pays, concernant aussi bien les demandes gouvernementales de suppressions de contenus hébergés ou référencés, que les demandes de renseignements sur les utilisateurs, les demandes de retraits de résultats de recherche reçues de titulaires de droits d'auteur, ou encore son traitement des demandes de « droit à l'oubli » imposé par la CJUE. Souhaitant peut-être alléger le fardeau de ses pairs en encourageant la privatisation de la fonction judiciaire, et contre l'avis de son avocat général qui avait prévenu que « *le droit d'un internaute à l'information serait compromis* »[307], la Cour a estimé que le moteur de recherche était « responsable du traitement » des données personnelles qu'il indexait, et qu'à ce titre il devait accorder le droit d'opposition à ceux que des résultats à des recherches de leur nom pouvaient gêner, mais pas sans avoir jugé lui-même au cas par cas de l'équilibre entre vie privée et droit à l'information. Google doit en effet censurer ce qu'un individu lui demande « *à moins qu'il existe des raisons particulières, telles que le rôle joué par cette personne dans la vie publique, justifiant un intérêt prépondérant du public à avoir, dans le cadre d'une telle recherche, accès à ces informations* »[308]. Cet arrêt qui divise la doctrine a incité Google à mettre en place son propre comité législatif ad hoc pour décider des règles à s'imposer dans le choix des droits fondamentaux à privilégier[309], et à faire œuvre de transparence à l'égard du public en livrant chaque jour des informations sur son application du « droit à l'oubli ».

---

304 *V.* AT&T, *Transparency Report*. <http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>

305 *V.* Vodafone, Law Enforcement Disclosure report, 2014, 20 p. <http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement.pdf>

306 *V.* Google, *Transparence des informations*. <http://www.google.com/transparencyreport/>

307 CJUE, *Google Spain c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, Conclusions de l'avocat général M. Niilo Jääskinen présentées le 25 juin 2013, §131. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=290179>

308 CJUE, *Google Spain c. Agencia de Protección de Datos (AEPD) et Mario Costeja González*, affaire C-131/12, 13 mai 2014, §99.

309 *V.* Google, *Comité consultatif*. <http://www.google.com/intl/fr/advisorycouncil/>

Le rapport de transparence de Google, très accessible grâce à une mise en page qui le rend lisible par un public non averti, montre ainsi qu'au 13 mai 2015, les utilisateurs d'internet en France avaient demandé la suppression de 174 311 adresses de sites internet au nom de leur « droit à l'oubli », mais que Google a préféré protéger la liberté d'expression et d'information dans 52 % des cas, en refusant d'accéder aux demandes qu'il jugeait insuffisamment fondées. Il montre aussi que Facebook est le site qui subit le plus de suppressions de résultats. Par ailleurs en dehors du « droit à l'oubli », Google dévoile qu'il s'oppose à plus de 40 % des demandes gouvernementales d'informations sur des internautes en France, expliquant qu' « *avant de répondre à la demande d'une autorité administrative, nous nous assurons qu'elle respecte la loi, ainsi que les règles de Google* »[310].

Aujourd'hui, près d'une quarantaine d'importants intermédiaires de l'internet publient eux aussi des rapports de transparence, que ce soit des fournisseurs d'accès, des réseaux sociaux, des hébergeurs de sites internet, des prestataires de messagerie électronique ou encore des opérateurs de téléphonie mobile[311]. Une grande majorité d'entre eux sont Américains, avec quelques Européens et quelques Sud-Coréens. Aucune des grandes entreprises du web Chinois (Baidu) ou Russe (Yandex) ne publie de rapport de transparence. Mais pour ceux qui en publient, ces rapports sont très souvent incomplets sur la protection des droits des individus, puisqu'ils rendent compte avec précision des atteintes aux droits fondamentaux sollicitées par les tiers, mais se font en revanche d'une discrétion remarquable sur les atteintes qu'eux-mêmes portent aux droits des utilisateurs.

b – une transparence limitée aux rapports avec les gouvernements

Tous les rapports de transparence publiés par les intermédiaires de l'internet font état du nombre de demandes gouvernementales qu'ils reçoivent, que ce soit pour fournir aux autorités judiciaires ou administratives des informations sur des utilisateurs (identité, adresse IP, adresse e-mail, contenus des messages échangés,…), ou pour supprimer ou bloquer l'accès à des contenus qui enfreindraient les lois restreignant la liberté d'expression. Parfois, ces rapports font aussi état des demandes reçues de la part d'individus ou d'entreprises, pour protéger leurs droits d'auteur. Le plus souvent, les rapports indiquent la proportion des demandes que l'intermédiaire a satisfaites en tout ou partie. Mais la transparence ayant visiblement ses limites, jamais ces rapports ne signalent le nombre des contenus que

---

310 *V.* Google, « FAQ », *Transparence des informations*. <http://www.google.com/transparencyreport/userdatarequests/faq/#compliance_rate>

311 Pour une liste, *V.* sur la page d'accueil du rapport de transparence de Google, *op.cit*.

l'intermédiaire a spontanément supprimé en vertu de ses propres politiques, et parfois rapporté aux autorités locales.

Ainsi par exemple, le rapport de transparence de Facebook concernant la France[312] indique qu'au dernier semestre 2014, le réseau social a reçu de l'État des demandes officielles concernant 2 885 utilisateurs, qu'il en a satisfaites 42,41 %, et que 13 contenus ont été interdits d'accès depuis la France en vertu des lois interdisant le négationnisme. Mais le rapport ne dit strictement rien du nombre d'utilisateurs qui ont été privés totalement ou partiellement de la liberté de s'exprimer sur Facebook suite à la mise en œuvre autonome de ses contrats privés. Le réseau social explique à ses utilisateurs qu' « *en vue d'établir un équilibre entre les besoins, la sécurité et les centres d'intérêt d'une communauté diversifiée, nous pouvons supprimer certains types de contenu sensible ou en restreindre l'accès* »[313], ce qu'il fait très régulièrement, mais ces actions-là ne font l'objet d'aucune transparence. C'est pourtant d'autant plus critique que les gouvernements incitent désormais Facebook et ses concurrents à censurer spontanément les individus[314]. En France, Facebook a aussi l'obligation « *d'informer promptement les autorités publiques compétentes* » d'un champ désormais large d'activités illicites signalées sur le réseau social[315], mais ces signalements ne font pas non plus l'objet de publications.

Entre autres exemples, Twitter est transparent sur les quelques centaines de comptes d'utilisateurs fermés suite à des demandes étatiques[316], mais ne dit rien des milliers d'autres comptes qu'il a lui-même choisi de fermer en application de ses règles internes. Or ce phénomène prend de l'ampleur et a parfois une dimension éminemment politique et diplomatique, qui exigerait la plus grande transparence. Ainsi par exemple, un collectif anonyme d'internautes (dit « Anonymous ») a décidé de dresser une liste de comptes suspectés d'être affiliés à l'État Islamique. Selon les chiffres du collectif dont l'action est

---

312 Facebook, « France — juillet 2014 – décembre 2014 », *Rapport des demandes gouvernementales*. < https://govtrequests.facebook.com/country/France/2014-H2/>

313 *V.* Facebook, « Encourager un comportement respectueux », *Standards de la communauté*. <https://www.facebook.com/communitystandards>

314 *V. supra,* §2.2.2, p. 49.

315 Aux termes de l'article 6.I.7 de la LCEN modifié en 2013 et en 2014, les hébergeurs doivent signaler aux autorités les infractions dont ils prennent connaissance concernant la répression de l'apologie des crimes contre l'humanité, la provocation à la commission d'actes de terrorisme et leur apologie, l'incitation à la haine raciale, la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap ainsi que la pornographie enfantine, l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, ainsi que les atteintes à la dignité humaine.

316 *V.* Twitter, *Transparency Report*. <https://transparency.twitter.com/>

encouragée en France par la secrétaire d'État au numérique[317], Twitter aurait suspendu plus de 23 500 comptes sur les quelques 36 500 signalés[318], ce qui n'apparaîtra pas dans ses rapports consacrés aux seules demandes gouvernementales reçues par voies officielles. Au risque de paraître prendre partie dans le conflit israélo-palestinien, en 2014 Twitter avait aussi suspendu des comptes de l'armée du Hamas ouverts depuis des années et très suivis[319], mais a laissé Tsahal exprimer ses vues lors des bombardements dans la bande de Gaza, et même autorisé le Premier ministre israélien à payer pour que des messages justifiant l'opération militaire contestée soient mis en avant sur la plateforme[320]. Le risque d'un « deux poids deux mesures » dans la liberté d'expression des belligérants de tous conflits est grand, mais Twitter ne justifie pas ses choix, et n'en fait pas état.

Il en va de même pour Google, véritablement exemplaire dans la transparence sur les demandes reçues des gouvernements ou des particuliers, mais qui ne livre aucune information sur le nombre des vidéos qu'il supprime de YouTube en raison de violations réelles ou prétendues de ses conditions d'utilisation, sur les sites dont il choisit de diminuer ou supprimer toute visibilité sur son moteur de recherche en raison de leur contenu qui ne serait pas conforme à la loi ou à sa propre morale, ou sur les termes de recherche qui sont censurés dans les recherches suggérées ou les résultats instantanés[321]. Même ses efforts concernant l'application du « droit à l'oubli » ont été jugés insuffisants par 80 universitaires du monde entier qui ont rappelé dans une lettre ouverte que « *le public devrait être capable de comprendre comment les plateformes numériques exercent leur immense pouvoir sur l'information librement disponible* », et détaillé toutes les informations précises auxquels ils

---

317 Lors d'un débat au Sénat, Axelle Lemaire a estimé que « *Anonymous est un exemple* » qui montre que « *la société civile a une fonction éminente* » dans la lutte contre la propagande d'organisations terroristes sur internet. *V.* Sénat, « Débat : Internet et la loi du 29 juillet 1881 sur la liberté de la presse », *Compte rendu analytique officiel du 24 mars 2015*.

318 *V.* Lucky Troll Club. <http://luckytroll.club/daesh/BISISBlock.htm>

319 *V.* Le Figaro, « Les comptes Twitter du Hamas fermés », 15 janvier 2014. <http://www.lefigaro.fr/flash-actu/2014/01/15/97001-20140115FILWWW00464-les-comptes-twitter-du-hamas-fermes.php>

320 *V.* Hayes BROWN. <https://twitter.com/HayesBrown/status/489180034641297408>

321 Lors de la saisie d'une requête, Google affiche automatiquement les résultats les plus pertinents pour la requête en cours de saisie (« recherche instantanée »), et suggère des requêtes qui peuvent correspondre aux premières lettres ou aux premiers mots saisis (« recherches suggérées »). Mais le moteur de recherche choisit de bloquer l'affichage des recherches instantanées lorsque certains termes sont saisis, ou d'écarter des mots clés de ses suggestions. Il peut s'agir de ne pas suggérer le mot « juif » accolé au nom d'une personnalité, pour ne pas alimenter l'antisémitisme, de ne pas afficher de mots grossiers ou de résultats conduisant à des sites pornographiques ou illégaux, mais aussi parfois de filtrages plus discutables, comme le blocage du mot « bisexuel ».

souhaitaient avoir accès[322]. Ils ont, à l'égard de cette entreprise privée, le même niveau d'exigence démocratique qu'à l'égard d'un État.

[322] The Guardian, « Dear Google: open letter from 80 academics on 'right to be forgotten' », 14 mai 2015. <http://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten>

CONCLUSION

Lorsqu'il déclarait avec éclat à Davos « l'indépendance du cyberespace » en 1996[323], l'essayiste, poète et activiste John Perry Barlow était imprégné de culture libérale, et redoutait ce qu'internet deviendrait s'il était sous contrôle des États. Son discours adressé aux représentants des gouvernements était une ode à l'auto-régulation, naïve et déraisonnablement optimiste. Il y exprimait le point de vue de ce qui était encore une élite de pionniers des réseaux numériques convaincus d'être investis de la construction d'un nouveau monde, immatériel, qui ne serait pas « perverti » par les lois et polices régnant dans le monde traditionnel :

> I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> […] Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours.
>
> […] You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.
>
> You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.
>
> […] We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.[324]

Le propos est fort et d'une esthétique incontestable mais l'histoire a toutefois montré que la Déclaration de Barlow n'a pas eu tout à fait le même impact que la Déclaration de Jefferson, les États ayant peu ou prou remporté leur bataille pour la régulation d'internet. Mais avec les restrictions croissantes qu'ils imposent à la circulation des informations, ou par l'exploitation des technologies numériques à des fins de surveillance de la population, les

[323] *V. supra*, note 105.

[324] *Idem.*

États restent perçus comme des menaces, qui réveillent de vieux réflexes. Aussi les initiatives techniques ou juridiques prises par les intermédiaires de l'internet pour protéger les droits de l'homme contre l'action négative des États signent-elles, avec certes plus de tact et de compromis, un retour vers la logique libérale « barlowienne » des années 1990. Mais elles illustrent aussi en creux ce que Barlow n'avait pas vu venir. Certains intermédiaires de l'internet, que l'on a coutume d'appeler les « géants du Web », ont acquis une telle puissance et un tel caractère incontournable qu'ils représentent eux-mêmes une menace et qu'ils peuvent se croire en certains domaines les égaux, voire les rivaux des États. Certains aspirent à représenter une véritable force diplomatique, ce qu'ils paraissent être effectivement lorsque la France organise pour eux un *e-G8 Forum* en marge du G8[325].

Leur force d'opposition est bénéfique lorsqu'elle permet d'apporter un écran de protection aux droits de l'homme contre les intrusions ou les restrictions disproportionnées voulues par les gouvernements. Mais tout comme les États se sont unis au 20ème siècle pour reconnaître des droits aux individus et pour apporter des mécanisme de garantie, il deviendra nécessaire que les intermédiaires de l'internet acceptent de restreindre et de soumettre au contrôle leur propre pouvoir de nuisance, dont ils feignent d'ignorer la réalité.

Il faudra que le temps fasse son œuvre pour réaliser à quel point des plateformes qui réunissent déjà près d'un quart des habitants de la planète représentent une menace bien plus importante encore que les États en matière de liberté d'expression, de violation de la vie privée ou simplement de liberté individuelle. L'avenir n'incite pas à l'optimisme lorsque l'on voit se développer ces objets connectés qui scrutent en permanence le comportement des individus et permettront de les sanctionner lorsqu'ils n'adoptent pas le comportement conseillé[326], ou ces intelligences artificielles qui obligeront à une réflexion nouvelle sur la place de l'humain dans une société de plus en plus organisée par et autour de robots contrôlés par une poignée d'entreprises. Un nouveau pacte social devra s'écrire pour protéger les individus non seulement contre les États, mais aussi contre les entreprises du numérique.

Le Pacte Mondial lancé en 2000 par l'ONU[327], par lequel des entreprises « *s'engagent à aligner leurs opérations et leurs stratégies sur dix principes universellement acceptés*

---

325 Étaient invités notamment Eric Schmidt (Google), Mark Zuckberg (Facebook), Jimmy Wales (Wikipedia), Jeff Bezos (Amazon), ou John Danahoe (eBay). *V.* <https://fr.wikipedia.org/wiki/E-G8>

326 *V.* Jaques HENNO, « Pourquoi les objets connectés font rêver les compagnies d'assurances », *Les Echos*, 3 mars 2015. <http://www.lesechos.fr/idees-debats/sciences-prospective/0204190147952-pourquoi-les-objets-connectes-font-rever-les-compagnies-dassurances-1098284.php>

327 *V.* Pacte Mondial de l'ONU. <https://www.unglobalcompact.org/>

touchant les droits de l'homme », n'est pas suffisant. Il ne dispose d'aucun mécanisme de pétition individuelle qui permettrait aux particuliers victimes du comportement d'entreprises de s'en plaindre, ni de mécanismes de contrôle mutuel et de sanctions. Autant de manques que l'on retrouve également dans la Global Network Initiative, louable mais à la portée limitée.

La question se posera donc de la possibilité d'accueillir dans un même accord contraignant de protection des droits fondamentaux, des États et des intermédiaires de l'internet, qui devront veiller les uns sur les autres et s'ouvrir aux saisines par des individus. Bien sûr, le temps n'est pas encore venu de reconnaître aux intermédiaires de l'internet la capacité de signer des traités internationaux au même niveau que les États. Entre autres difficultés, accorder une telle capacité serait leur reconnaître une forme de souveraineté et impliquerait que des entreprises ne soient plus liées exclusivement par le droit interne dérivé des accords internationaux, mais aussi directement dans certaines circonstances par le droit international lui-même. Mais n'était-ce pas déjà un abandon bénéfique de souveraineté que d'accepter de faire de l'individu un sujet de droit international, et non plus un domaine réservé de l'État ?

Ce sera là, peut-être, l'un des défis du 21ème siècle.

QUI DIRIGE INTERNET ?

AUCUN INDIVIDU, PERSONNE, ENTREPRISE, ORGANISATION OU GOUVERNEMENT UNIQUE NE DIRIGE INTERNET.

Internet est en soi un réseau d'ordinateurs répartis à l'échelle mondiale comprenant de nombreux réseaux autonomes volontairement interconnectés. De même, sa direction relève d'un réseau pluripartite décentralisé et international de groupes autonomes interconnectés provenant de la société civile, le secteur privé, les gouvernements, les communautés académiques et scientifiques ainsi que des organisations nationales et internationales. Ils travaillent en coopération selon leurs fonctions respectives pour créer des politiques et des normes partagées entretenant l'interopérabilité mondiale d'Internet pour le bien public.

QUI PARTICIPE :

IAB A C P S R
INTERNET ARCHITECTURE BOARD
Supervise le développement technique et d'ingénierie de l'IEFT et l'IRTF.
www.iab.org

ICANN C O P V
SOCIETE POUR L'ATTRIBUTION DES NOMS DE DOMAINE ET DES NUMEROS SUR INTERNET
Coordonne les systèmes d'identifiants uniques d'Internet : Adresses IP, registres protocole-paramètre, espace de domaines de premier niveau (zone racine DNS).
www.icann.org

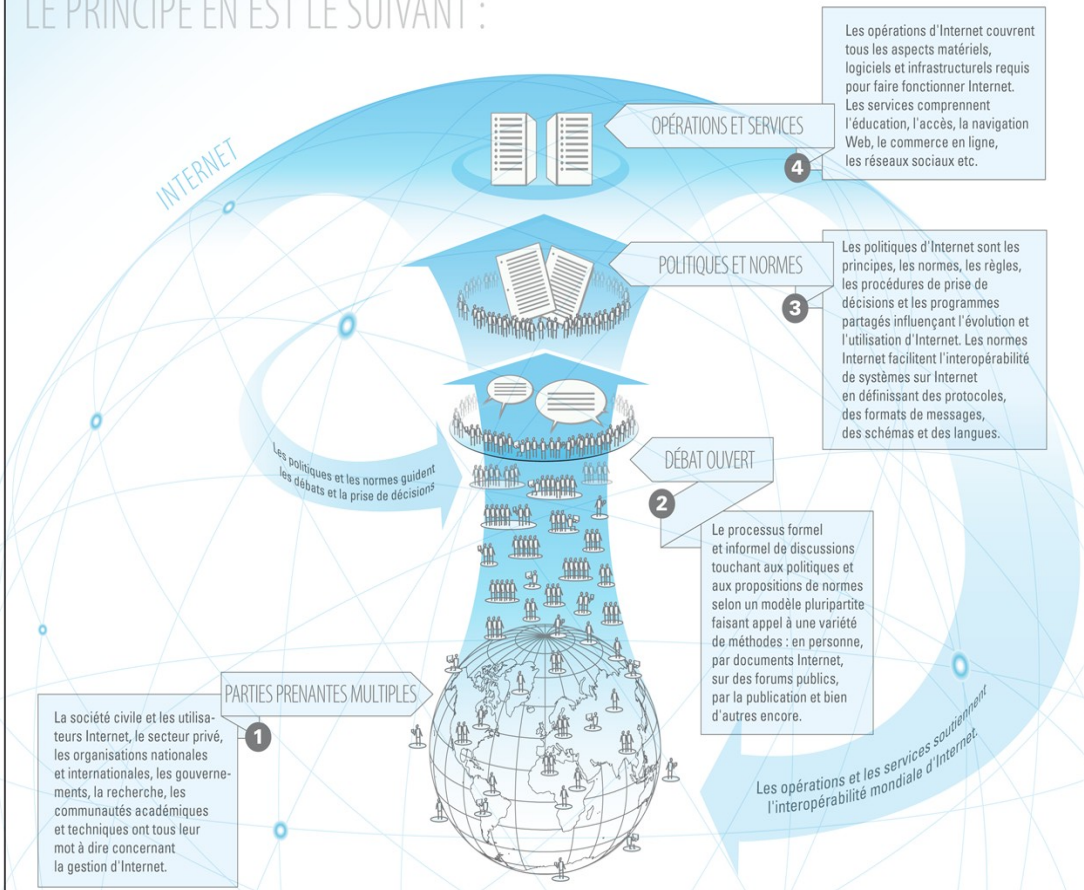
IETF C P S
INTERNET ENGINEERING TASK FORCE
Conçoit et facilite une vaste gamme de normes Internet relatives notamment aux normes de la suite protocole d'Internet. Leurs documents techniques influencent la manière dont Internet est conçu, utilisé et administré.
www.ietf.org

IGF A C P
FORUM SUR LA GOUVERNANCE D'INTERNET
Un forum ouvert pluripartite axé sur la discussion de problématiques liées à la gouvernance d'Internet.
www.intgovforum.org

IRTF R
INTERNET RESEARCH TASK FORCE
Encourage la recherche sur l'évolution d'Internet via la création de groupes de recherche spécialisés à long terme travaillant sur des sujets liés aux protocoles, aux applications, à l'architecture et à la technologie d'Internet.
www.irtf.org

GOUVERNEMENTS ET AGENCES INTERGOUVERNEMENTALES C P
Conçoivent des lois, des réglementations et des politiques applicables à Internet au sein de leurs juridictions ; participants à des forums multilatéraux et pluripartites régionaux et internationaux sur la gouvernance d'Internet.

LE PRINCIPE EN EST LE SUIVANT :



LÉGENDE : A Conseil · C Engagement communautaire · E Éducation · O Opérations · P Politiques · R Recherche · S Normes · V Services

QUI PARTICIPE :

ISO 3166 MA S
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, MAINTENANCE AGENCY
Définit les noms et les codes postaux des pays, des territoires dépendants et des zones spéciales d'importance géographique.
www.iso.org/iso/country_codes.htm

ISOC C E P V
INTERNET SOCIETY
Assure le développement, l'évolution et l'utilisation ouverts d'Internet dans l'intérêt de tous de par le monde. L'ISOC présente actuellement plus de 90 chapitres dans près de 80 pays.
www.internetsociety.org

RIRs O P V
5 REGISTRES INTERNET RÉGIONAUX
Gère l'allocation et l'immatriculation de ressources numériques d'Internet telles que les adresses IP dans des régions géographiques du monde.

www.afrinic.net	Afrique
www.apnic.net	Asie-Pacifique
www.arin.net	Canada et États-Unis
www.lacnic.net	Amérique latine et Caraïbes
www.ripe.net	Europe, Moyen-Orient et certaines parties d'Asie centrale

W3C S
WORLD WIDE WEB CONSORTIUM
Crée des normes pour le World Wide Web rendant possible une Plateforme web ouverte, en se concentrant sur les problématiques d'accessibilité, d'internationalisation et sur les solutions mobiles Web par exemple.
www.w3.org

GROUPES D'OPÉRATEURS DE RÉSEAUX INTERNET A O V
Débattre des sujets concernant les opérations et la réglementation d'Internet et les influencer au sein de forums informels constitués de fournisseurs Internet (ISP), de points d'échange Internet (IXP) et autres.

Ce graphique est un document vivant conçus pour offrir une vue d'ensemble expliquant le fonctionnement d'Internet. Celui-ci n'a pas vocation à être exhaustif. N'hésitez-pas à faire part de tout commentaire sur www.xplanations.com/whoruns theinternet

TABLE DES MATIÈRES

BIBLIOGRAPHIE

■ *Ouvrages généraux*

- DUPUY (P.-M), KERBRAT (Y.), *Droit international public*, Dalloz, Coll. « droit public science politique », 2014, 921 p.
- FAGES (B.), *Droit des obligations*, LGDJ, 4e éd., 2013, 513 p.
- SUDRE (F.) Ed., *Les grands arrêts de la Cour européenne des Droits de l'Homme*, 7e éd., PUF, Coll. « Thémis », 2015, 944 p.
- SUDRE (F.), *Droit européen et international des droits fondamentaux*, 12e éd., PUF, Coll. « Droit fondamental », 2015, 967 p.

■ *Ouvrages spécifiques*

- BLACK (E.), *IBM et l'Holocauste — L'alliance stratégique entre l'Allemagne nazie et la plus puissante multinationale américaine*, Robert Laffont, 2001, 595 p.
- CONSEIL D'ETAT, *Étude annuelle 2014 — Le numérique et les droits fondamentaux*, La Documentation Française, 2014, 441 p.
- COSTA (D.), PELISSIER (A.) Ed., *Contrats et droits fondamentaux*, Presses universitaires d'Aix-Marseille, 2011, 142 p.
- DECAUX (E.) Ed, *La responsabilité des entreprises multinationales en matière de droits de l'homme*, Bruylant, Coll. « Droit et justice », 2010, 292 p.
- DRAI (R.), THUAN (C-H.), VAN MINH (T.), BERNARD (J.-P.), FONTAINE (J.-M), *Multinationales et droits de l'homme*, PUF, 1984, 220 p.
- FAUCHOUX (V.), DEPREZ (P.), BRUGUIERE (J.-M), *Le droit de l'internet : Lois, contrats et usages*, 2ème éd., Lexis Nexis, 2014, 446 p.
- FÉRAL-SCHUHL (C.), *Cyberdroit : Le droit à l'épreuve d'internet*, 6ème éd., Dalloz, 2010, 997 p.
- LESSIG (L.), *Code and other laws of cyberspace*, New York, Basic Books, 1999, 297 p.

■ *Rapports*

- ARTICLE 19, *Intermédiaires Internet : dilemme de la responsabilité*, 2013, 28 p. <http://www.article19.org/data/files/WEB_French.pdf>
- CONSEIL NATIONAL DU NUMERIQUE, *Neutralité des plateformes : Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014. <http://www.cnnumerique.fr/wp-content/uploads/2014/06/CNNum_Rapport_Neutralite_des_plateformes.pdf>
- ERHEL (C.), DE LA RAUDIERE (L.), *Rapport d'information sur la neutralité de l'internet et des réseaux*, Assemblée Nationale, n° 3336, 13 avr. 2011. <http://www.assemblee-nationale.fr/13/rap-info/i3336.asp>
- FIDH, *Position paper — Surveillance technologies "made in Europe" : Regulation needed to prevent human rights abuses*, décembre 2014, 40 p. <https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe-1-2.pdf>

- GLOBAL NETWORK INITIATIVE, *Public report on the independant assessment process for Google, Microsoft, and Yahoo*, janvier 2014, 29 p. <http://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf>

- LA RUE (F.), *Rapport établi par le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression* , A/66/290, 10 août 2011. <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290>

- LA RUE (F.), *Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the internet*, A/HRC/17/27, 16 mai 2011. <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>

- NATIONS UNIES, *La responsabilité des entreprises de respecter les droits de l'homme : guide interprétatif*, 2012, HR/PUB/12/02. <http://www.ohchr.org/Documents/Publications/HR_PUB_12_2_fr.pdf>

- OCDE, *The Role of internet Intermediaries in Advancing Public Policy Objectives*, 2011, 200 p. <http://www.oecd-ilibrary.org/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_9789264115644-en>

- RSF, *Les ennemis d'Internet — Rapport 2012*, 2012, 73 p. <http://fr.rsf.org/IMG/pdf/rapport_ennemis_internet_2012.pdf>

- TELECOMMUNICATIONS INDUSTRY DIALOGUE, *The Telecommunications Industry Dialogue at Two Years : advances in respecting freedom of expression and privacy in 2014*, mai 2015, 16 p. <http://www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Dialogue-Annual-Report-2015.pdf>

- UIT, *The World in 2014: ICT Facts and Figures*, 2014, 8 p. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf>

- UNESCO, *Fostering Freedom Online: the Role of Internet Intermediaries*, 2014, 211 p. <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>

- UNESCO, *Réunion d'experts sur le rôle des pouvoirs privés comme facteurs de limitation des droits de l'homme, Alger, 5-8 décembre 1982, Rapport final SS-82/CONF.610/10,* 1983, 30 p. <*http://unesdoc.unesco.org/images/0005/000575/057537FB.pdf*>

- UNESCO, *Tendances mondiales en matière de liberté d'expression et de développement des médias*, 2014, 115 p. <http://unesdoc.unesco.org/images/0022/002275/227515F.pdf>

■ *Principales résolutions et décisions*

- CJUE, grande ch., 8 avril 2014, *Digital Rights Ireland c. Irlande*.

- CJUE, grande ch., 13 mai 2014, *Google Spain c. Agencia de Protección de Datos (AEPD) et Mario Costeja González*, affaire C-131/12,.

- CONSEIL CONSTITUTIONNEL, « Loi favorisant la diffusion et la protection de la création sur internet », décision n° 2009-580 DC du 10 juin 2009. <http://www.conseil-constitutionnel.fr/decision/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html>

- CONSEIL DE L'EUROPE, « Déclaration du Comité des Ministres sur les droits de l'homme et l'état de droit dans la Société de l'information », 13 mai 2005, CM(2005)56 final. <https://wcd.coe.int/ViewDoc.jsp?id=849009>

- CONSEIL DE L'EUROPE, Assemblée parlementaire, « Les opérations de surveillance massive », 18 mars 2015, Doc. 13734. <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-fr.asp?fileid=21583&lang=fr>

- CONSEIL DE L'EUROPE, Commissaire aux droits de l'homme, « La prééminence du droit sur l'internet et dans le monde numérique en général», 8 décelmbre 2014, CommDH/IssuePaper(2014)1. <https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2014)1&Language=lanFrench>
- COUR EDH, 16 juillet 2009, *Willem c. France* (req. N°10883/05).
- COUR EDH, 18 décembre 2012, *Ahmet Yildirim c. Turquie* (req. N°3111/10).
- COUR EDH, 24 août 1998, *Lambert c. France* (88/1997/872/1084)
- COUR EDH, 24 avril 1990, *Kruslin c. France* (req. N°11801/85)
- COUR EDH, 3 juillet 2007, *Copland c. Royaume-Uni* (req. N°62617/00)
- COUR EDH, 6 septembre 1978, *Klass et autres c. Allemagne* (req. N° 5029/71)
- NATIONS UNIES, « Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence «protéger, respecter et réparer» des Nations Unies », *Rapport du Représentant spécial du Secrétaire général chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises, John Ruggie*, A/HRC/17/31, 2011. <http://www.ohchr.org/Documents/Issues/Business/A.HRC.17.31_fr.pdf>
- NATIONS UNIES, Assemblée générale, « Le droit à la vie privée à l'ère du numérique », A/RES/68/167, 18 décembre 2013. <http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167>
- NATIONS UNIES, Conseil des droits de l'homme, « La promotion, la protection et l'exercice des droits de l'homme sur l'internet », A/HRC/RES/20/8, 5 juillet 2012. <http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20340>
- NATIONS UNIES, Conseil des droits de l'homme, *résolution 17/4 sur les droits de l'homme et les sociétés transnationales et autres entreprises*, A/HRC/RES/17/4, 16 juin 2011.
- NATIONS UNIES, Haut-Commissariat aux droits de l'homme, « Résumé de la réunion-débat du Conseil des droits de l'homme sur le droit à la vie privée à l'ère du numérique », 19 décembre 2014, A/HRC/28/39. <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Pages/ListReports.aspx>
- NATIONS UNIES, Haut-Commissariat aux droits de l'homme, « The right to privacy in the digital age », 30 juin 2014, A/HRC/27/37. <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Pages/ListReports.aspx>
- NATIONS UNIES, Sous-commission de la promotion et la protection des droits de l'homme, « « Normes sur la responsabilité en matière de droits de l'homme des sociétés transnationales et autres entreprises », 13 août 2003 (E/CN.4/Sub.2/2003/12/Rev.2).
- NETMUNDIAL, « Multistakeholder statement », 24 avril 2014. <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>

■ *Principaux articles de doctrine*

- ACHILLEAS (P.), « Droit international des télécommunications (communications électroniques) », *JurisClasseur Communication*, Fasc. 7350, 1er décembre 2013.
- BUSSUEIL (G.), « Arrêt Google : du droit à l'oubli de la neutralité du moteur de recherche », *La Semaine Juridique — Entreprises et Affaires*, n°24, 12 juin 2014, 1327
- DEBET (A.), « Google Spain : Droit à l'oubli ou oubli du droit ? », *CCE* n°7-8, juillet 2014, étude 13.
- ERRERA (R.), « Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques », *RTDH* 55/2003, pp. 851-870. <http://www.rtdh.eu/pdf/2003851.pdf>
- HAYEZ (P.), « L'effet Snowden », *Le Débat* 4/2014 (n°181), p. 93-102.

- KREIMER (S.), « Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link », *University of Pennsylvania Law Review*, Vol. 155, N°11, 2006. <http://ssrn.com/abstract=948226>
- LESSIG (L.), « Code Is Law — On Libery In Cyberspace », *Harvard Magazine*, janvier-février 2000. <http://harvardmagazine.com/2000/01/code-is-law-html>
- LOISEAU (G.), « La supra-territorialité du site internet », *CCE* n° 11, Novembre 2013, comm. 115.
- MARINO (L.), « Le droit d'accès à internet, nouveau droit fondamental », *Recueil Dalloz*, 2009, vol. 30, p. 2045.
- MEDEVIEILLE (G.), « La difficile question de l'universalité des droits de l'homme », *Transversalités* 3/2008 (N° 107) , p. 69-91. <http://www.cairn.info/revue-transversalites-2008-3-page-69.htm>
- REIDENBERG (J.R.), « Lex Informatica: The Formulation of Information Policy Rules Through Technology », *Texas Law Review*, Vol. 76, N°3, février 1998. <http://reidenberg.home.sprynet.com/lex_informatica.pdf>
- REIDENBERG (J.R), « La régulation d'Internet par la technique et la Lex informatica », *Droit et économie de la régulation, Vol. 3*, Paris, Presses de Sciences Po, «Hors collection», 2005, p. 81.
- ROSEN (J.), « The Deciders : The future of privacy and free speech in the age of Facebook and Google », *Fordham Law Review*, Vol.80, Issue 4 (2012), p. 1536. <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4774&context=flr>
- SUDRE (F.), « Les "obligations positives" dans la jurisprudence européenne des droits de l'homme », *RTDH*, n°1995/23, p.369. <http://www.rtdh.eu/pdf/1995363.pdf>
- WU (T.), « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863>

■ *Instruments d'auto-régulation*

- GLOBAL NETWORK INITIATIVE, « Accountability, Policy, and Learning Framework », février 2015. <https://globalnetworkinitiative.org/content/accountability-policy-and-learning-framework>
- GLOBAL NETWORK INITIATIVE, « Charte de gouvernance ». <https://globalnetworkinitiative.org/sites/default/files/GNI%20Governance%20Charter%20-%202015.pdf>
- GLOBAL NETWORK INITIATIVE, « Directives de mise en œuvre des Principes de liberté d'expression et de respect de la vie privée ». <https://www.globalnetworkinitiative.org/sites/default/files/pdfs/FR_Implementation_Guidelines_FRA.pdf>
- GLOBAL NETWORK INITIATIVE, « Principes de liberté d'expression et de respect de la vie privée ». <https://www.globalnetworkinitiative.org/sites/default/files/pdfs/FR_Principles_FRA.pdf>
- TELECOMMUNICATIONS INDUSTRY DIALOG, « Principes directeurs en matière de liberté d'expression et de protection de la vie privée dans les télécommunications », 12 mars 2013. <http://www.telecomindustrydialogue.org/wp-content/uploads/Telecoms_Industry_Dialogue_Principles_Version_1_-_FRENCH.pdf>