Habilitation à Diriger des Recherches, Volume 1: Synthèse du parcours scientifique; Volume 2: Mémoire scientifique "Pièces d'Internet, jeux de pouvoir: Penser la gouvernance d'Internet à partir des infrastructures"; Volume 3: Recueil d'articles

Francesca Musiani

Institut d'études politiques de Paris

Francesca Musiani

Mémoire scientifique
Pièces d'Internet, jeux de pouvoir :
Penser la gouvernance d'Internet à partir des infrastructures

Dossier préparé en vue de l'obtention de l'habilitation à diriger des recherches en sociologie

présenté le 15 novembre 2022

Volume 2

Jury :

Mme Sihem Amer-Yahia, directrice de recherche CNRS – LIG (Laboratoire d'informatique de Grenoble) (examinatrice)

M. Jérôme Denis, professeur à Mines ParisTech/PSL (garant et rapporteur)

Mme Nanette S. Levinson, Professor à l'American University (examinatrice)

M. Olivier Martin, professeur des universités à l'Université Paris Cité (rapporteur)

Mme Cécile Méadel, professeure des universités à l'Université Paris-Panthéon-Assas (examinatrice)

M. Sylvain Parasie, professeur des universités à SciencesPo (examinateur)

Mme Paola Tubaro, directrice de recherche CNRS-LISN (Laboratoire interdisciplinaire des sciences du numérique) (rapporteuse)

Table des matières

Introduction **5**
0.1. La gouvernance d'Internet, ensemble de pratiques et objet de recherche 8
0.2. Problématique et positionnement 11
0.2.1. La gouvernance d'Internet au prisme de la sociologie des techniques 11
0.2.2. La gouvernance (d'Internet), un objet (aussi) sociologique 15
0.3. Méthodologie 18
0.4. Apports de ce travail 19
0.5. Structure du mémoire 22
0.5.1. Première partie : Approches aux études de la gouvernance d'Internet 22
0.5.2. Deuxième partie : Les « pratiques situées » de la gouvernance par l'infrastructure 24

Chapitre 1. A la recherche de la gouvernance d'Internet : cadrages, acteurs et questions émergentes 27
1.1. Des « social implications of the Internet » aux études interdisciplinaires de ses facettes politiques 29
1.2. La gouvernance d'Internet en tant qu'objet de recherche 35
1.2.1. Qu'étudie-t-on en étudiant la gouvernance de l'Internet ? 36
1.2.2. Comment étudie-t-on la gouvernance d'Internet ? 46
1.3. Temps et temporalités (informés par la recherche) de la gouvernance d'Internet 49
1.3.1. Les premiers débats sur l'« exceptionnalisme » d'Internet 51
1.3.2. ICANN, un nouvel acteur controversé monte sur scène 52
1.3.3. Le SMSI, un espace de discussion global 53
1.3.4. Une gouvernance d'Internet « post-Snowden » ? Nouveaux périmètres et enjeux 54
1.3.5. « Plusieurs gouvernances » et « l'Internet de tout » 56

Chapitre 2. L'apport des *science and technology studies* à l'étude de la gouvernance d'Internet 59
2.1. Les STS rencontrent les *Internet studies* 60
2.2. Les STS rencontrent la gouvernance d'internet 63
2.2.1. La standardisation, mise en dialogue et interface des normes techniques 67
2.2.2. Les infrastructures comme incarnation et médiation de la gouvernance 69
2.2.3. Le rôle performatif des controverses dans la fabrique de la gouvernance 72
2.3. Que font les STS aux études de gouvernance (d'Internet) ? 74

Chapitre 3. Contrôle invisible : (études d') infrastructure et gouvernance d'Internet 78
3.1. Quelle matérialité pour les infrastructures numériques ? 81
3.2. La gouvernance d'Internet pensée à partir de ses infrastructures 83
3.2.1. La gouvernance *des* infrastructures d'Internet 84
3.2.2. La gouvernance *dans* les infrastructures d'Internet 86
3.2.3. La gouvernance *par* les infrastructures d'Internet 93
3.2.3.1. Gouvernance par l'infrastructure dans les conflits géopolitiques 94
3.2.3.2. Gouvernance par l'infrastructure et droits de propriété intellectuelle 97
3.2.3.3. Gouvernance par l'infrastructure et libertés citoyennes 101
3.2.3.4. Gouvernance par l'infrastructure comme proxy de redistribution du pouvoir 106
3.3. L'infrastructure, une « fonction » de gouvernance 108

Chapitre 4. Le *Domain Name System* comme instrument de gouvernance, entre cooptation et évasions 110
4.1. La gouvernance du DNS 113
4.2. Petite histoire du DNS 114
4.3. La gouvernance *par* le DNS : instrument d'application des droits de propriété intellectuelle 119
4.3.1. Le DNS et l'application du droit de propriété intellectuelle : le cas *Operation In Our Sites* 119
4.3.1.1. Critiques juridiques : inverser la charge de la preuve 121
4.3.1.2. Critiques techniques : manque de stabilité et inefficacité 124
4.3.2. La cooptation du DNS en pratique: les cas Rojadirecta et Dajaz1 127

4.4. Résistances « par l'infrastructure »: pour un DNS alternatif et décentralisé 131
4.4.1. Une histoire d'insatisfactions et de tentatives de changement 132
4.4.2. Ingénierie, adoption et gouvernance : le triple défi des alternatives au DNS 136
4.5. Le DNS, au cœur des infrastructures controversées d'Internet 138

Chapitre 5. Bitcoin, ou comment gouverner (par la technique) ce qui ne devait pas être gouverné 140
5.1. Comment fonctionne Bitcoin ? 141
5.2. Une infrastructure évolutive et controversée 145
5.3. La gouvernance de Bitcoin en trois « controverses d'infrastructure » 147
5.3.1. La « fourche involontaire » de mars 2013 148
5.3.2. La fermeture de MtGox 154
5.3.3. Les liens entre Bitcoin et Silk Road 158
5.4. La blockchain et son écosystème comme « gouvernance par l'infrastructure » 165

Chapitre 6. Signal, ou comment « quasi-standardiser par le code » un protocole de messagerie sécurisée 169
6.1. Chiffrer nos communications, un problème toujours plus « socio-politique » 171
6.2. Messageries chiffrées : un secteur foisonnant et fragmenté 175
6.3. Un processus de « quasi-standardisation » 180
6.4. Une variété d'applications du protocole Signal 183
6.3.1. La « quasi-standardisation » comme modèle d'affaires 184
6.4. La gouvernance de la vie privée « par les protocoles » au temps du chiffrement de masse 187
6.4.1. « Quasi-standardiser » dans un monde institutionnalisé 189

Chapitre 7. Gouverner par les « boîtiers noirs » : surveillance et évasion numérique dans l'Internet russe 192
7.1. Trois niveaux de contrôle d'Internet « par l'infrastructure » en Russie 195
7.1.1. La « SORMisation » de la Russie : mesures de surveillance et « d'interception légale » 196
7.1.1.1. La loi Yarovaya : quand le droit précède (inhabituellement) la technique 199
7.1.2. Stockage des données et restrictions des flux 201
7.1.3. Erreur 451 : Filtrage de sites Web et restrictions d'accès aux contenus 204
7.2. Le marché russe de la surveillance et de la censure Internet 206
7.2.1. Les fournisseurs d'accès Internet face au SORM : contraintes et bricolages 207
7.2.2. Roskomnadzor et l'offensive de blocages Web 211
7.2.2.1. La controverse Revizor 215
7.2.3. Les coûts d'un régime de « surveillance par l'infrastructure » 217
7.3. La gouvernance du RuNet entre cooptations et résistances « d'infrastructure » 219

Chapitre 8. Conclusions 223
8.1. Vers une typologie des « formes d'action » de la gouvernance par l'infrastructure 224
8.2. La recherche comme actrice de la gouvernance d'Internet 232
8.3. La gouvernance de et par l'infrastructure se rapproche de la gouvernance des contenus 236
8.4. Souveraineté(s) numérique(s) par l'infrastructure 239
8.5. Infrastructures de contrôle, infrastructures de résistance 242
8.6. Quand l'humain se fait infrastructure (Internet) : croisements avec les études du *digital labor* 244
8.7. Internet comme « méta-infrastructure » : quel périmètre pour sa gouvernance (et ses études) ? 246

Bibliographie 251

Introduction

Le 14 décembre 2020, le Conseil de l'Union européenne adopte une résolution relative au chiffrement des communications[1]. Dans ce document, le Conseil souligne la « nécessité d'assurer la sécurité grâce au chiffrement et malgré le chiffrement ». D'un côté, le Conseil insiste sur le soutien qu'il apporte au développement, à la mise en œuvre et à l'utilisation du chiffrement fort, y voyant « un moyen nécessaire pour protéger les droits fondamentaux et la sécurité numérique des pouvoirs publics, des entreprises et de la société » ; de l'autre côté, le Conseil note cependant « qu'il faut veiller à ce que les autorités répressives et judiciaires compétentes soient en mesure d'exercer leurs pouvoirs légaux, tant en ligne que hors ligne, pour protéger nos sociétés et nos citoyens ». Le Conseil déclare son souhait d'engager une discussion « avec le secteur des technologies, (…) la recherche, le monde universitaire, les entreprises, la société civile et d'autres parties prenantes », pour trouver un « juste équilibre » entre le respect de la vie privée et des droits fondamentaux, l'accès à la preuve de la part des autorités judiciaires, et les avantages apportés par le progrès technologique. Dans les mois qui suivent, l'avis du Conseil donnera lieu à plusieurs débats et prises de position contrastées, notamment entre des autorités nationales et supra-nationales, qui prônent la nécessité du contrôle et de la contrainte dans les environnements en ligne et hors ligne, et des développeurs et fournisseurs de technologies de communication chiffrées, qui mettent en avant l'impossibilité d'un « affaiblissement sélectif » du chiffrement et le dommage pour les libertés numériques qui résulterait d'un affaiblissement généralisé.

Cette résolution est l'un des derniers exemples – mais qui aura sans doute été suivi par bien d'autres au moment où je soutiendrai ce travail – de comment les outils de communication en ligne, notamment l'Internet, sont traversés par de multiples controverses et enjeux de reconfiguration et redistribution du pouvoir. Cet exemple montre aussi très bien comment ces enjeux sont souvent inscrits dans les technologies et les infrastructures d'Internet elles-mêmes, dont les choix de conception, de développement et d'implémentation technique deviennent des

[1] https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/fr/pdf

outils stratégiques pour l'appropriation ou le maintien du pouvoir. L'exemple montre comment la gouvernance de ce réseau des réseaux qu'on appelle l'Internet – de la multiplicité de ses composantes, des infrastructures physiques aux interfaces qui donnent accès à l'utilisateur – est une question d'alliances et de confrontations entre de multiples acteurs, des institutions à la société civile en passant par le secteur privé. Et l'exemple montre, enfin, comment la gouvernance d'Internet est le plus souvent une question de systèmes normatifs qui se croisent, se superposent, se confrontent et s'affrontent – des instruments juridiques protégeant les droits fondamentaux à l'innovation technologique et les lois du marché.

Le mémoire scientifique que vous êtes en train de lire constitue la pièce centrale de ce dossier d'habilitation à diriger des recherches. Il souhaite contribuer à éclairer cet ensemble de phénomènes d'importance croissante. Je montre comment une perspective qui relève de la sociologie – en particulier de la sociologie de l'innovation et des techniques – permet d'analyser des facettes de la gouvernance d'Internet qui resteraient autrement dans l'ombre, ou pourraient plus difficilement être définies comme en faisant partie.

Au-delà de la régulation, nous allons découvrir qu'Internet, un assemblage complexe de technologies qui a pris une part considérable dans nos vies depuis une trentaine d'années, fait l'objet d'actions de gouvernance, et est saisi comme outil de gouvernance : des protocoles de transport et de communication qui sous-tendent Internet, en passant par son système de noms de domaine (DNS) jusqu'aux algorithmes de recommandation qui sous-tendent de nombreux services Internet. La gouvernance d'Internet est en effet de plus en plus contestée et « matérielle » : la redistribution du pouvoir sur et par Internet est, de façon croissante, inscrite dans ses architectures et ses infrastructures techniques. Ce mémoire se propose de montrer les apports de la sociologie des sciences et des techniques (*science and technology studies* ou STS en anglais) aux recherches sur la gouvernance d'Internet ; j'examine tout particulièrement les apports du sous-domaine des STS qu'on appelle les études des infrastructures, ou *infrastructure studies*. En effet, jusqu'à il y a quelques années seulement, les questions relatives à la gouvernance d'Internet étaient principalement abordées au travers des sciences politiques, des relations internationales et du droit, mais plusieurs travaux récents ont démontré l'intérêt d'agrandir cette focale afin d'explorer certaines dimensions de la gouvernance qui resteraient autrement dans l'ombre, et qui sont par

ailleurs centrales quoique dotées d'une importante dimension « informelle » (ce que je détaille dans les sections suivantes).

Le mémoire est structuré autour d'une série d' « histoires d'objets techniques », de leur développement et déploiement ; ces chapitres sont précédés et suivis par une discussion des apports des STS aux études sur la gouvernance de l'Internet existants, avec une attention particulière à la « valeur ajoutée » que peuvent représenter les approches par les infrastructures.

Ce travail commence par une discussion théorique et une revue de littérature qui présentent tout d'abord les cadrages principaux qui structurent les recherches sur la gouvernance d'Internet. Les deux chapitres suivants rétrécissent progressivement la focale sur les approches STS et leurs apports à l'étude de ce domaine, pour déboucher enfin sur une discussion des rapprochements entre études des infrastructures et études de la gouvernance d'Internet. Ces chapitres se fondent sur un ensemble de travaux théoriques que j'ai menés au cours des dernières années à la fois seule et en binôme ou trinôme avec des collègues tels que Ksenia Ermoshina (Centre Internet et Société, CNRS), Cécile Méadel (CARISM, Université Paris-Panthéon-Assas), Alexandre Mallard (CSI, MINES Paris), Benjamin Loveluck (i3-SES, Télécom Paris), Laura DeNardis (American University), Dmitry Epstein (Hebrew University of Jerusalem) et Christian Katzenbach (Humboldt Institut für Internet und Gesellschaft, Berlin).

Le mémoire se poursuit par une re-visitation de certaines des enquêtes que j'ai effectuées durant les dix dernières années (lors de mon post-doctorat, et, après mon recrutement en tant que chargée de recherche au CNRS, au sein de différents projets et équipes de recherche, notamment l'H2020 NEXTLEAP et l'ANR ResisTIC), qui montrent en pratique comment s'exerce dans des contextes différents la « gouvernance par l'infrastructure » du réseau des réseaux. Ces cas d'étude sont le système de noms de domaine (*Domain Name System* ou DNS), le réseau décentralisé de crypto-monnaie Bitcoin, le protocole de chiffrement Signal, et le système de « boîtiers » de surveillance mis en place ces dernières années par l'État russe au sein de son réseau national.

Ce mémoire se termine enfin par un chapitre où j'élabore une typologie des dispositifs et systèmes de « gouvernance par l'infrastructure », afin de montrer comment des « pièces » importantes

d'Internet sont mobilisées dans des jeux de pouvoir pour servir des objectifs de gouvernance ; je montre comment chacun de ces cas produit une définition de gouvernance – et différents registres et pratiques de justification de la gouvernance. Le chapitre final discute également les directions de recherche ouvertes par ce mémoire, qui incluent la relation entre la gouvernance par l'infrastructure et la gouvernance des contenus en ligne, le « dialogue » constant entre infrastructures de contrôle et de résistance qui marque l'internet d'aujourd'hui, ou encore les opportunités d'une approche *par les infrastructures* pour essayer de démêler la nébuleuse, aujourd'hui très populaire, de « souveraineté numérique ».

0.1. La gouvernance d'Internet, ensemble de pratiques et objet de recherche

Beaucoup d'encre a coulé, depuis au moins deux décennies, pour tenter de définir la « gouvernance d'Internet », tout en reconnaissant que cette étiquette désigne l'une des questions géopolitiques les plus pressantes de l'ère contemporaine. Comme j'expliquerai plus en détail par la suite (voir la section « Apports de ce travail »), l'un des objectifs de ce mémoire est de montrer comment la notion de gouvernance d'Internet a évolué dans la pratique au fil des années, aussi grâce aux questions que chercheurs et praticiens se sont posées sur son périmètre, sa nature et ses acteurs ; il serait donc contre-productif pour ce travail d'essayer de produire en amont une seule et précise définition, ou un périmètre complètement établi, de ce que sont Internet ou sa gouvernance. Cependant, en guise d'introduction ici, je propose un point de départ pour nos réflexions, qui comprend « l'Internet » comme l'ensemble, mondial et interconnecté, de technologies et de services numériques en réseau qui facilitent la communication et la création, le stockage, l'analyse et le partage de données et d'information, et la « gouvernance d'Internet » comme l'ensemble de fonctions de conception, coordination, contrôle et maintenance, exercées par une variété d'acteurs publics et privés, qui permettent à l'Internet de fonctionner et régulent les interactions qui peuvent avoir lieu par son biais.

Les façons dont l'Internet est conçu et administré ont des implications pour une variété d'enjeux de politique publique, tels que la vie privée, la stabilité économique, la sécurité nationale, la liberté

d'expression et l'égalité numérique. Les gouvernements abordent des questions de gouvernance d'Internet et de cybersécurité en même temps que d'autres types d'enjeux nécessitant d'une action collective globale, tels que le terrorisme, la sauvegarde de l'environnement et la protection des droits humains. En même temps, de nombreuses fonctions relatives à la gouvernance d'Internet ne relèvent pas principalement des prérogatives des gouvernements, mais sont mises en œuvre par des formes d'ordonnancement privé, de conception et d'implémentation techniques. Le rôle des acteurs privés comme intermédiaires et médiateurs de fonctions de gouvernance acquiert un poids toujours croissant. Ces acteurs privés se voient confiées – ou revendiquent d'eux-mêmes – des tâches de déréférencement d'informations sur les moteurs de recherche ou d'élimination de contenus réputés sensibles ou diffamatoires ; ils ont par ailleurs à disposition des grandes masses de données personnelles de leurs utilisateurs, qu'ils peuvent utiliser à des fins publicitaires, ou ils sont contraints de révéler ces informations aux autorités pour des raisons politiques ou juridiques. L'action de gouvernance d'Internet s'est progressivement installée à l'échelle de la planète toute entière.

Ce qui était autrefois un ensemble de questions à haute technicité, reléguées à la communauté technique et à quelques universitaires, figure désormais en bonne place sur l'agenda politique de tous les gouvernements, et a vu par ailleurs naître les « empires numériques » qui sont réunis sous l'acronyme de GAFAM (Google, Amazon, Facebook, Apple et Microsoft). On peut trouver plusieurs raisons à la base de cette augmentation de l'intérêt pour la manière dont l'Internet est administré et gouverné. Les enjeux économiques du marché numérique sont immenses, tous les secteurs industriels dépendant d'Internet pour leur fonctionnement et le commerce numérique se chiffrant en milliards de dollars par an. Une panne d'Internet implique le plus souvent un dommage pour l'économie mondiale. Les politiques liées à Internet ont également une incidence profonde sur les libertés individuelles et les discours politiques autour des élections. Les gouvernements ont rapidement compris que la gouvernance de l'Internet incluait, mais ne se limitait pas au pouvoir de l'État, et d'autres sources de normativité acquéraient de l'importance dans des domaines allant des conflits cybernétiques aux systèmes de filtrage et de censure.

Un certain nombre de controverses liées à Internet, largement couvertes par les médias – comme les révélations d'Edward Snowden sur la surveillance de masse mise en œuvre par le

gouvernement des États-Unis, les violations massives de données et le piratage informatique piloté par la Russie lors de l'élection présidentielle américaine de 2016 – ont attiré l'attention du public sur les questions relatives à la manière dont Internet est contrôlé et administré, que ce soit par des intermédiaires de la diffusion de contenus comme les médias sociaux, par les gouvernements et les États, ou encore par de nouvelles institutions conçues pour gérer la sécurité et la stabilité des ressources critiques d'Internet.

Les importants enjeux liés aux questions de gouvernance d'Internet ont également entraîné, de la part des décideurs politiques et du secteur privé, un intérêt considérable pour des études empiriques – ayant pour objet le traitement des données personnelles en ligne, la régulation des plateformes ou encore la géopolitique d'Internet à travers le monde – qui sont en mesure de fournir une base à leurs décisions. Ces acteurs sont également preneurs d'études qui contribuent à rendre visibles les tenants et aboutissants du pouvoir qui construit et contrôle l'Internet, de l'auto-régulation des plateformes aux processus multi-parties-prenantes, et qui en expliquent les implications pour la société et l'économie.

Une communauté épistémique de chercheurs et universitaires, très interdisciplinaire et répartie dans le monde entier, se définit quant à elle comme une communauté de recherche sur la gouvernance mondiale de l'Internet. Cette communauté d'universitaires est de plus en plus organisée, depuis la création du réseau universitaire mondial sur la gouvernance de l'internet (*Global Internet Governance Academic Network* ou GigaNet[2]) en 2006 et depuis l'apparition de près d'une centaine de centres interdisciplinaires, hébergés par les institutions académiques du monde entier, qui se consacrent à l'étude des politiques de l'Internet, de la cyber-gouvernance et de la gouvernance d'Internet. Un nombre croissant d'étudiants et de doctorants, d'organisations de soutien aux internautes, de centres universitaires, de décideurs politiques et de nouveaux types d'entreprises cherchent à mieux comprendre les choix et les implications de la manière dont les réseaux numériques mondiaux sont gouvernés.

[2] https://www.giga-net.org

0.2. Problématique et positionnement

Le présent travail a ses racines, et sa raison d'être, dans ce contexte qui inclut à la fois les enjeux de plus en plus centraux, et la visibilité augmentée, des controverses liées au contrôle de l'Internet, et l'agrégation et la maturation croissante d'un domaine interdisciplinaire qui a fait de la gouvernance d'Internet un objet de recherche. Si la gouvernance d'Internet est devenue une question sensible et centrale pour les équilibres de pouvoir mondiaux depuis quelques années, en parallèle, la recherche qui s'y consacre s'est profondément transformée. Ce mémoire vise à la fois à faire le point sur ces transformations et à défendre l'intérêt de développer un regard attentif aux dynamiques de gouvernance qui se passent « à même les infrastructures » du réseau des réseaux. Cette section détaille plus spécifiquement la problématique et le positionnement théorique de ce travail.

0.2.1. La gouvernance d'Internet au prisme de la sociologie des techniques

Mon travail repose largement sur l'hypothèse suivante, dont plusieurs années d'enquêtes de terrain m'ont confirmé la pertinence : suite aux évolutions de la gouvernance d'Internet comme ensemble de pratiques et domaine d'étude, il est important de mettre à contribution les perspectives et les outils méthodologiques des sciences sociales – voire d'en forger de novateurs – afin de mieux prendre en compte certaines dimensions de la gouvernance d'Internet. Mon travail est soutenu par la conviction qu'une sociologie des infrastructures d'Internet comme outils de gouvernance permet de renouveler la compréhension d'un certain nombre de phénomènes qui transforment aujourd'hui l'Internet et le numérique.

Ce mémoire s'attache donc à conceptualiser, de façon largement inédite en langue française jusqu'ici, la gouvernance de l'Internet telle qu'elle peut être appréhendée par la sociologie des techniques et les STS. Plus particulièrement, au sein de ce domaine qui propose des approches et des lectures sensiblement différentes, je me fonde ici sur ce courant des STS qui étudie la relation entre les machines/technologies, leurs développeurs/producteurs, et leurs utilisateurs afin de montrer comment certaines valeurs et certains objectifs politiques peuvent être atteints grâce à la construction et à l'emploi des technologies (Winner, 1986 ; Latour, 1992 ; Bowker & Star, 1996).

Appliquée aux recherches sur la gouvernance d'Internet, cette approche constitue un déplacement conceptuel et disciplinaire important.

Dès les débuts de la conception de l'Internet en tant que technologie, et des mécanismes de prise de décision liés au « réseau des réseaux » (Braman, 2011), la trajectoire de la gouvernance d'Internet comme champ de recherche a été définie à la fois par les types de questions posées et les types d'approches disciplinaires utilisées. Comme le décrivent van Eeten et Mueller, la gouvernance d'Internet a tout d'abord été façonnée par les politiques et les controverses entourant la coordination mondiale des noms de domaine et des adresses Internet (2013, p. 724), qui sont un facteur important, mais pas le seul, affectant l'Internet. Les recherches concernant la gouvernance d'Internet se sont pendant longtemps principalement concentrées sur des institutions telles que l'*Internet Corporation for Assigned Names and Numbers* (ICANN)[3], sur des processus chapeautés par les Nations Unies, tels que le Sommet mondial sur la société de l'information (SMSI)[4] et le Forum sur la gouvernance de l'Internet (FGI)[5], et sur l'idée du système « multi-parties-prenantes » comme modèle novateur de prise de décision politique liée à l'Internet. Sur le plan conceptuel, le champ a été dominé par les recherches en droit, en relations internationales et en économie institutionnelle, dont la plupart sont axées sur le rôle de l'État-nation dans la gestion des ressources Internet critiques ; pour la même raison, les premières sous-disciplines de la sociologie qui se sont intéressées aux politiques de l'Internet sont la sociologie politique et la sociologie du droit, dont j'examine rapidement les contributions dans la section suivante.

Ces approches sont de plus en plus questionnées pour leur focalisation sur les institutions formelles et le rôle de l'État, ce qui les amènerait à négliger certains aspects de ce qui constitue la gouvernance dans un environnement en réseau. Van Eeten et Mueller, par exemple, suggèrent que la portée de la gouvernance d'Internet en tant que champ de recherche est beaucoup plus large que ce qui est étiqueté comme tel ; ils suggèrent de repenser le champ pour y inclure « la diversité de la gouvernance sur et avec l'internet », y compris « les environnements peu formalisés, les formes organisationnelles hétérogènes (…) et les formes d'autorité et de pouvoir massivement distribuées » (2013, p. 730). Van Eeten et Mueller appellent également à étudier l'économie et les

[3] https://www.icann.org
[4] En anglais *World Summit on the Information Society*, ou WSIS: https://www.itu.int/net/wsis/
[5] https://www.intgovforum.org/multilingual/

pratiques des organisations qui s'occupent de la gestion des flux d'information sur l'internet, qu'il s'agisse des noms et des numéros, de la sécurité ou du filtrage des contenus.

DeNardis (2010, 2013) a par ailleurs remarqué que les recherches concernant la gouvernance d'Internet ont pendant longtemps mis au deuxième plan les arrangements privés en matière de routage, d'interopérabilité, de définition de normes ou de filtrage de contenu en ligne. Raymond et DeNardis (2015) ont plaidé en faveur d'un cadre plus large pour les études sur la gouvernance d'Internet – un cadre qui mettrait en lumière ces arrangements de pouvoir de nature privée et souvent opaque. Leur cadre conceptuel couvre six domaines fonctionnels allant du « contrôle des ressources Internet critiques » à « l'application des droits de propriété intellectuelle basée sur l'architecture » (2015, pp. 589-594), qui se concentrent tous sur la gouvernance d'Internet telle qu'elle se déroule « en pratique ». Raymond et DeNardis identifient un ensemble d'entités qui, en mettant en œuvre des arrangements liés à la prise de décision, agissent comme points de contrôle des flux d'information en ligne.

Cependant, de nombreuses orientations proposées dans le champ restent conceptuellement et substantiellement axées sur le niveau institutionnel de l'analyse. En effet, une focalisation sur ce niveau permet d'interroger conceptuellement tant les relations internationales que les théories de l'économie institutionnelle. Les approches institutionnelles se prêtent également bien à l'investigation empirique, puisque la plupart de ces institutions ont établi clairement leur périmètre et leurs membres, et ont mis en place un ensemble de procédures formelles, de résultats et de la documentation, qui sont généralement mûrs pour l'analyse (van Eeten & Mueller, 2013). Cependant, l'accent mis sur les institutions néglige largement les pratiques quotidiennes, parfois discrètes, parfois banales (*mundane*) qui font fonctionner ces institutions, laissant ainsi d'importantes zones d'ombre dans la compréhension conceptuelle et substantielle des pratiques et des dispositions de pouvoir qui constituent la gouvernance d'Internet. L'accent mis sur les institutions et les instruments politiques formels néglige l'analyse empirique des diverses formes d'activité et de prise de décision et de coordination liées à l'internet qui se déroulent en dehors de frontières formelles et bien définies (Musiani, 2015 ; van Eeten & Mueller, 2013). Le fait de traiter les institutions comme des entités stables et statiques cache l'important travail d'évolution et de reconfiguration institutionnelles qui se passent dans la gouvernance d'Internet, et ne tient pas compte des biais fonctionnels et structurels ancrés dans les arrangements institutionnels existants

(Hofmann, Katzenbach et Gollatz, 2016 ; Ziewitz et Pentzold, 2014). En outre, l'accent mis sur les institutions met au deuxième plan l'ensemble de pratiques des concepteurs, des décideurs et des utilisateurs des technologies Internet -- alors qu'elles interagissent, de manière distribuée, avec les normes et les dispositifs, ce qui entraîne des conséquences imprévues ayant des effets systémiques (Epstein, 2015 ; Musiani, 2015). Il semble important d'explorer ce volet de la gouvernance d'Internet pour donner corps empirique à des définitions de la gouvernance telles que celles adoptées par Sandra Braman, « prise de décision avec un effet constitutif (structurel), qu'elle ait lieu dans le secteur public ou privé, et de manière formelle ou informelle » (Braman, 2009, p. 3), ou par Jeanette Hofmann et ses co-auteurs alors qu'ils reconnaissent que la gouvernance « peut être juste un effet secondaire d'actions ayant des objectifs non liés à la gouvernance » (Hofmann et al., 2016, p. 4).

Ce mémoire se situe donc dans le récent courant d'études sur la gouvernance d'Internet qui préconise que, afin d'aborder pleinement les questions « macro » de politique et de pouvoir liées au réseau des réseaux, il est nécessaire d'explorer les « micro-pratiques » de gouvernance telles que les mécanismes de coordination distribuée, semi-formelle ou réflexive, de contrainte exercée par les acteurs privés, et d'utilisation des ressources Internet. Les arrangements apparemment stables de la gouvernance d'Internet découlent effectivement d'un ensemble peu ou pas hiérarchisé, et souvent peu organisé, d'activités de conception, de régulation et d'utilisation de l'internet considérées comme « allant de soi » et apparemment déconnectées entre elles. C'est cette focalisation sur les pratiques et les routines, les discours et la conception qui m'a amenée, avec Dmitry Epstein et Christian Katzenbach, à conceptualiser la gouvernance d'Internet comme un « *doing internet governance* » (faire la gouvernance d'Internet), en tant que « accomplissement intégré dans l'interaction quotidienne » (West & Zimmerman, 1987, p. 125). Poursuivant la trajectoire tracée par un certain nombre d'arguments récents en faveur d'une utilisation plus large des sciences sociales pour donner du sens aux dynamiques de gouvernance (Flyverbom, 2011 ; Hofmann et al, 2016 ; Musiani, 2015 ; Ziewitz & Pentzold, 2014), ce mémoire présente et discute les façons dont les STS peuvent contribuer à mieux comprendre ce domaine en rapide évolution et aux implications sociétales de plus en plus importantes et variées.

Conceptuellement, la recherche sur l'IG fondée sur les STS repose sur la compréhension de la gouvernance d'Internet comme un « système de systèmes » normatif et reconnaît l'agence, souvent

discrète et omniprésente, d'acteurs et d'infrastructures humains et non humains. De manière empirique, les approches STS à la gouvernance d'Internet se concentrent sur la dynamique d'« ordonnancement » des assemblages et des arrangements hybrides de la gouvernance d'Internet ; sur les effets structurels et performatifs des controverses et des déstabilisations sur les normes et la prise de décision, ou sur la construction de l'autorité et de la confiance ; et enfin, sur les forums hybrides, les arrangements privés, les utilisateurs et leurs pratiques.

Dans cette galaxie de concepts et d'approches, les travaux que j'ai menés pendant la dernière décennie se sont concentrés tout particulièrement sur les architectures et sur les infrastructures techniques, et les manières dont celles-ci ont progressivement évolué de *cibles* de la gouvernance à *instruments* de gouvernance, servant des objectifs très variés et souvent inattendus lors de leur création. Les intermédiaires des flux d'information, les ressources Internet critiques, les points d'échange internet, les dispositifs de surveillance et de sécurité jouent un rôle de gouvernance crucial aux côtés des institutions politiques, nationales et supranationales et des organisations de la société civile (Musiani, Cogburn, DeNardis et Levinson, 2016). La gouvernance d'Internet prend forme à travers une myriade d'infrastructures, de dispositifs, de flux de données et d'architectures techniques souvent discrets et invisibles, mais néanmoins cruciaux pour co-construire un réseau de réseaux de plus en plus public, complexe, et articulé. Ces entités sont des « points de contrôle » infrastructurels, autour desquels s'entremêlent des questions d'efficacité technique et économique, ainsi que des négociations et des controverses sur les valeurs humaines et sociétales telles que les droits de propriété intellectuelle, la vie privée, la sécurité, la transparence (Musiani, 2012 ; DeNardis, 2014 ; DeNardis & Musiani, 2016).

0.2.2. La gouvernance (d'Internet), un objet (aussi) sociologique

Comme la section précédente le montre, d'une part, l'évolution de la gouvernance d'Internet nécessite d'adopter des méthodes et cadre théoriques issus des sciences sociales, et d'autre part, en retour, se saisir de cet objet permet de faire évoluer les sciences sociales. Ma démarche s'inscrit dans une problématisation sociologique transversale, dont il convient de tracer rapidement un portrait avant de revenir au focus plus spécifique de ce mémoire.

En effet, l'Internet comme objet de recherche « fait travailler » la sociologie à de nombreux égards : la sociologie politique, la sociologie du droit et la sociologie économique contribuent depuis plusieurs années à éclairer comment l'Internet et ses politiques sont co-produits par l'interaction sociale, et co-produisent en retour des visions particulières de la société.

La sociologie politique a montré à quel point la gouvernance d'Internet est une politique publique « en train de se faire », du fait que les structures et les responsabilités ne sont pas figées, les statuts juridiques en cours de définition et les objectifs le plus souvent sujets à controverses. Dans une perspective de sociologie politique, l'étude de la gouvernance d'Internet peut offrir un terrain de recherche stratégique à partir duquel saisir des recompositions en cours de l'action publique et notamment l'instrumentation croissante de la régulation publique (Halpern et al., 2014). La gouvernance d'Internet est notamment révélatrice de trois dynamiques qui affectent plus généralement les modes d'exercice du contrôle social et de l'autorité politique : la privatisation, la globalisation et l'automatisation des instruments de gouvernement. Il s'agit pour la sociologie politique de spécifier comment ces dynamiques se renforcent, s'atténuent ou convergent autour des nouveaux dispositifs de régulation, tout en précisant leur inscription dans un processus global de transformation des modes de gouvernement à l'ère numérique (Bellon, 2018).

A l'ère des profonds bouleversements entraînés par le numérique et de la « privatisation » croissante de la gouvernance d'Internet – le fait que les acteurs privés, notamment les grandes plateformes du Web, sont désormais en mesure de créer ou promouvoir leurs propres systèmes normatifs – la sociologie économique examine les relations entre organisations, États et marchés (Carruthers et Uzzi, 2000). Les efforts dans ce champ se sont consacrés notamment à comprendre les changements politiques, économiques, technologiques et *corporate* intervenus à l'ère du numérique, et comment ces changements transforment les relations et rôles des acteurs économiques (Courmont et Le Galès, 2019) – pour faire émerger de nouvelles identités qui modifient en profondeur les façons dont la richesse est produite et distribuée, jusqu'au développement de phénomènes tels que ledit « capitalisme de surveillance » (Zuboff, 2019).

Les apports de la sociologie du droit permettent, quant à eux – en dialogue avec des contributions de juristes tels que Mireille Delmas-Marty sur l'Internet comme « révélateur, perturbateur et producteur de règles » (2012) – de comprendre l'Internet et le numérique en tant que catalyseurs de plusieurs phénomènes qui ont contribué à un renouveau des études socio-juridiques : « la globalisation du droit, les mutations du rapport à la norme, (…) ainsi que, de manière générale, le désordre et la complexité des normes qui caractérisent les régimes juridiques actuels » (Villegas et Lejeune, 2011). Particulièrement pertinent pour l'étude de la gouvernance d'Internet aujourd'hui est l'approche de la sociologie du droit qui consiste à analyser le « droit tel qu'il se fait », au-delà du droit qui est écrit – qui considère le droit non seulement comme un ensemble de règles établissant des devoirs et des droits, mais aussi comme une source de normes qui co-produisent des opportunités d'action pour les acteurs sociaux ; une telle approche met l'accent sur l'ethnographie des « pratiques » du droit en situation (Colemans et Dupret, 2018), sur les dimensions informelles de la normativité, sur les processus de négociation entre acteurs, et sur la co-existence du droit avec d'autres formes de contrôle (Lascoumes et Serverin, 1986). Bien que les liens entre la sociologie du droit et les études de gouvernance d'Internet restent à ce jour sous-exploités, ses approches au pluralisme normatif et à la construction de la norme sont très pertinentes pour appréhender la pluralité et le chevauchement des systèmes normatifs sur la Toile.

Les évolutions récentes de la gouvernance d'Internet, en particulier celles qui ont trait aux usages « politiques » de ses infrastructures, ont amené au premier plan des questions telles que le rôle des intermédiaires techniques, le maintien de ou les entraves à la neutralité du net, les spécificités techniques du Web en tant que média avec des coulisses et des interfaces, ou encore la circulation de l'information et ses « goulots d'étranglement » technologiques. Ces questions ont trouvé dans la sociologie des techniques et de l'innovation des outils théoriques et méthodologiques adaptés à analyser les façons dont le pouvoir s'inscrit dans des architectures et infrastructures techniques complexes. Le reste de ce mémoire se focalise principalement sur ces apports à l'étude de la gouvernance d'Internet, mais il faut garder à l'esprit qu'il s'inscrit plus généralement dans une sociologie de l'Internet qui, en puisant dans ces différents courants, vise à retracer les conditions d'émergence de nouvelles formes de co-production de la norme sur et par les réseaux numériques, et à rendre compte des acteurs et des instruments à travers lesquels elle s'exerce.

0.3. Méthodologie

Mon approche méthodologique dans ce travail est qualitative et inductive, et se situe au croisement du « penser par cas » de Passeron et Revel (2005) et de l'ethnographie multi-sites (voir par exemple Muir, 2011). D'un côté, j'ai choisi de « procéder par l'exploration et l'approfondissement des propriétés d'une singularité accessible à l'observation (…pour) en extraire une argumentation de portée plus générale, dont les conclusions pourront être réutilisées pour fonder d'autres intelligibilités » (Passeron et Revel, 2005, p. 9). Par ailleurs, mes recherches ont été menées, au fil des années, au sein de plusieurs sites avec des composantes en ligne et hors ligne, et j'ai explicitement conçu les infrastructures, protocoles et systèmes techniques spécifiques à chaque cas comme « faisant partie d'un contexte plus large qui dépasse les limites du site de terrain » (Muir, 2011); à noter a cet égard une réflexion récente sur la méthode ethnographique multi-site par son premier promoteur George Marcus, soulignant que cette méthode a été « à son plus créatif, critique et intéressant lorsqu'elle a été impliquée dans l'étude [STS] de systèmes d'information et de connaissance distribués » (Marcus, 2012).

J'analyse le développement des infrastructures et des architectures techniques comme des « points de rencontre » entre les objectifs des développeurs et concepteurs, les nécessités d'usage, et les efforts normatifs (Oudshoorn & Pinch, 2005). Ce faisant, je vise à donner un sens, informé par le travail de terrain, de la création de systèmes émergents et de communautés de pratique, au moyen de « descriptions analytiques épaisses » (*analytical thick descriptions* ; pour un traitement plus récent du concept, introduit pour la première fois par l'anthropologue Clifford Geertz, voir par exemple Ponterotto, 2006) d'événements, d'artefacts et d'organisations. En particulier, je me concentre sur les moments de controverse – de conflit, de crise, de débat, de polémique – pour essayer de comprendre comment un artefact technique prend forme, de sa création à son appropriation et reconfigurations par les utilisateurs, à sa transformation en sujet de débat public, de pression politique, de gouvernance. La principale méthodologie pour atteindre cet objectif a été d'observer, pendant des périodes relativement prolongées, des groupes ou des communautés spécifiques et leurs interactions avec les objets techniques qu'ils fabriquaient, construisaient ou utilisaient, tout en menant des entretiens approfondis avec leurs membres et en analysant des

documents tels que des comptes rendus de séances de travail et les notes de publication de versions logicielles.

Le fait de penser et travailler « par cas » présente un certain nombre d'avantages et d'opportunités méthodologiques. Identifier les moments où un objet, une dynamique, une action est controversée contribue à comprendre ou l'accès aux terrains est possible, même si le degré de « publicité » d'une controverse n'est pas toujours le même et la négociation de l'accès au terrain varie en conséquence. Analyser les moments et lieux de controverse participe à identifier et rendre saillants les « points de contrôle » (DeNardis, 2014) de l'Internet, en les rendant problématiques – comme on le verra notamment dans le troisième chapitre de ce mémoire, les controverses sont, dans cette optique, performatives, au sens de leur capacité à faire exister des aspects de la réalité. Ces approches présentent par ailleurs aussi un certain nombre d'écueils ou de difficultés, que je discuterai plus en détail notamment à la fin du deuxième chapitre et qui incluent le fait de devoir étudier des objets et dynamiques très souvent « invisibles », la nécessité d'allier une perspective sociologique et une compréhension fine d'objets techniques complexes, et le besoin de comprendre le fonctionnement d'acteurs privés dont les pratiques sont couvertes en grande partie par le secret industriel, ce qui peut amener à sur-étudier les systèmes ouverts et sous-étudier les systèmes fermés (voir notre travail récent dans DeNardis et al., 2020).

0.4. Apports de ce travail

Au fil des matériaux empiriques, sur lesquels je cherche à projeter une vue d'ensemble informée par les courants STS qui explorent les infrastructures, ce travail souhaite proposer plusieurs apports aux études de la gouvernance de l'Internet.

En premier lieu, comme les pages précédentes l'ont montré, il s'agit de contribuer à forger des outils novateurs de sciences sociales – dialoguant avec des disciplines telles que l'informatique et l'histoire notamment – qui permettent de mieux prendre en compte les dimensions informelles et distribuées de la « gouvernance par l'infrastructure » du réseau des réseaux. Il s'agit de rendre compte des processus hétérogènes qui lient la conception et la production techniques aux normes

sociales et aux hiérarchies socio-politiques, et d'explorer l'influence réciproque des arrangements de gouvernance et d'un ensemble de choix de contournement et de cooptation au niveau de l'infrastructure technique.

Il s'agit aussi de reconnaître et expliciter les jalons historiques de la gouvernance d'Internet, tout en reconnaissant la pluralité de ses histoires. Dans le chapitre 1, notamment, on fera certes référence aux origines de l'Internet en tant que projet du Département de la Défense des États-Unis – imprégné à la fois de la structure hiérarchique de la bureaucratie militaire et gouvernementale et des valeurs de la culture scientifique et technique des universités américaines. Cependant, ce travail doit beaucoup à des recherches d'historiens tels que Andrew Russell (2012) ou Valérie Schafer (2015), qui ont montré comment, à cause de ces origines états-uniennes marquées, la naissance et le développement de la société de l'information en réseau ont souvent été racontés dans une perspective téléologique et présentiste, qui voit les évolutions ayant façonné l'Internet dans sa forme actuelle comme résultat d'une série d'innovations linéaires et « obligées », et ses parcours alternatifs comme erreurs ou retards corrigés plus ou moins rapidement, plutôt que comme des moments de co-construction du *zeitgeist* de l'ère numérique. L'Histoire, avec un grand H, de l'Internet est bien composée de multiples histoires de l'Internet, distribuées géographiquement et techniquement ainsi que politiquement.

Une telle perspective permettra de faire la part des récits dominants de l'Internet d'aujourd'hui, tels que la surpuissance des GAFAM – qui est certes bien présente mais qui ne résume pas à elle seule les enjeux de pouvoir d'Internet – ainsi que des récits originaux d'un Internet symétrique, complètement ouvert et égalitaire. Il s'agit de montrer à quel point la gouvernance d'Internet est un dialogue constant d'arrangements infrastructurels visant le contrôle, la cooptation, la concentration du pouvoir sur Internet, ou encore développant des façons inédites de l'exercer ; et de réponses qui visent la résistance, la critique, l'évasion, souvent par le biais de bricolages ou de ruses techniques. Cette démarche permettra d'avancer dans la compréhension des différentes réalités qui forment actuellement l'Internet – ou, plutôt, les Internets – et de leurs articulations.

La gouvernance d'Internet est aussi l'apanage de multiples acteurs de différentes natures, déployant une variété de répertoires d'action et stratégies de positionnement. Les acteurs de cette gouvernance travaillent à l'intersection des institutions, des technologies, et de jeux de pouvoir et

d'influence en réseau. Des internautes dits « lambda », agissant en tant qu'individus avec leur double casquette de citoyens et de consommateurs, à la « société civile organisée » des associations et des ONG ; des services et plateformes Internet, parfois des écosystèmes numériques à plein titre, aux États et aux institutions nationales et supranationales ; des développeurs informatiques aux acteurs techniques qui assurent le fonctionnement quotidien du réseau (points d'échange Internet, fournisseurs d'accès…), ces acteurs seront analysés dans ce travail alors qu'ils reconfigurent des communautés et des institutions, stabilisent ou remettent en discussion des connaissances, co-produisent des structures d'autorité et des géographies politiques, donnent naissance à de nouveaux (dés-)équilibres de pouvoir à l'ère de la gouvernance globale d'Internet à partir de ses infrastructures.

Il s'agit également, pour ce travail, de montrer comment la notion de gouvernance d'Internet a évolué dans la pratique aussi grâce aux questions, explicites et analytiques, que chercheurs et praticiens ont posé au fil des années sur son périmètre, sa nature et ses acteurs. Il serait donc contre-productif d'essayer de produire en amont, comme nécessaire précondition à toute enquête significative, une seule et précise définition ou un périmètre complètement établi à priori de ce qu'est la gouvernance, ce qu'est Internet, ou ce qu'est la gouvernance d'Internet. Je montre ici comment les négociations et les controverses liées à Internet et ses enjeux de pouvoir sont performatives, dans la mesure où elles impliquent et sont impliquées dans la création de mondes dans lesquels des modes de gouvernance spécifiques ont du sens (voir aussi Ziewitz et Pentzold, 2014). Si ce mémoire discute de façon substantielle *qui* étudie la gouvernance d'Internet, et *ce* qu'on étudie quand on se revendique de ce concept, je ne chercherai pas à en donner une définition précise, mais j'observerai comment une pluralité de définitions ressortent des différents lieux – matériels, logiciels, géographiques – de mes enquêtes. L'exploration détaillée de plusieurs sites où les infrastructures d'Internet sont controversées, détournées, appropriées, revendiquées est *de facto* un moyen d'enquêter sur ce qu'est Internet et sa gouvernance, dont le périmètre se négocie au cas par cas.

Comme on l'a vu, il existe donc un rapport spécifique entre les recherches sur la gouvernance de l'Internet et leur objet ; la gouvernance et les recherches qui y sont consacrées sont étroitement liées, et nées quasi dans le même mouvement. Ce mémoire (en complément avec mon autobiographie intellectuelle) souligne donc, enfin, qu'on peut difficilement concevoir et penser

l'Internet et sa gouvernance comme objets de recherche, sans vouloir contribuer à informer la « mise en politique » de cet espace. Ce mémoire est donc aussi une occasion d'expliciter une façon possible d'être « normatifs » en se basant sur des apports scientifiques : pas en préconisant ce qu'il faut faire, mais en portant à la lumière des phénomènes qui passent souvent sous le radar des régulateurs. Il s'agit de montrer comment ces phénomènes peuvent le plus souvent être pensés sur le long terme et dans la continuité, plutôt qu'en mode réactif et dans l'urgence.

En synthèse, ce mémoire propose de systématiser les travaux qui m'ont conduite, au fil de la dernière décennie, à participer de la création d'une théorie de la gouvernance d'Internet à partir de ses infrastructures. Je détaille plus précisément la structure de ce mémoire dans la section qui suit.

0.5. Structure du mémoire

Ce mémoire se compose d'une première partie de trois chapitres visant à établir et affiner le cadre théorique de ce travail, suivie d'une deuxième partie qui présente quatre cas d'étude, et un chapitre conclusif.

0.5.1. Première partie : Approches aux études de la gouvernance d'Internet

Au cours des deux dernières décennies, les chercheurs sur la gouvernance de l'Internet se sont saisis d'un éventail de cadres analytiques et conceptuels, issus de diverses disciplines et traditions de recherche, pour rendre compte de leur objet. Le premier chapitre présente brièvement ces théories, concepts et outils méthodologiques – de l'économie politique aux études des mouvements sociaux, de la théorie des régimes à l'analyse des réseaux de discours, des théories néo-institutionnelles à la théorie de l'acteur-réseau, et montre comment ces différentes approches ont été utiles afin d'interroger plusieurs facettes, composantes et processus de la gouvernance d'Internet. Ce chapitre souligne deux aspects importants des questions de gouvernance et de leur étude : un nombre croissant d'enjeux de plus en plus visibles et publics, et une recherche académique qui s'est progressivement enrichie pour les aborder. Dans sa dernière partie, le

chapitre donne quelques repères historiques sur le champ, des premiers débats sur « l'exceptionnalisme » d'Internet jusqu'aux discussions plus récentes sur les nouveaux périmètres et enjeux de la gouvernance d'Internet, discussions suscitées notamment par des controverses de haut profil telles que la surveillance numérique de masse, révélée au grand jour par Edward Snowden.

Les premières recherches qui ont abordé la gouvernance d'Internet en s'inspirant des approches des STS ont commencé à se développer dans la deuxième décennie des années 2000. Le deuxième chapitre donne un aperçu des manières actuelles dont les approches STS sont appliquées à la recherche sur la gouvernance de l'internet, et en particulier, il se concentre sur les études des controverses et les études des infrastructures, deux sous-ensembles d'outils conceptuels et méthodologiques qui nous apparaissent particulièrement intéressants. Le chapitre s'ouvre en retraçant la façon dont les STS ont abordé l'Internet comme sujet d'étude, et en examinant comment certains concepts clés des STS ont trouvé leur place dans les études sur l'Internet. Dans sa deuxième partie, le chapitre traite plus en détail de trois aspects qu'on considère particulièrement importants à aborder, dans la « galaxie » gouvernance d'internet, avec des approches et des outils STS : le développement, formel et informel, de standards dans l'espace Internet ; l'analyse des effets structurants et performatifs des controverses sur la gouvernance ; l'agencement d'acteurs et d'infrastructures non humains en tant que lieux d'exercice et de médiation de la gouvernance.

Le troisième chapitre du mémoire restreint ultérieurement la focale des approches STS, pour présenter les approches sur lesquels les chapitres empiriques de ce mémoire se fondent plus particulièrement, dérivées des études d'infrastructures (*infrastructure studies*), en analysant comment ils peuvent apporter des contributions importantes et novatrices au champ de la gouvernance d'Internet. Le chapitre discute l'ensemble de travaux qui, à partir des recherches pionnières de Geoffrey Bowker, de Susan Leigh Star ou encore de Paul Edwards, s'est attaché à étudier les infrastructures – plus particulièrement les infrastructures informationnelles et numériques – en considérant qu'elles sont « matérielles » tout en étant numériques. Ces travaux se proposent de mobiliser la notion d'infrastructure comme instrument heuristique pour comprendre la gouvernance de l'information et du numérique, et en particulier de l'Internet. Avec

ces travaux en toile de fond, le chapitre examine successivement comment la gouvernance d'internet peut être comprise comme un enchevêtrement d'histoires d'infrastructures : des infrastructures comme *cible*s de gouvernance, en passant par l'inscription volontaire de valeurs et principes dans les infrastructures de la part d'ingénieurs, concepteurs et développeurs, jusqu'aux infrastructures comme *outils* de gouvernance – la 'politisation' et la cooptation d'infrastructures Internet particulières pour servir des objectifs souvent bien différents que leur fonction première.

0.5.2. Deuxième partie : Les « pratiques situées » de la gouvernance par l'infrastructure

La deuxième partie du mémoire consiste en une présentation de quatre cas emblématiques de formes d'action et « pratiques situées » liées à la gouvernance par l'infrastructure, qui vont de la standardisation plus ou moins formelle d'un protocole de chiffrement à la fabrication d'un « annuaire » pour l'Internet, ou encore présentent des développements techniques au sein desquels s'inscrivent des modèles d'organisation d'une communauté ou de distribution du pouvoir. Ces chapitres se fondent sur certaines des enquêtes de terrain que j'ai effectuées après 2012, toujours avec la question de la « gouvernance d'internet par l'infrastructure » en fil rouge.

Le quatrième chapitre aborde, comme premier cas d'étude, une des plus célèbres technologies de gouvernance d'Internet : le Domain Name System ou système de noms de domaine (DNS). Le DNS a été créé pour être l'« annuaire » de l'Internet, un système qui traduit entre les adresses IP (Internet Protocol) numériques utilisées par les ordinateurs pour acheminer des paquets d'informations sur l'internet et les noms de domaine alphanumériques que nous utilisons pour accéder aux sites web. Par ailleurs, l'importance de ce système de classification a des conséquences sociales, politiques et économiques de grande portée. En fait, le DNS est devenu l'un des principaux champs de bataille où le pouvoir social, politique et économique est arbitré dans la sphère publique en réseau (DeNardis, 2012). Il a notamment été envisagé comme possible moyen d'application « par l'infrastructure » des droits de propriété intellectuelle, et plus généralement comme moyen de régulation des contenus.

Le cinquième chapitre discute une technologie de réseau décentralisée qui a fait couler beaucoup d'encre au cours de la dernière décennie : Bitcoin, une crypto-monnaie créée sur l'onde de la crise financière de 2008 et du manque de confiance répandu dans les institutions monétaires et financières. Cette monnaie a donc été créée avec une technologie particulière – la chaîne de blocs ou *blockchain* – comme principe structurant, qui devait en théorie se substituer à une gouvernance humaine comprise comme peu fiable, si pas carrément malhonnête. Ce chapitre montre comment de nombreux points de « faiblesse » technique et organisationnelle (qui sont, en fait, autant de points de redistribution et de reconfiguration du pouvoir et de l'autorité) ont pris forme et contribué à forger la « gouvernance par l'infrastructure » de Bitcoin.

Dans le sixième chapitre, on analyse la « gouvernance par l'infrastructure » au sein de Signal, une des technologies de messagerie sécurisée/chiffrée de bout en bout les plus répandues à ce jour. Ce système comprend un protocole de communication appelé Signal et une application, s'appelant aussi Signal, développée par les auteurs du protocole ; par ailleurs, d'autres applications ont récemment vu le jour qui adaptent le protocole Signal à leurs besoins et publics. Le protocole Signal est développé au sein d'un secteur, la messagerie chiffrée, qui est actuellement – notamment après les révélations d'Edward Snowden sur la surveillance numérique de masse – très foisonnant et varié en termes d'arrangements d'architecture technique, organisation des processus de développement, et modèles d'affaires. La question se pose donc, dans ce secteur, de comment le standardiser/structurer. Le chapitre montre un cas de « gouvernance par l'infrastructure » qui a trait à cette standardisation : comment le protocole Signal est progressivement devenu un « standard informel » dans le secteur suite à un ensemble de pratiques et controverses autour de son implémentation, et plus largement sa reconnaissance dans la pratique comme « quelque chose qui marche ».

Le septième chapitre s'intéresse aux infrastructures de pouvoir mis en place au cours de la dernière décennie par l'Etat russe. En effet, l'Internet russe a récemment connu une augmentation rapide du contrôle juridique et de la centralisation de l'infrastructure technique. Son âge d'or en tant qu'espace de « semi-liberté d'expression », sans réglementation ni censure, semble être révolu : les lois adoptées ces dernières années, concernant la censure des sites web et la surveillance du trafic, façonnent la toile russe selon le projet d' « Internet souverain » promu par le gouvernement.

Ce chapitre porte plus particulièrement sur l'encadrement juridique et le déploiement d'un ensemble de boîtiers visant des objectifs divers de surveillance et censure (contrôler les flux et collecter des données personnelles notamment). Il explore la florissante industrie russe de la censure et de la surveillance, et dévoile des débats animés autour de technologies controversées que les acteurs de l'Internet russe doivent obligatoirement installer au sein de leurs systèmes infrastructurels, qui sont coûteuses et complexes à mettre en œuvre et qui soulèvent un certain nombre de préoccupations éthiques et politiques.

Un chapitre conclusif tire les fils des perspectives théoriques et des différents cas d'étude analysés, pour faire un bilan de cette décennie de recherches sur la gouvernance d'Internet « par l'infrastructure » et ouvrir des pistes de recherche pour le futur proche et pour le moyen terme.

Chapitre 1. A la recherche de la gouvernance d'Internet : cadrages, acteurs et questions émergentes

En mars 2019, le World Wide Web (WWW) a fêté son trentième anniversaire. A cette occasion, Tim Berners-Lee, l'inventeur du WWW, qualifie l'événement de « moment de célébration du chemin parcouru, mais aussi d'occasion de réflexion sur le chemin qu'il reste à parcourir ». Pour Berners-Lee, le développement futur de l'Internet exigerait que les gouvernements, le secteur privé et les utilisateurs du « réseau des réseaux » partagent la responsabilité de sa gouvernance :

> *« Les gouvernements doivent adapter les lois et les règlements à l'ère numérique. Ils doivent veiller à ce que les marchés restent compétitifs, innovants et ouverts. Et ils ont la responsabilité de protéger les droits et les libertés des personnes en ligne. (...) Les entreprises doivent faire davantage pour s'assurer que leur recherche de profit à court terme ne se fait pas au détriment des droits de l'homme, de la démocratie, des faits scientifiques ou de la sécurité publique. Les plateformes et les produits doivent être conçus en tenant compte de la vie privée, de la diversité et de la sécurité. (...) Et surtout, les citoyens doivent tenir les entreprises et les gouvernements pour responsables des engagements qu'ils prennent, et exiger qu'ils respectent le web en tant que communauté mondiale avec les citoyens à cœur »*
>
> *(Berners-Lee, 2019, ma traduction).*

Avec cet appel, Berners-Lee – sans doute une des personnes dont le travail a contribué de manière la plus significative à faire de l'Internet un espace de communication et d'information accessible au plus grand nombre – a reconnu publiquement l'importance de la politique et de la régulation pour le développement futur de l'Internet. Alors que des 'exceptionnalistes' de l'Internet comme John Perry Barlow ont pu déclarer, il y a vingt-cinq ans, l'indépendance du cyberespace du contrôle et de l'intervention des gouvernements (Barlow, 1996), plus de deux décennies de recherches ont depuis démontré que l'Internet d'aujourd'hui est le produit d'une myriade de choix effectués par les États (à la fois démocratiques et autoritaires), des entreprises, de la société civile et des utilisateurs (Mansell, 2012). La régulation de l'Internet se fait sous différentes formes et à

différents niveaux ; par ailleurs, la politique et la régulation – si elles sont motivées par de mauvaises intentions, ou mal appliquées – peuvent causer un préjudice très important au réseau mondial, à son infrastructure technique, à son environnement commercial et, surtout, à ses utilisateurs.

Beaucoup insistent sur le fait que les politiques de l'Internet devraient être élaborées et mises en œuvre principalement par des experts techniques, des entreprises ou, idéalement, une communauté mondiale multipartite, et mettent en garde contre les effets néfastes que les intérêts des États-nations peuvent exercer sur le réseau mondial (Mueller, 2020). En effet, dans une certaine mesure, de nombreux domaines de la politique de l'Internet ont été « privatisés », en ce sens que les entreprises privées y jouent un rôle central (Curran, Fenton & Freedman, 2012). Pourtant, dans de nombreux pays démocratiques du monde entier, le public se tourne de plus en plus vers les gouvernements nationaux et les organismes régionaux, comme la Commission européenne, pour obtenir des solutions réglementaires aux problèmes liés à l'Internet, tels que la protection des données, la désinformation, les contenus illégaux, la liberté d'expression, la neutralité du réseau et autres. Même Mark Zuckerberg, fondateur et directeur général de Facebook, a récemment appelé les législateurs et les régulateurs à s'efforcer de renforcer la réglementation de l'Internet mondial (Zuckerberg, 2019). Quelle que soit la motivation d'une telle demande, qui est sans doute assez différente pour les deux hommes, on retrouve dans le raisonnement de Zuckerberg le fil conducteur de celui de Berners-Lee : ce n'est qu'en (ré-)configurant soigneusement les règles de l'Internet qu'il sera possible de protéger les droits des utilisateurs et de préserver les réseaux numériques comme moyen de communication personnelle, de débat public et d'échange d'informations.

Malgré ces appels en faveur de politiques de l'Internet plus nombreuses et d'une meilleure qualité, et malgré la diffusion et l'importance croissantes du « réseau des réseaux » en tant qu'infrastructure de communication mondiale et plateforme pour les services d'information, la gouvernance de l'Internet est restée longtemps un sujet de niche dans la recherche sur les médias et la communication, si on la compare, par exemple, aux études des usages du numérique. En général, les sciences sociales et humaines ont été lentes à aborder la gouvernance d'Internet en tant que domaine de recherche (Brosda, 2015 ; Dutton, 2018), de sorte que la communauté de ses

spécialistes reste assez restreinte, distribuée au niveau international, pluridisciplinaire et diverse dans ses approches conceptuelles et méthodologiques. En même temps, il semble important à ce stade que le développement de la prochaine génération d'instruments de régulation de l'Internet soit éclairé par des chercheurs ayant une expertise dans le développement, la mise en œuvre et l'évaluation des politiques de communication dans l'intérêt du public, et qu'il soit éclairé par les lois, les politiques et les organisations existantes qui travaillent à la protection des droits individuels et collectifs. C'est ainsi que, dans le champ de la gouvernance d'Internet, on remarque souvent une co-construction, plus étroite que dans d'autres domaines, entre les problèmes soulevés du côté des acteurs concernés au sens large, les débats publics, et les problématisations dans le monde académique. La gouvernance de l'Internet a émergé à la fois « comme un label, un domaine de recherche et d'études universitaires, et une arène du monde réel où les parties prenantes et les groupes d'intérêt s'affrontent et coopèrent » (Mueller & Badiei, 2020). A plusieurs endroits au cours de ce mémoire, je montrerai ce lien particulier qui existe entre recherche et pratique du pouvoir dans le domaine de la gouvernance d'Internet ; la place et le rôle des chercheurs qui travaillent sur la gouvernance d'Internet, leur engagement, le statut de leurs analyses, feront notamment l'objet de la section 8.2[6].

1.1. Des « social implications of the Internet » aux études interdisciplinaires de ses facettes politiques

En 2001, le sociologue américain Paul DiMaggio et son équipe publiaient dans *l'Annual Review of Sociology* l'article « Social Implications of the Internet ». Cité désormais près de 3000 fois, cet article invitait les sociologues à « étudier l'Internet de façon plus active », et plus particulièrement à explorer comment on pouvait utilement croiser l'étude « micro » des comportements individuels et en groupe des utilisateurs d'Internet, et les analyses « macro » des facteurs institutionnels et politico-économiques qui façonnent ces comportements.

Vingt ans après, des nombreuses pièces se sont rajoutées à ce puzzle. La recherche et les chercheurs qui explorent la gouvernance de l'Internet proviennent de multiples disciplines et appliquent à cet

[6] Voir aussi les sections « Engagement dans les arènes politiques » du premier volume de ce mémoire d'HDR.

objet un éventail de théories et de méthodes, mais ils partagent la même volonté de comprendre la pratique de la gouvernance d'Internet en tant que infrastructure mondiale et nationale; l'impact de la régulation publique et privée sur les économies, les communautés et les cultures basées sur l'Internet ; et enfin les droits, les responsabilités, les normes et les principes invoqués par les utilisateurs et les non-utilisateurs. Alors que certains travaux évaluent les politiques élaborées par les acteurs étatiques, les entreprises privées et les institutions impliquées dans les processus formels de prise de décision politique, d'autres se concentrent sur une variété de formes de gouvernance alternatives, basées sur des approches liées aux biens communs ou à l'activisme numérique. D'autres encore s'intéressent aux définitions des problèmes, aux discours, aux lois, aux principes et aux imaginaires qui président aux débats politiques et à l'élaboration des politiques publiques.

Au cours des deux dernières décennies, les recherches sur la gouvernance de l'Internet ont appliqué un éventail de cadres analytiques et conceptuels issus de diverses disciplines et traditions de recherche[7]. Afin d'évaluer le rôle des acteurs dans l'élaboration des politiques de l'Internet, les chercheurs ont utilisé des théories, des concepts et des outils méthodologiques issus de l'économie politique, des études des mouvements sociaux, de l'analyse des réseaux, des théories de l'acteur-réseau, de la domestication, des champs et des régimes, ainsi que des approches plus classiques de l'analyse politique, comme l'*advocacy coalition framework* (par exemple, Mathiason, 2008 ; Milan, 2015 ; Pavan, 2012 ; Pohle, Hösl, & Kniep, 2016).

Pour l'analyse des discours, des intérêts et des stratégies dans les débats liés à la gouvernance et aux politiques de l'Internet, les chercheurs ont également déployé des approches « post-positivistes » telles que l'analyse des réseaux de discours, l'analyse politique interprétative et l'analyse des réseaux sociaux en ligne (par exemple, Epstein, Nisbet, & Gillespie, 2011 ; O'Rourke & Kerr, 2017 ; Pohle, 2018). Plus récemment, les chercheurs ont commencé à se concentrer sur le rôle des cadres institutionnels de la gouvernance d'Internet et sur les interrelations entre les pratiques et les institutions, en s'appuyant par exemple sur des théories néo-institutionnelles telles que l'institutionnalisme historique et sociologique (par exemple, Bannerman & Haggart, 2015 ;

[7] Cette section reprend des éléments de Kerr, Musiani & Pohle (2019).

Galperin, 2004 ; Puppis, 2010). En outre, les approches dérivées des études sociales des sciences et des techniques (STS, de l'anglais *science and technology studies*), auxquels ce mémoire sera en grande partie consacré, ont souvent été mobilisées pour analyser le rôle, dans la gouvernance de l'Internet, des « pratiques triviales et quotidiennes » (*mundane practices*) de tous ces acteurs qui entretiennent, piratent, développent, testent et utilisent le réseau de réseaux (Epstein, Katzenbach & Musiani, 2016).

En déployant ce large éventail d'approches conceptuelles, une grande partie des recherches sur la rencontre entre l'Internet et le politique se sont d'abord concentrées sur la nature « globale » des réseaux numériques. Les chercheurs ont tenté de comprendre les défis posés à la régulation par le caractère transnational de l'Internet et de ses services, en analysant les acteurs et les institutions impliqués dans sa coordination et sa gestion, en particulier celle de son infrastructure technique. En effet, une grande partie des premiers travaux de recherche était liée aux processus historiques qui ont conduit à l'institutionnalisation des mécanismes de coordination et d'élaboration des politiques de l'Internet, tels que l'administration du système de noms de domaine de l'internet (DNS) et son institutionnalisation dans l'Internet Corporation for Assigned Names and Numbers (ICANN) (par exemple Christou & Simpson, 2007 ; Klein, 2002) ou le Sommet mondial sur la société de l'information (SMSI) et son aboutissement avec la création du Forum sur la gouvernance de l'internet (par exemple, Frau-Meigs et al., 2012 ; Raboy, Landry, & Shtern, 2010 ; Padovani, 2004 ; Sarikakis, 2004). Un autre volet de ces recherches a examiné comment l'Internet, infrastructure mondiale, pouvait être non seulement une cible de gouvernance, mais aussi un *instrument* de gouvernance, en inscrivant des modèles, des contraintes et des opportunités particulières dans l'architecture technique de l'Internet (par exemple, DeNardis, 2009 ; Braman, 2016). Enfin, les chercheurs se sont interrogés sur les inégalités de diffusion et d'accès à Internet entre les régions et les pays. Les recherches sur la gouvernance de l'Internet ont réussi à déplacer les termes du débat de la question de l'*accès* à la technologie à une réflexion sur les compétences, les ressources et les capacités requises pour utiliser l'internet, et sur les inégalités découlant de ces modèles d'utilisation émergents. Ces recherches contribuent à explorer les façons dont les politiques et les technologies de l'Internet co-construisent les modèles d'inclusion et d'exclusion dans les sociétés contemporaines, en particulier vis-à-vis la problématique du genre (par exemple, Padovani & Shade, 2016 ; Stevenson, 2009).

Plus récemment, les tentatives de régulation par les autorités nationales ou régionales ont été mises en avant par les spécialistes de la gouvernance de l'Internet (par exemple, Collins, 2006 ; Löblich & Karppinen 2014 ; Daly & Thomas, 2017). La majorité des analyses empiriques dans ce domaine prennent la forme d'études de cas sur des questions politiques particulières, telles que la protection des données et la vie privée, le droit d'auteur, la sécurité, la culture numérique, la neutralité du réseau, la réglementation du contenu et, de plus en plus, la réglementation des données (voir par exemple Meyer, 2012 ; Pierson, 2012 ; Powell & Cooper, 2011 ; Van Audenhove, Vanwynsberghe, & Mariën, 2018). Les chercheurs se sont également concentrés sur des groupes particuliers d'acteurs impliqués dans l'élaboration des politiques nationales en matière d'Internet, par exemple les militants, les intermédiaires Internet ou les partis politiques (voir par exemple Breindl & Briatte, 2013 ; DeNardis & Hackl, 2015 ; Löblich & Wendelin, 2012 ; Macq & Jacquet, 2018). D'autres ont analysé le nombre croissant d'initiatives concernant les chartes nationales des droits de l'Internet, comme le Marco Civil au Brésil ou des initiatives similaires en Europe (voir par exemple Cristofoletti, 2015 ; Gill, Redeker, & Gasser, 2015 ; Padovani & Santaniello, 2018). Récemment, la tendance à une sécurisation et à une surveillance accrue de l'espace en ligne a conduit à ce que les chercheurs consacrent une plus grande attention aux compétences réglementaires en matière de cybersécurité et aux discours connexes dans divers pays (voir par exemple Hintz & Dencik, 2016 ; Maréchal, 2017 ; Tréguer, 2017, Zeng, Stevens, & Chen, 2017).

Pour beaucoup d'individus et de groupes, Internet est aujourd'hui un aspect acquis de la vie quotidienne, au vu des nombreuses activités humaines qui ont lieu sur et via Internet (Bortzmeyer, 2019). Cela a suscité de nombreuses discussions sur la relation entre les droits, les valeurs et le « réseau des réseaux », tant chez les praticiens des technologies numériques que chez les chercheurs et les décideurs politiques. Certaines de ces questions sont largement débattues, comme celles liées à la manière dont des services particuliers, tels que Facebook, luttent contre la désinformation ; d'autres sont beaucoup moins visibles et font l'objet d'un examen public moins approfondi, notamment la manière dont les droits et les valeurs sont liés aux protocoles et à l'infrastructure. La relation entre les droits de l'homme et les protocoles Internet commence néanmoins à être examinée dans un certain nombre d'arènes politiques et techniques (par exemple,

l'Internet Research Task Force[8] et son groupe de recherche Human Rights Protocol Considerations[9]).

La relation entre les nouvelles technologies dites d'intelligence artificielle, telles que le *machine learning*, et l'éthique, au sens large, est également une question politique clé au niveau européen, et ces technologies sont de plus en plus intégrées dans de nombreux outils développés et utilisés par les grandes entreprises pour régir le comportement des utilisateurs en ligne. En 2019, le groupe européen d'experts de haut niveau sur l'intelligence artificielle (IA), créé par la Commission européenne, a publié un ensemble de « lignes directrices éthiques pour une IA digne de confiance »[10] afin d'encourager les entreprises technologiques à examiner comment leurs outils d'IA pourraient porter atteinte aux droits fondamentaux ; plusieurs rapports et *white papers* ont vu la lumière depuis, aux niveaux nationaux, international et transnational.

Les questions clés pour ces documents sont récurrentes et incluent l'autonomie humaine, l'équité, la responsabilité, la vie privée, la discrimination, la diversité et l'impartialité. Ces initiatives en matière d'éthique ont été motivées par la prise de conscience que la conception et la mise en œuvre des outils d'intelligence algorithmique et artificielle peuvent introduire des pratiques hautement discriminatoires qui sont difficiles à évaluer, à tracer et à réglementer *ex post* (voir par exemple Dencik, Hintz, & Carey, 2017 ; Eubanks, 2018). Pour certains, il ne suffit pas de s'appuyer sur l'éthique – des cadres législatifs et de « bonnes pratiques » plus solides s'avèrent nécessaires. Pour d'autres, l'éthique peut être un mode de critique et un contrepoids utile aux discussions sur la sécurisation et le capitalisme des plateformes (voir par exemple Lyon, 2014). Pourtant, les lignes directrices qui émergent dans les temps les plus récents ont tendance à se concentrer sur l'éthique au niveau individuel plutôt que sur les valeurs et les droits d'intérêt collectif ou public, et n'éclairent pas pleinement la différence entre différents contextes de possible application des principes éthiques. Les questions politiques pourraient devenir encore plus complexes à mesure que l'IA s'intégrera dans l' « internet des objets » et que nos dispositifs s'effaceront dans l'arrière-plan de nos environnements quotidiens (voir par exemple Kitchin & Dodge, 2011).

[8] https://irtf.org
[9] https://datatracker.ietf.org/rg/hrpc/about/
[10] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Si les dispositifs et les contextes évoluent, le fait que les nouvelles technologies posent des défis aux droits fondamentaux n'est bien sûr pas nouveau. La mesure dans laquelle, et comment, les objets techniques sont imprégnés du « politique » au sens large, est une question très étudiée et controversée dans l'histoire des techniques. En ce qui concerne l'Internet, la question a été résumée de la façon la plus concise par le mantra « *code is law* » de Lawrence Lessig (1999), et reprise (de façon parfois inexacte) par ses nombreux descendants. Parmi ces travaux, les apports de Laura DeNardis (2009) ont été fondamentaux pour comprendre, avec des concepts et des méthodes dérivés des STS, de quelles manières les protocoles sont politiques. En effet – le chapitre 3 y reviendra notamment – bien qu'ils soient difficiles à appréhender parce qu'ils sont intangibles et souvent invisibles pour les internautes, les protocoles contrôlent les flux mondiaux d'information, influencent la compétitivité économique des nations et leur capacité à rivaliser équitablement, et prennent souvent des décisions par « procuration » ou « délégation » qui influencent les libertés civiles en ligne et un certain nombre de droits individuels, y compris, par exemple, l'accès au savoir (DeNardis, 2009, p. 6).

Au cours de plusieurs décennies, les travaux des historiens, des philosophes et des spécialistes des sciences sociales ont montré que les valeurs ont toujours eu un rôle dans la conception des infrastructures techniques ; les ingénieurs de l'Internet n'ont pas fait exception, se posant des questions non seulement sur l'optimisation technique, mais aussi sur ce que signifiait la mise en place de protocoles favorisant la vie privée des individus, l'accessibilité pour les personnes handicapées et d'autres préoccupations d'intérêt public (Russell, 2014 ; Nissenbaum, 2001 ; Braman, 2011). Des travaux récents ont également examiné comment les infrastructures de gouvernance de l'internet ont été « politisées » à des fins qui dépassent leur objectif d'origine, et les conséquences imprévues que ces usages entraînent pour la stabilité et la sécurité de l'Internet, ainsi que pour la protection des droits de l'homme en ligne (Musiani et al., 2016 ; le troisième chapitre y reviendra plus largement). Des contributions encore plus récentes ont fait valoir qu'il existe une lacune à combler vis-à-vis les droits humains dans la gouvernance de l'Internet, dans la mesure où les droits humains sont publics – jusqu'à très récemment, seuls les acteurs étatiques pouvaient être tenus pour responsables de leur non-respect – alors que l'architecture d'Internet est

principalement détenue ou exploitée par le secteur privé, bien qu'elle ait une fonction importante de médiation et de gouvernance des droits humains en ligne (Zalnieriute & Milan, 2019).

1.2. La gouvernance d'Internet en tant qu'objet de recherche

On voit comment les questions émergentes liées à l'interaction de l'Internet, des droits et des valeurs sont nombreuses, et les données existantes suggèrent que les problèmes varient d'un pays à l'autre et d'une région à l'autre. Actuellement, les questions politiques liées à l'Internet qui font l'objet de plus d'attention sont la diffusion de la désinformation en ligne et ses implications pour le processus démocratique, ainsi que la nécessité de trouver un équilibre entre la liberté d'expression, la surveillance et la vie privée (Badouard, 2017). La manière de parvenir à une diversité culturelle et de contenu sur des services numériques de plus en plus centralisés revêt également une importance croissante. La piste du « multi-partisme » ou des arrangements « multi-parties-prenantes » -- un partage des responsabilités entre les institutions transnationales, les gouvernements, les entreprises et les utilisateurs – est envisagée dans plusieurs sous-domaines au croisement entre politique et internet, mais les instruments qui permettront d'atteindre un équilibre acceptable entre les droits et les valeurs de tous ces acteurs sont loin d'être évidents.

On a déjà pu montrer dans l'introduction comment, en particulier au cours des dernières deux décennies, l'image de la gouvernance d'Internet comme enjeu à haute technicité, et très spécialisé, s'est considérablement complexifiée, et il s'agit désormais de l'une des questions géopolitiques plus pressantes de l'ère contemporaine. Au vu de ce statut, elle est désormais abordée par les gouvernements en même temps que d'autres types d'enjeux nécessitant d'une action collective globale, tels que le terrorisme ou la sauvegarde de l'environnement. Les choix qui sont faits dans la conception et l'administration d'Internet ont des implications de plus en plus importantes et multiples pour une variété d'enjeux de politique publique, tels que la vie privée, la stabilité économique, la sécurité nationale, la liberté d'expression et les inégalités dans des contextes en ligne et hors ligne. Les enjeux économiques du marché numérique sont quant à eux immenses, tous les secteurs industriels dépendant d'Internet pour leur fonctionnement, et le commerce numérique se chiffrant en milliards de dollars par an. Les gouvernements sont en passe d'utiliser

la gouvernance d'Internet comme un levier de pouvoir dans des domaines qui incluent la surveillance, la censure, la liberté d'expression, la démocratie elle-même. Des événements médiatiques éclatants, aux implications explosives pour les équilibres politiques mondiaux, ponctuent l'histoire récente d'Internet, tels que les révélations d'Edward Snowden sur la surveillance de masse mise en œuvre par le gouvernement des États-Unis, ou les violations massives de données et le piratage informatique piloté par la Russie lors de l'élection présidentielle américaine de 2016.

Le présent travail a pris forme, pendant la dernière décennie, dans ce contexte de visibilité croissante et de complexification des enjeux liés à la gestion (et au contrôle) d'Internet, et, au niveau de la recherche, de l'articulation et de la maturation du domaine interdisciplinaire qui identifie comme objet de recherche commun la « gouvernance d'Internet ». Dans les pages qui suivent, je vais explorer plus en détail cet objet ainsi que les profils de chercheur qui l'étudient, et les défis que ces chercheurs rencontrent. Il s'agit de proposer un portrait de la gouvernance d'Internet par les différentes façons dont elle est problématisée dans la recherche.

1.2.1. Qu'étudie-t-on en étudiant la gouvernance de l'Internet ?

L'Internet est – et a toujours été – organisé et géré, même si, à ses débuts, il n'était peut-être pas encore « gouverné » au sens strict. En effet, le lien entre pouvoir et réseaux numériques a toujours dépassé le sens traditionnel du « gouvernement » exercé par un État-nation ; le pouvoir sur Internet s'exerce via un ensemble de points de coordination et de contrôle qui traversent les frontières géographiques et sont répartis entre de nombreux acteurs, notamment le secteur privé, les structures gouvernementales, un certain nombre d'institutions mondiales créées spécifiquement pour gérer l'Internet, et les citoyens, à titre individuel ou organisés dans des structures relevant de la « société civile ». La gouvernance, donc, ne concerne pas seulement les gouvernements, mais elle est mise en œuvre également par le biais de la conception technique (y compris, comme on verra plus en détail en 2.2.1, les standards), la coordination des ressources, les contrats privées et les conflits aux points de contrôle.

On peut tenter une « définition de travail » de la gouvernance d'Internet comme l'administration, la gestion et la conception des technologies qui maintiennent l'internet opérationnel et fonctionnel,

et la mise en place de stratégies politiques autour de ces technologies. Dans les couches sous-jacentes à ce que la plupart des internautes considèrent « l'Internet » – contenus, applications et dispositifs – des milliers de points de contrôle se cachent en coulisses. S'il n'existe pas de seule et unique taxonomie idéale pour décrire ces nombreux points de coordination et de contrôle ainsi que leur conception, une façon d'organiser leurs *fonctions*, qu'on a proposée avec Laura DeNardis il y a quelques années, est la suivante (DeNardis et Musiani, 2016)[11] :

- Administration des ressources Internet critiques, telles que l'adressage Internet
- Établissement de normes techniques relatives à l'Internet (par exemple, protocoles d'adressage, de routage, de cryptage, de compression, de détection des erreurs, systèmes d'identité, authentification)
- Coordination de l'accès et de l'interconnexion (par exemple, IXP, neutralité du réseau, politiques d'accès)
- Gouvernance de la cybersécurité
- Intermédiation des flux d'information par des acteurs privés ayant un poids politique (par exemple, via la gouvernance des plate-forme, l'ordonnancement algorithmique, les conditions d'utilisation, la prise de décision via l'intelligence artificielle, et les politiques en matière de sécurité, de discours, de réputation et de respect de la vie privée)
- Application des droits de propriété intellectuelle basée sur l'architecture technique

Tous ces points de contrôle sont complexes et multi-variables, et ils se chevauchent à bien des égards. De plus, si chacune de ces fonctions peut être utilisée pour maintenir l'Internet libre et ouvert, toutes peuvent également être exploitées par les gouvernements ou le secteur privé pour mettre en place des dynamiques de censure ou de surveillance.

[11] Cette taxonomie, bien que vaste, limite en fait de manière importante le champ d'application de la gouvernance de l'internet comme objet de recherche. Elle distingue clairement, dans l'énorme corpus d'*Internet studies,* ceux qui ont trait à des aspects de gouvernance d'Internet de ceux qui abordent la plupart des usages de l'Internet, les discours sur l'Internet, ou des questions d'identité et de représentation de l'utilisateur sur les réseaux. Ces questions sont l'apanage de la sociologie des usages (voir parmi les travaux francophones notamment Jouët, 2000, et dans le monde anglophone, par exemple, Markham & Baym, 2008). Pour simplifier cette distinction, alors qu'une grande partie des études d'Internet analyse ce que les personnes expriment sur les médias sociaux - comme l'analyse du contenu de l'expression politique sur Twitter ou les questions d'identité, la représentation ou la formation de communautés – on se concentrera dans ce mémoire notamment sur les mécanismes de contrôle sous la couche du contenu, comme l'ordonnancement algorithmique, la sécurité, le coût des plateformes, les politiques de confidentialité instanciées en termes de service, les mécanismes de détection des faux comptes gérés par des robots, et les contextes réglementaires qui limitent ou permettent ces différents phénomènes.

Il est possible d'identifier plusieurs caractéristiques distinctives de la gouvernance d'Internet à travers ses multiples contextes: les choix de conception et de coordination technique sont partie intégrante des politiques publiques; les technologies de gouvernance de l'Internet, telles qu'elles sont actuellement conçues, traversent les frontières de manières qui compliquent l'application de la juridiction et le droit national des États; la gouvernance est répartie entre de multiples acteurs, selon un modèle généralement décrit comme « multi-parties-prenantes » où le secteur privé a de plus en plus de poids; la sécurité de l'Internet comporte à la fois des points de convergence et de divergence avec les enjeux de sécurité nationale; le contrôle de l'infrastructure d'Internet a de plus en plus une fonction de pouvoir politique et économique. On examine ces caractéristiques plus en détail ci-dessous.

L'un des traits distinctifs de la pratique de la gouvernance d'Internet est que la conception de l'architecture technique est un élément important de la mise en œuvre des politiques publiques. Par conséquent, une part importante de la recherche sur la gouvernance de l'Internet étudie les technologies sous-jacentes de l'Internet et la manière dont elles sont conçues. Par exemple, la conception technique du système de noms de domaine de l'Internet (DNS) a construit ou permis certaines formes de gouvernance, à la fois du DNS et *par* le DNS (voir notamment le Chapitre 4). Comme le suggèrent Bradshaw et DeNardis (2016), la façon dont les noms de domaine sont conçus peut entraîner des conflits relatifs à la liberté d'expression ; sa conception hiérarchique crée des goulots d'étranglement au niveau desquels le contenu peut être bloqué ; le DNS se base « by design » sur un ensemble de ressources finies (adresses Internet binaires) et soulève donc des questions de distribution de cette ressource au niveau mondial ; et enfin, l'exigence de noms et de numéros uniques a nécessité d'une administration centralisée pour garantir cette unicité pour l'ensemble du globe. Plusieurs recherches sur la gouvernance d'Internet se sont concentrées sur le DNS et ses systèmes de contrôle institutionnel (par exemple, l'ICANN, l'Internet Assigned Numbers Authority [IANA], ainsi que les registres nationaux ; voir Klein, 2002 ; Kleinwächter, 2000 ; Mueller, 2002 ; Pare, 2003).

Une des démarches les plus importantes pour le fonctionnement d'Internet qui se situent dans la myriade d'opérations qui participent à sa gouvernance est l'établissement de standards techniques

afin d'obtenir des formats universels pour adresser, coder, compresser, chiffrer et échanger des informations d'une manière interopérable avec d'autres appareils et logiciels qui adhèrent à ces normes. Il existe des centaines et des centaines de standards, dont les plus célèbres sont Wi-Fi, HTTPS (protocole de transfert hypertexte sécurisé), VoIP (protocole de voix sur Internet) et Bluetooth. Ces spécifications sont définies par de nombreuses institutions techniques transnationales, telles que l'Institute of Electrical and Electronics Engineers (IEEE), le World Wide Web Consortium (W3C) et l'Internet Engineering Task Force (IETF). Les normes remplissent une fonction technique, mais leur conception contribue également à établir des stratégies et des priorités de politique publique. Par exemple, les normes d'interopérabilité permettent la concurrence économique entre les acteurs privés et favorisent l'innovation et l'interconnexion mondiale. La stabilité et le consensus autour des normes de chiffrement informe de façon très importante les conditions de la protection de la vie privée. Les normes d'accessibilité au Web permettent aux personnes souffrant de déficiences auditives, visuelles, motrices ou autres, d'utiliser Internet.

Les caractéristiques techniques des technologies de communication et d'intermédiation de l'information en réseau permettent également de mettre en œuvre la gouvernance. Les intermédiaires de l'information, tels que les plateformes privées – par exemple, les plates-formes de médias sociaux, les moteurs de recherche, les plates-formes de messagerie, les fournisseurs d'accès et les infrastructures de *cloud computing* – permettent l'échange et l'agrégation de contenu et le structurent de façons particulières. Certaines caractéristiques de conception telles que les mécanismes de suivi, les obligations de s'identifier en ligne par son véritable nom dans certains contextes, ainsi que les décisions relatives à l'anonymat, construisent des droits – alors que les conditions de service de ces systèmes construisent les conditions des libertés civiles individuelles telles que les droits d'expression, la vie privée et la propriété des données. On commence à voir ici un point qui sera approfondi de façon récurrente par la suite : chaque fonctionnalité technique, chaque façonnage d'infrastructure, et même chaque choix d'interface peut, dans des contextes particuliers, être appréhendé comme une forme de gouvernance, ou en tout cas mettre en œuvre « un peu » de gouvernance dans l'ensemble d'opérations qui constituent la gouvernance d'Internet.

Parmi les caractéristiques récurrentes des initiatives qui prétendent, à leur échelle, participer à la gouvernance d'Internet, est aussi le fait que l'élaboration de politiques dont la cible est censée être un territoire national ou supra-national en particulier, et « son Internet », ne reste pas nécessairement à l'intérieur de ses frontières. Par exemple, le règlement général sur la protection des données (RGPD)[12] de l'Union européenne a touché des entreprises dont les stratégies d'affaires sont mondiales, et il a affecté des technologies transfrontalières telles que le système WHOIS[13], une base de données de détenteurs de noms de domaine enregistrés dans le monde entier. Les politiques locales, telles que le GDPR, la règle du droit à l'oubli et les politiques de localisation des données, ont des effets mondiaux car les technologies sous-jacentes de l'Internet – points d'interconnexion, infrastructures de *cloud computing*, réseaux de distribution de contenu, ou encore le DNS – ne sont pas censées, depuis leur création, correspondre à ces frontières nationales et supra-nationales.

Une réaction politique à la croissance et au succès d'Internet, aux caractéristiques techniques de ses technologies « transfrontalières », et à la mesure très importante dans laquelle des entreprises privées façonnent les droits de l'homme en ligne, est la montée en puissance des approches dites de « souveraineté numérique », dans lesquelles différents États cherchent à exercer un plus grand contrôle sur des parties d'Internet. Dans de nombreux cas, ils cherchent à imposer les frontières des États-nations sur l'architecture distribuée d'Internet. La Russie, la Chine et certains autres pays ont été les promoteurs de la « souveraineté numérique » sous couvert d'ordre social ; le système efficace de censure et de filtrage du contenu en Chine et les lois relatives à la surveillance en Russie sont probablement les meilleurs exemples de cette tendance. Pourtant, le langage de la « souveraineté numérique » est repris à son compte également par l'Union européenne et plusieurs de ses États membres, au nom d'une autonomisation et d'une plus grande protection pour leurs citoyens.

Un débat de longue date dans la gouvernance de l'Internet occupe ceux qui préconisent un plus grand contrôle gouvernemental du réseau des réseaux, via des modèles qui relèvent de la souveraineté numérique, et ceux qui préconisent un modèle de gouvernance plus distribué sur les

[12] https://gdpr-info.eu
[13] https://lookup.icann.org

différents acteurs et parties prenantes, y compris les organisations internationales, les institutions nationales et supranationales, le secteur privé, les nouvelles institutions mondiales, et la société civile. Cette situation a donné lieu à de nombreuses controverses en matière de gouvernance internationale, qu'il s'agisse des débats sur la réglementation des télécommunications internationales lors de la conférence mondiale de l'Union internationale des télécommunications à Dubaï en 2012[14], ou de la transition de pouvoir, controversée et discutée pendant près de deux décennies, du département américain du commerce vers l'ICANN dans la supervision des fonctions de l'IANA[15].

Internet a toujours été soumis aux contextes législatifs nationaux, mais le modèle distribué qui a sous-tendu initialement son architecture et qui perdure encore – ainsi que d'autres caractéristiques techniques – rendent la mise en œuvre de lois nationales difficile dans la pratique. Les entreprises privées transnationales doivent faire face à des exigences juridiques différentes pour chacun des marchés sur lesquels elles opèrent, ou dans chaque juridiction où les utilisateurs pourraient accéder à leurs services. Les gouvernements mettent également de plus en plus en place des politiques qui imposent des contraintes aux dispositions relatives aux infrastructures techniques. Par exemple, des lois récentes sur la localisation des données sont en vigueur en différents pays et régions du monde, qui incluent la Russie, l'Amérique latine, et l'Asie. Elles imposent des restrictions sur la manière dont les informations relatives aux clients des entreprises numériques sont stockées, et exigent souvent que les données soient stockées sur des serveurs situés à l'intérieur des frontières d'un pays. Ces politiques ne concernent pas seulement les entreprises du numérique, mais toute entreprise qui stocke des données sur ses clients, ce qui inclut les services financiers et de commerce. Certaines de ces politiques sont nées d'inquiétudes concernant la vie privée des citoyens et la surveillance de la part de pays étrangers, mais elles créent des complications du point de vue de l'ingénierie, de la protection des droits de l'homme, et des modèles économiques. La concentration des données en un seul endroit peut, par exemple, rendre plus difficile la protection de la vie privée, du fait de la possibilité d'un point unique d'échec. Ces exigences ne correspondent pas non plus à la conception technique distribuée de l'Internet, ou à la manière dont les réseaux de diffusion de contenu (CDN) décentralisent et distribuent les données dans le monde entier.

[14] https://www.itu.int/en/wcit-12/Pages/overview.aspx
[15] Voir par exemple https://www.internetsociety.org/iana-transition/

Il s'agit là d'un exemple de la tension entre les contextes de gouvernance nationale et la nature distribuée et mondiale de l'Internet. Un des moyens déployés pour mitiger cette tension est la mise en place de mécanismes de gouvernance dite « multipartite ». Le pouvoir de contrôler et de gouverner l'Internet est réparti entre le secteur privé, les institutions mondiales telles que l'ICANN et l'IETF, et dans certains cas par la société civile, ainsi que par les gouvernements. C'est cette forme de gouvernance distribuée qui est souvent appelée gouvernance multipartite, et qui implique des fonctions telles que l'application des droits de propriété intellectuelle, les droits et les devoirs des intermédiaires techniques de l'Internet, l'administration du DNS et du nommage Internet (c'est-à-dire les adresses IP), et la coordination des initiatives de cybersécurité. Collectivement, ces tâches permettent de maintenir l'Internet opérationnel et d'adopter des politiques qui établissent les conditions de l'innovation et de la préservation des libertés civiles dans la sphère numérique.

Suite à l'adoption novatrice de ces stratégies de gouvernance multi-parties-prenantes ou multi-partites (qui se retrouvent, outre que dans le cas de l'Internet, dans la gouvernance d'autres systèmes socio-techniques complexes tels que l'environnement ; voir Mabi & Massit-Folléa, 2013), une piste d'investigation majeure dans les études sur la gouvernance d'Internet explore la nature et la légitimité de ce type d'arrangements, et l'équilibre des pouvoirs entre les acteurs aux différents niveaux de gestion et de coordination d'Internet. De nombreuses interrogations persistent en ce qui concerne ce mécanisme de gouvernance, et il existe de nombreux modèles et de nombreux contextes de gouvernance multipartite. Raymond et DeNardis (2015), en s'inspirant de l'étude pionnière de John Ruggie sur le multilatéralisme, proposent une taxonomie de différents types de formes institutionnelles multipartites qui varient selon la combinaison de classes d'acteurs participantes et la nature des relations d'autorité entre ces acteurs. Le spécialiste des relations internationales Joseph Nye Jr. décrit quant à lui la gouvernance d'Internet comme un « *regime complex* », appliquant la théorie des régimes à la gouvernance d'Internet pour expliquer la constellation d'institutions, d'acteurs, de normes et de politiques qui constituent collectivement une gouvernance multipartite distribuée. Selon Nye, la gouvernance de l'Internet implique « un ensemble de normes et d'institutions associées de différentes façons, qui se situent quelque part entre une institution intégrée qui impose une réglementation par le biais de règles hiérarchiques,

et des pratiques et des institutions très fragmentées sans un noyau identifiable et avec des liens inexistants » (Nye, 2014 : 9, ma traduction).

Un point critique pour comprendre la gouvernance de l'Internet est qu'il n'y a pas un seul système de surveillance et de coordination, mais toute une constellation de fonctions, chacune supervisée par différentes structures de gouvernance réparties sur un ou plusieurs acteurs. Collectivement, cette administration et cette coordination des technologies nécessaires pour maintenir Internet opérationnel, et les politiques hétérogènes édictées autour de ces technologies, sont considérées comme une gouvernance multi-partite distribuée, même si dans la pratique les arrangements multipartites sont considérablement plus compliqués et nuancés que les discours qui les entourent, autour du multi-partisme comme principe. Les chercheurs étudient donc le rôle du droit national et international dans la gouvernance d'Internet (Goldsmith & Wu, 2006 ; Weber, 2010) mais aussi le rôle décisionnel du secteur privé (DeNardis, 2014 ; Gillespie, 2014 ; MacKinnon, 2012), les institutions de coordination technique (Klein, 2002 ; Kleinwächter, 2000 ; Mathiason, 2008 ; Mueller, 2002) mais aussi les organisations internationales (Levinson & Marzouki, 2015), et, ce qui sera au centre de ce mémoire, la conception technique elle-même et les processus d'innovation et de contournement par les technologies (Braman, 2011 ; DeNardis, 2009).

Depuis longtemps, une distinction rhétorique existe entre « cyber » et « Internet » pour une série de raisons historiques et culturelles. L'utilisation du terme « cyber » fait le plus souvent référence aux domaines de la cybersécurité ou de la sécurité nationale, alors que le terme « Internet » renvoie le plus souvent, aux enjeux d'une économie numérique mondialisée, ou à l'Internet libre et ouvert, ou encore à l'Internet des objets (*Internet of Things*, IoT) (DeNardis, 2020). Du point de vue de l'ingénierie d'Internet, la distinction n'est pas pertinente, car l'infrastructure sous-jacente est la même ; il peut cependant être utile de reconnaître les manières dont les discours et les communautés de pratique autour de ces nomenclatures se construisent de façons à la fois convergentes et divergentes, car cela permet d'illustrer une autre caractéristique de la gouvernance de l'Internet : celle-ci est parsemée d'endroits à la fois physiques et virtuels où s'exerce du contrôle et qui sont, en même temps, des points de médiation entre différents systèmes de valeurs.

D'une part, la sécurité d'Internet et la sécurité nationale convergent parce que la stabilité de l'économie, de la démocratie et de la sphère publique repose désormais entièrement sur la stabilité et la sécurité d'Internet. Chaque secteur de l'économie mondiale est médiatisé numériquement et, d'une manière ou d'une autre, connecté à l'Internet en tant que réseau « public ». Les failles de sécurité d'Internet ont des effets importants sur le fonctionnement de la société. Les attaques de type *ransomware,* par exemple, ont verrouillé d'un point de vue cryptographique, et donc paralysé, plusieurs systèmes de santé jusqu'à ce que les institutions concernées succombent au paiement d'une rançon, généralement sous la forme de Bitcoin. Les violations massives, et très médiatisées, des données des consommateurs, comme celles d'Equifax[16] ou de Target[17], ont des effets dissuasifs sur la confiance des citoyens dans l'économie numérique et parfois des effets dissuasifs sur la prise de parole et les comportements en ligne. Plus important encore, la prolifération de l'IoT augmente les enjeux de sécurité, car une panne ou une perturbation des systèmes cyber-physiques peut entraîner une perte de vies humaines et pas seulement une perte d'accès aux communications. Des systèmes démocratiques stables nécessitent également, de plus en plus, une cybersécurité renforcée, comme l'ont démontré, par exemple, les révélations des agences de renseignement américaines au sujet des ingérences russes dans les listes électorales, et d'autres cyber-incursions, lors de l'élection présidentielle américaine de 2016.

Par ailleurs, la cybersécurité et la sécurité nationale comportent également des points de divergence. D'autres tendances en matière de sécurité, comme par exemple la montée en puissance de capacités cyber-offensives telles que le code Stuxnet[18], ciblant les réacteurs nucléaires iraniens, permettent de considérer le « cyber » comme le front émergent des conflits entre États-nations, ce qui est ultérieurement confirmé par la centralité des éléments cyber dans le conflit russo-ukrainien de 2022, au moment où je finalise ce mémoire[19]. Le besoin d'une sécurité renforcée pour l'économie numérique et pour la confidentialité et la confiance des individus dans le cyberespace entre en conflit avec les exigences de sécurité nationale pour l'application de la loi, la collecte de renseignements et l'accumulation de capacités en matière de cybercriminalité. Le conflit entre la tendance du marché technologique vers un chiffrement accru d'un côté, et les exigences d'accès

[16] https://www.equifaxbreachsettlement.com
[17] https://redriver.com/security/target-data-breach
[18] https://spectrum.ieee.org/the-real-story-of-stuxnet
[19] https://www.washingtonpost.com/politics/2022/03/16/cyber-conflict-ukraine-is-growing-more-complex-by-day/

important aux données manifestées par les forces de l'ordre a notamment pris forme à la suite de l'attaque terroriste de San Bernardino, en Californie (2015), lorsque les autorités ont cherché à accéder à un smartphone Apple chiffré appartenant à l'attaquant[20]. Des valeurs telles que la sécurité et la confidentialité sont toujours en tension autour des lieux où s'exerce ou peut s'exercer le pouvoir sur Internet.

Des controverses au niveau mondial pour le contrôle du cyberespace existent depuis que l'Internet s'est commercialisé et internationalisé. Un exemple frappant est la controverse géopolitique de longue date concernant la gestion et l'attribution des noms de domaine et des adresses numériques par le département américain du Commerce, y compris son accord contractuel avec l'ICANN et son autorité sur les modifications apportées au fichier de la zone racine, jusqu'à ce que cette fonction de coordination soit transférée à la communauté multipartite mondiale avec ladite « IANA transition », en 2016. Au fur et à mesure que l'importance d'Internet pour l'économie et la sphère politique a augmenté, les conflits liés à Internet ont également augmenté. Les gouvernements et d'autres forces reconnaissent notamment qu'exercer du pouvoir sur les infrastructures techniques peut servir de stratégie pour le contrôle des idées, de l'économie et de la sphère politique, ce qui sera exploré plus en détail dans le troisième chapitre. Contentons-nous de rappeler ici que, par exemple, le DNS est devenu un outil de contrôle du contenu, utilisé par exemple par la Chine et son important système de censure, afin de bloquer l'accès aux sites qui partagent illégalement du contenu piraté ou vendent des produits contrefaits. Les normes et les implémentations du chiffrement, historiquement toujours chargées politiquement, sont de plus en plus devenues la cible de gouvernements souhaitant affaiblir ou créer des portes dérobées dans les mécanismes de chiffrement à des fins de sécurité nationale ou de renseignement, opposant dans certains cas le respect et l'application de la loi à la nécessité d'assurer un fort niveau de sécurité pour l'économie numérique. Comme dans tous les domaines de la gouvernance d'Internet – et comme on le verra tout au long de ce mémoire – les batailles pour le contrôle de l'infrastructure sont des sites de conflit entre des valeurs et des intérêts concurrents.

[20] https://www.trendmicro.com/vinfo/fr/security/news/online-privacy/apple-fights-court-order-to-unlock-shooters-iphone

1.2.2. Comment étudie-t-on la gouvernance d'Internet ?

La discussion ci-dessus, qui présente un certain nombre de caractéristiques et de défis liés à la *pratique* de la gouvernance d'Internet, se traduit directement en défis, pour les *études* et les recherches qui explorent la gouvernance d'Internet. Il est utile de tracer un rapide portrait de ces défis ici[21], car ils constituent la « toile de fond » de la posture théorique et méthodologique qui a informé cette décennie de travaux.

En premier lieu, les études de la gouvernance d'Internet s'attachent à trouver des manières de rendre visible ce qui est, a priori, le plus souvent invisible et discret. Les architectures techniques et les institutions de gouvernance ne sont pas visibles de la même manière que les contenus et les usages d'Internet le sont pour ses utilisateurs. Les chercheurs doivent creuser et rendre visibles ces infrastructures cachées – dans certains cas, avant même que la recherche ne commence.

En deuxième lieu, étudier la conception et la gouvernance d'Internet nécessite un travail constant et évolutif de compréhension des technologies sous-jacentes. Les technologies de gouvernance d'Internet comprennent des milliers de protocoles, de plates-formes, d'algorithmes, de systèmes de routage et d'interconnexion, ainsi que le DNS, l'Internet des objets, les normes de chiffrement, et d'autres mécanismes d'authentification. Ces systèmes constituent l'infrastructure sous-jacente soutenant à la fois le cyberespace et le monde cyber-physique qui y est désormais intégré de façon de plus en plus étroite. Des techniques telles que l'apprentissage automatique et l'intelligence artificielle, et leur utilisation comme mécanismes de gouvernance, complique encore plus ce sujet d'étude, ce qui soulève des défis spécifiques et invite à l'interdisciplinarité.

En troisième lieu, un « faisceau » de défis est lié à la difficulté d'étudier le secteur privé (voir Joergensen, 2020), qui possède et exploite la grande majorité des infrastructures et des plates-formes d'Internet, ce qui complique davantage l'accès aux données et contribue à dissimuler parfois la technologie dans des « boîtes noires », des boîtiers propriétaires, tels que des algorithmes protégés par le secret commercial ou des brevets. Un défi lié à cette problématique est le risque de « sur-étudier » les systèmes ouverts et sous-étudier les systèmes fermés : la gouvernance de

[21] Cette liste de « défis » doit beaucoup au travail commun avec Laura DeNardis dans (Musiani et al., 2016) et (DeNardis et al., 2020).

l'Internet a été, en pratique, généralement ouverte, dans la mesure où les principales institutions de coordination, telles que l'IETF et l'ICANN, permettent l'observation participante et ont rendu les procédures et les listes de diffusion généralement accessibles. En raison de la disponibilité de plus de données, ces institutions et leurs systèmes sous-jacents sont sur-étudiés de manière asymétrique par rapport aux systèmes impliquant un contrôle propriétaire plus important. Les acteurs à la logique plus fermée, y compris les consortiums et les alliances entre acteurs du secteur privé dans de nombreux domaines technologiques émergents, sont très difficiles à étudier.

Quatrièmement, étant donné que les lieux matériels et virtuels où s'exerce la gouvernance d'Internet sont de plus en plus des points de contrôle politiques, les recherches sur ces conflits comportent une position normative de la part des chercheurs, qui s'étend au choix même de ce qu'il faut étudier dans la gouvernance de l'Internet. Presque toutes les questions de gouvernance d'Internet intègrent des valeurs contradictoires, telles que la nécessité du contrôle de la part des autorités versus la préservation des libertés civiles individuelles, la vie privée versus la liberté d'expression, l'opportunité technique versus la sécurité, le capitalisme de surveillance en opposition à la protection de la vie privée, et la sécurité des consommateurs opposée à la concurrence économique. Ou encore, des questions telles que : un Internet universel et interopérable est-il toujours souhaitable, ou dans certains contextes (par exemple pour isoler certaines applications IoT), un Internet plus « fragmenté » présente-t-il des avantages ?

En cinquième lieu, en raison de la façon dont la technologie Internet traverse les frontières, et parce que même les décisions de gouvernance locale peuvent avoir des effets mondiaux, l'étude d'un acteur ou d'un domaine problématique peut parfois passer à côté d'importants facteurs contextuels ou empiriques. En même temps, les initiatives de recherche collaborative qui combinent différentes contributions disciplinaires, méthodes, et acteurs sont prometteuses pour aborder de très vastes domaines problématiques.

Enfin, les recherches sur la gouvernance d'Internet impliquent souvent la création d'outils techniques. En raison de la taille et de la complexité massives de l'infrastructure Internet, ainsi que de la nécessité de, parfois, franchir les frontières « numériquement » pour collecter des données, la recherche implique souvent une médiation logicielle et la coproduction d'outils techniques. C'est particulièrement le cas pour les recherches qui étudient comment des pannes ou des « *kill*

switch » sont provoqués sur Internet à des fins politiques, ou encore qui les études qui évaluent les stratégies de cybersécurité, mais c'est aussi le cas des études qui examinent les façons dont le trafic circule à travers les points d'interconnexion, et qui se consacrent à l'analyse des réseaux à grande échelle[22].

Pour résumer, les chercheurs en gouvernance d'Internet fouillent et examinent les invisibles « points de contrôle » (DeNardis, 2014) qui peuplent Internet, et les implications sociales, économiques et politiques de ces points de contrôle. La recherche sur la gouvernance de l'Internet, à la mesure de la gouvernance de l'Internet elle-même, n'est pas une pratique monolithique, mais est plutôt constituée de domaines disciplinaires indépendants mais en interaction constante et croissante, ainsi que de domaines intrinsèquement interdisciplinaires tels que les études sociales des sciences et des techniques ou les sciences de l'information et de la communication.

Les approches méthodologiques et les outils employés par ces chercheurs sont divers : analyse de texte à grande échelle, analyse de réseau, méthodes statistiques, analyse de discours, observation participante, ethnométhodologie et ethnographie, entretiens sémi-directifs et questionnaires. Tout en reconnaissant et en promouvant cette diversité, une communauté épistémique d'universitaires interdisciplinaires qui ont étudié les différentes dimensions de la gouvernance de l'Internet existe explicitement. Cette communauté s'est formée discrètement pendant des années, mais elle s'est plus visiblement donnée une cohérence et une identité affichée avec la fondation du réseau académique GigaNet en 2006, juste avant le premier Forum des Nations Unies sur la gouvernance de l'Internet à Athènes. En d'autres termes, un ensemble de chercheurs en droit, en économie, en histoire, en sciences politiques, en *science and technology studies*, en sociologie et au-delà situent désormais, de manière auto-réflexive, leurs démarche et objets de recherche en tant que recherches sur la gouvernance de l'Internet. En raison de la complexité technique des systèmes de gouvernance de l'architecture Internet, bon nombre de ces chercheurs possèdent de solides connaissances de base en informatique, en ingénierie, en technologies de l'information, et des connaissances spécialisées spécifiques sur l'architecture technique sous-jacente d'Internet. En effet, cette expertise technique s'avère une compétence nécessaire même lorsque l'on étudie les lois (sur la technologie), les institutions (qui conçoivent et administrent la technologie), ou le

[22] Le Citizen Lab de l'université de Toronto est pionnier dans ce domaine : https://citizenlab.ca

secteur privées (les entreprises qui possèdent et exploitent les technologies Internet). La nécessité de posséder cette expertise technique se pose avec une acuité particulière avec les approches STS, comme on verra dans le chapitre suivant.

« Internet » et « gouvernance » sont tous deux des termes malléables dont les significations sont changeantes, d'autant plus qu'il devient de plus en plus difficile de définir ce qu'est Internet, qu'il soit basé sur une architecture technique, des communautés d'utilisateurs ou des valeurs sous-jacentes. De plus en plus d'utilisateurs d'Internet aujourd'hui sont des robots et des artefacts, plutôt que des personnes. De plus en plus de réseaux dépendent de protocoles propriétaires, en particulier dans les systèmes cyber-physiques, plutôt que de protocoles ouverts tels que TCP/IP (le protocole de contrôle des transmissions/protocole Internet). L'Internet en Chine est fort peu semblable à l'Internet en Europe ou dans chacun de ses États membres – voir à l'Internet en Russie, qu'on tend pourtant à citer avec le chinois du fait du statut de « pays autoritaires » qui est attribué à ces deux pays. La constellation de problèmes de gouvernance et de contrôle autour d'Internet détermine désormais les conditions de confidentialité, de prise de parole, d'innovation, de sécurité et de stabilité de l'économie numérique. Les chercheurs sur la gouvernance de l'Internet cherchent à faire la lumière sur ces points d'exercice du contrôle et de prise de décision critiques, qui façonneront la société pour plusieurs générations.

Avant d'examiner plus particulièrement dans le prochain chapitre comment une « discipline des disciplines » – les études sociales des sciences et des techniques ou *science and technology studies* – a pris sa place dans ce domaine, notamment au cours de la dernière décennie, la dernière partie de ce chapitre se propose de fournir une esquisse de périodisation de la gouvernance d'Internet, qui sera utile pour comprendre à la fois comment les infrastructures d'Internet ont été et sont actuellement examinées en tant qu'objets de recherche, et quel est le contexte historique dans lequel ont trouvé leur place les usages et les contournements des infrastructures à des fins de gouvernance qu'on explorera dans les chapitres à prévalence empirique de ce mémoire.

1.3. Temps et temporalités (informés par la recherche) de la gouvernance d'Internet

La naissance de la gouvernance d'Internet a eu lieu dans un contexte plus large que le développement de l'Internet lui-même. D'un côté, l'histoire des derniers siècles est parsemée d'innombrables processus de standardisation relatifs aux grandes infrastructures de transport (routes, voies ferrées…) et de distribution de l'énergie, pour en arriver aux systèmes de communication qui ont précédé puis côtoyé l'Internet, du télégraphe aux satellites. Par ailleurs, la gouvernance de l'innovation et des techniques est devenue une question de plus en plus importante et articulée au cours des dernières décennies du 20ème siècle. Des problèmes tels que la gestion de l'environnement, la disponibilité des sources d'énergie, les nanotechnologies, la maîtrise des armements et la sécurité alimentaire sont apparus comme des objets d'intérêt à part entière pour la politique transnationale, et sont désormais régis par différents instruments de résolution des conflits dans le cadre du droit international, tels que les traités, protocoles et conventions. Des exemples de ces accords sont le Protocole de Kyoto (signé en 1997) puis l'Accord de Paris (signé en 2016) sur le changement climatique, le Traité d'interdiction complète des essais nucléaires (signé en 1996) et le Traité international sur les ressources phyto-génétiques pour l'alimentation et l'agriculture (signé en 2001).

Les États nationaux ont joué un rôle central dans la négociation, la rédaction et la mise en œuvre de ces systèmes juridiques. Cependant, les enjeux de gouvernance scientifique et technique dépassent le plus souvent les frontières nationales pour traverser de multiples sphères d'action souveraine et différentes juridictions, rendant nécessaire l'élaboration de nouveaux « forums hybrides » capables de réunir experts et société civile pour discuter et co-construire des décisions sur des sujets controversés à la fois sociaux et techniques, dans une nouvelle forme de « démocratie technique » (Callon, Lascoumes & Barthe, 2009). Des analystes provenant de diverses disciplines des sciences sociales se sont penchés sur la manière dont les régimes de gouvernance scientifique et technique prennent effet à la lumière de l'internationalisation des enjeux, de la complexité des dispositifs, des frontières changeantes de la gouvernementalité, de la mondialisation des acteurs. Cet ensemble hétérogène de travaux sur la « gouvernance mondiale » aborde la manière dont ces régimes redessinent les frontières des États nationaux, et, plus généralement, comment ils reconfigurent le sens et la mise en œuvre de la démocratie (Jasanoff, 2004 ; Hagendjik et Irwin, 2006) grâce à l'intervention de nouveaux acteurs, dont le périmètre se définit autour de leur implication dans la gouvernance d'enjeux techniques complexes. C'est principalement dans ce

contexte - qui dépasse le cadre des médias et de la communication et le lie à des notions plus larges, telles que les régimes techniques et la démocratie technique - que les débats autour de la gouvernance d'Internet ont pris forme ces dernières années.

Comme on a pu l'anticiper au début de ce chapitre, la gouvernance de l'Internet a émergé à la fois comme une étiquette, un domaine de recherche, et une arène de débat et de coopération (Mueller & Badiei, 2020). Alors qu'on a pu faire l'argument que des embryons d'au moins un de ces trois aspects étaient déjà présents dans les discussions sur les premiers principes de l'interconnexion de réseaux, ou dans la convergence de l'informatique et des TIC, ce n'est sans doute qu'au début et au milieu des années 1990 qu'il est devenu clair qu'Internet posait des problèmes de gouvernance uniques, à la fois en raison de ses protocoles sous-jacents spécifiques et de ses propres organisations et institutions de standardisation, qui se sont développées au-delà et en dehors de celles de la gouvernance mondiale des télécommunications.

De manière intéressante, parallèlement à la chronologie des grandes étapes et débats de la gouvernance de l'Internet, l'état de l'art dans le domaine académique montre comment des travaux de recherche fondateurs ont contribué à co-construire le concept de gouvernance globale de l'Internet. Des approches pionnières de Milton Mueller, Lawrence Lessig et Tim Wu à *The Internet in Everything* de Laura DeNardis (2020), la notion de gouvernance de l'Internet a évolué dans la pratique également en raison des questions explicites et analytiques que les universitaires se sont posées au fil des ans sur son périmètre, nature et acteurs. Il existe bien sûr des différences dans les manières dont les périodisations et les évolutions de la gouvernance d'Internet en tant que concept ont été établies (voir par exemple Bradshaw et al., 2015, confrontée à Mueller & Badiei, 2020) ; cependant, quelques périodes et moments clés semblent consensuels[23].

1.3.1. Les premiers débats sur l'« exceptionnalisme » d'Internet
(1996 - fin des années 1990)

[23] Cette section a été réélaborée dans une contribution en langue anglaise co-écrite avec Valérie Schafer (Musiani & Schafer, 2021).

La première période est centrée autour des débats sur la compréhension d'Internet comme espace à part entière, notamment du point de vue du droit et des juridictions. Si le premier document qui vient à l'esprit comme symbole de cette phase est peut-être la « Déclaration d'indépendance du cyberespace » (1996) de John Perry Barlow, d'un point de vue politique et académique, cette phase a été marquée par des discussions sur la question de savoir si Internet devait développer son système de régulation spécifique, plus décentralisé et multi-centré, et non principalement basé sur un contrôle étatique (Johnson & Post, 1997), ainsi que par des débats sur la « souveraineté du cyberespace » (Wu, 1997). Ces débats ont alimenté l'analyse – qui a été menée, en grande majorité, par des spécialistes de droit à l'époque – de l'Internet commercial naissant, avec des questions telles que le droit des marques, le droit de la propriété intellectuelle et le règlement des litiges en ligne qui sont devenues centrales.

1.3.2. ICANN, un nouvel acteur controversé monte sur scène
(1998 - milieu des années 2000)

À la fin des années 1990, dans ce qui est probablement une nouvelle et deuxième phase dans la périodisation de la gouvernance d'Internet, les discussions sur l'exceptionnalisme d'Internet se sont « incarnées » dans un débat plus concret sur la construction d'une nouvelle institution de gouvernance d'Internet, ou d'un ensemble d'institutions dédiées. En effet, s'il y avait un consensus général sur le fait que les gouvernements et/ou les organisations intergouvernementales n'étaient pas en mesure de porter entièrement le projet de gouvernance d'Internet, la question était de savoir comment construire un nouveau cadre ou une nouvelle structure pour cette gouvernance, et qui devait le contrôler ou le coordonner.

Ces questions sont devenues particulièrement importantes avec la création de *l'Internet Corporation for Assigned Names and Numbers* en 1998 (ICANN ; Mueller, 2002). D'un point de vue politique, l'ICANN, bien que nouvelle pour sa capacité à coordonner globalement les acteurs autour des problèmes posés par les ressources Internet critiques, était controversée en raison du rôle des États-Unis dans sa naissance et dans l'établissement de ses prérogatives. En tant qu'entreprise privée, bien que mondiale, à but non lucratif, l'ICANN a été habilitée par les États-Unis à émettre des contrats privés comme moyen de résoudre certains problèmes de politique

publique, et à avoir l'autorité exclusive sur les noms de domaine racine et les espaces d'adressage Internet, tout en expérimentant avec de nouvelles « expériences démocratiques » telles que des élections mondiales pour son conseil d'administration. Les chercheurs ont à leur tour analysé l'ICANN comme la quintessence de la nouvelle gouvernance en réseau pour l'ère numérique (Levinson, 2002), examiné comment les États-nations et leurs gouvernements ont joué un rôle dans la formation et le développement de l'ICANN, en particulier son ambigu Comité consultatif gouvernemental (GAC ; Weinberg, 2011), et ont critiqué la légalité – et surtout la légitimité – du modèle de gouvernance proposé par l'ICANN (Froomkin, 2000). Cette phase a également été marquée par des décisions judiciaires qui ont fait école, telles que *Yahoo! vs. France*, où un tribunal français a ordonné au géant de l'Internet Yahoo! de bloquer l'accès des internautes français sur un certain nombre de ses sites d'enchères vendant des souvenirs nazis (Goldsmith & Wu, 2006).

1.3.3. Le SMSI, un espace de discussion global
(2003 - premières années 2010)

Le Sommet mondial de la société de l'information (SMSI, WSIS en anglais pour *World Summit on the Information Society*), un sommet des Nations Unies, organisé en deux phases en 2003 (Genève) et 2005 (Tunis), est très probablement le processus principal qui incarne la troisième phase de la périodisation de la gouvernance d'Internet – un processus autour duquel la gouvernance de l'Internet en pratique, et la structuration de la gouvernance d'Internet en tant que domaine d'étude, ont convergé. Des importants débats sur la définition de la gouvernance d'Internet ont eu lieu tout au long du processus du SMSI, avec une variété de positions, allant des extrêmes de la seule gestion critique des ressources Internet par l'ICANN d'une part, à la réglementation de l'ensemble du spectre des TIC d'autre part. Une contribution pionnière aux efforts de définition a été fournie par le Groupe de travail sur la gouvernance de l'Internet (WGIG pour *Working Group on Internet Governance*) mandaté par le SMSI en 2004, qui a parlé de « principes, normes, règles, procédures de prise de décision et programmes partagés qui façonnent l'évolution et l'utilisation de l'Internet », et a fait clairement pour la première fois l'argument que l'IG était une question dite « multipartite », les acteurs concernés étant non seulement les États-nations, mais aussi les entreprises et la société civile dans ses différentes facettes (communauté technique, associations de libertés civiles et citoyens en leur capacité individuelle).

Le multipartisme en tant que nouvel arrangement de gouvernance est rapidement devenu un sujet de recherche central sur la gouvernance d'Internet pour des spécialistes dans une variété de domaines (une bonne critique se trouve dans Raymond & DeNardis, 2015), avec une attention particulière accordée à la capacité de la société civile de participer de manière significative aux processus d'IG (Hintz, 2005). Parmi les déceptions (exprimées en particulier par les acteurs qui souhaitaient que le SMSI dépasse le rôle unilatéral et prédominant des États-Unis dans l'ICANN, ce qu'il n'a pas réussi à réaliser), le SMSI a donné naissance à un espace de discussion mondial sur la gouvernance de l'Internet qui se poursuit à ce jour, non sans son lot de critiques : l'Internet Governance Forum ou IGF (voir Malcolm, 2008 pour une analyse de ses débuts). Fait intéressant, la principale association savante sur les questions de gouvernance d'Internet, GigaNet, est née du Forum sur la gouvernance de l'Internet et tient toujours sa conférence annuelle la veille du début officiel de l'IGF, ce qui contribue à éclairer le rapport spécifique entre les recherches sur la gouvernance d'Internet et leur objet : gouvernance et recherche sur la gouvernance sont étroitement liées, et nées quasi dans le même mouvement.

1.3.4. Une gouvernance d'Internet « post-Snowden » ? Nouveaux périmètres et enjeux (milieu des années 2010 - présent)

Les discussions sur la définition de la gouvernance d'Internet continuent d'être une question centrale en soi. En effet, la dernière – et actuelle – phase d'une hypothétique périodisation de la gouvernance d'Internet est marquée par une discussion en cours sur son périmètre et par l'inclusion d'un certain nombre de problèmes, au fur et à mesure qu'ils ont émergé et pris le devant de la scène dans l'arène politique mondiale. Pour plusieurs chercheurs dont Laura DeNardis (2014), la gouvernance d'Internet en soi doit être distinguée et traitée séparément des pratiques, usages et création et diffusion de contenus sur Internet, tandis que d'autres chercheurs soutiennent que la gouvernance d'Internet pourrait inclure de manière significative la « puissance d'agir » (*agency*) des concepteurs de technologies, des décideurs et des utilisateurs, car ceux-ci interagissent, de manière distribuée, avec les technologies, les règles et les réglementations, entraînant des conséquences imprévues avec des effets systémiques et pragmatiques vis-à-vis la (re)distribution du pouvoir sur Internet (Epstein, 2015 ; Musiani, 2015). Mettant l'accent sur la nature distribuée

et diffuse du pouvoir sur le réseau des réseaux, les chercheurs ont également fait valoir que cette configuration peut conduire à un manque de clarté sur l'endroit où réside l'autorité réelle de gouverner, en bref, « où est la gouvernance dans la gouvernance de l'Internet » (van Eeten et Mueller 2013 ; voir également Hofmann, Katzenbach & Gollatz, 2016).

Quelle que soit la position des spécialistes dans ces débats, on peut déjà en conclure qu'ils reflètent une évolution cruciale de la gouvernance de l'Internet en tant que domaine de pratique : alors qu'un certain nombre d'arènes et d'institutions politiques telles que le SMSI ou le Forum sur la gouvernance de l'Internet ont été examinées de près par les chercheurs, plusieurs questions qui *de facto* concernent la gouvernance d'Internet se développent de plus en plus « dans l'espace largement non institutionnalisé formé par les services et le commerce Internet transnationaux » (Mueller & Badiei, 2020). Ces problèmes incluent la neutralité du réseau ; les techniques de réglementation du contenu sur Internet (filtrage, blocage, techniques d'inspection approfondie des paquets ou *deep packet inspection*) ; les techniques de censure et de contournement ; l'intermédiation et la réglementation du contenu et de l'infrastructure gérées par le secteur privé ; la cybersécurité, la sécurité de l'information et les marchés associés ; la responsabilité des intermédiaires en ligne dans des situations telles que la diffamation, les violations du droit d'auteur et les litiges concernant les pratiques de commerce électronique.

La question prééminente liée à la gouvernance d'Internet de la dernière décennie est peut-être – catalysée par les révélations d'Edward Snowden, mais ayant ses racines dans des débats de longue date sur les données personnelles, l'identité sur Internet et le chiffrement – celle de la surveillance et de la confidentialité en ligne. En exposant des documents internes de la National Security Agency des Etats-Unis, qui révélaient l'étendue de sa surveillance mondiale omniprésente sur le réseau des réseaux, l'ancien contractant de la NSA a ouvert l'ère d'une « politique Internet post-Snowden » (Pohle & Van Audenhove, 2017), où le monde a pris toute la mesure de l'étendue de l'autorité mondiale « par l' infrastructure » que les États-Unis exercent de facto sur Internet, et a pris conscience de la profondeur des « liaisons dangereuses » du gouvernement américain avec les intermédiaires privés (Musiani, 2013). Cela a profondément mis en crise la légitimité des États-Unis de continuer à agir en tant qu'acteur principal de l'IG, et sans doute – même si ce processus était, lentement mais sûrement, déjà en cours avant Snowden – a contribué à la finalisation de

ladite « transition IANA », le processus au cours duquel les États-Unis ont renoncé à leur contrôle de la racine DNS, et qui est à l'origine de réformes substantielles dans les mécanismes de responsabilité de l'ICANN.

En parallèle, les années 2010 ont également vu la montée et/ou la stabilisation de nouvelles « superpuissances » dans la gouvernance d'Internet, notamment la Russie et la Chine (voir par exemple Litvinenko, 2021 et Negro, 2017), avec une stratégie prédominante de « souveraineté numérique » – l'idée que les États devraient réaffirmer leur autorité sur Internet et protéger l'autodétermination de leur nation dans la sphère numérique, non pas au moyen d'alliances supranationales ou d'instruments internationaux, mais en augmentant leur indépendance et leur autonomie aux niveaux technique, économique et politique. Enfin, des instruments juridiques tels que le RGPD, entré en vigueur en mai 2018, ont posé de nouvelles conditions en termes à la fois de la protection des données et de la gouvernance des plateformes, incarnant un enjeu – et un défi – réglementaire majeur pour les modèles économiques basés sur la récolte de données et l'offre de services « gratuits » en contrepartie.

1.3.5. « Plusieurs gouvernances » et « l'Internet de tout »

De plus, les questions de gouvernance ont envahi plusieurs domaines et institutions liés aux TIC et aux technologies numériques, tels que le Web, les infrastructures de recherche, Wikipédia et les archives Web en tant que « patrimoine nativement numérique ».

Comme on a pu l'explorer dans Musiani et Schafer (2018), le développement du World Wide Web, qui a émergé à la fin des années 1980 et surtout au début des années 1990, a englobé dès le départ des questions de gouvernance. Après sa genèse à l'Organisation européenne pour la recherche nucléaire (CERN), le Web a « déménagé » aux États-Unis, lorsque Tim Berners-Lee a rejoint le Massachusetts Institute of Technology (MIT) et a créé le World Wide Web Consortium (W3C) en 1994. Les procédures de l'Internet Engineering Task Force (IETF) étant estimées trop lentes pour l'évolution rapide du Web que Berners-Lee envisageait, il a établi un consortium dédié. Andrew Russell note que « le modèle du W3C occupe une terre de milieu entre l'IETF et l'ICANN : il contrecarre la lenteur du développement du code 'par le bas' en développant du code au sein du

W3C lui-même ; en incluant des membres de l'industrie, ses recommandations sont plus susceptibles d'être mises en œuvre rapidement et efficacement ; il considère également sérieusement et répond aux commentaires des membres et du grand public avant de publier le code en tant que recommandation » (Russell, 2003 : 28). Le W3C partage par ailleurs certains des enjeux de longue date de la gouvernance de l'Internet, notamment la normalisation, l'ouverture et le multipartisme.

Moins évidemment liées au problème de la gouvernance, mais néanmoins fortement liées à des questions telles que les normes, les communs, les droits d'auteur et le multipartisme, les initiatives d'archivage du Web sont une bonne étude de cas pour analyser la manière dont de nombreuses parties prenantes participent et négocient la gouvernance du patrimoine nativement numérique. En effet, les acteurs impliqués dans la gouvernance des archives Web comprennent des fondations (par exemple, Internet Archive), des organisations transnationales (par exemple, l'International Internet Preservation Consortium), des professionnels (bibliothécaires, archivistes), des représentants de la société civile (notamment des militants et des chercheurs) et des entreprises privées (par exemple, Facebook et Twitter ont leurs propres archives). Toutes ces parties prenantes mettent sur la table leurs propres approches divergentes du patrimoine numérique natif, des formats propriétaires à une vision ouverte des archives Web en tant que biens communs (voir Musiani et al., 2019). La typologie de la gouvernance d'Internet rédigée par Bing et Bygrave (2009), décrivant plusieurs types d'organisations et de rapports de force à l'œuvre dans la gouvernance d'Internet, est utile ici pour rendre compte de la gouvernance technique en jeu dans des arènes particulières (par exemple, les robots et les métadonnées). Elle permet également de rendre compte des différentes revendications de la société civile pour plus d'inclusivité (p. ex. l'initiative Documenting the Now[24], née en 2019 en lien avec le mouvement Black Lives Matter), de comprendre la variété des intérêts privés et commerciaux impliqués dans l'archivage du Web (p. ex. la présence de Facebook, Amazon et Twitter parmi les principaux acteurs des pratiques d'archivage du Web), et de saisir les tentatives nationales de conserver les archives du Web dans le patrimoine national (p. ex. les dépôts légaux des archives du Web en France, au Royaume-Uni, etc.).

[24] https://www.docnow.io

Les infrastructures numériques de recherche et les infrastructures de la connaissance tentent également de tester et de développer de nouvelles formes de gouvernance. Wikipédia est le meilleur exemple d'un cadre dans lequel la gouvernance d'une plate-forme d'organisation de la connaissance essaie d'inclure des questions telles que les communs, l'auto-organisation et l'autorité partagée (Cardon, 2012).

Enfin et surtout, la dernière frontière (pour l'instant) de la gouvernance de l'Internet est le problème que Michel van Eeten a récemment décrit comme « la disparition de la distinction entre les appareils avec et les appareils sans connectivité et capacités informatiques » (van Eeten, 2017) et que Laura DeNardis (2020) a résumé, dans le titre de son dernier livre, comme « l'Internet dans tout » : l'Internet en tant que réseau de réseaux devient la méta-infrastructure de la plupart des autres infrastructures, avec des implications cruciales pour l'économie, la sécurité et la gouvernance. Alors qu'on a longtemps cru que l'influence des acteurs du numérique resterait confinée aux logiciels, aux contenus dématérialisés et à l'information, il commence à être clair que ces acteurs usent de leur maîtrise de ces domaines pour se positionner sur les marchés non numériques, qu'il s'agisse des transports, la gestion des infrastructures, la santé ou les transactions bancaires.

Avec la connexion des infrastructures et des objets, l'organisation des flux physiques nécessite la maîtrise des flux d'information. Des quantités massives de données sont au cœur de ce mouvement, qui remet en cause les positions des acteurs historiques sur ces marchés. À terme, cela générera de nouvelles interactions entre la gouvernance de l'Internet et la gouvernance d'autres systèmes sociotechniques, qui sont actuellement discutées et mises en œuvre dans des cadres encore très largement séparés. Cela pourrait éventuellement conduire à des convergences sans précédent entre les institutions et les forums examinant, par exemple, la gouvernance de l'Internet et la gouvernance de l'environnement ou de la santé.

Chapitre 2. L'apport des *science and technology studies* à l'étude de la gouvernance d'Internet

Si dans le chapitre précédent on a souhaité donner un panorama inclusif des façons de cadrer, théoriser, s'intéresser à la gouvernance d'Internet comme objet de recherche – des plus traditionnelles aux émergentes – on a déjà pu commencer à montrer, notamment à la fin du parcours historique, ce que peut apporter une perspective dérivée des *science and technology studies* (STS). Ces spécificités font l'objet de ce chapitre.

L'ensemble de recherches qui ont adopté une perspective inspirée des STS pour étudier la gouvernance d'Internet a commencé à se développer dans la deuxième décennie des années 2000. Trois inspirations différentes des STS ont irrigué les travaux sur la gouvernance d'Internet. En premier lieu, complémentaires aux approches principalement institutionnelles qui définissaient l'agenda de la recherche sur la gouvernance d'Internet à ses débuts – et y figurent toujours en bonne place – les approches STS examinent la « capacité d'agir » ou « puissance d'agir » des concepteurs de technologies, des décideurs et des utilisateurs, ainsi que des artefacts techniques eux-mêmes, lorsqu'ils interagissent, de manière distribuée, avec les autres systèmes normatifs sur Internet, le droit en premier lieu, entraînant des conséquences systémiques qui peuvent parfois être involontaires. En deuxième lieu, l'ordre social et politique construit par les processus d'IG est compris comme un ensemble de processus continus et contestés – un ensemble de pratiques banales (*mundane*) qui contribuent à maintenir, pirater, contourner, développer, tester ou utiliser Internet. Ainsi, sur le plan conceptuel, la recherche sur la gouvernance de l'Internet inspirée des STS repose sur la compréhension de la gouvernance en tant que « système de systèmes » normatif, et elle cherche à retracer les actions et les pratiques, souvent discrètes mais omniprésentes, des acteurs et des infrastructures humains et non humains. En troisième lieu, les études des controverses et les études des infrastructures ont été mobilisées comme outils conceptuels et méthodologiques pour rendre compte de la co-construction, et des façons d'aborder les problèmes qui constituent le champ de la gouvernance d'Internet.

Le chapitre s'ouvre en retraçant comment les STS ont d'abord approché Internet en tant que sujet d'étude, et en examinant comment certains concepts clés de STS ont trouvé leur place dans les *Internet studies*. Il aborde ensuite certains aspects clés des STS ainsi qu'on a pu les rapprocher des recherches sur la gouvernance d'Internet : par exemple, les assemblages et les arrangements hybrides comme moyen d' « ordonner » dans la gouvernance de l'Internet, et les effets structurels et performatifs des controverses sur l'élaboration de normes et la prise de décision.

Ensuite, le chapitre aborde de plus près la manière dont les approches de gouvernance d'Internet fondées sur les STS analysent les effets structurants et performatifs des controverses sur la gouvernance. Il examine comment les controverses autour des revendications de gouvernance d'Internet (Epstein, Katzenbach & Musiani, 2016), portées par différents acteurs ou groupes, contribuent à la création de différents mondes dans lesquels des notions spécifiques de gouvernance ont un sens. Le chapitre discutera de la manière dont l'étude des controverses « décompose » la gouvernance en tant que concept théorique et opérationnel, en exposant la pluralité des notions auxquelles elle se réfère et leurs conflits potentiels (Cheniti, 2009 ; Ziewitz & Pentzold, 2014).

Enfin, le chapitre montre comment les approches STS de la gouvernance d'Internet se concentrent sur la « puissance d'agir » des acteurs « non humains », tels que les infrastructures, en tant que lieux de médiation de la gouvernance : par exemples, les intermédiaires des flux d'information, les ressources Internet critiques, les points d'échange Internet et les dispositifs de surveillance et de sécurité (Musiani et al., 2016). Le chapitre abordera comment la gouvernance de l'Internet prend forme à travers une myriade d'architectures et d'infrastructures techniques, des « points de contrôle » (DeNardis, 2014 : 11) souvent discrets et invisibles, mais néanmoins cruciaux dans la construction d'un « réseau de réseaux » de plus en plus public et complexe.

2.1. Les STS rencontrent les *Internet studies*

C'est désormais presque une « évidence de recherche » qu'Internet est un artefact socio-technique ; cependant, il peut être utile de rappeler que tous les processus menés sur et par le biais

d'Internet ont à la fois une composante technique et une composante humaine, y compris des approches de gouvernance. En effet, comme l'ont bien montré des articles fondateurs tels que celui de DiMaggio et al. (2001) au tournant du millénaire, Internet en tant que sujet de recherche a des « implications sociales » qui rendent son analyse tout à fait pertinente pour les chercheurs en sciences sociales.

Les approches issues des STS font partie des outils que les chercheurs en sciences sociales ont mobilisé pour enquêter sur le lien complexe entre Internet et la société. Janet Abbate note que

> *Les STS peuvent être utiles pour aborder les liens complexes entre la technologie Internet et la culture, qui ont brouillé les frontières des catégories traditionnelles. L'un des principes des STS est d' « ouvrir la boîte noire » de la technologie pour comprendre son fonctionnement et comprendre comment les relations sociales et les objectifs [de parties de la société] se traduisent en artefacts. Les STS proposent également des modèles pour décrire comment les acteurs humains et non humains exercent une action conjointe dans des environnements médiatisés (Abbate, 2012 : 170)*

Le « tournant STS » des recherches s'intéressant aux technologies de l'information et de la communication (TIC) est fondé sur l'intérêt de la sociologie de l'innovation pour les objets techniques et les pratiques sociales d'appropriation des technologies émergentes, sur l'intérêt croissant de la sociologie des médias pour les TIC, et sur le développement des sciences de l'information et de la communication en tant que discipline : les TIC deviennent des « artefacts interactionnels » (de Fornel, 1994 : 126). Avec l'avènement d'Internet, un champ d'études interdisciplinaire centré sur cet objet naît à la fin des années 1990 : c'est la création des *Internet studies*. Le tournant STS au sein de ce champ appelle une attention particulière au contexte et aux pratiques situées, ainsi qu'au dévoilement du travail invisible de l'innovation sur Internet. Les approches STS mettent l'accent sur les pratiques qui façonnent la gestion et la gouvernance d'Internet et de ses usages en tant que réalité vivante, et qui déterminent les manières dont il opère, travaille, résiste et fonctionne. De plus, les approches STS invitent à considérer les valeurs et les rationalités des praticiens d'Internet et du Web non pas comme des indicateurs de leur perception du monde, mais comme des ressources et des catégories qu'ils déploient dans des circonstances spécifiques afin de créer et de maintenir des configurations spécifiques – d'organiser activement leur monde (Cheniti, 2009).

Les STS ont permis de reconnaître le statut de médiateurs des artefacts techniques, dans la mesure où ils peuvent modifier la portée des actions sociales, au sens du « *politics by other means* » de Bruno Latour (1988) et des « *politics of artefacts* » de Langdon Winner (1986). Dans cette conception, il est moins pertinent de considérer les discours et les objets comme des sphères séparées que de comprendre les discours comme circulant au sein des objets, les deux sphères se co-construisant (Gillespie, Boczkowski & Foot, 2014).

Les notions de dispositif et d'objet-frontière font partie des concepts STS fondateurs qui ont été saisis par ce courant des *Internet studies*. Un dispositif sociotechnique est défini comme un assemblage d'acteurs humains et non humains, dont les compétences et les performances sont distribuées. De plus, la notion permet d'intégrer à l'analyse l'*agency*, que Serge Proulx a traduit par « puissance d'agir » (Proulx, 2009), pour une appréciation plus fine de sa dimension collective. Avec le concept d'objet-frontière, Susan Leigh Star et James Griesemer (1989) ont quant à eux cherché à décrire analytiquement ces processus dans lesquels des acteurs issus de mondes sociaux différents, et appelés à coopérer, parviennent à se coordonner malgré leurs points de vue divergents. Parce qu'ils rendent compte des processus de délégation du travail ou d'autres activités, ou de l'action performative des artefacts dans la production de connaissances, les objets-frontière permettent de conceptualiser le travail de coordination, d'alignement, d'alliance et de traduction entre les différents acteurs et les mondes qu'ils mobilisent (voir pour une discussion approfondie de la notion Trompette et Vinck, 2010).

Ces notions – qui sont à la fois des concepts et des outils méthodologiques pratiques – ont été reconnues comme utiles, aux côtés des approches en sociologie, science politique, droit international et économie, pour aborder les macro-questions de politique et de pouvoir liées à la gouvernance de l'Internet en dévoilant les micro-pratiques de la gouvernance en tant que mécanismes de coordination distribuée, semi-formelle ou réflexive (Hofmann, Katzenbach et Gollatz, 2016), d'ordonnancement privé (Elkin-Koren, 2012) et d'utilisation des ressources Internet.

2.2. Les STS rencontrent la gouvernance d'internet

Les notions de dispositif et d'objet-frontière ne sont que deux parmi les concepts et outils que les chercheurs en STS ont développés pour étudier l'ordre social, un « effet généré par des moyens hétérogènes » (Law, 1992 : 382), rendant les processus quotidiens et évolutifs d'ordonnancement – d'ordre économique, politique, discursif, technique ou autre – l'objectif principal de l'interrogation scientifique. Dans ce contexte, la gouvernance est comprise comme un ensemble de dynamiques d'ordre social, qui ne se produit pas exclusivement (et, peut-être, pas principalement) dans des institutions politiques, mais est également mise en œuvre par des pratiques « banales et quotidiennes », ordinaires (*mundane* ; voir Cheniti, 2009) de personnes engagées dans le maintien ou la remise en cause de l'ordre social (Flyverbom, 2016 ; Woolgar et Neyland, 2013). Cette approche à l'étude de l'ordre social implique de nouvelles manières de questionner et de réassembler ce que nous considérons à la fois comme Internet et sa gouvernance. En effet, cette sensibilité à l'ordre social en tant que processus continu et contesté se traduit par une attention croissante aux pratiques ordinaires de ces acteurs qui sont impliqués dans la gestion et la maintenance, le développement et le test, ou encore le piratage ou le contournement de certains aspects du réseau des réseaux (Musiani, 2015), élargissant ainsi la notion de ce qu'est la gouvernance dans la gouvernance d'Internet. Ces diverses pratiques ne sont pas considérées comme de simples objets de régulation, mais comme des éléments constitutifs de l'articulation, de la réification et de la remise en cause des normes établies, émergentes ou contestées – ce qu'on a appelé le « faire » la gouvernance d'Internet (*doing Internet governance* ; Epstein, Katzenbach & Musiani, 2016).

La perspective STS invite également à reconsidérer le fait qu'établir une définition ou un périmètre précis unique de la gouvernance d'Internet soit une condition préalable obligatoire à toute enquête significative (Ziewitz & Pentzold, 2014). Les approches STS considèrent même qu'une telle opération de définition a priori pourrait aller au détriment de la compréhension de certaines des manières dont la gouvernance d'Internet est forgée ou adoptée, de manière distribuée, en réseau, et souvent invisible.

Conceptuellement, la recherche sur la gouvernance de l'Internet fondée sur le STS repose sur la compréhension de la gouvernance en tant que « système de systèmes » normatif, et elle reconnaît la puissance d'agir, souvent discrète et omniprésente, des acteurs et des infrastructures humains et

non humains. Empiriquement, la recherche sur la gouvernance de l'Internet fondée sur le STS se concentre sur les dynamiques d'ordonnancement des assemblages et des arrangements hybrides de la gouvernance ; sur les effets structurels et performatifs des controverses et des déstabilisations sur la normalisation et la prise de décision, ou sur la construction de l'autorité et de la confiance ; et enfin, sur les forums hybrides, les arrangements privés, les utilisateurs et leurs pratiques. Tous ces éléments contribuent à étoffer la compréhension de ce qu'est ou peut être la gouvernance de l'Internet et peuvent être utiles pour revisiter certains de ses concepts centraux, mais encore définis de façon floue, tels que le multipartisme. Dans Epstein, Katzenbach & Musiani (2016) on a détaillé ces aspects clés, une discussion que je reprends et développe ici.

Premièrement, les approches STS reconnaissent que la gouvernance technique et politique sont inextricablement liées. Plusieurs spécialistes de la gouvernance d'Internet reconnaissent de plus en plus largement la pluralité de ces modes de gouvernance ; l'étape suivante consiste à intégrer leur incapacité à être complètement séparés. Il s'agit de comprendre la gouvernance de l'Internet comme coexistence de différents types de normes, élaborées dans une variété d'arènes partiellement juxtaposées, et appliquées, mises en œuvre ou parfois simplement suggérées via une pluralité de systèmes normatifs : droit, technologie, marchés, discours et pratiques (Brousseau, Marzouki & Méadel, 2012). Ten Oever, Milan et Beraldo (2020) donnent un aperçu utile de la mosaïque qui constitue cette multiplicité de sources normatives et soulignent à juste titre que certaines caractéristiques normatives qui n'avaient pas été techniquement intégrées à Internet à ses débuts (car, bien sûr, plusieurs de ses développements spectaculaires n'étaient pas prévisibles) ont dû, par la suite, faire l'objet d'une rétro-ingénierie, ou compensés par d'autres sources normatives ; par exemple, l'ensemble de spécifications DNSSEC (Domain Name System Security Extension) a ajouté des caractéristiques de protection et de robustesse au système de noms de domaine de l'Internet (DNS) qui, à ses débuts, ne prévoyait aucune fonctionnalité liée à la sécurité.

Reconnaissant ces diverses origines de normes pertinentes pour l'utilisation et la conception d'Internet, la plupart des chercheurs sur la gouvernance d'Internet informés par les STS fondent leur compréhension de la gouvernance sur l' « ordonnancement » (*ordering*) plutôt que sur la réglementation, la gestion ou le contrôle (Elkin-Koren, 2012 ; Flyverbom, 2011). Selon ces auteurs, le concept d'ordonnancement est utile non seulement pour saisir l'effet normatif des pratiques ordinaires et des routines quotidiennes ; il est également considéré comme

particulièrement bien adapté à l'analyse des formes organisationnelles de la politique mondiale non pas en tant qu'entités statiques mais en tant qu'assemblages – des configurations hybrides refaçonnant constamment leurs objectifs et leurs procédures afin de connecter et de mobiliser des objets, des sujets et d'autres éléments autour de problèmes particuliers. Dans cette optique, les institutions mêmes de la gouvernance de l'Internet peuvent également être explorées avec une approche basée sur les STS, comme Mikkel Flyverbom (2011) l'a fait pour les Nations Unies, cherchant à saisir la complexité des accords de la gouvernance politique mondiale au moyen de l'observation de ses pratiques intégrées dans des contextes particuliers et évoluant au fil du temps.

Une caractéristique importante des approches STS est l'investigation des acteurs et des infrastructures non humains en tant que lieux de médiation. En effet, les intermédiaires de l'information, les ressources Internet critiques, les points d'échange Internet et les dispositifs de surveillance et de sécurité jouent un rôle de gouvernance crucial aux côtés des institutions politiques, nationales et supranationales et des organisations de la société civile (Musiani et al., 2016). La gouvernance de l'Internet prend forme à travers une myriade d'infrastructures, d'appareils, de flux de données et d'architectures techniques qui sont souvent dans les coulisses, mais cruciales dans la construction d'un réseau de réseaux de plus en plus public, articulé, et complexe. Laura DeNardis (2014 : 11) définit ces entités comme des « points de contrôle » infrastructurels autour desquels s'enchevêtrent des questions d'efficacité technique et économique, ainsi que des négociations sur des valeurs humaines et sociétales telles que les droits de propriété intellectuelle, la confidentialité, la sécurité, la transparence.

Les discussions académiques et politiques sur la « gouvernance des algorithmes » se connectent à cet aspect et explorent les qualités de gouvernance et d'exercice du pouvoir que différents acteurs inscrivent au sein des algorithmes eux-mêmes (Mager, 2012 ; Ziewitz, 2016) lorsque ceux-ci prédisent et personnalisent le comportement des utilisateurs sur Internet et sa perception par d'autres acteurs (institutions, entreprises). Dans la lignée de cette approche, et un peu moins récemment, les contributions STS ont fourni un apport important à l'étude de la privatisation de la gouvernance de l'Internet (que Laura DeNardis a explorée dans plusieurs contributions, p. ex. 2010), c'est-à-dire comment les décisions et les actions qui s'appliquent à la gouvernance sont de plus en plus prises par des entités privées, en particulier par une poignée de « géants d'Internet » tels que Google et Facebook qui, en raison de leur taille et de leur statut de quasi-monopole, sont

en mesure d'établir des normes *de facto* dans plusieurs domaines considérés traditionnellement comme relevant des politiques publiques. Comme l'explique Rikke Frank Jørgensen (2020), la privatisation de la gouvernance de l'Internet pose également des défis méthodologiques au chercheur, en raison de la lourde dimension de secret industriel entourant les activités des géants d'Internet. En outre, l'omniprésence et la quantité considérable de données produites et disponibles sous forme numérique, ainsi que la multiplicité des méthodes à la disposition des sociétés Internet pour leur donner un sens, ajoutent des implications supplémentaires à la privatisation de la gouvernance de l'Internet en termes d'asymétrie informationnelle, de problèmes de confidentialité et de surveillance (Hall et al., 2020).

Une autre manière dont les approches STS ajoutent aux perspectives institutionnelles sur la gouvernance de l'Internet est la reconnaissance du rôle central des pratiques ordinaires et « considérées comme acquises » dans la constitution de la conception, de la réglementation et de l'utilisation de la technologie. Elles attirent l'attention, par exemple, sur les actions et les stratégies d'individus particuliers dans l'articulation des normes Internet, ou sur la façon dont l'instabilité a été intégrée au début d'Internet afin d'assurer la possibilité d'un changement constant (Braman, 2016), sur les aspects sociaux de l'élaboration et de la mise en œuvre de politiques liées à Internet, ou encore sur comment les formes non traditionnelles de participation aux débats sur les questions de gouvernance d'Internet (par exemple le multipartisme) s'institutionnalisent (Epstein, 2013). Cette partie des approches STS suggère que la gouvernance d'Internet, en tant que système sociotechnique, est une dynamique sociale autant que politique.

Les approches à la gouvernance d'Internet fondées sur les STS abordent également les effets structurants et performatifs des controverses sur la gouvernance. Plus particulièrement, elles analysent comment les controverses autour des revendications, exprimées par différents acteurs ou groupes, sur « faire la gouvernance d'Internet » contribuent en pratique à la création de différents mondes où des notions spécifiques de gouvernance ont un sens (Epstein, Katzenbach & Musiani, 2016). Ainsi, l'étude des controverses dé-compose la gouvernance comme concept théorique et opérationnel, en exposant la pluralité des notions auxquelles elle renvoie et les conséquences de leur mise en conflit (Cheniti, 2009 ; Ziewitz & Pentzold, 2014). Les processus par lesquels les normes sont créées, renégociées, mises à l'épreuve, réalignées et suscitent des conflits sont tout

aussi importants – et peut-être même plus importants – dans les analyses STS que les normes stabilisées elles-mêmes (De Filippi & Loveluck, 2016 ; Musiani, Mallard & Méadel, 2018).

Pour résumer, plusieurs notions et sensibilités STS peuvent aider à dévoiler un certain nombre de pratiques situées sur, par et pour Internet qui constituent sans doute une partie vitale de la gouvernance d'Internet. Par exemple, comprendre la gouvernance de l'Internet à travers le prisme des « forums hybrides » de Callon, Lascoumes et Barthe (2009) – entités censées transformer les controverses en dialogue productif et « produire » de la démocratie – peut enrichir et revisiter le concept de multipartisme (Malcolm, 2008) en mettant l'accent sur le positionnement des acteurs et l'évolution de leurs relations les uns avec les autres. Ou encore, la nature « inscrite dans la technologie » de la plupart des types d'interventions du secteur privé dans la gouvernance de l'Internet peut être mise en évidence par les méthodes STS. Examiner la relation des internautes avec leurs dispositifs et avec les valeurs qu'ils véhiculent relève de la gouvernance dans la mesure où elle reflète leur engagement vis-à-vis d'un ensemble de normes et d'une communauté (Elkin-Koren, 2012).

Compte tenu du contexte social, économique et politique actuel dans lequel Internet en tant que « dispositif de dispositifs » est placé, on souhaite ici mettre en relief trois aspects qu'on considère comme particulièrement importants à aborder, dans la « galaxie » gouvernance d'Internet, avec des approches et outils STS. Le premier est le développement, formel et informel, de standards dans l'espace d'Internet ; le second est l'effet structurant et performatif des controverses sur la gouvernance ; le troisième est la puissance d'agir des acteurs non humains, notamment des infrastructures, en tant que lieux où la gouvernance est mise en œuvre et reconfigurée. Ce dernier aspect sera introduit ici, avant qu'un chapitre y soit plus spécialement dédié, comme dernière partie du cadrage théorique de ce mémoire.

2.2.1. La standardisation, mise en dialogue et interface des normes techniques

La standardisation est de longue date un objet d'étude pour les STS. Dans un ouvrage pionnier, Bowker et Star (1999) avaient dressé un programme d'étude des normes applicables à la nomenclature et à la catégorisation. Ils y décrivent de manière remarquable la machine de

classification raciale de la population durant l'Apartheid en Afrique du Sud, ainsi que les trajectoires et les contraintes qu'elle imposa à la vie personnelle et professionnelle des individus dans ce pays. Le programme élaboré par Bowker et Star est développé et élargi dans l'ouvrage de Timmermans et Berg (2003), *The gold standard*, et dans le volume collectif *Standards and their stories* (Lampland et Star, 2009). D'autres travaux regroupés par Brunsson et Jacobsson (2000), Higgins et Larner (2010) et Ponte *et al.* (2011) présentent une perspective organisationnelle et de gouvernance sur la normalisation des processus, les publications sur les normes applicables aux technologies de l'information et de la communication, et leur utilisation dans la normalisation des comportements et de l'organisation sociale.

Pour Schmidt et Werle (1998), la conformité des appareils de télécopie aux normes Groupe III mises au point à l'Union internationale des télécommunications dans les années 1980 donne l'occasion de déterminer l'origine des normes formelles, la manière dont elles sont négociées et les pressions politiques, économiques et techniques auxquelles elles ont été soumises. Selon les auteurs, les normes techniques sont des technologies de coordination qui ordonnent et interfacent non seulement les mécanismes d'échanges, mais aussi les parties prenantes investies dans leur développement. Pour Galloway (2004), les protocoles Internet TCP/IP (*Transmission Control Protocol/Internet Protocol*) et le DNS (*Domain Name System*) sont symptomatiques des formes de production culturelles distribuées, et néanmoins sélectives, inhérentes au régime économique et politique actuel. Ce phénomène se reflète dans la manière théoriquement ouverte dont les protocoles sont développés et dans la logique de contrôle exercée par les protocoles eux-mêmes. La suite TCP/IP distribue la fourniture de contenu sur Internet, en spécifiant comment les données doivent être regroupées en paquets, où elles doivent se diriger, où elles seront transmises, et quel sera leur parcours et leur destinataire. Le DNS propose une grammaire à travers laquelle ce contenu est accessible, notamment en traduisant les noms de domaine qui nous sont familiers (.com, .fr et les adresses associées) en adresses entièrement numériques qui sont les identifiants uniques des ressources pour le réseau. Le protocole TCP/IP et le DNS ont donc tous deux des implications pour l'accès des internautes aux ressources en ligne, pour une variété de raisons qui vont de la capacité des paquets de données à rejoindre correctement leur destination, à la possibilité pour les internautes de rejoindre les sites Web qu'ils souhaitent sans devoir mémoriser des séquences de chiffres longues et peu intuitives. Ils peuvent donc être utilisés comme armes par des acteurs qui souhaiteraient faire obstacle à leur accès.

Les normes qui se sont imposées sont souvent difficiles à modifier ou à remplacer. Le protocole Internet IPv4, qui livre les paquets de données d'un expéditeur à un destinataire sur la base des adresses marquées sur ces paquets, a été conçu à une époque où l'Internet était beaucoup moins peuplé qu'aujourd'hui. Ainsi, il est notamment incapable à l'heure actuelle de satisfaire la demande globale de connectivité (DeNardis, 2009), en rapide croissance. Une nouvelle norme plus robuste, IPv6, qui augmente la longueur des adresses et en décréterait l'abondance sur le long terme, a donc été créée et est en train d'être déployée. Cependant, la transition vers cette nouvelle norme est très lente, progressive et continue. C'est ainsi que sont nées des technologies de pont entre ces deux infrastructures, les mécanismes de transition IPv6, qui facilitent la transition d'une version du protocole à l'autre et pallient ainsi le manque d'interopérabilité entre les deux.

Outre les mécanismes économiques, sociaux et techniques de normalisation, il existe des pratiques institutionnelles servant à vérifier et à certifier les normes (Loconto et Busch, 2010). Dans le cas notamment du protocole IPv4, l'adhésion à la norme s'autorégule. Un ordinateur de bureau incapable d'accéder à Internet serait quasiment inutile : IPv4 est donc indéniablement intrinsèque à tous les systèmes d'exploitation polyvalents.

On voit comment, pour cet ensemble d'auteurs, il convient d'aborder la diversité des standards et leurs modes de propagation sur le plan de la matérialité, de l'espace et du discours. Les standards techniques s'incarnent dans l'agencement des matériaux et des significations auxquelles elles donnent lieu. Elles sont concrétisées dans un environnement construit, qui s'incarne non seulement sous certaines formes physiques, mais aussi dans les manières dont elles sont utilisées et dans les modèles sociaux et économiques associés. Parfois, ce phénomène se produit accidentellement, car certaines décisions et actions apparemment mineures conditionnent à l'avance les effets spatiaux et temporels qui en découlent.

2.2.2. Les infrastructures comme incarnation et médiation de la gouvernance

Le terme « infrastructure » – dont on donnera une brève introduction ici avant d'y consacrer le troisième chapitre – est un terme potentiellement englobant qui peut être excessivement vague sans définition. Il fait généralement référence à l'équipement collectif nécessaire à l'organisation et à l'activité humaines, tels que les bâtiments, les routes, les ponts et les réseaux de communication,

en bref, des artefacts entièrement matériels et concrets. Cependant, lorsqu'il s'agit des technologies de l'information et de la communication (TIC), notamment Internet (et de leur gouvernance), Geoffrey Bowker et ses collègues notent qu'« au-delà des briques, du mortier, des tuyaux ou des fils, l'infrastructure englobe également des entités plus abstraites, telles que les protocoles (humains et informatiques), les standards et la mémoire », ainsi que « des installations et services numériques… [tels que] des services informatiques, des services d'assistance et des référentiels de données pour n'en nommer que quelques-uns » (Bowker et al., 2010 : 97-98).

Toute une tradition des STS a exploré les dimensions sociales et organisationnelles des TIC en tant qu'infrastructures, comprises donc dans ces sens multiples, non seulement en tant qu'artefacts purement matériels mais aussi comme substrat logistique. En particulier, les chercheurs en STS ont historiquement mis en évidence certaines caractéristiques inhérentes à l'étude de systèmes sociotechniques complexes, par exemple, que l'infrastructure existe généralement en arrière-plan, est invisible pour la plupart des utilisateurs et est souvent considérée comme allant de soi (Star et Ruhleder, 1994)[25]. Ainsi, soutient-on, la politique inscrite dans l'infrastructure au moyen de la conception et des encodages techniques est également difficile à retracer. C'est pourtant une tâche importante car la conception de la « plomberie » d'Internet (Musiani, 2012), les pratiques, usages et échanges sous-jacents dans un système en réseau, informent son adoption et (ré)appropriation par les utilisateurs, sa régulation, et ses formes organisationnelles. Plusieurs travaux, croisant les études d'Internet avec la branche des STS appelée études d'infrastructure *(infrastructure studies)*, ont cherché à explorer les qualités sociales et organisationnelles des infrastructures sous-tendant les réseaux d'information et à trouver la matérialité dans le virtuel du logiciel et du code (Blanchette, 2011 ; Fuller, 2008 ; Marino, 2020). De nouveaux concepts pour rendre compte de la puissance d'agir des infrastructures ont été proposés, comme le « regard vectoriel » d'Annalisa Pelizza (2016), qui explore comment l'interopérabilité des systèmes d'information, en tant que

[25] Il s'agit par ailleurs d'un aspect fondateur des *infrastructure studies* qui est assez débattu depuis quelques années, jugé par certains critiques comme étant marqué par une vision occidentale et de « premier monde ». Au croisement entre sciences urbaines et STS, plusieurs contributions (e.g. Graham & McFarlane, 2014 ; Anand, 2017 ; Baptista, 2019 ; Barry, 2020) soulignent que, d'un côté, l'invisibilité est une construction complexe dans les pays les plus riches, plutôt qu'une qualité intrinsèque des infrastructures. De l'autre côté, la séparation entre panne visible et fonctionnement ordinaire invisible n'est pas toujours à l'œuvre, car il existe de nombreux stades intermédiaires et la question des « publics » de la visibilité (invisible pour qui ?) est plus complexe que ne le suppose la définition initiale de Star et Ruhleder. Dans ces travaux, c'est plutôt la question de *taken-for-grantedness* (l' « allant de soi ») qui est riche pour l'analyse, puisqu'elle ouvre la question de la naturalisation de certaines choses qui vont de soi dès lors qu'elles sont infrastructurelles.

processus performatif de ré-ordonnancement des frontières entre systèmes, redistribue l'autorité et la responsabilité. Les petites opérations techniques qui sous-tendent et structurent les projets d'interopérabilité (par exemple, dans le cas d'étude analysé par Pelizza, l'introduction d'un plug-in dans le système informatisé des registres civils italiens pour assurer l'authenticité de la certification des données envoyées à d'autres autorités) deviennent des sites stratégiques où les changements institutionnels deviennent visibles.

Les perspectives fondées sur les STS examinant différents types d'infrastructures ont proliféré, mais elles ont dans un premier temps reçu relativement peu d'attention de la part des spécialistes de la gouvernance de l'Internet, la pionnière à cet égard ayant été Laura DeNardis avec son article « *Hidden Levers of Internet Control* » (2012), suivi par notre travail commun (de 2013 à 2015, avec pour résultat le livre *The Turn to Infrastructure in Internet Governance*); j'avais pour ma part théorisé ces enjeux dans le cadre de mes recherches doctorales sur les technologies pair-à-pair, dans l'article « *Caring about the Plumbing* », aussi de 2012. Ces perspectives sont désormais une partie substantielle des recherches sur la gouvernance d'Internet, comme le montrent par exemple les contributions de Braman (2016) et Malcic (2016), sur le travail des premiers concepteurs d'Internet, de De Filippi et Loveluck (2016), sur la gouvernance socio-technique de Bitcoin, ou encore de Mager (2017) sur la co-production de technologies de recherche d'information en ligne et de l'identité européenne dans le cadre de la réforme UE de la protection des données. Dans ces contributions, la gouvernance de l'Internet est comprise comme un ensemble de processus sociotechniques d'innovation, de numérisation, de régulation, de mobilisation, de cooptation et de contournement – une perspective qui dérive à la fois d'un approfondissement des approches STS de la part de la communauté de recherche sur la gouvernance d'Internet et de l'importance croissante des aspects infrastructurels dans l'Internet comme espace public.

En outre, les contributions tirées des approches STS ces dernières années ont reconnu non seulement que les fonctions administratives et de coordination liées à l'infrastructure Internet ont toujours été des instruments de pouvoir (DeNardis, 2009) mais que les points de contrôle de l'infrastructure, quelle que soit leur fonction initialement prévue, peuvent être mobilisés pour reprendre (ou gagner) le contrôle ou la manipulation des flux d'argent, d'informations et d'idées dans la sphère numérique – un phénomène qu'on a appelé le « tournant infrastructurel dans la gouvernance d'Internet » (Musiani et al., 2016). Cet ensemble de travaux, sur lequel on reviendra

dans le troisième chapitre, montre les implications de type « dommage collatéral » de la cooptation de l'infrastructure Internet pour exécuter des fonctions autres que leur objectif visé (DeNardis & Musiani, 2016), par exemple l'usage du DNS à des fins d'exécution des droits de propriété intellectuelle qui fera l'objet du quatrième chapitre. Les approches STS, avec leur attention aux pratiques situées et à la puissance d'agir inscrite dans les infrastructures, sont bien adaptées pour mettre ces aspects au premier plan.

2.2.3. Le rôle performatif des controverses dans la fabrique de la gouvernance

Dans la tradition STS, les différents types d'arguments mis en avant par les acteurs d'une controverse qui concerne un objet ou une arène socio-technique donnent l'opportunité au chercheur d'explorer les différentes conceptions de l'ordre social qu'ont ces acteurs. Internet présente aujourd'hui un nombre croissant d'objets et d'arènes sujets à controverses, tels que les accords d'interconnexion entre fournisseurs d'accès à Internet (Meier-Hahn, 2015), le débat autour de sa neutralité (Marsden, 2017), l'inspection approfondie des paquets (DPI ou *deep-packet-inspection*) (Mueller *et al.*, 2012), le déploiement de technologies de filtrage de contenu (Deibert & Crete-Nishihata, 2012), les mesures de surveillance omniprésentes et l'utilisation du DNS à des fins réglementaires (DeNardis & Hackl, 2015), la régulation du cloud (Yoo & Blanchette, 2015) ou encore la construction des algorithmes qui sous-tendent nos moteurs de recherche en ligne (Mager, 2017). En outre, les contentieux politiques, l'activisme et la contestation des citoyens, ainsi que les droits de l'homme, peuvent être inscrits dans les choix de conception et *design* de l'infrastructure Internet elle-même (Milan & ten Oever, 2017), ce que montrent également les recherches de Ksenia Ermoshina sur le façonnage et l'emploi des applications mobiles et Web axées sur la citoyenneté et l'activisme (e.g. Ermoshina, 2016). Les négociations et les controverses rattachées aux revendications concernant l'Internet peuvent être considérées comme performatives, dans la mesure où elles « impliquent et sont impliquées dans la création de mondes dans lesquels un certain mode de gouvernance a du sens » (Ziewitz & Pentzold, 2014, p. 20) ; les manières dont les problèmes sont formulés par certains acteurs portent inscrites en elles des définitions de la gouvernance et impliquent des actions de gouvernance spécifiques.

Contrairement à ce que certaines approches institutionnelles peuvent suggérer, la controverse, l'instabilité, la déstabilisation et la restabilisation constituent d'importants aspects des institutions mêmes de la gouvernance d'Internet. Comme le montre notamment Flyverbom (2011), le Forum sur la gouvernance d'Internet (IGF) et d'autres structures organisationnelles de la gouvernance d'Internet n'auraient jamais pu voir le jour sans la vaste reconfiguration de deux entités liées à l'ONU. Examinées dans l'optique des STS, les institutions montrent leur capacité à se renégocier et à se reconfigurer dans les moments d'épreuve, pour maintenir leur élan et, au bout du compte, leur autorité. Si on ne l'analyse pas de la sorte, l'autorité des institutions de gouvernance d'Internet « apparaîtrait autrement comme un *fait accompli* » (Flyverbom, 2011 : 6). En outre, comme le souligne Julia Pohle (2016), en centrant l'analyse sur les positionnements et les négociations des acteurs et sur les processus plutôt que sur les résultats, on peut mettre en lumière la contribution des processus multipartites et la validité de leurs résultats, même en l'absence d'une dimension contraignante (l'absence de contrainte est par exemple consubstantielle aux délibérations de l'IGF, de par sa mission).

La plupart du temps, les controverses et les conflits qui sévissent dans l'univers de la gouvernance d'Internet surgissent autour de « points de contrôle » (DeNardis, 2014 : 15) particuliers. Ces points de contrôle peuvent se matérialiser au sein des couches les plus profondes de l'infrastructure d'Internet jusqu'aux équipements de connexion des foyers, appelés le « dernier kilomètre » (ou *last mile*) du réseau, car le plus proche des utilisateurs. Ils incluent le blocage des flux financiers vers certains services Internet, ainsi que des réponses techniques aux violations des droits de propriété intellectuelle, telles que le dispositif de riposte graduée et les tentatives d'utilisation du système de noms de domaine (DNS) à des fins d'application du droit d'auteur (voir le chapitre 4 de ce mémoire). Enfin, des points de contrôle importants sont les intermédiaires privés de l'information, qui prennent *de facto* des décisions politiques dans tout l'éventail des cas où ils collectent, recueillent, regroupent, sélectionnent et présentent des données aux utilisateurs et aux autres acteurs de la chaîne de valeur d'Internet, exerçant ainsi de la gouvernance sur la liberté d'expression, la diversité culturelle et la réputation (DeNardis, *ibid*.). Les récents débats sur les *fake news*, la propagation organisée de la désinformation sur les réseaux, sont un exemple de cette privatisation de la gouvernance Internet : comme l'a récemment montré Romain Badouard, des plateformes telles que Facebook, Google et leurs homologues, puisqu'elles répondent à un souci commercial de personnalisation des informations, ont favorisé l'émergence d'une forme de

propagande individualisée, qui s'incarne au cœur des architectures techniques et des algorithmes qui font circuler les informations et non plus dans les informations elles-mêmes (Badouard, 2017). Il est important de souligner que les points de contrôle ne sont pas toujours « déjà là » en tant que tels, mais certaines controverses participent à les identifier, à les rendre saillants en les rendant problématiques. Le rôle « performatif » des controverses s'étend donc à leur capacité à qualifier et à problématiser d'une certaine manière des aspects de la réalité.

Le « réseau des réseaux » est considéré comme étant particulièrement bien adapté à toutes sortes de stratégies de sortie et à l'évolution des rapports de force ; c'est ainsi que les modes de régulation fondés sur le consensus deviennent essentiels car, dans l'impossibilité d'être totalement contraignantes, les normes se négocient et se contestent constamment (Brousseau *et al*., 2012, p. 35). Par conséquent, les processus mêmes de l'évolution des normes, mis à l'épreuve lorsqu'ils font l'objet de conflit et de réalignement, ou de déstabilisation et de re-stabilisation, deviennent essentiels, car ils offrent différents types de garanties aux diverses parties prenantes. Par exemple, nos recherches sur la « chaîne de blocs » ou *blockchain* qui sous-tend Bitcoin (Mallard *et al.*, 2014 ; Musiani *et al.*, 2017) ont montré que plusieurs moments d'épreuve et de controverse ont porté sur l'infrastructure de Bitcoin – notamment un événement dans son histoire qui a amené le système à effectuer involontairement une *fork*, c'est-à-dire une modification du code source entraînant la naissance d'une deuxième version. Or, ce sont ces moments de controverse qui ont amené les développeurs et utilisateurs de Bitcoin à questionner ce qui, au-delà de la rhétorique de la décentralisation, est un écosystème complexe d'intermédiaires, de médiations et de points de contrôle, et à déstabiliser puis re-stabiliser une définition de confiance partagée dans le système, *via* le système. Ces moments de controverse feront l'objet du chapitre 5 de ce mémoire.

2.3. Que font les STS aux études de gouvernance (d'Internet) ?

Lorsqu'on l'examine dans une perspective STS, Internet n'est pas une entité technologique donnée et statique qui a besoin d'être réglementée ; ce sont l'ensemble des éléments techniques du réseau des réseaux, et les différents acteurs qui en font partie, qui constituent, perpétuent et contestent l'ordre socio-politique. Outre les décisions techniques concernant la conception et la gestion du

réseau, les lois et les règlements, les forces du marché, un certain nombre d' « activités ordinaires », animées par des visions hétérogènes et souvent concurrentes, ou fondées sur des accords de confiance et de consensus intrinsèquement sociaux et politiques, contribuent à la gouvernance de l'Internet telle qu'elle est aujourd'hui.

Alors qu'Internet devient de plus en plus la principale infrastructure, le marché plus étendu, et la sphère publique plus importante de l'humanité, les controverses sociopolitiques et sociotechniques deviennent une partie toujours croissante de ce qui se trouve sous l'étiquette de « gouvernance d'Internet ». Les sensibilités STS, dans leur hétérogénéité mais avec un certain nombre de points communs qu'on a soulignés dans ce chapitre, offrent l'une des opportunités les plus intéressantes pour que ces controverses soient complètement pris en compte, richement décrites et analysées, au moyen de notions qui sont à la fois des concepts (car elles suggèrent une vision de comment « marche le monde », de ce qui motive ses opérations et de ce qui construit leur sens politique) et des méthodes (chacune de ces notions est aussi un moyen pratique d'appréhender les rouages de la gouvernance d'Internet sur le terrain). En ce sens, les recherches récentes cherchant à fusionner les STS et la gouvernance d'Internet guident une compréhension, basée sur l'étude des controverses et des infrastructures, des coulisses des politiques d'Internet d'aujourd'hui.

Les approches STS comportent, bien sûr, leur propre ensemble de défis. Ainsi qu'on a commencé à le souligner dans le chapitre précédent, regarder l'ordinaire, l' « invisible qui façonne » (Musiani, 2018), qui échappe généralement au radar public – souvent même au radar de la recherche – implique d'identifier le bon terrain, de choisir les moyens d'y accéder, et enfin de négocier patiemment l'accès à celui-ci (voir Jørgensen, 2020), car un travail ethnographique approfondi est une condition préalable nécessaire à une démarche STS significative. Cette négociation se fait, parfois, aussi bien avec les acteurs potentiels du terrain qu'avec l'ensemble des compétences du chercheur : analyser et, plus encore, décrire analytiquement de façon claire ces environnements nécessite un haut niveau de technicité qui doit d'abord être maîtrisé par le chercheur. Ainsi, les chercheurs STS en gouvernance d'Internet (comme c'est le cas pour de nombreux spécialistes de la gouvernance d'autres systèmes et dispositifs techniques complexes) ont souvent des formations disciplinaires composites, n'étant arrivés aux méthodes STS qu'après une formation précédente en informatique ou en ingénierie.

Le choix des terrains sur lesquels concentrer ses enquêtes – généralement au moyen d'une ou plusieurs études de cas – soulève des questions de sélection de critères pour ce choix, et de représentativité des cas sélectionnés ; si c'est le cas pour toute forme d'enquête en sciences sociales, le haut niveau de technicité est sans doute un critère supplémentaire à prendre en compte lors des recherches au croisement entre STS et gouvernance d'Internet. Enfin, étroitement lié au point précédent – et malgré la difficulté de généraliser à des principes plus larges, ce qui est intrinsèque à l'approche STS et parfois une de ses limites – pour que leur travail ait un sens dans un dialogue plus large avec d'autres disciplines, les chercheurs en gouvernance de l'Internet inspirés par les STS devraient se garder de tomber dans un piège commun de leur discipline des disciplines. Il faut éviter que, au nom du détail, du cas particulier et de l'analyse située, le langage de la complexité et de l'hétérogénéité devienne le principal protagoniste de leurs analyses au point d'en brouiller les conclusions.

L'attention croissante accordée par les chercheurs STS au domaine de la gouvernance de l'Internet ne s'est bien sûr pas développée de manière isolée. En plus de la lignée des *Internet studies* introduite plus tôt dans le chapitre, un corpus important de littérature STS existante contribue à éclairer d'autres mécanismes de participation distribuée aux controverses techno-scientifiques, et la recherche sur la gouvernance d'Internet peut tirer des enseignements de la gouvernance de et par la science et la technologie dans d'autres domaines sociotechniques complexes tels que l'environnement, la santé, les nanotechnologies et l'ingénierie génétique (voir, par exemple, Irwin 2006). De même, la recherche sur la gouvernance d'Internet dans d'autres disciplines plus historiques, principalement axées sur le niveau institutionnel et le rôle de l'État – science politique, droit, histoire, relations internationales et économie institutionnelle – peut dialoguer étroitement avec les STS et aider, par exemple, à atténuer certaines des conséquences indésirables des approches STS décrites précédemment.

Comme on l'a vu tout au long de ce chapitre, le courant de la sociologie des techniques et des STS qui se focalise sur les infrastructures et sur les controverses qui traversent leur création, leur développement, leurs usages, permet de mettre l'accent sur deux aspects. D'un côté, la dimension conflictuelle « macro » de l'Internet et de ses grands systèmes socio-techniques, de ses points de

contrôle importants et visibles (par exemple le rôle des GAFAM dans l'économie et la liberté d'expression, les intermédiaires dans un système de monnaie électronique tel que Bitcoin, le fonctionnement du DNS). De l'autre côté, les pratiques situées et ordinaires d'Internet, tels que les détails techniques de programmation et de gestion, ou les travaux discrets de la maintenance de composantes spécifiques de ces différents systèmes (par exemple la solution d'un « glitch » dans une base de données que sous-tend la blockchain, l'installation d'un plug-in, l'écriture d'une ligne de code).

Les analyses des manières dont une infrastructure prend forme, est développée, réappropriée voir détournée, semblent aujourd'hui un complément nécessaire, et non un substitut, à ces efforts qui chercher à élaborer des principes généraux et des théories sur la manière dont fonctionne la distribution du pouvoir et des ressources, en bref, le monde du politique et de la gouvernance. Le chapitre qui s'ouvre se concentre plus particulièrement sur comment les infrastructures d'Internet sont utilisées comme instruments de gouvernance, et pose les jalons d'une théorie de la gouvernance d'Internet basée sur l'infrastructure dont les chapitres suivants donneront ensuite des illustrations analytiques.

Chapitre 3. Contrôle invisible : (études d') infrastructure et gouvernance d'Internet

La notion d' « infrastructure » se réfère typiquement à des systèmes physiques et matériels à large échelle nécessaires pour l'organisation et l'activité humaines, tels que les routes, les ponts, les grilles d'alimentation ou les égouts. Une quantité importante de travaux en géographie, anthropologie et en *science and technology studies* (STS) a désormais été consacrée à explorer les dynamiques de pouvoir, les conflits et contestations, les significations et les rapports sociaux incarnés dans ces infrastructures physiques (par exemple, Harvey, 2012). Ces travaux définissent, à la base, les infrastructures comme la matière structurante de nos sociétés, tout en incluant dans l'analyse des infrastructures des aspects a priori immatériels, comme l'information et ses flux (comme on verra ci-dessous). L'analyse des infrastructures permet de penser des agencements à la fois techniques et politiques comme inducteurs, et producteurs, de structures sociales, qui co-façonnent des usages et permettent à des programmes politiques de prendre corps et matière.

Un aspect marquant de la portée analytique de la notion d'infrastructure, ainsi qu'elle est mobilisée par le courant dédié des STS, les *infrastructure studies*, mais aussi dans d'autres disciplines, est le dépassement de l'idée d'une évolution technologique linéaire, inscrite dans la continuité, et de l'idée de progrès des techniques ayant l'efficacité pour pierre angulaire. Les études des infrastructures mettent plutôt en avant les enchaînements de modifications et d'améliorations, et parfois de détournements, propres aux cycles de vie des objets techniques. L'anthropologie des sciences et des techniques place les aspects fonctionnels des infrastructures en arrière-plan, afin d'explorer comment elles sont enchevêtrées dans des ensembles complexes de relations sociales, donnant lieu à des formes infrastructurelles (Latour & Lemonnier, 1994). Il s'agit de réfléchir aux infrastructures en termes d'assemblage socio-économique, qui comporte des liens étroits entre objets techniques et acteurs, qui en sont affectés en retour.

Cette vision s'inscrit dans une réflexion de longue date sur la politique de la matière. Dans *Do Artifacts Have Politics?* (1980) Langdon Winner mettait déjà en avant l'idée « provocatrice » que les technologies possèdent des propriétés politiques, observant à quel point les formes du pouvoir,

la justice sociale, l'acte d'exercer ses libertés individuelles et collectives, sont étroitement liés aux structures techniques. La question des infrastructures et de leur relation à l'exercice du pouvoir a permis de proposer une perspective critique sur le développement et l'expansion de systèmes techniques complexes tels que les réseaux de transport ou d'énergie, compris comme substrat, ou support, de la modernité.

La notion d'infrastructure s'est invitée dans les études de l'innovation, porteuse d'interrogations sur la portée « systémique » de grands ensembles techniques et leur relation aux équilibres de pouvoir. Des questions centrales concernent la matérialisation des infrastructures à des niveaux multiples, qui vont du géopolitique au géologique (Edwards, 2003), les changements d'échelle (Subra, 2016), ou encore le dévoilement, aux trois niveaux micro-, méso- et macro-, des processus de co-construction idéologique induits par la conception, l'acceptabilité et les utilisations des infrastructures (Edwards, 2003). De son côté, Susan Leigh Star a travaillé avec Geoffrey Bowker et Martha Lampland à l'analyse des usages dans les infrastructures, en montrant comment les effets structurels sont insérés dans une approche plus large, où les usage(r)s contribuent à informer, classifier, catégoriser et standardiser les infrastructures (Bowker & Star, 1999 ; Lampland & Star, 2009). L'infrastructure est ici pensée comme co-produite par les usages, qu'elle contribue à structurer en retour de manière relationnelle, ce qui est censé « re-visibiliser » les infrastructures (Bowker, 1996). Les infrastructures se situent, dans ces perspectives, dans un réseau d'acteurs humains et non-humains qui les conçoivent, les gouvernent et les utilisent, contribuant ainsi à façonner la complexité du social (Akrich *et al.*, 2006 ; Harvey *et al.*, 2016). De son côté, Andrew Barry invite à être attentifs à la temporalité des infrastructures en plus de leur spatialité, en particulier pour ce qui est des infrastructures technoscientifiques qui équipent les tests et la supervision des infrastructures physiques, ce qui amène à examiner non seulement le présent des infrastructures, mais « l'anticipation des futurs infrastructurels » (Barry, 2020).

Au fur et à mesure qu'Internet est devenu un des systèmes structurants de nos sociétés, les *infrastructure studies* se sont consacrés à explorer les technologies de l'information et de la communication (TIC) dans leurs dimensions infrastructurelles. Une des notions de base discutée dans les travaux pionniers à ce sujet est que, notamment depuis l'introduction du numérique auprès du grand public et de l'Internet, une définition d'infrastructure exclusivement physique pourrait ne pas être la plus appropriée (voir Larkin, 2013). On a déjà rappelé la notion d'infrastructure

numérique élaborée par Geoffrey Bowker, qui inclut également des entités plus abstraites, telles que les protocoles (humains et informatiques), les standards et la mémoire (Bowker *et al*., 2010 : 97). Paul Edwards rappelle à cet égard que « les discussions sur la technologie tiennent rarement compte de l'ensemble des systèmes sociotechniques caractéristiques des sociétés modernes. En revanche, les discours sur la technologie portent presque systématiquement sur les hautes technologies, c'est-à-dire les technologies nouvelles ou en évolution rapide » (Edwards, 2003, p. 185). Dans le cas d'Internet, ces technologies « nouvelles » sont celles dont on peut avoir une connaissance directe : nos navigateurs Web, les interfaces de nos sites favoris, les contenus et les données qu'on partage sur les réseaux sociaux ou qu'on identifie grâce aux moteurs de recherche – les technologies d'usage quotidien qui rendent discret, voire invisible, le *pourquoi* du fonctionnement des choses.

Suivant le travail pionnier de Susan Leigh Star et Geoffrey Bowker, un ensemble de travaux interdisciplinaires, notamment STS, s'est attaché à étudier les infrastructures informationnelles et numériques en considérant qu'elles sont « matérielles » tout en étant numériques, et qu'il faut dépasser la compréhension des infrastructures comme des systèmes seulement physiques. Ces travaux se proposent de mobiliser la notion d'infrastructure comme instrument heuristique pour comprendre la gouvernance de l'information et du numérique, et en particulier de l'Internet.

Selon ces travaux, la qualité infrastructurelle du réseau des réseaux est relationnelle et conditionnelle ; les infrastructures peuvent plus utilement être comprises en termes de *fonction* que de *forme*. Ainsi, au-delà des objets dont l'aspect infrastructurel est immédiatement évident, comme les ponts ou les tuyaux, un certain nombre d'artefacts et d'entités qui peuplent et façonnent le réseau des réseaux pourraient être qualifiés d'infrastructures parce qu'ils ont une *fonction infrastructurelle* – car ils contribuent à structurer, façonner, modeler, permettre ou contraindre notre « être-ensemble » sur et avec l'Internet. Dans cette acception, les infrastructures de l'Internet incluent des objets physiques – par exemple les câbles sous-marins qui acheminent les télécommunications mondiales ou les centres de données qui hébergent nos contenus numériques – et des objets a priori beaucoup moins concrets, tels que le protocole qui permet à la *blockchain* sous-tendant Bitcoin de fonctionner.

Les infrastructures se réfèrent ici beaucoup moins à une technologie ou à un ensemble de technologies particulières, qu'à ces objets et pratiques qui assument une qualité ou une fonction

infrastructurelle dans des circonstances spécifiques. Cette conception implique au moins deux conséquences : d'une part, le fait d'exercer du contrôle sur ces fonctions infrastructurelles fournit à certains acteurs le pouvoir et l'opportunité d'agir à leur avantage ; d'autre part, il n'y a que très rarement une seule manière de mettre en œuvre ces fonctions ou un seul et unique acteur capable de les contrôler. Ainsi, les infrastructures de l'Internet sont politiques, contestables et contestées, cibles et instruments de gouvernance, objets d'intérêt d'une myriade d'acteurs ; des plus puissants et concentrés jusqu'à l'internaute lambda. Les infrastructures peuvent être comprises comme des lieux fondamentaux d'exercice du pouvoir économique et politique (DeNardis et Musiani, 2016 : 3). La mise au jour de cet exercice de pouvoir, qui est souvent implicite et tenue au second plan, est cruciale pour révéler les conflits autour de ce qu'est une infrastructure, qui peut en bénéficier, ou bien la contester (Bernards et Campbell-Verduyn, 2019).

3.1. Quelle matérialité pour les infrastructures numériques ?

Les travaux utilisant la notion d'infrastructure informationnelle et numérique, pour explorer les questions de gouvernance, partent souvent d'une question. Si l'information numérique n'est pas immatérielle, quels sont les biais qui la rendent matérielle, en dépit de la prévalence médiatique et culturelle d'un discours qui – comme le souligne Jean-François Blanchette (2011) – se fonde largement sur le virtuel et les nuages ?[26]

Pour Knoespel et Zhu, les infrastructures numériques sont dotées d'une « matérialité continue » (*continuous materiality*) : c'est ainsi qu'ils rendent compte de la hiérarchie des codes informatiques, qui naît des couches les plus basses pour évoluer vers des langages de programmation plus lisibles pour l'humain, et enfin vers les « codes » en général (structurels, législatifs, sociaux, culturels). Les auteurs avancent l'argument selon lequel « chaque niveau de code engage le langage naturel et le monde physique de façons différentes, qui varient du voltage inégal des circuits informatiques jusqu'à nos activités quotidiennes. Dans son ensemble, la hiérarchie du code constitue un champ de matérialité variée, qui est continu et interconnecté »

[26] Cette section repose sur un précédent travail effectué dans le cadre d'un numéro de la revue Tracés sur les infrastructures « techniques et politiques » (Musiani, 2018).

(Knoespel et Zhu, 2008 : 236). Selon ce concept de matérialité continue, le code informatique crée des relations entre plusieurs systèmes symboliques, ceux nécessaires au simple fonctionnement de la machine, et ceux nécessaires pour que ces opérations soient situées à l'intérieur du langage et donc, de l'ordre social (Blanchette, 2011). Plus concrètement, le numérique ne peut pas échapper aux contraintes matérielles des dispositifs physiques qui le manipulent, le stockent et (le) communiquent : la matérialité de l'information numérique a trait à la fois aux caractéristiques physiques des ressources computationnelles, qui ont des limites bien précises, et à l'adoption de la modularité[27] comme intermédiaire entre ces ressources et les applications qui manipulent l'information (ibid.).

Un argument semblable est exposé par Paul Leonardi (2010), quand il remarque que, bien qu'il ne soit pas doté de propriétés physiques, un logiciel existe clairement à d'autres niveaux que le conceptuel, au vu de sa fonction et des effets qu'il produit sur nos actions, « puisqu'il fournit des contraintes et des opportunités concrètes (*hard*) de la même façon que les artefacts physiques ». Leonardi suggère donc que, si la matérialité est utilisée pour représenter l'instanciation pratique et la signification d'un artefact, plutôt que la matière dont il est conçu, les artefacts numériques incluent bien de la matérialité. D'autres contributions soulignent que ce qui est arrivé avec la numérisation et la mise en réseau de l'information est un déplacement fondamental dans l'équilibre de pouvoir entre la matérialité physique et les idées, même si la première survit bien sûr. Selon Youngjin Yoo (2012), si cette dernière dominait les artefacts analogiques tels que les cassettes audio ou vidéo, la numérisation des artefacts informationnels ouvre la voie à de nouvelles formes de matérialité, de la représentation aux outils et aux formes d'organisation.

Quelques tentatives de théorisation de la matérialité numérique se fondent plus spécifiquement sur une étude de cas. C'est le cas du travail de Matthew Kirschenbaum (2008), qui avec son analyse approfondie du disque dur, propose un point de vue original sur les contraintes physiques qui influencent les médias numériques, en voulant comprendre comment « les données électroniques ont pu être perçues en tant qu'évanescentes et éphémères d'un côté, et remarquablement […]

[27] En informatique, la modularité est un regroupement de fonctions et de méthodes qui permettent de répartir le développement d'un logiciel sur plusieurs personnes, et de réutiliser certaines portions de code pour éviter de redévelopper entièrement des logiciels.

stables et persistantes de l'autre » (ibid. : 27). Tout au long de son analyse, Kirschenbaum énumère plusieurs types de matérialités numériques, tels que la capacité des ordinateurs à exécuter en continu des corrections de bugs – ce qui permet à l'environnement numérique de « propager l'illusion de l'immatérialité », ou les formats de fichiers et la structuration qu'ils imposent aux données numériques, par exemple avec différents niveaux de compression – des contraintes qui accompagnent les données lors de leur circulation dans les réseaux.

Si ces auteurs s'attachent à comprendre et à conceptualiser la matérialité des infrastructures numériques, c'est bien parce qu'ils reconnaissent leur rôle essentiel et fondateur d'un point de vue socio-technique et socio-politique. Pour le dire avec Blanchette, « sans des modes d'analyse ancrés dans les objets (*stuff*) du numérique, on se trouvera dans la situation bizarre de devoir recourir à des théories qui rendent compte de sujets incarnés, situés et interagissant au sein d'environnements qui manquent curieusement de contraintes matérielles spécifiques » (2011). Les infrastructures numériques, avec leurs contraintes et opportunités matérielles, sont de plus en plus centrales à la fois pour notre « puissance d'agir » et pour le fonctionnement d'autres infrastructures critiques, comme les transports, l'énergie ou la finance ; elles ont donc une importante valeur politique et de gouvernance (Yoo et Blanchette, 2015).

Faire ressortir la matérialité des infrastructures numériques et informatiques a des implications pour leur gouvernance. Comme le fait remarquer Matthew Fuller (2008), ce n'est que récemment que, grâce à cette mise en visibilité des infrastructures, les réseaux numériques ont été compris comme « quelque chose qui a une histoire [contestée], plutôt que d'être simplement dans un état d'amélioration perpétuelle ». L'allocation, la distribution et la mesure des ressources de l'Internet, ainsi que la conception des infrastructures qui les soutiennent, sont en passe de devenir de plus en plus visibles et sujettes à controverse, renchérit Blanchette (2011), en soulignant que la mise en lumière des infrastructures est une condition nécessaire pour qu'une palette d'acteurs plus vaste puisse davantage s'engager dans leur conception et leur gestion.

3.2. La gouvernance d'Internet pensée à partir de ses infrastructures

Comme on l'a anticipé au cours du deuxième chapitre, si les perspectives en STS examinant les infrastructures (et leurs composantes numériques) se sont multipliées au cours des dernières décennies, les spécialistes de la gouvernance d'Internet n'y ont prêté qu'une attention secondaire jusqu'au début des années 2010. Cependant, les ensembles de travaux discutés jusqu'ici ont progressivement ouvert la voie au développement d'une perspective qui permet de penser Internet à partir de ses infrastructures, qui comprend la gouvernance d'Internet comme un ensemble de processus sociotechniques d'innovation, de numérisation, de régulation, de mobilisation, de cooptation et de contournement[28].

3.2.1. La gouvernance *des* infrastructures d'Internet

Les objectifs des études et les politiques en matière de gouvernance d'Internet ont longtemps porté sur trois domaines : le rôle des États-nations souverains et la primauté du droit ; l'importance du Forum pour la gouvernance de l'Internet des Nations Unies pour les délibérations concernant l'Internet, et les fonctions particulières des institutions *ad-hoc* de gouvernance d'Internet, telles que l'ICANN, ou encore des organismes de normalisation et des registres Internet régionaux (RIR). Ces thèmes portent principalement sur les institutions et le rôle qu'elles jouent en matière d'établissement des politiques gouvernementales, inter-gouvernementales, supra-nationales et internationales (incluant des alliances entre le secteur public et le secteur privé) concernant les infrastructures d'Internet.

Si l'objectif de ce mémoire est de se concentrer assez rapidement sur les fonctions de gouvernance inhérentes ou inscrites dans l'infrastructure Internet, il faut donc rappeler ici, pour commencer, le scénario qu'on a décrit notamment dans la section 1.3 : depuis que des stratégies politiques et économiques pour l'Internet ont commencé à être esquissées (ce qui date au moins du début des années 1990), les infrastructures et les « ressources critiques » d'Internet sont la cible de stratégies de gouvernance et de débats animés concernant quelle institution ou ensemble d'institutions devrait « contrôler Internet » (Goldsmith & Wu, 2006). On a vu comment, de l'ICANN à l'IGF en

[28] J'ai posé des jalons pour cette section dans l'introduction à un numéro spécial de l'*Internet Policy Review* (Epstein, Katzenbach & Musiani, 2016), dans l'introduction au volume *The Turn to Infrastructure in Internet Governance* (DeNardis & Musiani, 2016), et dans un récent chapitre d'ouvrage (Musiani, 2020).

passant par les différents organismes de standardisation (W3C, IETF…) et les interventions directes des États sur leurs Internets « nationaux », l'histoire d'Internet est une histoire de tentatives de gouvernance *des* infrastructures Internet, plus ou moins réussies. Parmi ces derniers, on citera notamment les tentatives répétées de l'International Telecommunications Union (ITU), une agence onusienne consacrée à la régulation internationale des télécommunications, d'inclure la gouvernance de certaines infrastructures Internet dans son mandat. Ces tentatives ont suscité de très fortes oppositions, au vu du possible rôle disproportionné des États (y compris de certains États aux politiques Internet notoirement autoritaires) qu'une telle évolution aurait entraîné.

Un cas emblématique de la complexité institutionnelle que sous-tend la gouvernance des infrastructures Internet est celui de la gestion du système de noms de domaine d'Internet (DNS), qui remplit une fonction de base nécessaire au bon fonctionnement d'Internet, celle d' « annuaire » qui assure une traduction stable entre les noms de domaine alphanumériques (par exemple www.cnrs.fr) que les humains utilisent pour accéder à un site Web et l'adresse Internet purement numérique (par exemple 31.15.27.151) que les appareils informatiques utilisent pour accéder à ce site Web via des routeurs. L'ICANN est le superviseur principal du DNS, mais son autorité est également déléguée à ou distribuée sur plusieurs entités. Pour les domaines génériques de premier niveau (gTLD) tels que .com, .gov, .et edu, l'ICANN a une autorité hiérarchique directe sur les institutions (registraires et registres) responsables de l'attribution des noms de domaine aux clients et de la gestion des systèmes qui traduisent les noms en nombres. Les registraires (par exemple GoDaddy) sont des sociétés accréditées par l'ICANN pour vendre des enregistrements de noms de domaine Web aux clients. Les registres (par exemple VeriSign) sont des sociétés qui maintiennent la base de données des noms de domaine pour un domaine de premier niveau particulier, tel que .com. Le registre génère le fichier de résolution des adresses qui fait autorité pour la conversion entre les noms de domaine et les adresses Internet. Le DNS a nécessité d'une grande coordination administrative (Paré, 2003), afin de décider qui se charge de la distribution des noms et des numéros, qui autorise l'ajout de nouveaux noms de domaine de premier niveau (par exemple .info,), qui détermine les tenants et les aboutissants d'une éventuelle censure d'un nom de domaine, qui est susceptible de résoudre les litiges relatifs aux marques (Geist, 2001), qui peut conserver l'archive officielle des associations entre noms de domaine et adresses IP, et enfin, qui a le droit d'exploiter les serveurs racine qui transmettent cette cartographie officielle des associations entre

noms et numéros aux serveurs Internet du monde entier. Les controverses autour du DNS ont par exemple fait l'objet d'excellentes études de Milton Mueller (2002 ; 2010).

La gouvernance *des* infrastructures Internet est depuis longtemps un sujet sensible pour une raison principale : le fonctionnement de notre monde « virtuel » implique l'allocation et la consommation de ressources telles que les adresses Internet, les noms de domaine, ou encore les numéros de système autonomes (ASN), les identifiants uniques utilisés pour le routage du trafic Internet. Ces ressources, étant limitées et fondamentales pour le bon fonctionnement d'Internet, sont historiquement considérées comme « ressources Internet *critiques* » et leur gouvernance est gérée par un ensemble d'entités qui est techniquement et institutionnellement complexe. Dans la prochaine section, on se concentrera sur un premier déplacement conceptuel, celui de la gouvernance *des* infrastructures Internet à la gouvernance *dans* les infrastructures Internet – en examinant la mesure dans laquelle un certain nombre de valeurs, de droits, de contraintes sont inscrits dans la conception même des technologies qui composent l'Internet.

3.2.2. La gouvernance *dans* les infrastructures d'Internet

L'accent historique placé sur certaines institutions de gouvernance des infrastructures d'Internet a pu amener à mettre au deuxième plan un certain nombre d'importantes fonctions de gouvernance mises en œuvre *au moyen* des arrangements d'architecture technique et à travers les stratégies et les prises de décision d'acteurs du secteur privé. Le point de départ d'une théorie de la gouvernance d'Internet basée sur l'infrastructure repose sur l'idée que les arrangements de l'architecture technique sont intrinsèquement des rapports de force. Internet présente, sous la couche de ses applications et de ses contenus, une architecture technique complexe – qui reste généralement, comme on a pu le dire plus haut, hors de la vue du public. Cette architecture comprend un vaste écosystème de technologies de gouvernance d'Internet, autrement dit des systèmes et des processus numériques intrinsèquement conçus pour maintenir l'Internet opérationnel. Parmi ces technologies et processus figurent de nombreux protocoles et systèmes. Par exemple, les « ressources Internet critiques » qu'on vient de mentionner, telles que les adresses IP (Internet Protocol), les noms de domaine et les numéros de système autonomes (ASN), le système de noms de domaine d'Internet (DNS) et les systèmes de la couche « accès réseau ». S'il convient d'analyser

les jeux de pouvoir entre les institutions qui s'occupent, ou souhaiteraient s'occuper, de la gouvernance de ces infrastructures, il est aussi primordial d'éclairer comment la conception, la mise en œuvre et l'innovation de ces infrastructures naturalisent des valeurs politiques et économiques qui finissent par influencer le champ de la liberté et de l'innovation en ligne. Ces technologies de gouvernance d'Internet portent inscrites en elles un certain nombre de valeurs et de droits, notamment la vie privée, l'accès au savoir et la liberté d'expression.

Une partie très importante de la gouvernance d'Internet est l'ensemble de fonctions, à la fois techniques et administratives, qui sont exécutées par le biais de décisions de conception technique et par l'implémentation de composantes infrastructurelles de la part du secteur privé, souvent en lien avec des institutions « globales » et avec les politiques des gouvernements. On a pu voir dans le chapitre précédent comment une abondante littérature STS et, plus largement, pluridisciplinaire, a pu examiner les façons dont les technologies incarnent généralement des valeurs et contribuent à créer des architectures techno-juridiques (par exemple, Winner, 1980 ; Lessig, 1999 ; Nissenbaum, 2001 ; Zittrain, 2008). Les choix de conception et de mise en œuvre concernant les technologies que forment l'Internet, ainsi que les technologies numériques plus largement, ne dépendent pas seulement de l'opportunité technique ou de l'efficacité économique, mais de l'équilibre des intérêts et des valeurs des groupes sociaux impliqués dans ces choix (comme le remarquent par ailleurs des philosophes tels que Feenberg, 1999 ou Bauwens, 2005). Le reste de cette section donne un aperçu des infrastructures qui portent inscrites en elles des fonctions de gouvernance d'Internet, et montrent comment elles font l'objet de controverses qui portent sur les valeurs ancrées dans chacune d'entre elles. Cette section n'a pas l'ambition d'être exhaustive, mais se propose d'illustrer la gouvernance d'Internet *dans* les infrastructures – de montrer comment, de façon récurrente, il existe des liens inhérents entre les architectures et les infrastructures d'Internet et la « fabrique » de sa gouvernance et des valeurs sociales sous-jacentes.

Les protocoles sont l'un des composants infrastructurels les plus fondamentaux de la gouvernance d'Internet (DeNardis, 2009, 2012). Les protocoles Internet sont les règles, ou les modèles, qui permettent l'interopérabilité entre les technologies conçues par différents acteurs. Le modèle Internet actuel implique l'engagement direct de centaines de protocoles, notamment Bluetooth, Wi-Fi, le format MP3 pour l'encodage et la compression de fichiers audio, la norme JPEG pour

les fichiers image, diverses normes MPEG pour les formats de fichiers vidéo, HTTP pour l'échange d'informations entre les navigateurs Web et les serveurs, Voice over the Internet Protocol (VoIP) pour la téléphonie en ligne, et la suite de protocoles fondamentaux TCP/IP, sur lesquels Internet repose au niveau du réseau et de la couche de transport. Ce ne sont là que quelques-uns des protocoles qui fournissent un « ordre » et une structure à des flux binaires de 0 et de 1, et agissent sur des formes informationnelles plus élaborées, afin de représenter des informations dans des formats courants, chiffrer ou compresser des informations, exécuter des fonctions telles que la détection et la correction d'erreurs, et fournir des structures d'adressage communes. Ces normes sont établies par des institutions mondiales réunissant une partie de la communauté technique et du secteur privé, telles que l'Internet Engineering Task Force (IETF), le World Wide Web Consortium (W3C), l'Institute of Electrical and Electronics Engineers (IEEE) et de nombreuses autres entités.

Le but fondamental des protocoles est celui de remplir des fonctions techniques pointues et hautement spécialisées. Par ailleurs, ils sont aussi des artefacts de médiation et intermédiation très importants dans les débats sur un certain nombre de valeurs politiques et économiques (Morris et Davidson, 2003). Un exemple de cette affirmation est sans doute le protocole BitTorrent, qui est certes un protocole « politiquement chargé » au vu des usages qui en sont faits après sa conception, à savoir ses nombreuses associations avec des pratiques de piratage de fichiers audio et vidéo protégés par le droit d'auteur (Izal et al., 2004). Mais il est aussi « politique » dans sa définition technique de base (la spécification d'une approche standard pour le transfert de fichiers volumineux sur Internet), qui permet des échanges décentralisés par l'intermédiaire de méthodes de hachage. D'autres protocoles, tels que l'effort de normalisation « DoNotTrack » du W3C, sont conçus pour assurer la confidentialité, en l'occurrence la possibilité pour les internautes de ne pas être suivis à des fins de publicité en ligne (Kamara & Kosta, 2016). Encore d'autres protocoles, tels que les normes d'accessibilité du Web, portent inscrits en eux un certain nombre de décisions concernant, par exemple, l'étendue de l'accès à Internet pour les malentendants et les personnes souffrant d'autres handicaps. Les standards liés aux processus d'authentification et de chiffrement servent de « médiateur technique » entre des valeurs historiquement concurrentes, telles que la vie privée et la confidentialité d'un côté, et les fonctions de préservation de la sécurité nationale et d'application du droit de l'autre. Les protocoles, lorsqu'ils sont publiés de façon ouverte,

fournissent par ailleurs une plate-forme commune qui uniformise les « règles du jeu » pour l'innovation et la concurrence entre acteurs économiques, et aboutit potentiellement à de multiples produits concurrents basés sur un même standard (Ghosh, 2005). Cette forme d'élaboration de politiques publiques et économiques n'est pas établie par des parlements ou par des gouvernements, mais généralement par des consortiums ou acteurs de standardisation ou encore par des entreprises, ce qui soulève des questions sur la façon dont l'intérêt public est reflété dans la conception des protocoles et comment, sur le plan procédural, ces acteurs peuvent arriver à posséder la légitimité nécessaire pour se charger de telles décisions de conception et de développement.

Les ressources Internet critiques (ou *critical Internet resources*, CIR) et le système de noms de domaine sont des autres domaines de la gouvernance d'Internet qui portent inscrits des questions politiques de fond. Le contrôle de ces ressources a été au centre d'un ensemble de controverses central de la gouvernance de l'Internet : autour de cette question se sont croisés et se croisent des débats sur la souveraineté nationale, sur le droit des marques, sur l'économie du développement et sur la liberté d'expression. Les CIR sont des ressources virtuelles uniques à Internet, telles que les adresses IP (Internet Protocol), les noms de domaine et les numéros de système autonomes (ASN).

Les adresses IP sont sans doute la ressource la plus fondamentale requise pour l'échange d'information sur Internet. Tout dispositif informatique envoyant des informations sur Internet doit utiliser un numéro binaire unique identifiant son emplacement virtuel, soit attribué temporairement pour une session, soit attribué de manière permanente. Les routeurs Internet utilisent des adresses IP pour acheminer des « paquets » (des sous-ensembles d'informations) sur Internet. Des importantes questions de gouvernance d'Internet ont toujours concerné ces adresses IP. L'un des problèmes est que les adresses IP, en substance, fournissent un identifiant unique qui, combiné à d'autres informations, peut identifier un individu – ou au moins un appareil informatique – qui a accédé à, ou transmis, certaines informations, ou effectué une activité en ligne. Cette caractéristique place les adresses IP au centre des tensions entre l'application du droit et de la propriété intellectuelle d'un côté, et l'accès à la connaissance et la vie privée de l'autre. Comme on l'a dit, un problème de gouvernance de longue date sur ces questions porte plutôt sur la gouvernance *des* infrastructures – la question de savoir qui doit contrôler la distribution de ces

ressources rares, ce qui a mis sous les feux des projecteurs l' « écosystème » complexe composé par l'ICANN, l'Internet Assigned Numbers Authority (IANA), les registres Internet régionaux (RIR) et les relations entre les structures de gouvernance traditionnelles et ces institutions. Mais un autre problème urgent d'intérêt public lié aux adresses IP est strictement lié à leurs « incarnations techniques » et concerne l'épuisement de la réserve des 4,3 milliards d'adresses uniques, et la lutte pour passer au nouveau protocole (IPv6) conçu pour augmenter le nombre d'adresses (voir DeNardis, 2009).

Les ASN sont, quant à eux, une ressource Internet critique qui n'est généralement pas visible par les utilisateurs d'Internet. Les ASN sont des numéros uniques attribués aux opérateurs de réseau, généralement appelés « systèmes autonomes ». Cette ressource virtuelle est fondamentale pour le bon fonctionnement du système de routage d'Internet. Les préoccupations politiques concernant les ASN sont similaires à celles concernant les adresses IP : qui est éligible pour recevoir un ASN, comment les contraintes liées à ces ressources façonnent-elles l'économie politique de ces systèmes, et quelles sont les implications mondiales de la prolifération des numéros de système autonome *privés*, qui sont conçus pour conserver des ASN uniques au niveau mondial, mais qui ne sont pas interopérables avec l'Internet mondial ?

D'autres fonctions de gouvernance d'Internet inscrites dans l'infrastructure incluent la gestion et la sécurité de la dorsale Internet (son infrastructure permanente qui assure le haut débit) et plus généralement des équipements qui assurent l'accès à Internet. Il s'agit d'un domaine très vaste de la gouvernance d'Internet, géré par une variété d'acteurs publics et privés dans le monde. Deux exemples de comment ces fonctions doivent équilibrer une variété de valeurs, qui relèvent de l'intérêt public, sont l'utilisation des techniques d'inspection approfondie des paquets (*deep packet inspection* ou DPI) par les fournisseurs d'accès Internet (FAI) et la neutralité du net, dont je parle brièvement ci-dessous.

Le DPI est une technique invasive qui inspecte l'intégralité du contenu des paquets d'informations transmis sur Internet (Bendrath & Mueller, 2010 ; Ohm, 2009). Les FAI utilisent la DPI pour diverses raisons : exécuter des fonctions de gestion de réseau, qui relèvent plutôt des routines de sa maintenance ; identifier les virus, vers et autres problèmes de sécurité ; diffuser des publicités

en ligne ciblées sur le comportement ou le contexte de l'activité d'un utilisateur… mais aussi, potentiellement, pour participer à des demandes de censure et de surveillance gouvernementales ou d'application de la propriété intellectuelle. Indépendamment de son objectif affiché, l'utilisation du DPI soulève des implications importantes pour la vie privée et des préoccupations concernant ses possibles effets dissuasifs sur la liberté d'expression. Un problème de gestion de réseau qui équilibre de la même manière une variété de valeurs sociales et économiques est la neutralité du réseau (Schafer, Le Crosnier et Musiani, 2011 ; Marsden, 2017). La question politique fondamentale derrière la neutralité du réseau est de savoir si les FAI devraient être autorisés à donner la priorité à la transmission de types particuliers de contenu ou de trafic par rapport à d'autres. La controverse liée à la neutralité du réseau a entraîné comme corollaires une série de débats sur les modèles commerciaux des FAI et d'autres acteurs de la chaîne de valeur Internet, sur le pouvoir de monopole, sur la liberté d'expression, ou encore sur la concurrence économique (Felten, 2006 ; Wu & Yoo, 2007).

À un niveau plus proche du contenu, les décisions techniques et les choix de conception de ces acteurs qui ont été appelés les « intermédiaires de l'information en ligne » – les plateformes qui assurent la médiation entre le contenu Internet et les humains qui fournissent et accèdent à ce contenu – influencent des questions telles que la confidentialité et la réputation, et contribuent à façonner l'application de la propriété intellectuelle et de la censure. Les décisions qui façonnent les moteurs de recherche, par exemple, croisent des questions telles que le respect de la confidentialité dans la publicité personnalisée en ligne, les demandes de censure des gouvernements et les problèmes de réputation liés aux classements et aux évaluations (Gillespie, 2010 ; Grimmelmann, 2007 ; Zuckerman, 2010 ; Mager, 2017). Les décisions des médias sociaux et des intermédiaires de publicité en ligne ont des implications importantes en matière de confidentialité et de réputation (boyd et Hargittai, 2013). Les sites d'agrégation de contenu (photos, actualités, vidéos) contribuent à façonner des questions d'intérêt public telles que la mémoire et la pluralité culturelles, la médiation de la propriété intellectuelle et la confidentialité. Les politiques des systèmes de réputation ont une influence sur l'anonymat, la transparence et l'économie de la réputation en ligne (Solove, 2007). Ces intermédiaires ne fournissent pas directement de contenu, mais facilitent la circulation des flux d'information (et d'argent…) entre ceux qui fournissent et ceux qui accèdent à ce contenu. Les infrastructures virtuelles et matérielles

de ces plateformes, et les décisions politiques qui y sont intégrées, négocient intrinsèquement les transactions en ligne – entre marchés et acteurs sociaux.

Cet écosystème de technologies comprend également ces artefacts techniques, composantes essentielles d'Internet, dont la fonction infrastructurelle est plus immédiatement évidente : il s'agit des infrastructures physiques de bas niveau, qu'on a pu assimiler aux autoroutes ou aux artères de la société de l'information, et que Star (1999 : 379) nous invite « plus sobrement » à considérer également comme des « égouts ». Ces infrastructures incluent, par exemple, les câbles sous-marins, des milliers et milliers de kilomètres de fibre optique, posés au fond des océans et des mers, liens indispensables entre les réseaux de télécommunication du monde entier. Les enjeux géopolitiques de ces câbles ont une longue histoire (Griset, 1992), et ils posent aujourd'hui des questions telles que le poids des entreprises privées par rapport à celui des Etats dans leur gestion, le lien de ces infrastructures aux systèmes de surveillance numérique, ou leur impact environnemental à long terme. Ou encore, ces infrastructures comprennent les centres de données ou *data centers*, de grands sites physiques sur lesquels se regroupent des équipements constituant un système d'information, notamment des puissants ordinateurs appelés serveurs qui constituent les archives des grandes plateformes (Marquet, 2018). Ces centres de données soulèvent des enjeux tels que la concentration des infrastructures pour un gain économique, de territorialisation du numérique, et du manque de visibilité institutionnelle de ces points de gestion et d'accès à de masses importantes de données (Carnino et Marquet, 2018). Enfin, les Internet Exchange Points ou IXPs (dont DeNardis, 2012b propose une analyse nuancée) sont aussi un exemple de ces infrastructures physiques : il s'agit de grands immeubles hébergeant plusieurs commutateurs de réseau, qui évitent aux opérateurs d'établir des liens directs entre eux, le raccordement au point d'échange permettant à chacun d'échanger du trafic avec tous les autres opérateurs présents. Les IXPs jouent un rôle essentiel notamment dans les marchés numériques émergents, en rapprochant le contenu des utilisateurs, en promouvant la connectivité locale entre les opérateurs régionaux, en réduisant les coûts d'interconnexion et en réduisant la dépendance de la connectivité locale par rapport aux points d'échange étrangers. Dans l'ensemble, ces infrastructures physiques posent des questions de privatisation et donc de stratégies économiques, de coûts pour l'environnement, de géographies juridiques ; elles soulèvent dès lors des problèmes de gouvernance qui rejoignent ceux soulevés par la gestion des protocoles et des ressources Internet critiques.

Cette section a décrit de nombreuses façons dont les infrastructures de gouvernance d'Internet intègrent dans leurs caractéristiques techniques des préoccupations d'intérêt public, telles que la confidentialité, l'accès au savoir et la liberté d'expression. Comme ces exemples le montrent, les processus de conception et de développement nécessaires pour maintenir Internet opérationnel contribuent, en fin de compte, à la construction de la sphère publique numérique et arbitrent les arrangements de pouvoir, de liberté et d'autorité dans cette sphère. Beaucoup de ces fonctions sont cachées à la vue du public – pas intentionnellement cachées, mais pas nécessairement visibles pour les internautes. Presque aucune des fonctions de « gouvernance dans les infrastructures » décrites dans cette section n'est principalement gérée par les États et leurs gouvernements, et rarement ces fonctions de gouvernance impliquent une manipulation directe des contenus, ou un engagement direct des individus en ligne.

Or, de plus en plus – et grâce notamment à cette privatisation et cette omniprésence discrète – les infrastructures d'Internet sont appropriées ou cooptées à des fins de contrôle direct du contenu, et plus largement pour servir des fonctions très différentes que les objectifs originaux pour lesquels elles ont été conçues. C'est l'objectif de la prochaine section que d'aborder ce « tournant » dans la gouvernance d'Internet, qui est à la fois très pratique et conceptuel.

3.2.3. La gouvernance *par* les infrastructures d'Internet

Les contributions tirées des perspectives STS ces dernières années reconnaissent non seulement que les fonctions administratives et de coordination liées à l'infrastructure d'Internet ont toujours été des instruments de pouvoir (DeNardis, 2009), mais aussi que les points de contrôle infrastructurels, quelle que soit leur fonction d'origine, peuvent servir d'intermédiaires pour reprendre (ou remporter) le contrôle ou manipuler les flux d'informations, d'idées (et d'argent…) dans la sphère numérique. En effet, la mondialisation et l'évolution des technologies ont réduit la capacité des États-nations souverains et des producteurs de contenus médiatiques à contrôler directement le flux d'information. Cette perte de contrôle par rapport au contenu et l'incapacité des lois et des marchés à reprendre les rênes ont réorienté les luttes politiques et économiques dans

le domaine des infrastructures et, en particulier, des technologies de gouvernance d'Internet. Certaines infrastructures de l'Internet peuvent notamment être cooptées afin d'exécuter des fonctions politiques qui diffèrent des fonctions originelles et affichées comme « techniques » pour laquelle elles ont été conçues – ayant trait, à l'origine, au fonctionnement du réseau et à la gestion de ses flux. Il est bon de le rappeler, les *infrastructure studies* nous montrent que chaque « fonction technique » est aussi politique en tant que telle – que dès lors qu'on organise le fonctionnement du réseau, on fait de la politique ; le « bon déroulement » des processus techniques du réseau ou la gestion de ses flux ont déjà des dimensions politiques. Cependant, la dernière décennie a entraîné une prolifération de « nouveaux usages » politiques de certaines infrastructures, qui diffèrent sensiblement des objectifs affichés au début de leur conception et mise en œuvre. On a particulièrement exploré ce déplacement dans nos travaux sur le « tournant infrastructurel » (*turn to infrastructure*) dans la gouvernance d'Internet (Musiani *et al.*, 2016).

Les travaux qui suivent cette approche traitent notamment de l'utilisation du DNS comme outil d'exécution des droits de propriété intellectuelle (Merrill, 2016), ou du pouvoir discrétionnaire dont jouissent les intermédiaires de l'information pour hiérarchiser leurs intérêts stratégiques par rapport à leurs engagements en matière de confidentialité (Sargsyan, 2016). Ces contributions et bien d'autres montrent, dans l'ensemble, l'évolution d'une approche basée sur les « valeurs inscrites dans la conception » (« *values-in-design* ») (Flanagan *et al.*, 2008) vers une véritable *politisation* des infrastructures de la gouvernance d'Internet (DeNardis, 2009). Autrement dit, si, comme on l'a vu, les valeurs font partie de la conception des infrastructures depuis le début du « réseau des réseaux », elles sont intégrées à l'infrastructure technologique principalement pour remplir ses fonctions essentielles. Or, l'utilisation d'une infrastructure d'Internet pour remplir des fonctions autres que l'objectif pour lequel elle a été conçue peut, en réalité, entraîner d'importants « dommages collatéraux » quant à la stabilité et à la sécurité d'Internet et à la protection des libertés civiles en ligne. Dans les sections qui suivent, je présente plusieurs exemples de ce phénomène[29].

3.2.3.1. Gouvernance par l'infrastructure dans les conflits géopolitiques

[29] Cette section est une réélaboration de (DeNardis & Musiani, 2016).

Plusieurs types de tensions géopolitiques trouvent leur inscription dans les couches infrastructurelles de l'écosystème de gouvernance d'Internet. Ces tensions impliquent des conflits géopolitiques entre les États-nations, entre les gouvernements et les citoyens/activistes, et entre les juridictions des États-nations ou d'entités supra-nationales (telle que l'Union européenne) et des intérêts commerciaux particuliers.

Le système de noms de domaine est de plus en plus politisé en tant que site où se manifestent des tensions politiques et économiques mondiales ; les luttes de pouvoir mondiales pour le contrôle du DNS sont devenues un *proxy* des préoccupations internationales concernant l'hégémonie américaine sur Internet et ses pratiques de surveillance de masse, révélées par Edward Snowden. Si on a déjà abordé les caractéristiques techniques du DNS et la complexité institutionnelle, chapeautée par l'ICANN, qui préside à son fonctionnement, il faut ici mettre en relief que le DNS est également devenu un système d'infrastructure utilisé comme instrument pour résoudre des conflits culturels, et des controverses entre des régions géographiques, « contraintes » par un territoire, et des entreprises multinationales et leurs intérêts économiques – qui traversent les frontières via l'infrastructure physique et virtuelle décentralisée et distribuée de l'Internet. Par exemple, lorsque l'ICANN a lancé un appel à propositions pour augmenter le nombre de domaines de premier niveau (*top-level domain*, TLD), bon nombre des domaines de premier niveau proposés sont devenus des espaces contestés. Un exemple particulièrement éclairant a vu la société Amazon proposer de gérer un TLD « dot amazon » (.amazon), mais le comité consultatif gouvernemental (GAC) de l'ICANN s'est opposé à son introduction car .amazon est également considéré comme un marqueur culturel et géographique par les pays dont les frontières englobaient la forêt amazonienne. Le TLD « dot Patagonia » (.patagonia), convoité par la célèbre marque de vêtements, a fait l'objet de tensions similaires entre une entreprise internationale détenant une marque et une réalité géopolitique.

La manifestation de tensions géopolitiques dans les infrastructures Internet est peut-être encore plus claire à l'intersection de la cybersécurité et des infrastructures. Le ver informatique Stuxnet est à ce sujet le cas le plus emblématique de comment les tensions géopolitiques mondiales peuvent devenir profondément ancrées dans les infrastructures. Le cas de Stuxnet a montré comment les vers, virus et autres types d'attaques à la sécurité des réseaux, telles que les attaques par déni de

service distribué (DDoS), ne sont pas l'apanage exclusif de pirates informatiques isolés, ou de ceux qui se livrent à la cybercriminalité organisée ou à l'espionnage industriel. Ce sont des technologies qui agissent sur la base d'une stratégie politique, en perturbant intentionnellement un réseau, un site Web ou une application. Stuxnet était un ver informatique, détecté en 2010, qui (tel qu'il a été présenté dans les médias, sans que les gouvernements le reconnaissent officiellement), était un effort coordonné des États-Unis et d'Israël pour entraver le programme nucléaire iranien. Un ver est un code informatique à propagation automatique qui se réplique sans intervention humaine et en exploitant les failles de sécurité des protocoles, des systèmes d'exploitation ou des applications. Dans le cas de Stuxnet, un code sophistiqué a ciblé et désactivé les systèmes de contrôle, de supervision et d'acquisition de données (SCADA) de Siemens utilisés dans les installations nucléaires iraniennes. Alors que la première apparition de Stuxnet semblait ouvrir la voie à une nouvelle ère de cyberconflit, la mesure dans laquelle il reste une anomalie – la seule cyber-arme ultra-sophistiquée connue pour avoir été réellement déployée – est une énigme intéressante. Pourtant, il ne fait aucun doute que la guerre numérique par l'infrastructure reste un domaine d'enquête largement inexploré, en termes de construction des cyber-armes, de sélection de leurs cibles, et surtout en termes de sensibilisation du public à cette menace dans un contexte d'obfuscation très forte (Roberts, 2014).

Des cas plus largement documentés et mieux compris de conflits géopolitiques, se manifestant par des intrusions dans la cybersécurité, impliquent des attaques DDoS, soit utilisés par des gouvernements contre des sites militants ou des médias alternatifs et citoyens, soit par des citoyens contre des gouvernements, ou encore par des regroupements politiques faiblement structurés et motivés par des préoccupations idéologiques spécifiques. Ces types d'attaques neutralisent un ordinateur ciblé en le submergeant d'un nombre excessif de demandes envoyées simultanément à partir de centaines ou de milliers d'appareils informatiques. Plusieurs logiciels DDoS sont disponibles gratuitement en ligne, relativement faciles à utiliser et difficiles à empêcher. L'incident DDoS politiquement le plus médiatisé a peut-être été la désactivation massive de nombreux sites Web gouvernementaux et d'entreprise, en Estonie en 2007. Les attaques se sont poursuivies pendant plusieurs semaines et ont désactivé des sites critiques, notamment des banques, des médias et des serveurs gouvernementaux. Les autorités estoniennes avaient déplacé une statue militaire de l'ère soviétique d'un parc ; les minorités russes se sont engagées dans des manifestations de rue,

mais en ligne, les manifestations se sont manifestées sous la forme d'attaques politiques DDoS qui ont paralysé l'infrastructure informatique de l'Estonie.

Il est intéressant de remarquer que les attaques dans le domaine de la cybersécurité sont souvent considérées comme des outils « d'activiste » contre les gouvernements, mais, comme toutes les technologies, exactement le même code peut être utilisé par les gouvernements contre les citoyens, les médias et d'autres institutions dotées d'une présence en ligne. Qu'il s'agisse des conflits pour le contrôle des domaines de premier niveau, ou de l'exploitation de vulnérabilités particulières de certains protocoles pour mener des attaques de cybersécurité, ces conflits géopolitiques illustrent que les infrastructures d'Internet sont de plus en plus mobilisées comme des outils de défense des intérêts de différents acteurs – ou, au contraire, comme des leviers de préjudice pour des adversaires géopolitiques.

3.2.3.2. Gouvernance par l'infrastructure et droits de propriété intellectuelle

Les « points de contrôle » de l'infrastructure Internet sont également de plus en plus mobilisés pour faire respecter les droits de propriété intellectuelle en ligne. A l'aube des années 2000, les progrès technologiques tels que la facilité et le coût minimal de la distribution, de la réplication et du stockage des contenus numériques en ligne, ainsi que l'essor des systèmes distribués de partage de fichiers *peer-to-peer*, ont bouleversé les modèles commerciaux traditionnels des industries de contenu multimédia, et ont considérablement compliqués l'application des droits de propriété intellectuelle. Les industries des contenus multimédias ont traditionnellement cherché à appliquer la protection du droit d'auteur en ligne en poursuivant les personnes soupçonnées de partager illégalement du matériel protégé par le droit d'auteur, ou via des approches qui demandent le retrait de contenu spécifique contrevenant ; par exemple, Google a été sollicité à plusieurs reprises pour bloquer les vidéos YouTube portant atteinte au droit d'auteur, en vertu du mécanisme de notification et de retrait mis en place par le Digital Millennium Copyright Act (DMCA) aux Etats-Unis.

Les approches ciblant des individus spécifiques, ou des contenus contrefaits spécifiques, n'ont pas considérablement diminué l'étendue du partage de fichiers illégal à grande échelle. Ainsi, les

industries du contenu et les forces de l'ordre ont également tourné leur attention vers l'infrastructure Internet pour lutter contre la violation du droit d'auteur. Trois exemples clairs de ce « tournant infrastructurel » dans l'application des droits de propriété intellectuelle sont l'utilisation du DNS pour bloquer l'accès aux sites Web contenant des médias piratés ou vendant des produits contrefaits ; les approches de « réponse graduée » qui mettent fin à l'accès Internet des utilisateurs qui sont identifiés comme partageant à plusieurs reprises des médias piratés, et l'utilisation des algorithmes des moteurs de recherche pour bloquer ou faire reculer, dans les classements de liens qui résultent d'une requête, de sites Web soupçonnés de violer les droits de propriété intellectuelle.

Comme on le verra plus en détail dans le chapitre 4, le DNS a pu être utilisé comme mécanisme pour bloquer l'accès aux sites Web qui vendent ou partagent illégalement du contenu protégé par des droits d'auteur, ou des contrefaçons de produits de luxe, de marque, de produits pharmaceutiques, ou de films et de musique piratés. Des efforts législatifs ont cherché à inscrire ces approches de « blocage DNS » dans le droit. Ces approches impliquent généralement que les forces de l'ordre approchent une institution privée servant de registre de suivi des noms et des adresses, et demandent au registre de rediriger la résolution du nom de domaine vers une adresse IP qui pointe vers un message des forces de l'ordre plutôt que vers son site Web associé. En d'autres termes, le serveur et le site Web ne sont pas confisqués ou supprimés ; c'est le « chemin » vers le site Web qui est redirigé.

Un autre exemple notable du « tournant infrastructurel » dans l'application du droit d'auteur est la méthode dite de « riposte graduée », dont le but est de mettre fin à l'accès à Internet d'individus qui violent (prétendument et) à plusieurs reprises le droit d'auteur. Un certain nombre de pays ont au fil des années adopté ou envisagé des stratégies de réponse graduée, mais peut-être aucune n'a été aussi visible que celle mise en œuvre par l'HADOPI (Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet). L'HADOPI (acronyme qui a indiqué à la fois une loi et l'agence créée pour mettre en œuvre ses préconisations) a été très controversée et son cas a bien illustré que les stratégies de gouvernance « par l'infrastructure Internet » peuvent souvent avoir une efficacité douteuse par rapport à l'usage auquel elles sont destinées, mais avoir un fort potentiel perturbateur « collatéral », dans ce cas en ce qui concerne les droits d'accès à Internet.

En effet, l'HADOPI a permis la collecte automatique, sur des réseaux *peer-to-peer*, des adresses Internet de personnes procédant à des téléchargements illégaux. Ces personnes devaient été notifiées par l'Autorité à deux reprises de l'identification de la violation et, à terme, leur connexion Internet pouvait être interrompue.

L'inadaptation de cette procédure à certaines caractéristiques techniques d'Internet – et le risque qu'elle introduise de nouveaux problèmes sans résoudre ceux qu'elle souhaitait cibler – a été maintes fois soulignée (e.g. Le Fessant, 2009). Premièrement, le système de réponse graduée présuppose que les internautes sachent qu'ils commettent un délit par le fait de télécharger, alors que la complexité d'Internet rend impossible la distinction a priori des transferts légaux et illégaux, rendant ainsi très difficile d'obtenir une preuve de l'intention délictueuse. Deuxièmement, le système d'identification du coupable, basé sur l'adresse IP, entraîne un besoin de « sécurisation » des équipements informatiques domestiques hors de portée pour l'utilisateur final moyen, ainsi que pour la majorité des entreprises privées. Troisièmement, des spécialistes ont correctement prédit (p. ex. Le Fessant, 2009) que le système d'identification automatique des téléchargeurs illégaux tomberait rapidement en désuétude, poussant les internautes vers d'autres systèmes de consommation de contenu, potentiellement plus difficiles à contrôler – un mouvement qui s'est effectivement produit dans les années qui ont suivi, avec à la fois le streaming sites Web et les réseaux privés virtuels. À l'été 2013, le ministère français de la Culture a supprimé de la loi « le délit supplémentaire passible de la suspension de l'accès à un service de communication », prétendument parce que « le mécanisme [de la riposte graduée] n'avait pas profité aux services autorisés comme promis ». Pourtant, la valeur symbolique de la riposte graduée, dans la mesure où elle déplace l'application des droits de propriété intellectuelle du traitement de contenu spécifique contrefait vers une approche « par les infrastructures », reste forte et crée un précédent troublant. Aux États-Unis, les approches de type riposte graduée ne sont pas inscrits dans la loi, mais sont plutôt un système volontaire privé dans lequel les FAI acceptent de se prêter à une variété de mesures de type coercitif. Par exemple, après qu'une industrie du contenu ait informé un FAI de cas répétés d'infraction, et après des avertissements répétés à la partie contrevenante présumée, le FAI peut convenir de réduire la vitesse d'accès de cet utilisateur ou d'y mettre fin, selon ce que prévoient ses conditions d'utilisation du service.

Les moteurs de recherche, et les algorithmes associés, peuvent également servir de « goulot d'étranglement » (Tusikov, 2016) de l'infrastructure Internet, étant à leur tour considérés comme un possible mécanisme pour traiter les violations du droit d'auteur. Les lois sur le secret commercial protègent les algorithmes utilisés pour renvoyer et classer les sites Web dans les résultats de recherche, qui ne sont pas visibles ou accessibles publiquement ; cependant, les très grandes entreprises qui gèrent les moteurs de recherche les plus populaires, notamment Google et Yahoo!, ont reconnu que plus de deux cents facteurs entrent dans ces calculs algorithmiques. Comme pour toute conception technologique, la construction de ces algorithmes intègre les valeurs et les intérêts de leurs concepteurs et développeurs. Plusieurs spécialistes (p. ex., Gillespie, 2014) ont examiné les implications de la conception de ces algorithmes pour les questions qui ont trait à l'accès au contenu par les utilisateurs, telles que la pertinence de l'information ou son importance pour les individus. Mais les algorithmes des moteurs de recherche vont bien au-delà de l'analyse des informations et de son utilisation, pour inclure un certain nombre de droits et de restrictions concernant le contenu.

Les entreprises qui gèrent les moteurs de recherche (Google, en particulier) ont reconnu de manière transparente qu'elles prennent en compte les demandes de suppression de contenus protégés par le droit d'auteur dans les algorithmes, et rétrogradent (ou ne renvoient pas de liens vers) les sites Web identifiés comme étant en train de violer à plusieurs reprises les statuts du droit d'auteur. En 2012, Google a annoncé explicitement, et non sans controverses, que l'entreprise prendrait en compte les avis de suppression des droits d'auteur dans ses algorithmes de recherche. Amit Singhal, vice-président pour l'ingénierie de Google, déclara à cette occasion que l'entreprise avait développé « plus de 200 signaux » pour garantir que ses algorithmes de recherche fournissent les meilleurs résultats possibles, et qu'un « nouveau signal » allait désormais être pris en compte : le nombre d'avis valides de suppression de droits d'auteur reçus pour un site donné. Les sites avec un nombre élevé d'avis de suppression apparaîtraient désormais plus bas dans les résultats de recherche[30]. Google a reçu à ce jour (fin mars 2022) près de six milliards d'avis de violations du droit d'auteur et de demandes de supprimer les contenus associés[31] et intègre ces demandes

[30] Voir par exemple Kathryn McConnachie, « Google to implement 'pirate penalty' », ITWeb, https://www.itweb.co.za/content/VKA3Ww7dP6r7rydZ

[31] Selon le dernier *Google Transparency Report* : https://transparencyreport.google.com/copyright/overview?hl=en (consulté le 25 mars 2022).

directement dans les résultats de recherche. Il est important de noter que les moteurs de recherche n'évaluent pas la légitimité ou la pertinence de ces avis, bien qu'ils proposent un processus d'appel (ou de contre-avis).

Ces trois exemples du « tournant infrastructurel » dans l'application des droits de propriété intellectuelle (qui impliquent le DNS, l'équipement d'accès à Internet de l'utilisateur final, et les algorithmes de recherche) ont plusieurs caractéristiques communes qui ont des implications critiques pour l'écosystème de gouvernance d'Internet, l'accès à la connaissance, et leurs transformations. La première est que l'application du droit, dans ce cas des droits de propriété intellectuelle, est médiée par, voire trouve son origine dans le secteur privé, et en particulier, les intermédiaires privés d'information, soulevant des questions qui ont trait à leur légitimité et leur responsabilité envers le public, mais aussi au poids croissant de l'industrie privée dans des fonctions d'intermédiation ou d'exécution traditionnellement exercées par les gouvernements. De plus, chacune de ces approches entraîne des « dommages collatéraux » considérables, qui modifient l'infrastructure elle-même. Dans le cas du DNS, plutôt qu'effectuer une instance individuelle de blocage de contenu, des sites Web entiers sont bloqués ou rétrogradés. Dans le cas de la riposte graduée, un ménage entier peut voir son accès à Internet interrompu pour tout type d'activités, y compris les transactions commerciales, les activités pédagogiques en ligne ou l'accès aux services gouvernementaux. La question de l'efficacité de ces mesures se pose également, et ce indépendamment de leurs conséquences : par exemple, lorsqu'un nom de domaine est bloqué via une redirection DNS, l'opérateur d'un site Web contrefait peut facilement enregistrer un nouveau nom de domaine.

Pour résumer, ces approches ont des implications importantes pour l'accès au savoir et à la sphère publique démocratique, en plus d'ajouter une complexité potentiellement déstabilisatrice aux infrastructures déjà complexes de la gouvernance d'Internet qui impliquent des centaines de milliards de transactions en temps réel par jour.

3.2.3.3. Gouvernance par l'infrastructure et libertés citoyennes

Au sein des infrastructures Internet, on peut également observer comment les dynamiques de censure, de protection de la vie privée et de surveillance se déroulent de manières inédites dans l'écosystème Internet contemporain. Alors que l'histoire de la dissidence et de la résistance (et l'histoire de leur répression) ont toujours présenté des cas de retraits d'information, et des moyens de les empêcher, elles sont désormais, et ce de plus en plus, focalisées sur des dynamiques de perturbation technologique et de contournement des infrastructures critiques, ainsi que sur la recherche de nouveaux outils par lesquels différentes voix peuvent s'exprimer. En parallèle, un certain nombre de politiques au niveau national ou régional (par exemple, les lois sur la localisation des données, ou les réglementations en matière de *cloud computing* spécifiques à une région ou à un pays) appellent à des modifications de l'architecture d'Internet afin de créer des conditions spécifiques pour la protection de la vie privée et de la sécurité. Mais ce faisant, ces actions institutionnelles locales peuvent également contribuer à la fragmentation de l'Internet (Chander & Le, 2014). Et enfin, le rôle des intermédiaires de l'information dans la création et l'application *de facto* de normes concernant la vie privée est de plus en plus important, « élevant » ainsi ces acteurs d'un rôle identifié comme économique à des parties prenantes importantes, voire des « créateurs », de définitions spécifiques de la liberté d'expression et d'autres libertés civiles. Cette troisième sous-section du chapitre aborde quelques exemples de ces manières interconnectées dont le « tournant infrastructurel » affecte les libertés civiles.

Un lien prononcé entre infrastructure et gouvernance se produit dans celles que l'on appelle familièrement les interventions « *kill-switch* » sur Internet, dans lesquelles les gouvernements, par l'intermédiaire d'acteurs de l'industrie privée, provoquent des pannes des infrastructures de télécommunications et d'Internet, que ce soit via des protocoles, des blocages d'applications particulières, ou la suspension de l'ensemble des services de téléphonie mobile ou d'accès Internet. Si le système de commutation de paquets sous-tendant Internet a bien été conçu de manière à rendre le « réseau des réseaux » résilient à toute panne unique et généralisée, il existe des points de concentration et de vulnérabilité qui peuvent permettre à certains acteurs qui gèrent le réseau de perturber temporairement son fonctionnement. Les pannes d'Internet peuvent être mises en œuvre de diverses manières ; les niveaux de perturbation, à la fois en ce qui concerne leur degré d'intentionnalité et d'efficacité, varient considérablement, du filtrage d'une page ou d'un site Web

spécifique au blocage d'une application ou d'un protocole, en passant par la coupure de l'infrastructure physique à certains de ses endroits particulièrement concentrés ou stratégiques.

Un certain nombre de pannes d'Internet déclenchées par des gouvernements en réponse à des soulèvements citoyens ont fait l'actualité tout au long des années 2010 et jusqu'à ce jour, depuis le « printemps arabe » pendant lequel le gouvernement égyptien a demandé aux fournisseurs de services de suspendre leurs opérations de réseau, jusqu'aux très récentes coupures en Iran, en Zimbabwe, au Cambodge et, bien sûr, pendant le conflit russo-ukrainien de 2022. Ces pannes peuvent potentiellement causer des dommages aux infrastructures en soi, mais le plus grand défi qu'elles posent réside peut-être dans les préjudices qu'elles peuvent causer à la liberté d'expression et à la sécurité des populations. Dans l'Internet d'aujourd'hui, de plus en plus peuplé de tentatives de surveillance, de censure ou d'obtention et d'agrégation d'informations à diverses fins, ces tentatives ne peuvent que rarement être menées de manière indépendante par les États et leurs institutions, qui se tournent vers des intermédiaires d'information privés et leurs infrastructures pour atteindre leurs objectifs. Les intermédiaires d'information sont ainsi en mesure d'exercer une gouvernance déléguée dans une variété de situations, ce qui en fait non seulement des acteurs centraux de l'économie numérique, mais aussi *de facto* des acteurs de la gouvernance, dans la mesure où leurs politiques de confidentialité, leurs pratiques de collecte de données, leurs accords et alliances avec d'autres acteurs privés et institutionnels leur permettent de façonner fortement les définitions dominantes de la confidentialité et du contenu « légitime » sur Internet.

Toutes les entreprises du Web qui permettent aux individus de publier du contenu en ligne (Reddit, Facebook, Twitter, Google) sont aux prises avec des problèmes liés à la médiation et la modération des contenus (voir Badouard, 2020). Ces questions sont fortement compliquées par l'absence de frontières géographiques sur Internet, obligeant les entreprises à naviguer à travers des ensembles de lois et de traditions culturelles très hétérogènes. Ces entreprises reçoivent un nombre considérable de demandes de suppression de contenus ; Google, en particulier, s'est constamment référé à ses conditions d'utilisation pour supprimer uniquement le contenu qui enfreint la loi (ou ses propres conditions d'utilisation), et ce uniquement à la demande explicite des utilisateurs, des gouvernements ou des tribunaux. Un cas particulièrement critique s'est produit en septembre 2012, lorsque la publication sur Internet d'une vidéo réalisée par un individu de nationalité américaine,

ridiculisant le prophète Mahomet, aurait contribué aux dites « *Embassy Riots* », secouant le monde arabe pendant plusieurs journées. La décision de Google de bloquer sélectivement l'accès à la tristement célèbre vidéo dans deux des pays qui ont connu les bouleversements les plus sévères, l'Égypte et la Libye, tout en choisissant de ne pas la supprimer complètement de son site Web, a soulevé des questions fondamentales sur le contrôle que les entreprises du Web ont sur les formes d'expression en ligne. Les entreprises devraient-elles décider elles-mêmes des normes qui régissent ce qui est vu sur Internet ? Dans quelle mesure ces politiques devraient-elles être appliquées et sont-elles appliquées de facto ? Que faire des « précédents critiques » par la suite ? A l'occasion des *Embassy Riots*, le juriste Peter Spiro déclara notamment :

> *Google est le gardien mondial de l'information, donc si Google veut re-définir le Premier Amendement[32] pour exclure ce type de matériel, le reste du monde ne peut pas faire grand-chose à ce sujet (et) cela rend cet épisode encore plus significatif si Google décidait d'élargir son blocage (Spiro, en Miller, 2012).*

En bref, les intermédiaires de l'information sur Internet disposent désormais de pouvoirs et d'obligations similaires à ceux d'un tribunal, qu'ils exercent via l'infrastructure, et ils sont *de facto* en mesure de décider quel contenu reste public et ce qui est supprimé. Mais le cadre techno-juridique régissant la liberté d'expression en ligne – et avec ce cadre, la transparence et la responsabilité des individus, des entreprises et des gouvernements – est encore en devenir : ainsi, tout épisode de ce genre, initié par l'un des « géants » du Net, a créé depuis un précédent critique pour la protection ou l'atteinte aux libertés civiles.

Google a également été au centre d'une controverse importante, qui revient régulièrement à ce jour, sur sa mise en œuvre, à la suite d'un arrêt de la Cour de justice européenne, du « droit à l'oubli ». Les racines de ce concept se trouvent dans la volonté de l'individu de « déterminer le développement de sa vie de manière autonome, sans être perpétuellement ou périodiquement stigmatisé en conséquence d'une action spécifique accomplie dans le passé » (Mantelero, 2013), et, sur le plan opérationnel, consiste en la demande d'un individu de faire supprimer certaines données afin que des tiers ne puissent plus les retracer (Weber, 2011). Cependant, dans la pratique,

[32] La première clause de la Constitution des États-Unis, stipulant notamment que le gouvernement ne peut émettre des lois qui posent des limitations arbitraires à la liberté d'expression.

l'application de ce concept a suscité de vives controverses. Certaines d'entre elles sont liées à l'interaction du droit à l'oubli avec d'autres droits, notamment la liberté d'expression, et d'autres concernent quels acteurs peuvent faire respecter ce droit et – ce qui nous intéresse plus particulièrement ici – par quels moyens et instruments.

L'arrêt de 2014 de la Cour européenne de justice dans l'affaire Google Spain contre AEPD et Mario Costeja Gonzalez[33], considérant qu'un opérateur de moteur de recherche est essentiellement responsable du traitement qu'il effectue des informations personnelles qui apparaissent sur les pages Web publiées par des tiers, a reconnu de facto un droit à l'effacement sans toutefois accorder explicitement un droit à l'oubli. Cela a créé un précédent critique en termes d'obligations pour les moteurs de recherche d'examiner les demandes d'individus de supprimer des liens vers des pages Web librement accessibles à la suite d'une recherche de leur nom. Depuis la décision, Google a reçu des dizaines de millions de demandes ; plusieurs d'entre elles ont suscité des discussions selon qu'elles aient été prises en compte ou négligées, et au sujet de la conséquence de certains de ces effacements sur la liberté d'expression et sur l'accès à une pluralité de sources sur des sujets controversés (Mitrou & Karyda, 2012). Alors que le Règlement général sur la protection des données (RGPD) de l'Union européenne est entré en vigueur en mai 2018, la controverse autour du droit à l'oubli souligne, une fois de plus, le rôle prééminent des intermédiaires informationnels privés dans la gouvernance d'Internet par les infrastructures.

Un dernier exemple, et peut-être le plus important, de l'impact du « tournant infrastructurel » pour la définition et la protection des libertés civiles est la pertinence croissante des approches dites de « protection de la vie privée dès la conception », ou *privacy by design* (PbD) (Cavoukian, 2006, 2010 ; Schaar, 2010). Cette approche préconise que la protection de la vie privée doit être prise en compte et « intégrée » tout au long du processus d'ingénierie, et s'y conformer tout au long du cycle de vie d'une technologie particulière, afin de proposer la confidentialité « par la conception technique » plutôt que « par la politique ». La protection de la vie privée est intégrée à la technologie, intégrant un dispositif technique de protection juridique à la conception des services Internet. Alors que le concept et l'ontologie même de la PbD font l'objet de vifs débats, des objets, des marchés, des réalités économiques ont commencé à se construire autour de ce concept,

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

suscitant l'intérêt et le suivi des autorités de régulation nationales, supranationales et internationales. Au Canada, principalement en raison du travail d'Ann Cavoukian en tant que commissaire à l'information et à la protection de la vie privée de l'Ontario, la PbD a été proposée dès le début des années 2010 comme une intégration obligatoire dans les technologies qui ont d'importantes composantes liées à la communication et à la sécurité, et basées sur la collecte, l'analyse et l'échange de données personnelles, telles que la vidéosurveillance. En Europe, la protection des données par la conception technique a été intégrée à l'article 25 du RGPD. La protection de la vie privée est de plus en plus intégrée aux infrastructures.

3.2.3.4. Gouvernance par l'infrastructure comme proxy de redistribution du pouvoir

Chacun des grands domaines abordés dans ce chapitre fournit de nombreuses illustrations de comment un ensemble d'intérêts économiques et politiques se tourne vers l'infrastructure Internet et vers les systèmes de gouvernance de l'Internet en tant qu'instruments pour aborder des controverses, voire des conflits, socio-techniques diversifiés, survenant à la fois hors ligne et en ligne. En d'autres termes, les systèmes de gouvernance et d'architecture d'Internet ne sont plus relégués aux préoccupations qui concernent le fait de maintenir l'Internet opérationnel et sécurisé. Ces systèmes sont désormais clairement reconnus par les décideurs politiques, les acteurs privés et même les citoyens – dans une variété de configurations – comme des sites d'intervention pour une variété d'autres objectifs, qu'il s'agisse de protéger des intérêts économiques, d'influencer une situation politique, de reconfigurer des équilibres de pouvoir, ou d'obtenir un contrôle matériel ou symbolique sur une ou plusieurs composantes du cyberespace.

Comme ce chapitre – ainsi que, plus largement, une longue histoire de travaux STS sur les infrastructures, au-delà de l'Internet, l'a montré – l'incorporation de valeurs ou de droits particuliers à la technique a toujours fait partie de la conception des infrastructures technologiques. Les ingénieurs Internet n'ont pas fait exception, en concevant des protocoles qui affectent la confidentialité individuelle, l'accessibilité pour les personnes handicapées et d'autres préoccupations d'intérêt public ; ces valeurs sont entrées à faire part de l'infrastructure technologique, pour la plupart, dans un objectif de préservation, de « bon » fonctionnement et de sécurité du « réseau des réseaux ». Ce qui est intéressant et semble novateur dans ce qui est en

train de se passer pour les protocoles, algorithmes et infrastructures d'Internet, au cours notamment de la dernière décennie, est l'investissement de ces infrastructures par une variété d'acteurs afin de faire de la « politique par d'autres moyens » (Latour, 1988 : 229). On se trouve donc à observer deux « couches » politiques de ces infrastructures : une composée de fonctions dont l'objectif central et affiché est principalement procédural et technologique, quoiqu'intrinsèquement politique – comme la résolution de noms en chiffres, ou le renvoi algorithmique à des liens pertinents. Une deuxième couche politique de ces infrastructures est celle qui intervient après une re-spécification, où les problèmes et les programmes qui leur sont attachés sont modifiés pour servir des objectifs de surveillance, de censure, de coercition ou de résistance, ayant souvent des effets collatéraux importants pour la stabilité et la sécurité d'Internet ainsi que pour la protection des droits de l'homme en ligne. L'investissement[34] politique dans les aspects infrastructurels d'Internet met par ailleurs en lumière, de manière contrastée, ses « fonctions infrastructurelles » : pour chacun des exemples qu'on a proposés, ce n'est pas seulement ou simplement l'ajout d'une forme de contrôle sur une infrastructure qui se joue, mais bien des transformations plus profondes de ces infrastructures elles-mêmes, et de comment elles mettent en relation des personnes, des entités et des artefacts.

Cette reconnaissance de l'infrastructure comme moyen de faire avancer différents objectifs de contrôle et de protection juridique nous ramène également à la question de qui devrait contrôler la gouvernance et l'architecture d'Internet. Les luttes de pouvoir autour des infrastructures Internet, telles que le contrôle du fichier de la zone racine, existent depuis des années, mais se sont intensifiées parallèlement à la reconnaissance croissante du rôle des infrastructures dans la médiation des conflits politiques et économiques. Ces questions sont encore amenées à évoluer, alors qu'Internet évolue d'un système de communication à un « Internet des objets » utilisé non seulement comme une sphère publique au sein de laquelle on communique et échange du contenu, mais comme un système de contrôle qui connecte aussi bien des humains que des systèmes industriels aux appareils ménagers.

[34] Mot qui, de façon intéressante, peut être compris pour parler de la gouvernance par l'infrastructure dans le triple sens de « miser sur » quelque chose, « rentrer dans » quelque chose afin d'obtenir (plus de) pouvoir, mais aussi « habiller » quelque chose d'une couche supplémentaire afin de lui donner de la valeur.

Une grande partie de l'écosystème de gouvernance de l'Internet, à la fois l'architecture technique et les institutions et entreprises qui garantissent sa coordination, reste souvent dans ses couches inférieures, mais croise de nombreux enjeux d'intérêt public (et est d'ailleurs de plus en plus traité également par la presse généraliste). Cette transformation en une ère de gouvernance mondiale par l'infrastructure Internet présente une opportunité, pour la recherche, de ramener ces infrastructures politisées au premier plan.

3.3. L'infrastructure, une « fonction » de gouvernance

Au cours de ce voyage dans les infrastructures gouvernées, les infrastructures comme porteuses de valeurs « dès leur conception », et enfin dans les infrastructures comme outils de gouvernance, on a vu comment les analyses de la construction et de la matérialité des infrastructures numériques offrent de nouvelles perspectives sur la portée et les limites du changement technologique lié à Internet et sur son potentiel de gouvernance, pour au moins deux raisons.

En premier lieu, la (re)découverte du caractère infrastructurel des systèmes sociotechniques permet de (re)voir comment les applications des nouvelles technologies se mêlent aux acteurs, aux objets et aux processus dominants. L'infrastructure, comme le dit Star (1999 : 382), « ne se développe pas de toutes pièces ; elle se débat avec l'inertie de ce qui est déjà installé et hérite de ses forces et de ses limites ». Les approches axées sur l'infrastructure d'Internet et son poids politique contribuent à mettre explicitement en avant la nature contestée et relationnelle du changement technologique.

En second lieu, mettre en évidence les efforts qui tendent à positionner les systèmes numériques en réseau comme matériels et infrastructurels nous invite à considérer les contradictions du changement technologique. La dénaturalisation des systèmes sociotechniques, considérés comme des acquis ou « boîtes noires », attire l'attention sur la prédisposition à l'échec et la nature faillible de ces systèmes. Star (1999 : 382) souligne comment « la qualité normalement invisible de l'infrastructure opérationnelle devient visible lorsqu'elle s'effondre ». On est, par exemple, bien plus susceptible de remarquer notre dépendance au réseau électrique à l'occasion d'une coupure

d'électricité que lorsque tout fonctionne bien[35], ce qui peut également s'appliquer aux systèmes numériques qui connectent les individus, qui leur permettent l'accès à Internet en haut débit ou qui convertissent des adresses purement numériques en adresses plus intelligibles pour le cerveau humain, ou encore, de la *blockchain* qui sous-tend Bitcoin.

Comme manifestations de l'échec, les défaillances au niveau des matériaux et des processus qui sous-tendent les systèmes sociotechniques ne sont cependant pas *uniquement* pertinentes dans les instants d'instabilité qui le démasquent. Au contraire, elles sont *toujours* importantes. Les limites contribuant à « l'inégalité de l'infrastructure » (Nelms, 2016 : 511) peuvent contribuer à mettre en avant des questions plus générales d'accès et à problématiser les informations qui peuvent être normalisées et opérationnalisées, et celles qui ne le peuvent pas.

En un mot, c'est en analysant la politique des infrastructures technologiques et en la fondant dans leur matérialité, qu'on peut travailler à développer une perspective permettant d'appréhender ce qui, en dernier lieu, constitue des modèles contestables – et contestés – de continuité et de changement.

On en vient maintenant à la deuxième partie de ce mémoire, qui consiste en une présentation de cas emblématiques de formes d'action liées à la gouvernance par l'infrastructure – d'un processus de standardisation informelle d'un protocole à la fabrication d'alternatives pour l'annuaire d'Internet, d'un développement technique qui permet de rétablir l'intégrité d'un système distribué à la création de points de contrôle, surveillance et censure dans un Internet « national ». Tirés des différents terrains de recherche que j'ai effectués après 2012, ces chapitres auront la question de la « gouvernance par l'infrastructure » en fil rouge et en montreront l'importance conceptuelle et pratique dans l'Internet d'aujourd'hui.

[35] On rappellera par ailleurs que la critique des *infrastructure studies* par des perspectives de « Global South » montre que cette affirmation est à nuancer. C'est dans un monde très particulier que certaines infrastructures fonctionnent sur ce mode, alors que dans beaucoup d'endroits (pays, villes, campagnes), il est plus difficile de distinguer entre phases de coupure et état « normal » de fonctionnement, et les systèmes d'infrastructure sont loin d'aller complètement « de soi ».

Chapitre 4. Le *Domain Name System* comme instrument de gouvernance, entre cooptation et évasions

Le système de noms de domaine d'Internet (*Domain Name System* ou DNS) est un des plus célèbres systèmes technologiques d'Internet, de par son rôle central dans le bon fonctionnement de l'écosystème du réseau des réseaux (comme on l'a vu lors des chapitres précédents, il revêtit une fonction d'« annuaire ») et au vu de l'histoire controversée de l'institution qui en assure la gestion, l'ICANN. Ce chapitre montre comment la fonction de base du DNS a été progressivement élargie, reconfigurée ou cooptée pour d'autres objectifs, notamment comme moyen d'application des droits de propriété intellectuelle et régulateur de contenus. Dans la deuxième partie du chapitre, je montre comment des projets de DNS alternatif et décentralisé se sont développés afin de contrer cette cooptation, également en se servant de moyens « d'infrastructure »[36].

Le DNS est un système de nommage hiérarchique distribué qui assure la traduction entre les adresses numériques du protocole Internet (IP), utilisées par les ordinateurs pour acheminer les paquets d'informations (texte, vidéo, audio, etc.) sur l'Internet (par exemple 147.9.2.4) et les noms de domaine alphanumériques que les individus utilisent pour accéder aux sites Web (par exemple, www.cnrs.fr). Au sommet de ce système de classification se trouve le fichier de la zone racine, un répertoire faisant autorité pour tous les domaines de premier niveau (TLD) – les identifiants qui suivent le « point » dans une adresse Web (par exemple, le *.com* dans *google.com*) – et leurs numéros d'adresse IP correspondants. Les domaines de premier niveau peuvent être divisés en deux catégories distinctes : les domaines génériques de premier niveau (gTLD) (par exemple, .com, .org et .edu) et les domaines de premier niveau de code pays (ccTLD) (par exemple, .uk, .us et .fr). À première vue, le DNS remplit une fonction technique apparemment banale mais très complexe, en traduisant les noms en chiffres. Cependant, l'importance de ce système de

[36] Il ne me semble pas déplacé de rappeler ici que, ayant effectué mon enquête de terrain pour cette recherche aux Etats-Unis, et plus précisément à Washington, DC (2012-2013), plusieurs éléments de contexte techno-juridiques sont principalement centrés sur ce pays. Une partie de cette enquête a fait l'objet d'un chapitre dédié dans le volume *The Turn to Infrastructure in Internet Governance* (Musiani, 2016), dont une version préliminaire a été récompensée par le Best Paper Award de la Communication Policy & Technology Section de l'IAMCR en 2013. Je dois beaucoup aux échanges avec Kenneth Merrill, dont la thèse « *Domains of Convenience* » j'ai contribué à encadrer de 2016 à 2018 à l'American University.

classification a des conséquences sociales, politiques et économiques considérables. En fait, le DNS est devenu l'un des principaux champs de controverse où le pouvoir social, politique et économique est « inter-médié » dans la sphère publique en réseau (DeNardis, 2012).

Les controverses sur le contrôle de la zone racine du DNS ont eu un rôle de premier plan dans le monde entier, car diverses parties prenantes de l'Internet, des plus hauts dirigeants mondiaux aux groupes de la société civile, ont remis en question la nature ostensiblement non-gouvernementale de la gouvernance de l'Internet et le rôle d'organisations telles que l'Internet Corporation for Assigned Names and Numbers (ICANN), qu'on a déjà pu introduire plus haut – un organisme à but non lucratif basé en Californie et chargé par le ministère américain du commerce (DoC) de superviser la gestion de la racine. Parmi les responsabilités déléguées à l'ICANN figure la « fonction IANA », qui comprennent l'attribution des adresses IP mondiales, les numéros de systèmes autonomes et la gestion de la racine. Alors que le scepticisme à l'égard du rôle de l'ICANN dans la gouvernance de l'Internet a couvé depuis des années avant cet événement, les révélations sur la surveillance massive des réseaux de communication mondiaux, divulguées en 2013 par l'ancien contractant de la NSA Edward Snowden ont recentré l'attention sur ce domaine apparemment obscur de la politique d'information sur les réseaux et sur la mesure dans laquelle les revendications de « multipartisme » peuvent être prises au sérieux. Le contrôle de la zone racine est par ailleurs le dernier d'une longue série de controverses politiques et économiques sur le contrôle du DNS, y compris les questions relatives aux modes de censure directs et indirects.

Parmi les exemples, on peut citer le projet chinois du Bouclier d'or (communément appelé dans les médias anglo-saxons le « Great Firewall », en jouant sur les mots anglais correspondants à « muraille » et « pare-feu »), dans lequel les autorités bloquent, en essence, la connexion entre le nom de domaine d'un site web figurant sur une liste noire et son adresse IP, empêchant ainsi les utilisateurs d'accéder à des sites web politiquement sensibles (Zittrain & Edelman, 2003). De même, les autorités iraniennes utilisent depuis longtemps le filtrage DNS, entre autres techniques, pour bloquer l'accès aux sites web de l'opposition tout en poursuivant une initiative plus large visant à créer un intranet national alternatif approuvé par l'élite religieuse, communément appelé l'« Internet Halal » (Dehghan, 2012). Ces modes de censure étatique ont attiré une grande attention de la part des chercheurs et des décideurs politiques, mais des modes de médiation de contenu de

plus en plus indirects et subtils sont apparus, dans lesquels les gouvernements exercent une pression politique et économique sur les intermédiaires du secteur privé, y compris ceux qui remplissent des fonctions liées au DNS, pour qu'ils agissent en tant que médiateurs et modérateurs des contenus numériques (Benkler, 2011). Mais si les gouvernements considèrent des ressources Internet critiques comme le DNS en tant que technologies de contrôle potentiellement efficaces, d'autres acteurs exploitent leur potentiel d'outils de dissidence et de résistance. En effet, les possibilités offertes par ce système de nommage sont accessibles à tous, y compris aux acteurs étatiques et non étatiques ayant des intérêts et des valeurs divergents sur toute une série de questions, allant de la vente de biens illicites (par exemple, Silk Road) aux jeux d'argent en ligne (par exemple, Bovada.lv).

C'est en ce sens que les noms de domaine sont des objets relationnels – ils revêtent des significations différentes pour différents acteurs (Bowker & Star, 1999). En effet, tant les contrevenants au droit d'auteur que les organismes de réglementation gouvernementaux exploitent le DNS pour servir leurs propres intérêts, ce qui donne lieu à ce qui s'apparente souvent à un jeu mondial de montée en puissance réglementaire. Pourtant, les noms de domaine sont également des éléments centraux du commerce électronique, offrant des opportunités « de marque » souvent surprenantes, comme dans le cas de la petite nation insulaire de Tuvalu, dont le ccTLD *.tv* est l'un des plus importants au monde en raison de sa valeur pour les sites web associés à l'industrie de la télévision. De même, les domaines de premier niveau (TLD) peuvent être considérés comme matériels et sémiotiques (Latour, 2005 ; Law, 2009) dans la mesure où ils sont composés d'objets matériels habitant des espaces physiques entretenus et exploités par des individus aux intérêts et valeurs variés. En ce sens, ils sont l'amalgame matériel d'objets techniques (serveurs, points d'accès à la dorsale Internet, câbles sous-marins, etc.) et d'acteurs sociaux (des techniciens qui entretiennent le centre d'information réseau [NIC] d'un TLD, jusqu'à ceux qui façonnent la politique du TLD au niveau local).

La représentation du DNS sous forme d'une carte montrerait un réseau d'acteurs techno-sociaux distribué dans le monde entier, notamment des serveurs de noms de domaine qui résolvent les noms et les numéros de manière décentralisée, indépendamment des contraintes géographiques. Pour rendre ce processus plus rapide et plus efficace, des « serveurs récursifs » sont utilisés pour

accélérer la résolution du DNS à la périphérie du réseau (c'est-à-dire au plus près des utilisateurs finaux). Sans un DNS universel et pleinement fonctionnel, les utilisateurs finaux seraient contraints de mémoriser de longues chaînes de chiffres pour accéder à leurs sites web de prédilection, une perspective qui doit sembler familière à toute personne ayant vécu avant l'ère des annuaires téléphoniques électroniques, des listes de contacts des téléphones intelligents et de l'identification de l'appelant. Ce n'est qu'une des raisons pour lesquelles le DNS est considéré comme une ressource Internet critique nécessaire au bon fonctionnement de l'Internet, et c'est pourquoi la gouvernance du DNS continue d'être une affaire très scrutée et souvent controversée.

4.1. La gouvernance du DNS

L'autorité sur le DNS revient essentiellement à l'ICANN, qui a été historiquement chargée par le ministère du commerce des États-Unis de superviser le DNS et les opérations liées au DNS. À cette fin, l'ICANN exerce son autorité de deux manières : en accréditant les bureaux d'enregistrement (par exemple GoDaddy), qui fournissent des noms de domaine aux clients, et en supervisant les registres (par exemple Verisign), qui gèrent la base de données des noms et des numéros pour chaque domaine de premier niveau. Toutefois, ces fonctions administratives assez simples ne sont qu'une partie du rôle de l'ICANN dans la gouvernance du DNS. Par exemple, l'ICANN est chargée de coordonner le fonctionnement des serveurs racine, qui font autorité en matière de correspondance entre les noms de domaine et les numéros correspondants, et que tous les autres serveurs du monde imitent (Mueller, 2002). L'ICANN résout également les litiges relatifs aux marques commerciales sur les noms de domaine (par exemple, qui a le droit d'exploiter le domaine candyland.com : Hasbro, propriétaire du célèbre jeu de société pour enfants, ou le site Web de divertissement pour adultes portant le même nom ?) (Geist, 2001). Enfin, l'ICANN participe également à la définition de ce qui constitue une censure au sein du DNS.

En plus de ces tâches administratives, qui sont à elles seules lourdes de conséquences politiques et économiques, les noms de domaine eux-mêmes sont imprégnés de valeurs politiques, économiques et culturelles, qui doivent toutes être prises en compte. En effet, l'aspect multi-dimensionnel des noms de domaine est devenu de plus en plus apparent dans les années les plus récentes (depuis

2011-2012), avec l'expansion d'une nouvelle série de gTLD qui nécessitent la coordination d'intérêts apparemment disparates. C'est le cas de l'extension .amazon, dans laquelle le géant de la vente en ligne Amazon.com a cherché à prendre le contrôle du nouveau gTLD, malgré les revendications légitimes de ceux qui ont des liens locaux plus directs avec la région amazonienne. Alors que, en 2019, Amazon a gagné une bataille de plus de 7 ans contre une alliance de huit pays sud-américains et a désormais le droit de gérer .amazon, on voit à quel point les disputes concernant les noms de domaine reflètent la myriade d'intérêts – culturels, politiques et économiques – impliqués dans la création et la distribution des noms de domaine, et la mesure dans laquelle ceux-ci peuvent être considérés comme des sites de ce que l'anthropologue Anna Tsing appelle la « friction » mondiale (Tsing, 2011).

Cependant, alors que l'ICANN est chargé de la gouvernance du DNS, d'autres acteurs - des États-nations à l'industrie privée, en passant par des individus avec une variété de motivations plus ou moins légitimes – ont de plus en plus utilisé le DNS lui-même comme un mode de gouvernance basé sur l'infrastructure. La première partie de ce chapitre traitera de l'utilisation du DNS comme moyen de contrôle du contenu sur le Web ; plus précisément, elle aborde le DNS comme mode d'application des droits de propriété intellectuelle basé sur l'infrastructure, et comme outil potentiel de censure politique. Avant de s'y concentrer, on présente tout d'abord une brève histoire du DNS, comme prélude nécessaire à la compréhension des façons dont ses usages ont été multipliés et cooptés par la suite.

4.2. Petite histoire du DNS

En tant que l'un des prédécesseurs de ce que nous appelons aujourd'hui Internet, l'ARPANET de l'Advanced Research Projects Agency a été conçu avec deux objectifs. Premièrement, en tant que projet de défense, l'architecture distribuée du réseau était destinée à fournir un moyen de communication résilient en cas de frappe nucléaire sur les États-Unis. Deuxièmement, en tant qu'outil de recherche, ARPANET permettait aux informaticiens et aux ingénieurs (les personnes qui allaient ensuite favoriser le développement de l'Internet mondial et du World Wide Web) de communiquer et de partager des connaissances indépendamment de l'endroit géographique auquel

ils se situaient (Abbate, 2000). Au début, il y avait si peu d'ordinateurs connectés à ARPANET que ces chercheurs saisissaient simplement l'adresse IP numérique de l'ordinateur auquel ils souhaitaient se connecter, de la même façon dont on aurait saisi un numéro de téléphone d'un ami proche ou d'un parent à l'époque où les carnets d'adresses numériques et l'identification de l'appelant n'existaient pas encore.

Avec le développement d'Internet au milieu des années 80, la liste des adresses IP est devenue trop longue à mémoriser et des identifiants alphanumériques ont donc été utilisés pour représenter les adresses IP des ordinateurs hôtes des différentes institutions de recherche connectées au réseau. Pour faciliter la traduction de ces noms en numéros correspondants, Jon Postel et Paul Mockapetris ont développé le système de noms de domaine (DNS) en 1983. Ce système de dénomination hiérarchique a permis aux ordinateurs de rechercher systématiquement, de façon efficace, dans cette hiérarchie de noms et de numéros. Lorsqu'un utilisateur saisit un nom de domaine, par exemple le pionnier « stanford.edu », l'ordinateur interroge le DNS en commençant par les réseaux locaux (le bas de la hiérarchie du DNS), en remontant le DNS jusqu'aux domaines de deuxième niveau, aux domaines de premier niveau et, si nécessaire, à la zone racine, jusqu'à ce que l'adresse IP de Stanford soit localisée. En tant que répertoire faisant autorité pour tous les domaines de premier niveau, y compris les domaines génériques de premier niveau (gTLD) et les domaines de premier niveau de code pays (ccTLD), le fichier de la zone racine est une ressource particulièrement critique pour le fonctionnement de l'Internet. Par conséquent, il est devenu un point central de la contestation politique et économique dans les débats sur la gouvernance de l'Internet ; Mueller écrit que « le pouvoir politique, ainsi que les avantages économiques, sont impliqués dans les décisions concernant qui ou quoi est publié dans la zone racine » (2004 : 51).

Conformément à l'architecture distribuée des débuts d'Internet, il existe treize fichiers de zone racine identiques répliqués sur des serveurs au Royaume-Uni, au Japon et aux États-Unis (quoique la majorité soit basée aux États-Unis). Ces serveurs racine sont étiquetés de A à M, le serveur de zone racine A contenant le fichier faisant autorité, contrôlé par l'ICANN.

Avant la création de l'ICANN, les domaines de premier niveau (TLD) étaient attribués sur une base *ad hoc* par Jon Postel, qui a personnellement géré le DNS en tant qu'administrateur de

l'Internet Assigned Numbers Authority (IANA) jusqu'à sa mort en 1998. L'influence de Postel ne peut être surestimée, notamment en ce qui concerne la création de normes pour l'administration du DNS. Décrivant la manière apparemment « laissez-faire » avec laquelle des ressources Internet essentielles comme les ccTLD ont été déléguées, Postel a expliqué le processus par lequel il a sélectionné les gestionnaires de TLD : « généralement la première personne qui demande le poste (et qui est en quelque sorte considérée comme une 'personne responsable') » (Mueller, 2002). Alors que le nombre de demandes de ccTLD passait de 46 en 1990 à 108 en 1993, Postel a pris les premières mesures pour créer un ensemble de normes pour la délégation des ccTLD, en rédigeant le RFC 1951, qui codifiait l'utilisation de l'ISO 3166-1, un document de l'Organisation internationale de standardisation (ISO) fournissant une liste de codes pays à deux caractères, à utiliser comme ccTLD. Le raisonnement de Postel pour l'utilisation de l'ISO 3166-1 était clair : il fournissait un système uniforme et cohérent d'attribution des noms de ccTLD, tout en évitant le champ de mines politique d'assumer cette tâche lui-même. La sélection de tout ensemble de normes est par ailleurs, comme on en a déjà fait l'argument dans les chapitres précédents, une décision intrinsèquement politique, et cette décision ne faisait déjà pas exception malgré les efforts de Postel – un fait qui est devenu très vite apparent dans les controverses sur la décision d'utiliser .uk au lieu de .gb, l'élimination progressive du ccTLD .su de l'Union soviétique, la décision de déléguer .ps au Territoire palestinien, et l'inclusion, à terme, de .eu comme premier ccTLD délégué à une entité supranationale (von Arx & Hagen, 2002).

Alors que la bulle des « dotcoms » était en pleine expansion au milieu des années 1990, l'administration Clinton a entamé le processus de privatisation officielle du DNS, ayant compris – Internet devenant rapidement le principal moyen de communication mondial – qu'elle devait se distancer de la perception croissante selon laquelle les États-Unis contrôlaient l'Internet mondial. Cette perception était loin d'être sans fondement, notamment en ce qui concerne le DNS : le fichier de la zone racine était à l'époque sous l'administration directe du ministère du Commerce américain. À cette fin, l'administration Clinton a publié en 1998 ce qui allait être connu sous le nom de « Livre vert », décrivant le transfert, facilité par le gouvernement, du contrôle du DNS à une entité privée sous contrat avec le ministère du Commerce. En raison notamment du moment de sa publication, le livre vert a suscité une vive controverse, en particulier de la part de parties prenantes internationales telles que l'Union internationale des télécommunications (UIT) et

l'Organisation mondiale de la propriété intellectuelle (OMPI), une alliance qui reste un acteur important dans les questions de gouvernance de l'Internet. En réponse, le ministère du commerce américain a publié ce que l'on a appelé le « Livre blanc du DNS », en revenant sur certaines des formulations qui avaient suscité le plus d'objections. Ce document établit quatre principes censés gérer la gouvernance du DNS dans le futur : la stabilité, la concurrence, la coordination privée ascendante, et la représentation. Caractéristique centrale du livre blanc, celui-ci appelait officiellement à la création d'une entité privée qui reprendrait le contrôle du DNS au gouvernement américain. A cette fin, le livre blanc stipulait « que ni les gouvernements nationaux agissant en tant que souverains, ni les organisations intergouvernementales agissant en tant que représentants de gouvernements, ne devraient participer à la gestion des noms et adresses Internet » (National Telecommunications and Information Administration, 1998).

Le 30 septembre 1998, l'ICANN fut constituée en tant qu'organisation privée à but non lucratif basée à Los Angeles, en Californie. Sa mission consistait à prendre en charge plusieurs tâches liées à l'Internet, notamment la coordination des adresses IP et la gestion du système de noms de domaine, auparavant assurée par l'IANA. Conformément à l'engagement de l'organisation à rechercher la représentativité, l'ICANN a mis en place plusieurs comités consultatifs, dont le Comité consultatif gouvernemental (GAC), créé pour permettre aux représentants des États-nations et des organisations intergouvernementales, comme l'UIT et l'OMPI d'exprimer leurs préoccupations. En février 2000, le GAC a présenté ses « Principes de délégation et d'administration des ccTLD », dans le but de codifier les règles régissant la délégation des ccTLD sous le nouveau régime de l'ICANN. Toutefois, cet effort a été accueilli avec désapprobation par les gestionnaires de ccTLD, qui ont considéré les principes comme un faux-fuyant.

Malgré le transfert ostensible du contrôle de la racine à l'ICANN, de nombreuses parties prenantes, notamment celles représentées par le GAC, ont considéré que cette initiative n'était rien de plus que de la poudre aux yeux. Soulignant la mesure dans laquelle la perception du public et les cadres médiatiques (Pavan, 2012) ont façonné la politique à l'époque, le président de l'ICANN Stuart Lynn a écrit « si l'ICANN vient à être considéré comme un simple outil du gouvernement américain, il n'aura plus aucun espoir d'accomplir sa mission originale » (Lynn, 2002). Ce sentiment a été à l'origine d'une série de réformes adoptées par l'ICANN en 2002, dont la création

de la *Country Code Domain Name Supporting Organization* (ccDNSO) pour faciliter davantage les intérêts des gestionnaires de ccTLD et des États-nations. Pourtant, tout comme des politiques telles que les Principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine (*Uniform Domain-Name Dispute-Resolution Policy*, UDRP) de l'ICANN ont été créées en réponse à la commercialisation du web et à la prise de conscience collective de la valeur des noms de domaine en tant que propriété, la ccDNSO reflète la reconnaissance par les États-nations du potentiel de marque des ccTLD. Dans certains cas, la valeur sémiotique des ccTLD reflète des notions, très sensibles, d'identité nationale (par exemple la redélégation du ccTLD .za à l'Afrique du Sud). Dans d'autres cas, comme celui de la nation insulaire polynésienne de Tuvalu, le désir de récupérer son ccTLD .tv était motivé par le potentiel économique d'un code pays commercialisable (de nombreux sites Web de l'industrie de la télévision ont demandé des domaines .tv).

Pendant ce temps, les débats continuaient de faire rage sur le rôle approprié des États-nations dans l'ICANN et la gouvernance de l'Internet en général. Les révélations d'Edward Snowden concernant la surveillance électronique du trafic Internet ont relancé les débats sur le contrôle des ressources Internet essentielles ; en octobre 2013, l'ICANN a figuré parmi les nombreux gestionnaires de l'infrastructure Internet qui ont signé la « déclaration de Montevideo sur le futur de la coopération Internet », qui prônait entre autres l'accélération de la transition vers une gestion pleinement mondialisée de la fonction IANA[37]. En réponse à ces révélations et à la perception de l'hégémonie des États-Unis sur le DNS, certains ont suggéré des approches alternatives pour gouverner le DNS, allant de nouveaux modèles de gouvernance multipartites avec un plus grand rôle pour les gouvernements et les organisations intergouvernementales (von Arx & Hagen, 2002), à la création de DNS alternatifs, comme on le verra dans la deuxième partie du chapitre. La controverse autour du DNS et de sa gouvernance a notamment débouché, plus récemment, sur la finalisation formelle de la transition IANA, qui a vu l'ICANN terminer son contrat avec le ministère du commerce américain (octobre 2016). Mais les débats sur l'influence de facto des Etats-Unis sur des composantes vitales de l'Internet mondial ne se sont pas arrêtés pour autant, alors que des nouveaux défis se posent pour l'ICANN, par exemple la prise en compte du Règlement général sur la protection des données européens dans le système d'adressage.

[37] https://www.icann.org/en/announcements/details/montevideo-statement-on-the-future-of-internet-cooperation-7-10-2013-en

4.3. La gouvernance *par* le DNS : instrument d'application des droits de propriété intellectuelle

Parmi les nombreuses conséquences de la propagation rapide de l'économie de l'information en réseau, la circulation libre et non-contrainte par les frontières géopolitique des flux d'information mondiaux s'est avérée particulièrement perturbante pour ceux qui tentent de contrôler la propriété, tout particulièrement la propriété intellectuelle, dans cette sphère en réseau. Le défi inhérent à l'exploitation de ces flux pleinement globalisés est d'autant plus critique que plusieurs pays dans le monde continuent leur transition d'une économie industrielle produisant des biens tangibles à une économie de l'information reposant essentiellement sur des contenus et des données créatifs. Dans ce contexte, comme l'a souligné tout récemment Schwemer (2021), la dernière décennie a vu le développement de plusieurs mécanismes de modération des contenus et d'application de la propriété intellectuelle qui ont lieu dans les « couches inférieures » de l'Internet, et non pas suite à une prise de décision d'un modérateur humain, par rapport à un contenu particulier, et de façon visible par l'utilisateur : le droit est délégué à des propriétés de la matière technique (Latour, 2000). Le DNS est une des technologies « de couches inférieures » qui sont désormais mobilisées à cet égard.

4.3.1. Le DNS et l'application du droit de propriété intellectuelle : le cas *Operation In Our Sites*

Au début des années 2010, le plan stratégique conjoint de l'administration Obama aux États-Unis a demandé à l'*Intellectual Property Enforcement Coordinator* (IPEC), en coordination avec divers organismes fédéraux chargés de l'application de la loi sur le territoire américain, d'élaborer un plan pour enrayer la prolifération des produits contrefaits et des œuvres piratées en ligne. L'une des initiatives lancées par la loi *Pro IP* est l' « *Operation In Our Sites* », une initiative de répression qui a suscité des critiques de la part d'un large éventail d'experts juridiques et techniques.

Operation In Our Sites tire son autorité de la section 2323 de la loi *Pro IP*, qui, entre autres choses, introduit le concept juridique de la confiscation civile en cas de violation de la propriété intellectuelle, y compris les violations criminelles du droit d'auteur et de la contrefaçon de marque. L'un des plus anciens modes d'application de la loi dans le système juridique américain, la

confiscation civile est fondée sur le principe que « la propriété elle-même peut être déclarée coupable » (Kopel, 2013). En vertu de la loi, les enquêteurs doivent démontrer l'existence d'une cause probable, un processus qui implique généralement l'agence *Immigration and Customs Enforcement* (ICE) du ministère de la sécurité intérieure et le *National Intellectual Property Rights Coordination Center* (NIPRCC) travaillant en coordination avec des avocats du ministère de la justice (DOJ), qui déterminent ensemble s'il existe des preuves suffisantes pour procéder à une saisie. Si les preuves sont suffisantes, les enquêteurs déposent un *affidavit* auprès d'un magistrat fédéral qui, s'il est convaincu qu'il existe une cause probable suffisante, délivre un mandat pour la saisie du bien en question. Toutefois, la différence entre les saisies et les confiscations est d'une importance capitale : alors qu'une saisie permet au gouvernement de s'emparer temporairement d'un bien, la confiscation est la perte permanente d'un bien au profit du gouvernement pour un crime sans compensation. C'est cette distinction qui est particulièrement épineuse en ce qui concerne la saisie des noms de domaine, car le gouvernement ne peut pas « saisir » un nom de domaine de la même manière que, par exemple, une automobile. Au lieu de cela, il s'appuie sur des registres tels que Verisign, basé à Washington DC (qui fait office d'opérateur de registre pour l'espace .com, entre autres), pour couper la connexion entre le nom de domaine d'un site web ciblé et son adresse IP correspondante, en redirigeant cette connexion vers une page web gouvernementale expliquant la saisie :

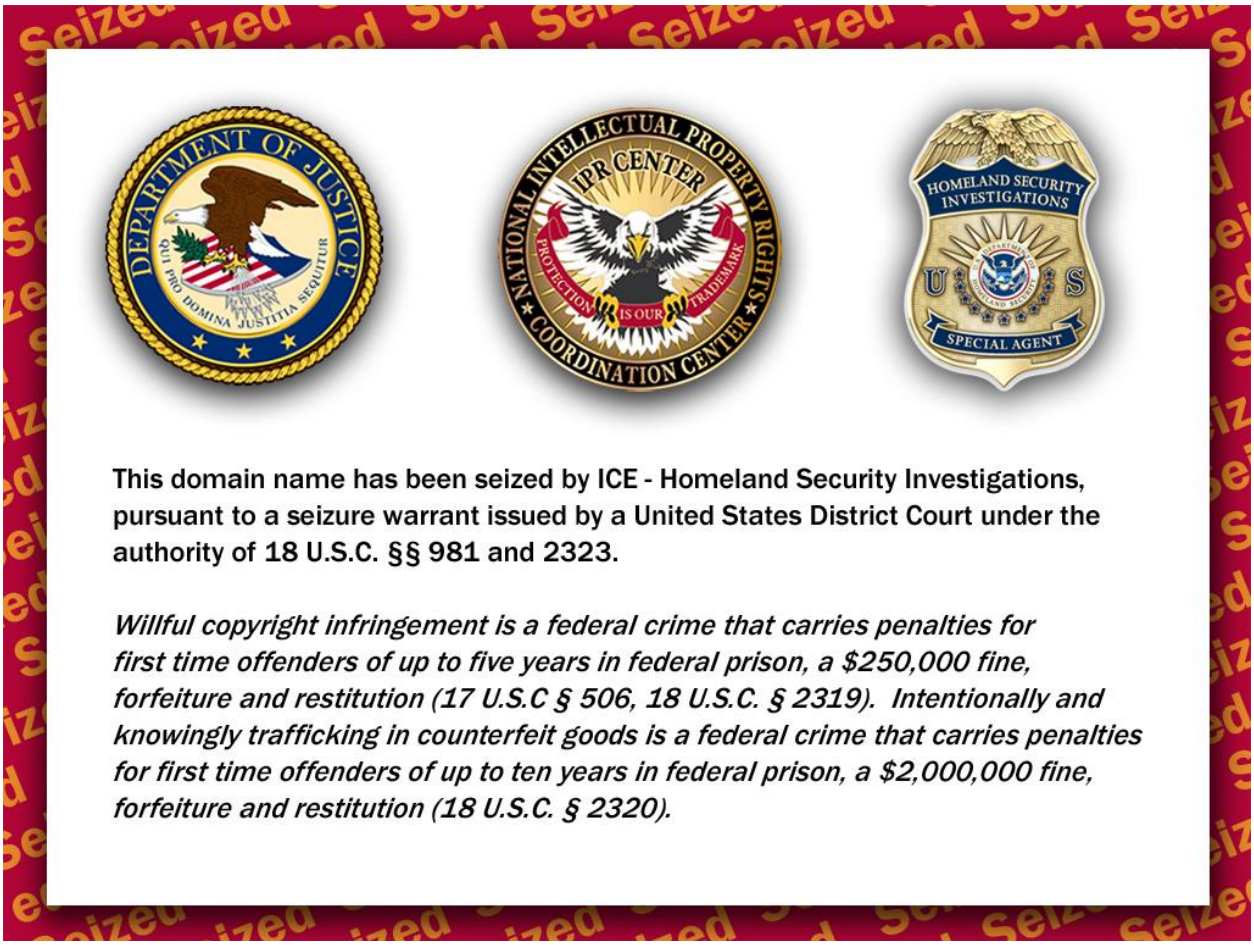

Figure 1. Notice visible sur les domaines saisis par l'ICE, le NIPRCC et le DoJ. Source : Gouvernement fédéral états-unien, via https://en.wikipedia.org/wiki/Operation_In_Our_Sites .

Le contenu du site web présumé en infraction étant inaccessible via son nom de domaine, les agents fédéraux sont alors libres de procéder à la procédure de confiscation civile, plus longue et plus rigoureuse. C'est ce processus de saisie (dit *in rem ex parte*) qui a conduit les juristes à s'interroger sur la constitutionnalité de Operation In Our Sites et, plus généralement, des mécanismes d'application du droit basés sur le DNS, et les techniciens à s'interroger sur sa faisabilité.

4.3.1.1. Critiques juridiques : inverser la charge de la preuve

Depuis que l'Internet est devenu un « phénomène de masse », la nécessité de renforcer l'application des droits de propriété intellectuelle sur le Web a été une controverse acharnée, les

avis divergent aussi bien sur le principe que sur les manières de mettre en œuvre de telles mesures. Les ayants droit et les groupes industriels tels que, aux États-Unis, la Recording Industry Association of America (RIAA), se sont engagés dans une longue campagne de pression sur le Congrès pour qu'il adopte des mesures législatives, ce qui a donné lieu à une série de propositions de loi. De la loi Pro IP précitée, à la « loi sur la lutte contre la contrefaçon et les infractions en ligne » (*Combating Online Infringement and Counterfeits Act*, COICA), en passant par le débat vigoureux qui a suivi la proposition de la « loi sur l'arrêt de la piraterie en ligne » (*Stop Online Piracy Act*, SOPA) et de la « loi sur la prévention des menaces réelles en ligne contre la créativité économique et le vol de propriété intellectuelle » (*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*, PIPA), ceux qui représentent les intérêts des ayants droit ont, d'une manière générale, soutenu tout effort visant à réduire les atteintes à la propriété intellectuelle, quels que soient les mécanismes juridiques et techniques utilisés pour y parvenir. À ces groupes s'opposent ceux qui considèrent que des projets de loi comme le COICA, la SOPA et la PIPA sont mal conçus et potentiellement préjudiciables à la liberté d'expression, à l'application régulière de la loi, à l'innovation, à la sécurité, à la stabilité et au fonctionnement du DNS, pour n'en citer que quelques-uns.

Parmi les nombreux détracteurs de *Operation In Our Sites*, les plus virulents sont peut-être ceux qui affirment que la procédure de saisie va à l'encontre des notions de base de la procédure régulière du droit (*due process*). En fait, ce n'est qu'après qu'un site web a été saisi et que son nom de domaine a été redirigé vers une bannière des forces de l'ordre que les individus ont la possibilité de contester une saisie. Après avoir reçu une notification du gouvernement, le propriétaire d'un site web peut déposer une plainte pour contester la saisie ou la confiscation. La charge de la preuve incombe alors au gouvernement, qui doit démontrer la validité de la saisie ou de la confiscation. Toutefois, il convient de noter que sur les milliers de domaines saisis à ce jour dans le cadre de *Operation In Our Sites*, seuls deux ont mis à l'épreuve les actions du gouvernement, un fait qui étaye deux récits contrastés concernant l'application de la législation sur la propriété intellectuelle basée sur les DNS.

Le premier de ces récits concerne le fait que de nombreux domaines saisis sont clairement coupables d'infraction. En effet, l'écrasante majorité des domaines saisis dans le cadre de

Operation In Our Sites sont des sites web basés à l'étranger qui trafiquent des produits physiques (par exemple, des vêtements de sport et de marque) contrefaits. Cependant, pour les quelques sites web inculpés de l'accusation nettement plus complexe d'infraction au droit d'auteur (y compris le simple fait d'établir un lien vers un contenu illicite), un deuxième constat s'est imposé : défier le gouvernement peut s'avérer extrêmement coûteux et long. Même lorsque des arguments valides sont mis en avant, comme l'ont découvert les propriétaires de Dajaz1.com et Rojadirecta.com (les deux sites Web qui ont réussi à contester le gouvernement, dont on parlera ci-dessous), le processus peut s'avérer extrêmement difficile – une bataille qui équivaut à ce que certains critiques ont appelé une forme de « restriction préalable par procuration » (Seltzer, 2010).

Ainsi, les détracteurs des approches d'application du droit sur la propriété intellectuelle basés sur le DNS soutiennent que ces méthodes constituent une menace pour la liberté d'expression et pourraient par ailleurs être utilisées comme outil de censure sur le Web, de la même manière que le Great Firewall chinois utilise le filtrage DNS pour censurer les contenus considérés comme indésirables par le gouvernement, notamment ceux produits par les organisations de presse étrangères, les groupes dissidents et les organisations de défense des droits de l'homme (Hoang et al., 2021). Outre ces modes de censure plus manifestes et systémiques, les critiques du filtrage basé sur les DNS suggèrent que la nature *in rem* et *ex parte* des saisies de noms de domaine, telles qu'elles sont mises en œuvre dans *Operation In Our Sites*, représentent un cas clair de restriction préalable. Dans la jurisprudence américaine, la restriction préalable est définie comme la censure imposée à un discours ou à un contenu avant que le discours en question puisse avoir lieu, ou que le contenu soit publié. Appliqué au contexte actuel, les critiques soutiennent que les mécanismes de saisie des noms de domaine empêchent effectivement le contenu du site web (discours) d'être entendu (lu) avant que le propriétaire du site web ait la possibilité de défendre la légitimité de sa publication.

S'ajoute à cela l'utilisation d'une terminologie considérée comme trop large pour catégoriser les infractions, comme la définition de sites web « dédiés à des activités illicites », ce qui amène les critiques à s'inquiéter du fait que l'application du droit basée sur le DNS puisse entraîner des saisies erronées, voire une censure ciblée. En effet, la catégorie des sites « dédiés à des activités de contrefaçon » est particulièrement douteuse car elle peut concerner les sites Web qui incluent

des liens vers du matériel de contrefaçon à côté de contenus non contrefaits. Dans ce cas, l'utilisation du DNS à des fins d'application du droit équivaudrait à « utiliser un canon alors qu'une sarbacane suffirait » (Merrill, 2016). Au lieu d'une suppression chirurgicale d'un contenu illicite spécifique, et uniquement de celui-ci, les sites web accusés de contrefaçon secondaire – qui tient les accusés pour responsables de l'incitation, de la contribution ou de la facilitation de la contrefaçon par des tiers – perdent l'intégralité de leur site web, y compris ses composantes non-contrefaites. En se référant notamment à l'avis de la Cour suprême des États-Unis dans l'affaire *Bantam Books, Inc. v. Sullivan* (1963), dans laquelle la Cour a écrit que « tout système de restrictions préalables de l'expression se présente à cette Cour avec une lourde présomption contre sa validité constitutionnelle », on comprend comment les juristes sont extrêmement préoccupés par la tendance à l'application du droit basé sur le DNS dans les efforts législatifs centrés contre le piratage. Mais les experts juridiques ne sont pas les seuls à critiquer l'application de la propriété intellectuelle basée sur le DNS.

4.3.1.2. Critiques techniques : manque de stabilité et inefficacité

L'utilisation de modes d'application du droit sur la propriété intellectuelle basés sur l'infrastructure a également attiré l'attention des ingénieurs et des technologues de l'Internet qui s'inquiètent des conséquences involontaires de la cooptation de ressources Internet critiques comme le DNS dans le but de contrôler le contenu. Ces critiques relèvent généralement de trois catégories connexes, qui ont trait à l'universalité et la cohérence de cette approche, ses conséquences pour la sécurité et la stabilité d'Internet, et l'inefficacité et le possible contournement de ces mesures.

En tant que réseau de communication décentralisé, Internet a été dès le départ, comme on l'a vu, imprégné de valeurs politiques et sociales spécifiques (Abbate, 2000). La principale de ces valeurs était l'importance du contrôle décentralisé. Au lieu de s'appuyer sur une autorité centrale, le réseau se gouvernerait lui-même par le biais de ce que l'informaticien David Clark a décrit comme « un consensus approximatif et un code en cours d'exécution » (*rough consensus and running code*). En fait, bon nombre des protocoles sur lesquels repose l'Internet d'aujourd'hui incarnent cette philosophie libertaire. Par exemple, la commutation par paquets (la principale méthode de

transmission de données utilisée sur Internet) dépend d'un ensemble uniforme de normes et de protocoles afin que les bits d'information envoyés d'un ordinateur à l'autre puissent circuler librement et efficacement sur le réseau, pour finalement arriver intacts à leur destination. Sans confiance dans l'universalité des normes et la cohérence des protocoles, le réseau est susceptible d'être sérieusement affecté. C'est pourquoi de nombreux technologues et ingénieurs Internet ont été fort préoccupés par les tentatives – principalement par les États-nations – de coopter l'architecture Internet (comme le DNS) afin d'exercer un plus grand contrôle sur la couche « contenus » du web.

Tout comme la commutation par paquets, le DNS repose sur un système de serveurs distribués à l'échelle mondiale qui, ensemble, favorisent un certain degré de confiance dans la fiabilité et l'universalité du système. Cette cohérence universelle donne aux utilisateurs l'assurance que la saisie du nom de domaine www.lemonde.fr les conduira au même contenu, qu'ils se trouvent sur un ordinateur à Paris ou à Montréal. Comme l'écrit le pionnier de l'Internet Steve Crocker, « l'universalité des noms de domaine a été l'un des principaux moteurs de l'innovation, de la croissance économique, de l'amélioration des communications et de l'accès à l'information déclenchés par l'Internet mondial » (Crocker et al., 2011). Le filtrage basé sur le DNS ainsi que proposé dans les projets législatifs américains de lutte contre le piratage menace cette universalité, en forçant certains serveurs DNS à renvoyer des résultats différents, ce qui entraîne des recherches incohérentes et, en fin de compte, une érosion de la confiance dans le réseau dans son ensemble.

L'application du droit basée sur le DNS peut également constituer une menace pour la sécurité de l'Internet, dans la mesure où elle recourt à certaines des techniques utilisées par les cybercriminels pour voler des informations privées et monter des cyberattaques. En particulier, le filtrage DNS est incompatible avec le déploiement des extensions de sécurité DNS (DNSSEC), une suite de sécurité cryptographique introduite en 2005[38] et utilisée pour authentifier de bout en bout la résolution des noms de domaine. DNSSEC empêche les attaques dites « *man-in-the-middle* », dans lesquelles l'attaquant redirige les utilisateurs vers une ressource fictive afin d'obtenir des informations sensibles. Cette méthode peut à ce moment de la lecture sembler familière : en effet, elle est presque identique à celle utilisée par les forces de l'ordre dans les opérations de répression

[38] Request for Comments 4033 de l'IETF, https://datatracker.ietf.org/doc/html/rfc4033

basées sur le DNS, comme Operation In Our Sites. En redirigeant les utilisateurs vers des ressources auxquelles ils n'avaient pas l'intention d'accéder, l'application du droit basée sur le DNS érode la confiance dans l'ensemble du DNS en remettant en question l'authenticité de la résolution des noms de domaine. En outre, du point de vue d'un utilisateur, il est impossible de distinguer un échec de résolution DNS ordonné par un tribunal de celui d'un serveur piraté utilisé à des fins malveillantes (Crocker et al., 2011). Ce ne sont là que quelques-unes des raisons pour lesquelles de nombreux membres de la communauté technique soutiennent que le filtrage DNS est « fondamentalement incompatible avec les DNSSEC », et *de facto* avec la sécurité du DNS (Crocker et al., 2011).

L'argument le plus déployé à l'encontre des mesures juridiques basée sur le DNS est peut-être le fait qu'elles ne réduisent pas de manière significative les infractions. Au contraire, les sites Web qui se consacrent véritablement à la contrefaçon se limitent à contourner, de façon souvent très efficace pour eux, le filtrage basé sur le DNS. Cette question n'es pas nouvelle dans l'histoire de l'Internet de ces vingt dernières années : lorsque les premiers sites de partage de fichiers comme Napster ont été fermés en raison de poursuites judiciaires pour violation des droits d'auteur, ils ont été rapidement remplacés par des plateformes de partage de fichiers peer-to-peer plus distribuées, comme Kazaa et, finalement, par le protocole BitTorrent, qui a été conçu, en partie, avec le but explicite d'échapper aux saisies gouvernementales.

Aujourd'hui, un jeu du chat et de la souris similaire, dans lequel la dialectique du pouvoir et du contre-pouvoir en réseau est pleinement exposée, se déroule autour du DNS. Rappelons que le filtrage DNS ne supprime pas complètement le contenu présumé illicite ; il rompt simplement la correspondance entre le nom de domaine d'un site web et son adresse IP correspondante. Le site web reste donc accessible par plusieurs moyens, qui présentent tous des risques potentiels pour la sécurité et menacent la stabilité du DNS et plus largement de l'Internet.

La méthode la plus simple pour contourner le filtrage DNS consiste à contourner le nom de domaine alphanumérique d'un site web et à saisir son adresse IP, ce qui permet un accès direct au contenu. Si cette tactique semble inoffensive, elle montre l'importance d'un DNS sûr et stable, car

le fait de dépendre uniquement des adresses IP pour naviguer sur le web ralentirait le trafic et étoufferait l'innovation.

Par ailleurs, les entreprises qui hébergent du contenu illicite peuvent tout simplement se déplacer vers un TLD étranger qui est hors de portée des forces de l'ordre américaines (ou d'un autre pays souhaitant engager des poursuites). En fait, les opérateurs de sites Web ont à leur disposition un vaste marché mondial dans lequel ils peuvent chercher un TLD avec des politiques plus souples concernant les droits de propriété intellectuelle. De plus en plus, ce marché de réseaux est composé de domaines de premier niveau de code pays (ccTLD), dont les politiques reflètent les valeurs culturelles et politiques des nations qu'ils représentent[39].

L'existence de ces stratégies de contournement, ainsi que la popularité croissante du recours à l'infrastructure Internet pour la médiation du contenu, ont donné naissance à toute une industrie de technologies de contournement, des services de proxy DNS (p. ex. Smart DNS Proxy de Global Stealth Inc.) aux plug-ins de navigateur comme MafiaaFire. Ensemble, ces modes de contre-pouvoir basés sur le marché soulignent la futilité du filtrage DNS et la résilience du pouvoir distribué en réseau.

4.3.2. La cooptation du DNS en pratique: les cas Rojadirecta et Dajaz1

Le 1er février 2011, l'agence américaine de l'immigration et des douanes (ICE), une unité du département de la sécurité intérieure, a saisi les domaines de dix sites Web accusés de fournir « l'accès à des retransmissions illégales et piratées d'événements sportifs en direct ». Parmi ces saisies figure Rojadirecta.com, un site web hispanophone proposant des liens vers des retransmissions en direct d'événements sportifs internationaux ainsi que des forums de discussion et des commentaires. S'inscrivant dans le cadre d'*Operation In Our Sites*, la saisie a été autorisée par un magistrat fédéral du district sud de New York. Comme l'explique le mandat, le site Web a été saisi parce que « plus de la moitié du matériel disponible sur le site Web de Rojadirecta à tout

[39] Par exemple, en 2012, WikiLeaks a diversifié son portefeuille de TLD après la saisie de son TLD .org. Cette stratégie a consisté à déplacer le TLD principal du site web vers le .ch suisse, dont la culture d'indépendance et les lois strictes sur le secret de l'information sont ancrées dans le ccTLD de la nation.

moment pendant l'enquête des forces de l'ordre semblait être consacré à la mise à disposition de contenu illicite », ajoutant que le site Web avait « été utilisé pour commettre et faciliter des infractions criminelles au droit d'auteur » (Anderson, 2012). Cependant, contrairement aux neuf autres sites Web saisis au cours de cette itération particulière de *Operation In Our Sites*, Rojadirecta a contesté la décision de saisie devant un tribunal fédéral et, ce faisant, a mis en évidence une série de problèmes constitutionnels et procéduraux liés aux processus de saisie et de confiscation relatifs à l'application des droits de propriété intellectuelle basés sur le DNS.

Toutefois, avant d'engager une action en justice, les propriétaires de Rojadirecta ont rapidement transféré le contenu du site web sur Rojadirecta.me. Cherchant un ccTLD avec un ensemble de lois plus favorables en termes de droits de propriété intellectuelle, le site web a choisi le ccTLD .me du Monténégro, rendant ainsi l'impact pratique de tout jugement américain sans importance. Bien que les experts juridiques négligent souvent ce point, cette forme de « forum shopping » met en évidence, dans la pratique, l'inefficacité de l'application de la loi basée sur le DNS et montre par ailleurs la démocratisation de l'espace TLD suite à son internationalisation, qui a marqué la fin d'un espace dominé par le .com.

Après avoir migré vers Rojadirecta.me, le site a poursuivi le gouvernement (le premier et le seul site Web à le faire dans le cadre de *Operation In Our Sites*) pour récupérer son domaine .com. Les enquêteurs, sans doute ayant été pris par surprise par cette initiative, ont engagé une procédure de confiscation contre Rojadirecta, probablement pour faire de ce site un exemple. Les avocats de Rojadirecta, Mark Lemley et Ragesh Tangri, experts américains en propriété intellectuelle, ont riposté en faisant valoir que la saisie du domaine constituait une restriction préalable, car le site Web comprenait des contenus légaux à côté des liens prétendument illicites visés par le gouvernement. En outre, Lemley et Tangri ont souligné le fait que le site web n'hébergeait pas directement de contenu illicite, mais fournissait des liens vers des sites web tiers où le contenu prétendument illicite pouvait être trouvé[40]. Bien que ce fait n'exempte pas Rojadirecta de l'accusation de contrefaçon indirecte, il innocente le site Web de toute accusation criminelle. Enfin, les avocats de Rojadirecta ont fait valoir que deux tribunaux espagnols distincts avaient déclaré que le site Web ne s'engageait pas dans la contrefaçon, ce qui laisse supposer une

[40] Entretien, 7 novembre 2012, Washington DC.

dérogation importante aux normes internationales relatives aux droits de propriété intellectuelle en ligne.

Après deux procès tendus, le gouvernement a finalement renoncé à ses accusations, rendant Rojadirecta.com à son propriétaire près de 18 mois après sa saisie initiale. Mais qu'est-ce qui a conduit le gouvernement à changer de cap de manière aussi radicale, et quelles leçons peuvent être tirées de ce procès ? Tout d'abord, cela réitère en pratique que les procédures utilisées pour saisir un nom de domaine en vertu de la loi sont très problématiques, si mises à l'épreuve tant d'un point de vue juridique que technique. Sherwin Siy, vice-président des affaires juridiques de Public Knowledge, un groupe de défense des libertés sur Internet, a affirmé à ce propos : « Il est beaucoup trop facile pour le gouvernement de saisir des noms de domaine et de les conserver pendant une période prolongée, même lorsqu'il n'est pas en mesure d'établir un cas de violation durable. L'expansion constante des lois d'application du droit d'auteur nous a donné un système où les propriétaires de sites Web sont effectivement traités comme coupables jusqu'à preuve du contraire »[41]. Le cas Rojadirecta semble montrer l'importance, pour les exploitants de sites Web, d'être informés au préalable de l'intention de saisie et des accusations portées contre eux, ce qui contribuerait grandement à légitimer le processus, du moins d'un point de vue juridique. Ce cas montre aussi que des problèmes techniques subsistent, notamment la forte probabilité que l'application de la loi basée sur le DNS entraîne des dommages collatéraux au contenu non contrefaisant et au DNS en général, tout en s'avérant totalement inefficace pour réduire la contrefaçon du fait de l'existence de stratégies de contournement.

L'affaire Dajaz1 constitue une deuxième étude de cas révélatrice des dynamiques de la cooptation DNS. En novembre 2011, les agents de l'ICE ont saisi le site Web Dajaz1.com, un site proposant des critiques, des nouvelles, des commentaires et des forums de discussion sur les artistes et la culture hip-hop. En plus de ce contenu, le site proposait souvent des téléchargements gratuits de chansons récemment sorties, dont il s'est avéré par la suite qu'elles étaient proposées avec l'autorisation des artistes. Néanmoins, les enquêteurs fédéraux ont saisi le site Web, affirmant qu'il fournissait des liens vers du matériel protégé par le droit d'auteur. Cependant, en saisissant le site,

[41] Entretien, 16 novembre 2012, Washington DC.

les autorités ont également empêché les utilisateurs d'accéder à la quantité considérable de matériel non contrefait qui s'y trouvait.

Par la suite, il s'est avéré que l'enquêteur principal de l'ICE a fondé la plainte du gouvernement sur des informations obtenues auprès d'un contact de la *Recording Industry Association of America* (RIAA), un puissant groupe de pression représentant les artistes et les maisons de disques. Malgré le fait que les ayants droit aient donné à Dajaz1 la permission de publier le matériel en question, un magistrat fédéral a accordé une ordonnance de saisie. Le gouvernement a ensuite déposé une demande de confiscation et, selon l'avocat de Dajaz1, Andrew Bridges, a eu recours à des tactiques dilatoires afin d'inciter le site web à céder[42], ce qui n'a pas été le cas et le 8 décembre 2011, près d'un an après la saisie du site par les autorités, Dajaz1.com a été rendu à son propriétaire.

Ce qui semble ressortir avec force dans ce cas est la priorité que le gouvernement a donné au fait de réduire au silence une quantité considérable de contenus non considérés comme des contrefaçons, dans une tentative de suppression de contenus qui, prétendument, l'étaient. Sur ce point, Andrew Bridges a comparé dans la presse la saisie du site web de ses clients « à la saisie d'une copie papier du New York Times parce que le journal, dans son calendrier de concerts, renvoie les lecteurs à quatre concerts dont les promoteurs n'ont pas payé les licences à l'ASCAP [*l'American Society of Composers, Authors and Publishers*] pour les performances correspondantes » (Kopel, 2013).

Par ailleurs, à l'instar de l'affaire Rojadirecta, l'histoire de la saisie du domaine de Dajaz1 et de sa restitution ultérieure est un cas particulièrement instructif dans la mesure où il expose l'une des nombreuses alliances puissantes – groupes industriels et décideurs politiques – qui influencent l'élaboration des politiques en matière de télécommunications et d'Internet aux Etats-Unis, et plus largement dans le monde. Du point de vue de la « gouvernance par l'infrastructure », ces cas montrent comment le DNS semble constituer, en fin de comptes, un outil assez inadapté pour filtrer le contenu, aussi illégal ou indésirable soit-il, avec des conséquences qui varient entre le disproportionné et l'inefficace. La première partie de ce chapitre a mis en lumière, via le cas du DNS, le complexe écheveau de modifications et de défis auxquels fait face une infrastructure

[42] Entretien, 5 décembre 2012, Washington DC.

lorsque ses fonctions de base sont utilisées pour servir des objectifs politiques plus larges, et l'étendue des ramifications techno-juridiques auxquelles peuvent donner lieu ces usages élargis.

4.4. Résistances « par l'infrastructure » : pour un DNS alternatif et décentralisé

La partie finale de ce chapitre se base sur une enquête menée entre 2012 et 2014 au sujet des projets de co-construction d'une alternative décentralisée au DNS – l'idée centrale de ces projets étant que la résistance aux cooptations du DNS peut avoir lieu non seulement, et même pas principalement, dans les arènes juridiques (comme dans les cas ci-dessus) mais également en se servant de l'infrastructure Internet.

À la fin de 2010, l'organisation WikiLeaks rend publics des milliers de câbles diplomatiques américains secrets, perdant quelques jours plus tard son hébergeur et le domaine wikileaks.org. Des discussions sur un « nouveau serveur racine concurrent », capable de rivaliser avec celui administré par l'ICANN, suscitent une nouvelle vague d'intérêt sur le Web, à l'initiative de l'« anarchiste » de l'Internet Peter Sunde, déjà impliqué dans la création de The Pirate Bay. Un registre alternatif de noms de domaine est envisagé, un système décentralisé, de type peer-to-peer (P2P-DNS), dans lequel les utilisateurs hébergeraient chacun une partie du DNS sur leurs ordinateurs, de sorte que tout domaine rendu temporairement inaccessible par un registre, pour quelque raison que ce soit, puisse toujours être accessible sur le registre alternatif. Au lieu de simplement ajouter un certain nombre d'options DNS à celles déjà gérées par l'ICANN (comme l'avaient fait auparavant des projets tels que OpenNic ou NewNet), ce projet vise à remplacer ou à contourner l'institution et l'architecture principales de gouvernance du DNS en faveur d'un modèle distribué, basé sur l'infrastructure fournie par les utilisateurs, dans lequel ceux-ci gèreraient chacun de façon bénévole une partie du DNS sur leurs propres ordinateurs. Face à la cooptation de l'infrastructure Internet pour des fonctions de médiation de contenu qui finit par restreindre leur liberté d'expression et d'accès, les utilisateurs/développeurs cherchent, à leur tour, à contourner cette cooptation de manière perturbatrice. Et par ce détournement (Akrich, 1998), ils créent de nouveaux arrangements de gouvernance-utilisation de l'infrastructure.

Le reste de cette section explore les débats sur la création de cette infrastructure décentralisée, contrôlée par les utilisateurs, en réponse à la cooptation du DNS ; ce faisant, on aborde les défis auxquels un DNS décentralisé pourrait être confronté, y compris les problèmes de sécurité possibles, la manière de garantir l'unicité mondiale dans la façon dont les ressources sont distribuées, et une fragmentation possible de l'Internet qui pourrait découler du manque d'interopérabilité entre les différentes alternatives, et/ou entre celles-ci et le DNS « dominant ».

4.4.1. Une histoire d'insatisfactions et de tentatives de changement

Les mécontentements concernant la manière dont le DNS est géré ne sont pas nouveaux. En raison de son caractère hiérarchique (organisé en une structure arborescente où chaque organisation locale ne gère les informations DNS que pour ses propres domaines, ou sous-arbres) et du fait qu'il n'a pas été construit initialement dans un souci de sécurité, des acteurs peu recommandables en ont fait le centre de leur attention par le passé ; les controverses mentionnées précédemment, et en particulier le contrôle *de facto* du système racine par les États-Unis, en ont fait le sujet de plusieurs réunions internationales et intergouvernementales animées.

Comme nous l'avons vu, le COICA puis le PIPA ont attiré l'attention sur le risque d'un contrôle de l'Internet exercé via le DNS. L'affaire de la saisie du nom de domaine de WikiLeaks a également bien illustré les pressions exercées via le DNS contre la liberté d'expression, et les risques de concentration : Wikileaks.org a été indisponible pendant plusieurs jours parce qu'il n'y avait qu'un seul hébergement DNS pour ce domaine. Bien qu'illustrée par de nombreux épisodes dont des institutions et des entreprises américaines ont été à l'origine, cette problématique n'est pas spécifique aux États-Unis. En France, la Loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) prévoit un filtrage obligatoire des noms de domaine que le gouvernement juge menaçants, une mesure dont la mise en œuvre pourrait se faire via le DNS.

Les frustrations concernant la gestion du DNS, présente et future, sont – comme souligné jusqu'à présent – nombreuses et légitimes. Le flamboyant « appel aux armes » de Peter Sunde en 2010 s'est avéré particulièrement médiatique et médiatisé, de par la personnalité et le parcours de

l'individu[43], mais historiquement, ces frustrations ont déjà conduit à un certain nombre de projets alternatifs liés au DNS, visant à créer des serveurs racine alternatifs afin de contourner l'ICANN ou les bureaux d'enregistrement existants, ou à développer des systèmes de résolution de noms n'utilisant pas la hiérarchie du DNS, par exemple basés sur les tables de hachage distribuées (*Distributed Hash Tables*, DHT). Il semble y avoir un consensus parmi les développeurs sur le fait que les nouveaux projets de DNS alternatifs devraient donc commencer par se demander pourquoi ces projets, dont certains (comme CoDoNS ou le serveur racine alternatif Open Root Server Network, ORSN, arrêté en 2008) bien que techniquement solides et innovants, n'ont jamais connu de déploiement significatif. Sinon, ils risquent de connaître, tôt ou tard, le même sort.

D'un point de vue technique, les développeurs qu'on a interrogés font plusieurs remarques différentes sur la faisabilité d'un DNS décentralisé ou P2P. Le DNS sert trois opérations fondamentales : l'enregistrement des noms (la gestion de la réservation des noms de domaine Internet par différentes entités) ; la résolution des noms (la tâche en coulisse consistant à convertir les noms de domaine en leur adresse IP correspondante) ; et le maintien de la confiance des acteurs (la création d'une infrastructure capable de promouvoir une confiance généralisée dans le système grâce à une association unique de ressources). Historiquement, le terme « système de noms de domaine » a fait référence aux deux comme s'ils étaient nécessairement liés. Or, ce n'est pas le cas, même si le service d'enregistrement des noms et le protocole de résolution ont des interactions - les deux ont une structure arborescente, par exemple. Le mécanisme d'enregistrement garantit l'unicité des noms, l'une des fonctions les plus importantes du DNS, et le mécanisme de résolution permet à une machine d'obtenir des informations – par exemple, des adresses IP – en échange d'un nom de domaine. On pourrait donc prévoir de ne remplacer qu'un seul d'entre eux, ce que faisait par exemple le projet CoDoNS : remplacer la fonction de résolution par une table de hachage distribuée, tout en conservant le mécanisme d'enregistrement intact dans sa forme précédente.

Le remplacement du mécanisme de résolution, bien qu'il s'agisse d'une tâche colossale (il devrait modifier des centaines de milliers de machines) est possible : aujourd'hui, des mécanismes alternatifs existent déjà. Changer le système de nommage et d'enregistrement semble beaucoup plus irréaliste à un certain nombre de développeurs, pour une raison qui n'est pas principalement

[43] https://slashdot.org/story/10/12/01/1320253/the-pirate-bay-co-founder-starting-p2p-dns

technique : le fait qu'il soit déjà connu et adopté par tant d'utilisateurs. L'un des développeurs décrit les utilisateurs comme étant « plus compliqués à mettre à jour que les logiciels », faisant référence à l'effet cumulatif de type « boule de neige », qu'une masse critique d'individus utilisant un système d'information a sur d'autres individus.

Une question cruciale et controversée consiste donc à clarifier la fonction à laquelle un projet DNS P2P devrait s'attaquer. Dans son appel initial, Peter Sunde évoque la création d'une racine alternative, ce qui impliquerait des évolutions fondamentales dans le mécanisme d'enregistrement des noms de domaine. D'autres ont parlé dans le passé de la création d'un nouveau nom de domaine de premier niveau, .p2p, et d'autres encore semblent vouloir remplacer le DNS par un mécanisme basé sur BitTorrent. Plusieurs projets différents coexistent parmi les développeurs, chacun avec des spécifications différentes, ne partageant qu'une insatisfaction technique et politique commune avec le système actuel – et une culture inspirée du P2P. Les développeurs sont conscients de ce scénario d'ensemble et des fils rouges qui pourraient les rapprocher les uns des autres, mais jusqu'à présent, ces projets sont restés relativement isolés.

Une autre question discutée dans le contexte des projets de DNS alternatifs est la mesure dans laquelle les dispositions actuelles de gouvernance du DNS pourraient être remplacées ou complètement effacées. Plusieurs développeurs impliqués dans des projets DNS P2P mentionnent la possibilité que des organisations qui gèrent toujours une racine alternative, comme OpenNic, participent à ces projets en tant qu'instances alternatives de gouvernance. Une telle organisation pourrait être le registre du domaine .p2p ; dans ce cas, cependant, comme l'a fait valoir une personne interrogée, les problèmes actuellement représentés par des instances telles que l'ICANN, VeriSign ou les registres nationaux seraient probablement simplement déplacés vers OpenNic : « Le pouvoir ne serait pas dissous, mais déplacé ou transféré d'un acteur à un autre, et cela n'entraînerait pas, en soi, de solution au problème ».

Le plus souvent, c'est à ce moment-là que les discussions entre développeurs se déplacent vers la question cruciale, à la fois technique et profondément politique : quels services le DNS fournit-il, et quels intérêts sert-il ?

« Le DNS a survécu et s'est bien adapté, d'une manière quelque peu surprenante », souligne un développeur. Il fournit des noms uniques, qui peuvent être mémorisés par un humain de manière relativement facile, et qui peuvent être résolus par un programme. De plus, il fonctionne depuis plus de 20 ans, malgré les changements importants qu'a connus l'Internet au cours de son évolution, passant d'une utopie tranquille et « symétrique » d'intellectuels passionnés à un média de masse agité.

En fin de compte – affirme un développeur basé à Boston qu'on a pu interviewer – avant de passer à un autre système, toutes les parties intéressées devront considérer le système auquel il faudra renoncer pour y parvenir. Cette nécessité de peser le pour et le contre, notamment le fait qu'aucune solution ne résoudra tous les problèmes sans inconvénient ni effet secondaire, est bien connue de la communauté des développeurs P2P, même si plusieurs déclarations, notamment suite à l'annonce du projet de Sunde, ont laissé l'enthousiasme pour l'utopie décentralisée l'emporter, de manière quelque peu a-critique (voir Geere, 2010). Deux alternatives sont possibles pour faciliter la recherche et la récupération de fichiers dans un système P2P : soit un système hiérarchique est utilisé – c'est le cas du BitTorrent classique, où la récupération d'un fichier .torrent se fait par le biais d'un Uniform Resource Locator (URL), donc d'un nom de domaine ; soit le système fonctionne de manière complètement P2P et décentralisée, et dans ce cas, il n'y a pas d'unicité, pas de racine unique. Le même nom peut faire référence à deux fichiers complètement différents, il peut être enregistré par deux entités différentes, et faire référence à des contenus complètement différents.

Comme le souligne un analyste politique d'une entreprise de Washington, la question de savoir si cette implication de la décentralisation est un problème qui vaut la peine d'être affronté dans toute sa complexité technique et politique, est « liée à l'évaluation subjective des différentes parties prenantes du système DNS ». Plusieurs des techniciens qu'on a interrogés ne sont cependant pas optimistes quant aux implications pratiques de ces évaluations. Si certains acteurs peuvent considérer que « le fait de contourner ou d'éliminer l'ICANN, les bureaux d'enregistrement actuellement fortement hiérarchisés, etc., vaut bien la peine de supporter certains inconvénients », les changements importants dans les modèles de sécurité et d'authentification que le DNS P2P entraînerait semblent gravement sous-représentés dans les débats en ligne et hors ligne

principalement non techniques, si on les compare à leur importance. Ils ne sont mentionnés explicitement et clairement que dans une poignée de contributions, qui semblent par ailleurs avoir un consensus sur le fait que : « Et oui, il ne sera pas sécurisé et authentifié comme le système actuel. Nous devrons simplement nous en accommoder » (Coldewey, 2010). L'enregistrement de noms uniques dans un environnement P2P, sans besoin d'un registre central, a déjà été théorisé et codé. Cependant, son bon fonctionnement repose sur une prémisse très difficile à réaliser dans des contextes P2P réels, comme l'ont montré des décennies d'histoire de cette technologie : toutes les parties doivent coopérer.

Qu'y a t-il à gagner, et qu'y a t-il à perdre, de la modification substantielle du système de résolution ? Ici, les développeurs insistent à nouveau sur le fait que le DNS actuel est basé sur plus de vingt ans d'expérience et d'interaction avec le « monde réel ». Tout autre mécanisme – bien que ceux basés sur les DHT soient techniquement solides, et méritent certainement l'attention de tout développeur ambitieux – va certainement prendre des années avant d'atteindre un stade de développement suffisamment mature, et il faut s'attendre à une longue coexistence ; un développeur insiste sur le fait que « les affirmations selon lesquelles on pourrait remplacer les opérateurs DNS actuels et les entités de gouvernance en trois mois ne sont guère plus que des fanfaronnades irréalistes ».

4.4.2. Ingénierie, adoption et gouvernance : le triple défi des alternatives au DNS

Selon nos interviews de développeurs et d'ingénieurs, les alternatives au DNS sont confrontées à un triple défi. Le premier a trait à la « bonne ingénierie » : la sécurité du mécanisme de résolution des noms. Actuellement, la confiance de l'utilisateur dans le résultat de la résolution vient du fait qu'une machine a interrogé un serveur connu. Dans un environnement P2P, ce mécanisme de validation « unidirectionnel » disparaît, ce qui donne lieu à un scénario où n'importe quel nœud participant au système peut apporter tout et n'importe quoi à la DHT, sans qu'un serveur agisse comme une autorité « légitimant » la validité de cette information. Le projet CoDoNS a résolu le problème en appliquant le DNSSEC à son système, une manière techniquement correcte de traiter le problème. Mais ce faisant, on a simplement changé le système de résolution, alors que l'infrastructure d'enregistrement et sa gouvernance restent les mêmes, avec leurs défauts. Plus

généralement, il est de plus en plus évident qu'il est impossible de parvenir à une sécurité totale dans un environnement P2P « pur ».

Dans le cas où l'un des projets DNS décentralisés atteindrait le stade de l'appropriation par les utilisateurs, la question cruciale pourrait être la confiance des utilisateurs envers les autres utilisateurs. Avec la configuration actuelle, nous faisons confiance aux serveurs DNS comme OpenDNS, Google DNS, etc. pour nous indiquer la bonne direction lorsque nous voulons accéder à un site web. Avec le schéma proposé par P2P-DNS, nous devrons compter sur les autres utilisateurs du réseau pour nous diriger, et « c'est une chose de faire confiance à OpenDNS, Google, etc., mais c'en est une autre de faire la même chose avec un ordinateur aléatoire[44] ».

Au-delà des choix de conception et d'innovation, se pose la question de la gouvernance politique, dont les développeurs ont une conscience aiguë (et peut-être surprenante). Les questions à l'origine de la prolifération des propositions de P2P-DNS sont profondément politiques : elles concernent le contrôle, la liberté et la censure. Or, remarque un développeur : « Cette 'gouvernance par l'infrastructure', comme vous l'appelez, si elle ne se fait pas via le DNS, elle se fera via le Border Gateway Protocol, ou via l'un des nombreux mécanismes de filtrage IP qui existent sur Internet »[45] Ainsi, les solutions techniques aux questions controversées qui ont une composante politique devraient, à un moment donné, être accompagnées d'évolutions des institutions, de peur que la gouvernance de l'Internet ne soit réduite à une guerre de technologies de surveillance et de contre-surveillance, de cooptation et de contre-cooptation des infrastructures. En définitive, de la part d'acteurs faisant part de la communauté technique, c'est une préoccupation commune très politique qui semble se dégager. L'Internet peut en effet trouver des moyens de « traiter la censure comme un dommage et de la contourner », comme l'a fait remarquer David Clark, pionnier de l'Internet. Toutefois, à long terme, les solutions durables aux restrictions des libertés sur Internet ne pourront pas se passer d'institutions de gouvernance d'Internet capables de s'engager dans une réflexion et un examen de leurs moyens, de leurs objectifs et de leurs rôles délicats dans la gestion de la principale « infrastructure globale » d'aujourd'hui.

[44] https://slashdot.org/story/10/12/01/1320253/the-pirate-bay-co-founder-starting-p2p-dns
[45] Entretien, 16 janvier 2013, Cambridge (MA, États-Unis).

4.5. Le DNS, au cœur des infrastructures controversées d'Internet

Dans ce chapitre, j'ai montré comment le DNS, système qui assure la traduction entre les adresses numériques utilisées par les ordinateurs pour acheminer les paquets d'informations sur Internet, et les noms de domaine alphanumériques que les individus utilisent pour accéder aux sites Web, est devenu l'un des principaux champs de controverse où le pouvoir social, politique et économique est inter-médié dans la sphère publique en réseau. La fonction de base du DNS a été progressivement élargie, reconfigurée ou cooptée pour d'autres objectifs, notamment comme moyen d'application des droits de propriété intellectuelle et régulateur de contenus, ce qui a amené des acteurs techniques et des activistes numériques à développer des projets de DNS alternatif et décentralisé afin de contrer cette cooptation, également en se servant de moyens « d'infrastructure ».

Le cas du DNS est intéressant dans la mesure où il est traversé par des multiples controverses au niveau de la gouvernance *des* infrastructures Internet (concernant par exemple le rôle d'organisations telles que l'ICANN, son lien privilégié avec le ministère américain du commerce, et sa capacité à évoluer vers un organisme pleinement multi-parties-prenantes), de la gouvernance *dans* les infrastructures Internet (par exemple, les revendications d'identité nationale et le potentiel économique de certains ccTLD tels que .za ou .tv), et de la gouvernance *par* les infrastructures Internet (par exemple, les utilisations du DNS comme instrument d'application du droit de la propriété intellectuelle).

Le cœur du chapitre s'est concentré plus particulièrement sur ce troisième aspect. J'ai examiné comment les noms de domaine, notamment les ccTLD, ont acquis un rôle important dans les débats mondiaux sur les droits de propriété intellectuelle, alors que plusieurs acteurs ont cherché à saisir des noms de domaine pour exécuter ces droits. J'ai présenté deux cas qui mettent en évidence la mesure dans laquelle les controverses sur les noms de domaine surviennent souvent à l'intersection de la gouvernance d'Internet et de questions de juridiction : dans le contexte d'un Internet mondial, dans lequel un contenu légal dans une juridiction peut être illégal dans une autre, les implications des politiques ccTLD deviennent évidentes.

Les ccTLD sont devenus un élément central des débats mondiaux sur les droits de propriété intellectuelle, à la fois pour mettre en œuvre ces droits, et comme moyen d'en contourner l'application. L'utilisation croissante des saisies de noms de domaine comme moyen de réglementer le contenu met en évidence la mesure dans laquelle les opérateurs techniques de ccTLD (par exemple, les registres) peuvent être exploités « pour imposer les lois nationales de leur pays d'incorporation sur un contenu mondial, sous les ccTLD et les gTLD qu'ils gèrent » (de La Chapelle & Fehlinger, 2016). De cette façon, les ccTLD peuvent être utilisés comme des outils pour l'extension extraterritoriale de la souveraineté dans le cyberespace, entraînant ce que de La Chapelle et Fehlinger (2016) appellent « une course juridique aux armements », dans laquelle les gouvernements adoptent des lois visant à utiliser l'infrastructure afin de réaffirmer leur souveraineté dans le cyberespace. La question est de savoir comment affirmer le contrôle « par l'infrastructure » sans bafouer les droits civils, politiques et humains fondamentaux tels que la liberté d'expression et sans endommager les technologies qui ont permis aux réseaux de communication mondiaux de prospérer.

En proposant des projets de DNS décentralisé, certains acteurs proposent de se libérer de ce dilemme en construisant une infrastructure « autre », qui permette de bâtir dans les choix techniques eux-mêmes moins de hiérarchie et de goulots d'étranglement que dans le DNS existant, tout en reconnaissant qu'une série de limites importantes, inscrites dans les technologies et dans les usages potentiels, compliquent ces alternatives. En définitive, parmi les promoteurs de ces projets, on retrouve la prise de conscience que la décentralisation comme « désintermédiation » et comme « libération » de mécanismes de gouvernance perçus comme contraignants est bien plus difficile à mettre en œuvre qu'on ne pourrait penser. Le prochain chapitre en fournira, avec le cas de Bitcoin, une autre illustration.

Chapitre 5. Bitcoin, ou comment gouverner (par la technique) ce qui ne devait pas être gouverné

Dans ce chapitre, j'aborde une des technologies de réseau décentralisées les plus médiatisées de la dernière décennie : Bitcoin. Crée sur l'onde d'une crise financière et du manque de confiance répandu dans les institutions monétaires, Bitcoin s'est proposé comme système ayant pour principe structurant la *blockchain* ou chaîne de blocs, principe technique censé, en théorie, se substituer à une gouvernance humaine comprise comme peu fiable, si pas carrément malhonnête. Dans un travail d'enquête mené entre 2012 et 2016, Alexandre Mallard, Cécile Méadel et moi avons montré comment de nombreux points de « faiblesse » technique et organisationnelle (qui sont, en fait, autant de points de redistribution et reconfigurations du pouvoir et de l'autorité) ont pris forme et contribué à forger la « gouvernance par l'infrastructure » de Bitcoin[46]. Au fil de l'histoire de Bitcoin, on apprend à découvrir comment la pratique de la gouvernance s'invente au-delà de la régulation et du contrôle au sens strict, ce qui résonne avec le travail de Kelty (2005) : une partie des infrastructures d'Internet sont des infrastructures de gouvernance au sens d'organisation explicite de formes de relations entre les personnes, et entre elles et leur environnement.

Est-il possible de mettre en place des mécanismes de gouvernance fiables pour Bitcoin, la technologie qui, de par sa conception et son *manifesto*, n'était au départ « pas censée être gouvernée » ? Cette question a été soulevée à plusieurs reprises depuis la création de ce système de monnaie numérique. En effet, depuis sa création, Bitcoin a été présenté comme une monnaie « alternative » censée contourner les institutions financières et économiques soutenues par l'État ; ce n'est pas une coïncidence si la naissance et l'ascension rapide du bitcoin ont eu lieu au moment même de l'histoire récente, en 2008, lorsque la crise financière mondiale a mis en évidence les failles et les coulisses douteuses du système financier mondial. N'étant pas censée être contrôlée par une autorité centrale, l'offre monétaire du bitcoin est façonnée et définie par son protocole éponyme – sa pierre angulaire étant que, dès la création du système, le nombre total de bitcoins pouvant être créés était connu et établi à l'avance (vingt et un millions), tout comme leur taux de

[46] Ce chapitre se fonde sur les articles et chapitres écrits ensemble dans le cadre de cette enquête (Mallard, Méadel & Musiani, 2014, Musiani, Méadel & Mallard, 2015, et notamment Musiani, Mallard & Méadel, 2017).

génération au fil du temps. La génération de bitcoins repose sur une activité appelée « minage », dont le principe est que les bitcoins sont attribués en récompense aux utilisateurs, les *mineurs*, qui prêtent leurs ressources informatiques et leurs disques durs au système à des fins opérationnelles et de sécurité. L'établissement du fonctionnement « purement » technique du système, comme nous l'avons mentionné, était strictement lié à l'objectif présumé d'éradiquer la corruption et les pratiques dangereuses et spéculatives « d'origine humaine » de la finance et des marchés – on ne pouvait plus faire confiance aux banques et aux États, ce qui ouvrait la voie à une solution reposant sur la cryptographie et l'architecture technique. Cependant, lorsque le bitcoin a commencé à devenir un système mondial et à susciter l'intérêt et les opportunités commerciales de divers acteurs, dont un certain nombre de nouveaux intermédiaires de marché, la question de la confiance est revenue au premier plan. Et avec elle, ont (res-)surgi des questions telles que la redistribution de l'autorité et du pouvoir – et la gouvernance.

5.1. Comment fonctionne Bitcoin ?

La construction de nouvelles formes de monnaie électronique est l'un des domaines d'application de la technologie pair-à-pair qui a conduit à des développements innovants au cours des dernières années. Bitcoin est certainement parmi les exemples les plus intéressants à cet égard. Basée sur un protocole P2P publié en 2008 par un mystérieux développeur ou groupe de développeurs (Nakamoto, 2008), à ce jour toujours non identifié, et rapidement adoptée par un nombre surprenant d'utilisateurs de l'Internet, cette monnaie s'est rapidement développée, au point qu'elle a déjà connu plusieurs crises. Plusieurs dizaines de milliers de transactions ont lieu chaque jour en Bitcoin, et le volume total des transactions qui y ont lieu est soupçonné d'avoir atteint 1 milliard de dollars. Comme c'est souvent le cas dans l'univers P2P, les développeurs visent à offrir des solutions alternatives à différents types de services existants, puisque les caractéristiques de base des architectures de réseaux distribués permettent à la fois d'explorer différentes pistes techniques et de promouvoir, dans la pratique quotidienne des services Internet, des principes socio-politiques différents de ceux qui ont cours dans la vie « hors ligne ».

Une des caractéristiques principales de Bitcoin est la promesse de « faire sans », c'est-à-dire sans

les intermédiaires de la finance, telles les banques, les institutions financières ou les autorités politiques nationales et supranationales qui s'occupent de l'échange et de la régulation monétaire. Ces différents intermédiaires sont accusés d' « éloigner » la monnaie de ses utilisateurs, de façon coûteuse de surcroît, et d'abandonner ce qui pourrait être considéré comme un « bien commun » à un capitalisme aujourd'hui confronté aux nouveaux défis résultant de la crise économique mondiale de 2007-08. Se passer des intermédiaires impliquerait de se débarrasser des garants institutionnels de la confiance monétaire, c'est-à-dire la reconnaissance, par toutes les parties au sein d'un système juridique, qu'un moyen de paiement est valable pour répondre à une obligation financière. Le fonctionnement des monnaies « officielles » se fonde sur l'existence d'acteurs comme les banques centrales, les garants ultimes de la valeur des biens et des titres en circulation. Inversement, Bitcoin offre la possibilité d'effectuer des transactions via la communication directe entre les utilisateurs, sans la nécessité de recourir à des tiers chargés de légitimer la valeur monétaire concernée. Ainsi, Bitcoin semble souligner, et peut être insuffler une nouvelle signification, à la centralité de la nature sociale de l'échange monétaire (Graeber, 2011). En outre, il permet d'observer de façons inédites l'économie politique de la production entre pairs : les nouvelles dynamiques de production, de gouvernance et de propriété qui émergent de la transformation progressive de certains des systèmes complexes qui entourent notre vie quotidienne en réseaux distribués (Bauwens, 2005). Bitcoin conteste la notion de confiance liée à une banque centrale avec l'idée d'une « confiance distribuée », étroitement liée à l'architecture technique en pair-à-pair.

En tant que service fonctionnant sur un réseau P2P, Bitcoin permet aux utilisateurs d'exécuter des paiements en rajoutant une signature numérique à leurs transactions. Il cherche à maintenir l'unicité des transactions à travers un service d'horodatage distribué. Les utilisateurs qui souhaitent entreprendre des transactions Bitcoin doivent installer un logiciel de P2P sur leur ordinateur, ce qui leur permet d'émettre et de recevoir des unités monétaires. Le logiciel permet aux utilisateurs de générer des adresses électroniques sous la forme de clés chiffrées que seul l'utilisateur peut authentifier. Ces adresses fonctionnent également en tant que « comptes » dans lesquels les bitcoins peuvent être stockés. Chaque transaction consiste à envoyer une quantité prédéterminée d'une adresse à l'autre au sein du réseau. Chaque transaction entre deux utilisateurs est recueillie sous forme agrégée dans un « bloc », qui est lui-même intégré à un répertoire, la *blockchain* ou

« chaîne de blocs ».

Selon un modèle répandu dans les applications dotées d'une architecture P2P, la chaîne de blocs n'est pas stockée dans un endroit centralisé, mais elle circule, et est constamment partagée entre tous les membres du réseau. Ainsi, la chaîne de blocs fonctionne en tant que référentiel public, qui inclut l'historique de toutes les transactions conclues après que le système a été lancé. Elle permet de savoir à tout moment quelle est la répartition des bitcoins entre les différentes adresses actives dans le réseau. Afin de garantir la fiabilité de cette information, seuls les blocs relatifs aux transactions authentifiées peuvent être ajoutés à la chaîne de blocs. Ainsi, chaque bloc est soumis à une vérification qui consiste - pour le dire vite - à examiner la séquence des transactions afin de s'assurer, par comparaison avec les transactions antérieures, que les utilisateurs sont effectivement en possession des biens qu'ils souhaitent échanger. Ce processus de vérification est effectué par certains des ordinateurs connectés au réseau.

Le logiciel Bitcoin installé sur les ordinateurs de tous les membres de cette communauté monétaire vise à suivre le flux permanent des transactions, mais il permet également, si les utilisateurs acceptent, de contribuer à la puissance de calcul nécessaire à l'ensemble du système pour la vérification en continu de la chaîne de blocs. En échange de cette contribution, l'utilisateur est récompensé par une quantité donnée de bitcoins. Ainsi, la création monétaire se réalise grâce à la contribution donnée par les utilisateurs à l'authentification des transactions, appelée minage (*mining)*.

Le protocole technique a été conçu de telle manière que la quantité d'argent qui est progressivement « libérée » par le processus de *mining*, et correspondant à la masse monétaire disponible pour l'échange, ne peut pas dépasser une quantité prédéterminée de 21 millions de Bitcoins. Cette limite est inscrite dans l'algorithme de Bitcoin. Le système n'est par ailleurs pas soutenu ou légitimé par aucun gouvernement ou autre entité juridique ou politique, et n'est pas remboursable contre de l'or ou d'autres biens reliés à des processus de légitimation par ces organismes. Son architecture décentralisée et distribuée n'implique aucune entité centrale chargée de la régulation de la valeur ou de la quantité totale de bitcoins. Ces fonctions sont déléguées au réseau d'utilisateurs lui-même.

L'architecture P2P de Bitcoin redistribue donc les responsabilités du bon fonctionnement du système, et ce à plusieurs égards. Premièrement, les utilisateurs doivent accepter un système dont le fonctionnement est basé sur le partage et la mise en commun des ressources individuelles. Cela implique un acte explicite d'adhésion au système, et une participation explicite par la suite, ce qui vise à préserver le système comme un dépôt de valeur. Deuxièmement, sa complexité technique est à la fois une garantie et une faiblesse potentielle. Une infrastructure technique complexe et résistante, permettant des routes d'échange alternatives en raison de sa décentralisation, peut susciter la confiance. Toutefois, et pour les mêmes raisons, elle peut aussi être une source de problèmes, des spéculations, des controverses, de comportements inappropriés, d'utilisations abusives. Enfin, si l'élaboration collective du code et du « contenu » dans le système est décentralisée, elle n'est que très rarement égalitaire : les rôles des utilisateurs, les niveaux d'engagement et les types d'intervention dans le système diffèrent, et ces discontinuités - entre ceux qui co-développent le code et ceux qui ne le font pas, entre ceux qui « minent » et ceux qui se limitent à échanger - ont des effets structurants sur la durabilité du système Bitcoin.

Le développement de la crypto-monnaie s'accompagne en effet de controverses multiples, non seulement chez les spécialistes de la monnaie mais aussi plus largement dans la presse et dans l'espace public. La viabilité de la monnaie fait l'objet de nombreux débats qui s'interrogent d'une part sur la durabilité et la fiabilité de ce moyen d'échange monétaire et d'autre part sur la capacité d'un tel dispositif a-régulé à s'autogouverner (Jacobs, 2011).

Du point de vue numéraire, le cours de la monnaie a connu plusieurs moments de fébrilité intense, avec des chutes importantes de sa valeur d'échange, cette volatilité mettant en cause la confiance dans le dispositif (Mallard et al., 2014). Plusieurs faillites, plus ou moins frauduleuses, des vols de monnaie par des intermédiaires, la fermeture de MtGox, la plus grosse plateforme d'échange, qui s'est dit victime de manœuvres frauduleuses, suivi par l'arrestation de son responsable (en août 2015) ont englouti des masses financières importantes et ont par la même mis en évidence des points de vulnérabilité du système.

L'autorégulation de la monnaie est également controversée. Le principe d'égalité des porteurs a été ébranlé par le succès de la monnaie : si chacun pouvait à l'origine produire des bitcoins contre

de la CPU (du temps machine), il faut désormais des capacités techniques qui dépassent celles de l'individu lambda. Ainsi, co-existent désormais dans le système deux catégories d'acteurs aux droits et compétences différenciés, ceux qui produisent de la monnaie et ceux qui se contentent de l'utiliser. Par ailleurs, l'ambition de Bitcoin de se débarrasser des intermédiaires n'a pas abouti et ceux-ci prolifèrent au contraire dans le monde de la crypto-monnaie en particulier pour convertir la monnaie, la gérer ou la produire. Enfin, les autorités publiques ont multiplié les tentatives pour intervenir dans la régulation du bitcoin, qu'il s'agisse de contrôler les échanges illégaux ou de réintroduire des règles communes pour les transactions. C'est cette « gouvernance malgré elle » que souhaite aborder ce chapitre.

5.2. Une infrastructure évolutive et controversée

Ce chapitre aborde la question de la gouvernance de Bitcoin en examinant les controverses autour d'éléments d'infrastructure spécifiques et critiques. Dans l'histoire courte mais chargée de Bitcoin existent de nombreux débats de ce type, d'ampleur variable (ils peuvent se limiter à une dispute temporaire sur un forum en ligne, ou s'étendre à un large éventail d'acteurs intervenant sur la crypto-monnaie), où, par exemple, ce qui semblait être une question technique s'est transformé en problème politique, où les explications d'un crash mélangent limites techniques et crise financière, où un doute est soulevé sur la frontière entre ce qui appartient à la *blockchain* et ce qui appartient aux intermédiaires, et ainsi de suite. De tels événements dans l'histoire de Bitcoin, qui ont mis en lumière des tensions, des conflits ou des divergences entre les acteurs concernés de Bitcoin sur des aspects spécifiques – qu'il s'agisse de la modification d'une caractéristique technique, de l'organisation et de la hiérarchie entre les développeurs principaux, ou de l'introduction ou de la disparition d'un intermédiaire – sont des lieux utiles pour observer la « fabrique » de la gouvernance de Bitcoin. Ainsi, en observant de tels événements, ce chapitre cherche à répondre à des questions telles que : comment des phénomènes structurants de la gouvernance, telles que l'action collective et le débat, le consensus et l'intervention des acteurs publics, sont-ils « dévoilés » par des dynamiques de controverse ? Qui sont les acteurs qui s'emparent, ou qui se voient confier, la responsabilité et l'autorité, en particulier lorsqu'il s'agit de décentraliser ou recentraliser des composantes spécifiques du système ?

Ce chapitre s'appuie bien sûr sur deux des principaux courants de la littérature STS dont on a discuté dans les chapitres 2 et 3 de ce mémoire : d'une part, les travaux qui explorent le rôle des intermédiaires de l'information et des infrastructures et architectures techniques en tant qu'instruments de gouvernance de l'Internet et « points de contrôle », autour desquels se jouent les questions de performance technique et économique, mais aussi des batailles liées aux valeurs et aux libertés. D'autre part, les recherches qui traitent des effets structurants et performatifs des controverses socio-techniques sur la gouvernance, et analysent les processus mêmes par lesquels les normes sont créées, négociées et mises à l'épreuve, considérés comme étant non moins importants que les normes « stabilisées » elles-mêmes.

En s'appuyant sur ces perspectives, quelques contributions ont cherché à appliquer les perspectives STS plus spécifiquement à l'étude de Bitcoin et de l'interaction entre la technologie et la politique qui y est en jeu. Bill Maurer et al. (2013) ont élaboré la notion de « métallisme numérique », en s'inspirant à la fois des STS et de l'anthropologie de la monnaie, pour rendre compte de la combinaison de matérialité et de virtualité qui caractérise le bitcoin. Le concept souligne la dématérialisation du bitcoin, dans lequel la valeur est « incorporée » comme l'est la monnaie dans l'or ; il souligne également comment, comme pour toute technologie soutenue par des réseaux numériques, la dématérialisation de la monnaie elle-même s'accompagne de la mise en place d'une infrastructure matérielle lourde. Dans un mélange de STS et de sociologie économique, Henrik Karlstrøm (2014) voit dans « l'encastrement matériel » des interactions marchandes la principale clé analytique pour comprendre la manière dont les monnaies virtuelles sont intimement liées à la configuration institutionnelle du monde matériel, tout comme les monnaies non virtuelles, ce qui permet de faire le pont entre les spécificités du bitcoin et l'histoire de la monnaie pour en tirer des leçons utiles. Il note également le défi que représente une étude qualitative des sciences sociales sur Bitcoin, en raison de la nouveauté du phénomène, de l'anonymat généralisé des principaux acteurs et de la nature des sources, dont beaucoup « sont, dans une certaine mesure, non vérifiables au sens académique traditionnel – beaucoup proviennent de pages web éphémères plutôt que de recherches publiées ». Dans une contribution centrée sur les méthodes, utilisant également Bitcoin comme un cas particulièrement emblématique de défi aux approches des sciences humaines et sociales, Pablo Velasco (2016) note le statut de la monnaie distribuée comme objet de recherche

« métamorphique » et observe que « parce que le bitcoin est à la fois un protocole, une monnaie, un logiciel, un réseau et un phénomène culturel, il peut jouer le rôle discontinu d'instrument, de méthode et d'objet de recherche » ; il note également que les données sur les crypto-monnaies sont « démocratiquement rares », contrairement à celles dont disposent les chercheurs sur les réseaux sociaux, par exemple.

Dans le contexte actuel de battage médiatique fréquent autour de la technologie blockchain, vantant notamment sa capacité à s'autoréguler entièrement via l'algorithme qu'elle sous-tend, la contribution de Primavera De Filippi et Benjamin Loveluck (2016) s'appuie sur la controverse (fin 2015/début 2016) autour du *fork* Bitcoin XT pour illustrer les limites d'une confiance excessive dans des outils purement techniques pour aborder des questions complexes de gouvernance, incluant des éléments de coordination sociale et d'échanges économiques. Une contribution antérieure d'Alexandre Mallard, Cécile Méadel et moi-même (2014) a montré comment, en introduisant et en discutant des dispositifs, des dynamiques ou des opérations spécifiques comme étant d'une certaine manière liés à l'établissement de la confiance, les connaissances expertes pionnières sur le bitcoin ont contribué à la définition et à la mise en forme mêmes de cette confiance au sein du système Bitcoin, contribuant finalement à réaliser la définition partagée de sa valeur en tant que monnaie.

Dans l'ensemble, ces contributions s'appuient sur des analyses détaillées et situées de la conception, la construction, l'établissement et l'appropriation de la technologie dans un système complexe tel que Bitcoin, et explorent finalement les liens entre la politique de l'infrastructure Internet et l'infrastructure en tant que politique Internet.

5.3. La gouvernance de Bitcoin en trois « controverses d'infrastructure »

Cette section centrale du chapitre présente trois aspects fondamentaux de l'histoire de Bitcoin que nous avons identifiés comme particulièrement pertinents pour étudier la question de la gouvernance, car ils ont fait l'objet d'un large débat public dans les cas où des événements « révélateurs » ont eu lieu. Une première dimension concerne la fiabilité des réseaux et des

protocoles sous-tendant la *blockchain* et son intégrité, qui a été mise à mal, par exemple, par un certain nombre de défaillances et de détournements de sécurité entre 2010 et 2014, ou plus récemment, par la mise en œuvre d'un « *hard fork* », Bitcoin XT, fin 2015. Une deuxième dimension explore le développement d'un écosystème articulé d'intermédiaires Bitcoin qui a progressivement introduit la monnaie numérique dans les réseaux internationaux du commerce et de la finance et l'a exposée à un certain nombre de points de vulnérabilité et d'exploitation « non purement techniques » – un épisode marquant à cet égard étant la fermeture, aux conséquences éclatantes, de la plateforme MtGox en 2014. Une troisième dimension aborde les liens ambigus avec l'économie souterraine incarnée par l'affaire Silk Road, débutée en 2011, affaire qui met en lumière l'impact des enquêtes policières sur le fonctionnement de l'architecture Bitcoin.

5.3.1. La « fourche involontaire » de mars 2013

Pour aborder la question de la relation entre la fiabilité du protocole technique et la confiance des utilisateurs – et ses conséquences pour la gouvernance de Bitcoin – les événements entourant la « fourche (*fork*) involontaire » de mars 2013[47] sont particulièrement intéressants, car ils montrent comment la communauté Bitcoin, des développeurs principaux aux mineurs en passant par les utilisateurs en général, a répondu à un moment de crise profondément ancré dans l'architecture technique, pour lequel il fallait développer à la fois une réponse technique et un consensus politique sur la solution. Les faits essentiels de l'événement sont les suivants : les 11 et 12 mars 2013, un mineur utilisant la version 0.8 du logiciel Bitcoin a créé un bloc invalide, de taille importante. Cela a créé une scission ou « fourche » involontaire dans la *blockchain*, puisque les ordinateurs équipés de la version la plus récente du logiciel à l'époque (0.8) ont accepté le bloc invalide et ont continué à construire sur la chaîne divergente, tandis que les versions plus anciennes du logiciel l'ont rejeté et ont continué à étendre la *blockchain* sans le bloc incriminé. Cette scission a entraîné la création de deux ensembles de transactions distincts, sans consensus clair ni même connaissance de l'existence de l'autre, ce qui a permis de dépenser deux fois les mêmes fonds sur chaque chaîne.

[47] J'ai été le « *lead* » de ce volet de l'enquête.

En plus de relater l'incident de manière directe, il est intéressant de noter que le compte-rendu de Wikipedia sur le sujet ajoute que « les mineurs ont résolu la scission en rétrogradant à la version 0.7, ce qui les a remis sur la voie de la *blockchain* canonique. Les fonds des utilisateurs n'ont pratiquement pas été affectés et étaient disponibles lorsque le consensus du réseau a été rétabli. Le réseau a atteint le consensus et a continué à fonctionner normalement quelques heures après la scission ». Cela soulève un certain nombre de questions intéressantes liées à notre question centrale de recherche, dans la mesure où ce « pépin » technique sans précédent a nécessité la négociation d'une nouvelle norme pour réorganiser les opérations de Bitcoin en une seule et unique *blockchain* -- et la mise en œuvre d'un « mélange » réussi d'éléments techniques, politiques et sociaux pour y parvenir. Que s'est-il effectivement passé derrière la résolution de la scission, et qui en est responsable ? Comment le réseau est-il « parvenu à un consensus » ? Le réseau a-t-il « fonctionné normalement » après cet épisode ? Qui étaient les acteurs et les actants de cette séquence d'événements ?

Le premier document à partir duquel il fallait commencer notre exploration a été, sans aucun doute, le rapport d'alerte sur le site web de Bitcoin et la proposition d'amélioration « post-mortem » associée, cette dernière ayant été rédigée par l'un des principaux développeurs de Bitcoin, Gavin Andresen. Bien que succinct et impersonnel, le rapport commence à donner une consistance « située » à certains aspects de l'affaire. Par exemple, il devient plus clair que la cause du problème était la création, l'extraction et la diffusion d'un « gros bloc [...] incompatible avec les versions antérieures de Bitcoin », le problème avec le bloc étant – précise la proposition d'amélioration – qu'il affichait un « plus grand nombre d'entrées de transactions totales que précédemment ». Dans son analyse ultérieure de l'incident, Vitalik Buterin (2013) précise que l'incident était lié à la publication de la version la plus récente de bitcoind, l'implémentation la plus populaire de Bitcoin utilisée par les mineurs. Les développeurs de cette version, appelée 0.8, ont changé la base de données utilisée par bitcoind pour stocker les blocs et les transactions, passant d'une base appelée BerkeleyDB à une autre appelée LevelDB, considérée comme plus efficace et plus adaptée pour réduire le temps de synchronisation de la *blockchain*. Cependant, explique Buterin,

> *ce que les développeurs n'ont pas réalisé à l'époque, c'est qu'en faisant cela, ils ont aussi accidentellement introduit un changement dans les règles du protocole Bitcoin. Afin d'effectuer une mise à jour de la base de données, le processus de base de données doit effectuer un 'verrouillage' sur la partie de la base de données qui stocke cet élément d'information particulier, un mécanisme mis en œuvre pour empêcher deux changements de se produire simultanément.*

LevelDB ne plaçait aucune restriction sur le nombre possible de verrous, mais BerkeleyDB en avait, et a échoué lorsqu'un seul bloc a nécessité plus de verrous que cette limite supérieure.

Les nœuds exécutant la version la plus récente du logiciel, 0.8, ont pu gérer ce gros bloc, mais certains nœuds exécutant des versions antérieures du logiciel l'ont rejeté. Cette bifurcation involontaire de la *blockchain*, apprend-on du rapport d'alerte, est due au fait qu'au moment de l'incident, les nœuds exécutant les versions antérieures à la version 0.8 du logiciel disposaient d'une puissance de calcul supérieure à celle des nœuds exécutant la version la plus récente, ce qui leur conférait automatiquement la prééminence :

> *La chaîne incompatible avec la version pré-0.8 (ci-après dénommée "chaîne 0.8") disposait à ce moment-là d'environ 60 % de la puissance de hachage minière, ce qui a empêché la scission de se résoudre automatiquement (comme cela aurait été le cas si la chaîne pré-0.8 avait dépassé la chaîne 0.8 en termes de travail total, obligeant les nœuds 0.8 à se réorganiser en faveur de la chaîne pré-0.8).*

À cet endroit, le compte-rendu de l'incident commence à mentionner certains acteurs spécifiques de l'écosystème Bitcoin au sens large – par exemple, deux pools de minage[48], BTCGuild et Slush, qui ont rétrogradé leurs nœuds Bitcoin 0.8 en 0.7 « afin que leurs pools rejettent également le bloc le plus large ». En raison de leur position centrale dans le processus de minage de Bitcoin, le geste de ces deux acteurs a déplacé la majorité du pouvoir de calcul sur la chaîne sans le bloc le plus important, provoquant finalement la réorganisation des nœuds 0.8 vers la chaîne pré-0.8. Plus loin, le rapport mentionne cet aspect – l'un des premiers mouvements déterminants pour revenir à une seule et unique norme stabilisée – comme un aspect positif, dans lequel les deux acteurs ont eu un comportement altruiste, car la rétrogradation de leurs nœuds a été bénéfique pour le système mais

[48] *Mining pools*, services qui permettent aux mineurs de s'associer sous une même entité afin de miner des cryptomonnaies.

« leur a fait sacrifier des sommes d'argent importantes », étant donné qu'ils avaient précédemment exploité la version 0.8 et qu'en revenant à 0.7, ils ont perdu ce qu'ils avaient miné.

Le rapport fait état d'un cas important de double dépense, c'est à dire le fait de réussir à dépenser de l'argent plus d'une fois – ce contre quoi le grand répertoire de la blockchain distribuée mais unique qui sous-tend Bitcoin protège généralement, mais la bifurcation involontaire l'a rendu temporairement possible. L'individu à l'origine de la double dépense s'est ensuite identifié comme un utilisateur expérimenté qui tentait d'établir la preuve que ce type d'opération était possible, et a révélé les détails de ses actions (un dépôt d'une somme importante, équivalente à 10 000 dollars, sur le système de paiement en ligne OKPay). Le rapport « post-mortem » de l'incident inclut cet événement dans la liste de « ce qui a marché » – soulignant que les actions de l'utilisateur ont finalement rendu le système plus fort, parce qu'il a testé une de ses défaillances sans intention malveillante. Par ailleurs, les analyses ultérieures contestent quelque peu cette interprétation, affirmant que « une bifurcation perdurant dans le temps aurait probablement exacerbé le problème et permis à des attaquants malveillants de trouver un moyen systématique de créer des transactions de type double dépense » et soulignant que d'autres points d'échange ou services de paiement auraient pu prendre encore plus de temps pour mettre à niveau leurs clients (ou désactiver des transactions) dans des contextes bien plus défavorables (Naranayan, 2015).

La principale arène de négociation d'une possible solution était le canal IRC[49] bitcoin-dev, où la plupart des développeurs principaux se sont rapidement réunis. La question centrale de la controverse était de savoir laquelle des deux *blockchains* devait être supportée – sachant qu'un choix devait être fait, et le plus rapidement possible. La chaîne supportant la 0.8 avait à son avantage une plus grande puissance de calcul par nœud que celle de la 0.7 : les nœuds étaient moins nombreux, mais plus puissants. Cependant, comme l'explique Buterin (2013), légitimer la chaîne basée sur 0,8 aurait imposé une charge plus lourde à beaucoup plus d'utilisateurs : « des milliers d'utilisateurs de la version 0.7 auraient été contraints de procéder à une mise à niveau pour pouvoir utiliser Bitcoin, ce qui ne se produirait pas si le fork 0.7 prenait le relais puisque les deux

[49] *Internet Relay Chat*, protocole de communication textuel qui sert à la communication instantanée, principalement sous la forme de discussion de groupe par l'intermédiaire de canaux de discussion (voir Latzko-Toth, 2010).

versions de bitcoind peuvent le lire ». Le temps était également un facteur essentiel, ce qui tendait à faire pencher en faveur d'une action menée par quelques acteurs puissants mettant leur poids dans la balance, au lieu d'une réponse distribuée et plus longue. Comme l'a souligné le développeur Pieter Wuille dans les discussions IRC : « Nous ne pouvons pas demander à tous les utilisateurs de bitcoins du monde de passer instantanément à la version 0.8, alors non, nous devons revenir à la chaîne 0.7 » (Naranayan, 2015). Pour ces raisons, un consensus a finalement été atteint sur la rétrogradation à 0,7.

À ce stade, pour que la décision soit appliquée, il fallait que la plupart des acteurs majeurs – « majeurs » en termes de ressources informatiques dédiées et de confiance des utilisateurs – se rallient à cette décision. Ainsi, le canal IRC bitcoin-dev est devenu le lieu où les développeurs ont déployé, pour reprendre les termes de Callon (1986), des mécanismes d'intéressement et d'enrôlement vis-à-vis des mineurs principaux, des opérateurs de pools miniers et des marchands. Un facteur déterminant à cet égard semble être la décision de l'opérateur de pool minier BTCGuild, en particulier, d'aller de l'avant avec le déclassement. À un moment donné, l'opérateur souligne, en substance, qu'il a la capacité de calcul nécessaire pour mettre fin à l'incident : « Je peux à moi seul remettre 0,7 à la puissance de hachage majoritaire. J'ai juste besoin de la confirmation que c'est ce qu'il faut faire », ce qui est rapidement confirmé par plusieurs développeurs. La plupart des plateformes d'échange et de dépôt procèdent à la fermeture de leurs dépôts, mettent à jour leurs serveurs sur la blockchain 0.7 et reprennent leurs activités. Il est intéressant de noter que, dans le message IRC qui résume essentiellement les instructions des développeurs aux acteurs de Bitcoin et met effectivement fin à l'urgence, le rôle central de BTCGuild est cité par le développeur Wuille comme confirmation que la rétrogradation à la version 0.7 est effectivement le bon choix, et que les choses rentreront effectivement dans l'ordre bientôt en raison de la simple puissance de calcul, car BTCGuild s'est rallié à ce choix : « Si vous êtes un mineur, veuillez ne pas utiliser le code 0.8. Arrêtez, ou repassez en 0.7. BTCGuild passe à 0.7, donc l'ancienne chaîne obtiendra bientôt un taux de hachage majoritaire. » (Naranayan, 2015). Le basculement de la puissance de hachage a suivi de peu, comme le rapporte Buterin (2013) : « vers 03:30, le point de basculement est arrivé. La chaîne 0.7 a rapidement rattrapé son retard de seulement 10 blocs, puis de 8 blocs, et à 06:19 les deux chaînes ont convergé vers la même longueur au bloc 225454, ce qui a conduit presque tous les mineurs restants à abandonner l'autre. »

L'incident était terminé, et la bifurcation involontaire réparée – mais pas avant d'avoir donné quelques indications éclairantes sur la façon dont le pouvoir est co-construit dans Bitcoin, quels sont les nœuds d'autorité, de pouvoir et de hiérarchie dans ce système hautement distribué, quelle part est technique et quelle part est sociopolitique, et comment les deux se croisent. Plus précisément, la bifurcation involontaire de Bitcoin dévoile un certain nombre de dynamiques qui concernent de près la définition de la gouvernance dans Bitcoin, et plus largement dans les environnements distribués basés sur la blockchain.

Premièrement, nous observons comment le *leadership*/initiative individuel et la recherche d'un consensus communautaire ont tous les deux été essentiels pour résoudre un moment de tension et de controverse qui aurait pu conduire à la disparition de Bitcoin. A côté de processus décisionnels « classiques », faits du dialogue entre l'individu et le collectif, nous pouvons également observer les asymétries de pouvoir inhérentes entre les acteurs qui sous-tendent le fonctionnement de la *blockchain* : plus particulièrement, l'asymétrie entre une multitude d'utilisateurs et une petite oligarchie de pools miniers. Deuxièmement, ce cas montre que ce qui a fait de cet incident « juste » un incident, plutôt qu'un *hard fork* durable ou un dommage permanent au système, a été la combinaison d'une « semi-centralisation » humaine, ou d'une centralisation tout court, dans la réponse au risque, et une décentralisation de la *blockchain* elle-même qui est restée compatible avec elle. L'existence d'une blockchain décentralisée présuppose une infrastructure dont la réparation doit être recentralisée d'une manière ou d'une autre, et s'inspirer de mécanismes de gouvernance capables d'engager une variété d'acteurs (utilisateurs, mineurs, développeurs) mais se coordonnant selon des dynamiques bien connues et typiques des communautés open source. Troisièmement et enfin, cet événement souligne la matérialité de l'infrastructure de Bitcoin en tant qu'outil de gouvernance. Avec son écosystème complexe d'intermédiaires, de médiations et de points de contrôle, cette « gouvernance par l'infrastructure » se révèle à la fois dans la cause de l'incident (un changement dans le type de base de données utilisée pour stocker les résultats a des conséquences inattendues sur l'organisation de la communauté et la valeur de la monnaie) et dans sa solution (un acteur « puissant » en termes de puissance de calcul est capable de ramener à lui seul la controverse à un point stabilisé, voire à sa fin).

5.3.2. La fermeture de MtGox

La fermeture de la plateforme MtGox[50] a été l'occasion d'étudier les mécanismes de gouvernance sous-jacents à l'infrastructure Bitcoin sous un autre angle : contrairement au cas du *fork*, les incertitudes sur la gouvernance ne concernent pas le cœur du système, la blockchain, mais l'un des intermédiaires techniques et économiques qui y sont branchés et assurent une interface avec d'autres acteurs. MtGox ayant été un acteur majeur de l'écosystème Bitcoin lors de son essor, les troubles qu'il a rencontrés offrent un éclairage fructueux sur les questions de gouvernance liées à la position spécifique des intermédiaires au sein de son infrastructure.

MtGox a été créé en 2007 par un innovateur Internet nommé Jed McCaleb. Ce n'est qu'en juillet 2010 qu'elle est devenue à part entière une plateforme d'échange de bitcoins. En 2011, elle a été rachetée par un autre entrepreneur Internet, Mark Karpeles. Karpeles a développé MtGox pendant la période où le bitcoin a connu son immense succès, débutant en 2011 avec un taux de change de 1 $ et atteignant 1000 $ fin 2013. MtGox a ensuite joué un rôle central sur le marché du bitcoin, captant parfois 80% des échanges mondiaux. La plateforme est également en partie associée à l'effondrement qui a suivi cette phase d'euphorie, à travers une série de soubresauts qui ont conduit le taux de change du bitcoin à un niveau d'environ 250 $ au début de l'année 2015. La fermeture de MtGox en février 2014 est une étape importante dans ce long parcours ponctué de crises, de crashs et de rebonds. Mais la plateforme a rencontré de nombreux problèmes bien avant sa fermeture : entre 2011 et 2014, une série de problèmes mêlant dimensions techniques, juridiques et économiques sont survenus. Nous examinerons ici quatre épisodes mettant l'accent sur les problèmes de gouvernance posés aux intermédiaires dans un écosystème organisé autour d'une blockchain.

Le premier épisode est connu sous le nom de l'affaire « Dwolla ». En mai 2013, les autorités financières américaines ont enjoint Dwolla, un e-business de paiement et de transfert d'argent, de cesser ses transactions avec Mutum Sigillum LLC. Cette société était en fait une filiale de MtGox et servait d'intermédiaire pour opérer des transactions entre Dwolla et MtGox : les clients

[50] Qui a été principalement analysée par Alexandre Mallard.

utilisaient leur compte Dwolla pour faire circuler de l'argent sur le compte de Mutum Sigillum LLC, duquel il circulait à son tour sur la plateforme pour convertir des dollars en bitcoins. Le rapprochement de Dwolla (implanté aux Etats-Unis) et de MtGox (domicilié au Japon) par l'intermédiaire de Mutum Sigillum LLC était problématique pour les autorités fédérales américaines car il actait la circulation systématique et massive de devises au niveau international qui n'avaient jamais été déclarées comme telles aux autorités : il enfreignait ainsi la loi sur les « activités de transmission d'argent sans licence ». Du point de vue de la gouvernance, il s'agit d'un cas classique de conflit avec des acteurs économiques opérant par le biais de médias électroniques aux frontières des territoires nationaux : un Internet sans frontières contre des transactions économiques entre pays, qui sont soumises à des réglementations spécifiques. Le scénario décrit dans la presse inclut toutes les caractéristiques d'une telle situation de conflit : une tentative de régulation, un montage financier contestable avec des sociétés écrans, un juge, un mandat et, au final, une lourde sanction financière. En effet, en août 2013, l'affaire s'est terminée par une saisie de 2 900 000 dollars sur le compte de Mutum Sigillum LLC, une sanction qui a contribué à la détérioration de la situation financière de MtGox. Dans ce contexte, la gouvernance – de manière plus « classique » – se réduit au respect de la réglementation.

Un deuxième cas qui s'avère instructif est celui où la plateforme rencontre des problèmes techniques entravant le flux normal des transactions. C'est ce qui s'est produit en novembre 2013, lorsque les échanges ont été temporairement ralentis, voire paralysés, par une défaillance technique qui a ensuite été décrite comme une attaque par déni de service (DDoS). Ce type d'interruption du fonctionnement fluide et silencieux du marché déclenche généralement deux réactions : d'une part, les utilisateurs se rendent sur les forums Internet afin de recueillir des informations ou d'exprimer leur mécontentement ; d'autre part, la presse en ligne se fait l'écho du problème et se livre à des tentatives de diagnostic. Ces deux processus permettent d'activer les espaces publics associés au marché en tant que lieux où les conflits techniques et économiques peuvent être exprimés – et parfois résolus. En outre, ces processus mettent en place des mécanismes de gouvernance qui sont à la fois génériques et très révélateurs des particularités de Bitcoin. Ils sont génériques dans la mesure où le recours à ce type d'arène constitue un moyen habituel de favoriser le débat public sur les modalités d'organisation du marché. La notion de « forum hybride » peut être mobilisée pour appréhender les modalités de gouvernance qui sont ici en jeu (Callon et al., 2009). Mais ces

processus de communication sont également symptomatiques de Bitcoin et particulier, non seulement parce que les forums et la presse en ligne ont joué un rôle majeur dans la diffusion des pratiques et des usages associés à la monnaie électronique (Mallard, Méadel et Musiani, 2014), mais aussi parce que cette modalité d'intervention s'appuie sur les effets de transparence des transactions propres à son fonctionnement : notamment, dans ces débats en ligne, les acteurs évoquent le décalage entre les informations sur les transactions données sur la plateforme et dans la *blockchain*. Par exemple, le 18 novembre 2013, un utilisateur poste la question suivante sur l'un des principaux forums Bitcoin

> *Je viens de retirer des BTC de Mt Gox à l'adresse 1Mvk4YAtKZAP43wEhZ6ZQrTzLZwzPxtTJ, id de transaction 3dfa979af56ff061efbceed0dd7c9dc9fd8c774249544018f6bbf646323ff03b, mais je n'ai pas reçu les pièces et la transaction n'est pas dans la chaîne. Dois-je m'inquiéter ?*

Les modalités de traçabilité permises par la blockchain, quel que soit leur caractère partiel, fournissent des ressources spécifiques pour les processus de gouvernance basés sur la communication au sein de ce marché.

Un troisième épisode emblématique s'est produit dans la tourmente de l'effondrement de MtGox. Début février 2014, la plateforme rencontre de nouveaux problèmes, caractérisés dans un premier temps par un retard dans l'exécution des retraits d'argent et, finalement, par l'interruption complète de ce service. Dans un premier temps, le marché dans son ensemble est perturbé et les prix montent et descendent de manière erratique, faisant craindre un effet domino. Les signes d'une défaillance technique de la plateforme s'accumulent, et MtGox publie une série de communiqués de presse reçus par les acteurs du marché comme de moins en moins réconfortants et crédibles. Dans ces déclarations, Mark Karpeles indique qu'un problème de « malléabilité » de la monnaie Bitcoin pourrait être à l'origine de la panne, problème que le personnel de la plateforme et les développeurs de Bitcoin tenteraient conjointement de résoudre. L'argument est intéressant car il montre une tentative de déplacer le problème et d'attribuer la responsabilité de la défaillance de MtGox à une faiblesse qui serait inhérente à Bitcoin. De nombreux membres de la communauté Bitcoin ont considéré cette tentative comme une insulte à la cryptomonnaie elle-même. Mais surtout, cette tentative s'est avérée peu convaincante, d'autant plus qu'il est devenu évident que les problèmes rencontrés par MtGox ne se propageraient pas aux autres acteurs du marché. Cela est devenu

évident lors de la dernière transaction enregistrée sur la plateforme vers le 20 février, à un moment où elle affichait un cours de 110 dollars pour 1 bitcoin, alors que les autres plateformes maintenaient un cours autour de 50 dollars.

Au final, MtGox s'est effondré sans entraîner le reste du marché dans sa chute. La raison exacte de cet effondrement a demeuré l'objet de plusieurs spéculations au cours des mois suivants. L'un des scénarios qui a émergé pendant le crash et qui a été confirmé bien plus tard, implique une défaillance technique de la plateforme MtGox elle-même et non du protocole Bitcoin : une « fuite » aurait été en place depuis longtemps, provoquant la soustraction progressive de 750 000 bitcoins, et n'a été découverte qu'au début de 2014. Il est important de souligner ici que la capacité à décréter la frontière entre ce qui est du ressort de la blockchain et ce qui est du ressort d'un acteur intermédiaire est en soi une composante de la dynamique de gouvernance qui est ici en jeu. Le travail de délimitation de l'infrastructure (et la réponse, par conséquent, à des questions telles que « où s'arrête l'infrastructure ? » ou encore « qui en est responsable ? ») est crucial.

La fin de l'histoire de MtGox révèle enfin une dernière modalité intéressante de gouvernance pour les intermédiaires économiques inscrits dans l'écosystème de Bitcoin. L'épisode se passe le 24 février 2014, alors que la plateforme est quasiment arrêtée. Mark Karpeles prend acte de sa défaite en démissionnant du conseil d'administration de la Bitcoin Foundation. Ainsi, il admet publiquement la déconnexion entre la trajectoire suivie par la plateforme et les nouvelles entreprises des innovateurs du bitcoin. Cette action fait écho à une déclaration publique faite à la même période par 6 leaders de l'industrie du bitcoin (Blockhain.info, Coinbase, Kraken, Bitstamp, BTC China, et Circle) pour rompre les rangs avec MtGox. Le texte de la déclaration montre clairement la volonté de prévenir toute confusion entre le sort de MtGox et l'avenir du bitcoin : « Cette tragique violation de la confiance des utilisateurs de MtGox est le résultat des actions d'une seule entreprise et ne reflète pas la résilience ou la valeur du bitcoin et de l'industrie de la cryptomonnaie (...) Comme pour toute nouvelle industrie, il y a certains acteurs sans scrupules qui doivent être éliminés, et c'est ce que nous voyons aujourd'hui ». L'affichage public de la sortie de l'un des membres de la coalition soutenant le marché Bitcoin, et la revendication d'une déconnexion entre ce qui lui est arrivé et ce que font les autres acteurs relèvent en fin de comptes

d'une modalité de gouvernance précise : restaurer la confiance dans le marché, par le biais d'une confiance restaurée dans l'infrastructure qui la soutient.

5.3.3. Les liens entre Bitcoin et Silk Road

La troisième étude de cas de ce chapitre présente les liens de Bitcoin avec le marché noir en ligne Silk Road[51], et aborde la question de l'attribution des responsabilités au sein de cette plateforme. Ce cas montre le grand nombre d'intermédiaires, techniques ou non, impliqués dans un marché exclusivement basé sur le bitcoin – et, plus spécifiquement, il aborde le rôle des autorités publiques face au marché illégal que constitue l'espace virtuel Silk Road.

Silk Road était un site du « dark web » destiné au commerce entre particulier, à l'instar d'eBay ou d'Amazon, mettant en relation fournisseurs et clients par le biais d'une plateforme d'infrastructure de transaction et financé par des commissions sur les ventes. Contrairement à d'autres marchés numériques, Silk Road présentait une double spécificité : la seule monnaie acceptée était le bitcoin et la transaction s'effectuait via une interface TOR. Toutes deux étaient censées assurer l'anonymat des acteurs et des transactions, deux conditions majeures compte tenu de la spécificité des marchandises proposées : des drogues, dans leur grande majorité, avec un large choix de LSD, d'héroïne, d'ecstasy, de cannabis, etc. (dans un listing de 13.000), mais aussi des services de piratage informatique, des logiciels malveillants, des faux passeports, des relevés de cartes de crédit... et peut-être même, selon les accusations portées par le Federal Bureau of Investigation (FBI), les services de tueurs à gages. Silk Road (SR) a fonctionné entre janvier 2011 et octobre 2013, avant sa fermeture lorsque Ross William Ulbricht, propriétaire et inventeur présumé du site, a été arrêté par le FBI[52]. Bien qu'il ait plaidé non coupable, il a été condamné à perpétuité en mai 2015. Le récit de ce cas s'appuie, comme déjà les deux précédents, sur trois ressources : des matériaux de presse, avec une attention particulière au magazine Wired qui a suivi cette histoire de près, les débats sur le forum Bitcoin et des documents juridiques disponibles en ligne.

[51] Qui a été principalement analysée par Cécile Méadel.
[52] Des tentatives de réouverture subséquentes ont connu le même sort, jusqu'en 2017.

Dès sa création, Silk Road s'est présenté comme un système militant, prônant la promotion de la philosophie libertaire du « marché libre » d'inspiration de l'école autrichienne[53] ; il a revendiqué sa continuité avec le paradigme de Bitcoin, méfiant à l'égard des politiques publiques de marché. SR promouvait explicitement un modèle libertaire de marché reliant directement l'offre et la demande de produits interdits à tort par les États ; il considérait que les gens sont libres de consommer des drogues dans la mesure où leur consommation ne dérange personne. Le site affirmait qu'il bannissait tout ce qui pouvait causer du tort à une autre personne (le statut du commerce de certaines armes, par exemple, restait toutefois ambigu). Ce discours a été accueilli favorablement par la communauté Bitcoin. Comme l'explique l'un des premiers articles consacrés à SR en juin 2011 : « Depuis son lancement en février dernier, Silk Road représente la mise en œuvre la plus complète de la vision de Bitcoin. Nombre de ses utilisateurs sont issus de la communauté *geek* de Bitcoin et considèrent Silk Road comme plus qu'un simple endroit où acheter de la drogue » (Chen, 2011). Ulbricht, interviewé juste avant son arrestation, a affirmé qu'il avait « un message important pour le monde » : « Le peuple peut maintenant contrôler le flux et la distribution de l'information et le flux d'argent. Secteur par secteur, l'État est éliminé de l'équation et le pouvoir est rendu à l'individu » (en Greenberg, 2013). Sur le forum Bitcoin, ce discours semble avoir du succès : certains commentateurs présentent Roberts comme un « héros », « notre Che Guevara à nous », « un nom [qui] vivra [parmi] les plus grands hommes et femmes de l'histoire comme un soldat de la justice et de la liberté », etc.

Cependant, comme le mettront en évidence les enquêtes policières, ce modèle de marché « parfait », chassant les intermédiaires et les interventions de l'État, était surtout une expérience de pensée et ne pouvait pas fonctionner en indépendance ; un tel marché nécessitait en réalité un modèle de gouvernance solide et impliquait une multiplicité d'acteurs. Comme le montre cette partie du chapitre, l'enquête policière, qui durera trois ans, permettra de faire la lumière sur le fonctionnement du site mais aussi, en retour, de modifier son organisation tout au long de la procédure.

[53] Fondée sur l'individualisme méthodologique, le concept que les phénomènes sociaux résultent exclusivement des motivations et des actions des individus.

Cela nous amène à la première et centrale question posée par les différents services qui s'intéressent à SR depuis l'été 2011 : qui était responsable du trafic illicite sur le site ? Les acheteurs et les vendeurs, conformément à la philosophie de SR ? Les premiers étaient faciles à trouver pour les enquêteurs, qui n'avaient qu'à proposer des bons prix pour les séduire – et en effet, partout dans le monde, des procès ont été intentés contre eux. Les vendeurs étaient plus difficiles, bien que pas impossibles, à identifier : selon la presse, la police nationale a pu localiser et poursuivre des vendeurs dans plus de dix pays différents, dont les États-Unis, l'Australie, l'Europe et Israël. Bientôt, cependant, la police en a voulu davantage et a recherché le « cercle intérieur » : les enquêteurs ont exploré dans toutes ses dimensions le fonctionnement du SR et ont mis en évidence la chaîne d'intermédiaires nécessaire pour effectuer, dans des conditions appropriées, une « transaction directe ». Suivant les pas de la police, la question de la répartition des responsabilités peut être abordée en trois points. La première dimension concerne le système bancaire capable de faciliter l'utilisation des bitcoins et de réguler les échanges de devises. La deuxième dimension nous conduit plus directement aux infrastructures techniques de SR, contrôlées *de facto* par une autorité centrale ; la troisième se concentre sur les règles spécifiques du marché de SR et leur application, concernant la résolution des conflits, la réglementation des biens interdits, la gestion de la concurrence, etc.

En ce qui concerne le système bancaire, les enquêtes de police montrent que SR avait besoin d'un système spécifique et ne pouvait pas s'appuyer entièrement sur l'algorithme de Bitcoin ; une nouvelle couche de services a été mise en place avec différentes fonctions. Tout d'abord, SR agissait comme une banque ou, plus exactement, comme un dépôt fiduciaire. Comme cela a été expliqué en juin 2011 sur le forum Bitcoin, ce dépôt protégeait les acheteurs et les vendeurs contre les escrocs (puisque l'argent déposé sur un compte SR n'était envoyé au vendeur que lorsque la transaction était terminée de manière satisfaisante). Ce tiers de confiance faisait office de « point de passage obligé », ce qui implique un contrôle centralisé. *De facto*, les investigations ont conclu que le dépôt fiduciaire était contrôlé directement et exclusivement par Ulbricht. Le FBI l'a tenu pour responsable d'un premier niveau de responsabilité et il a été personnellement inculpé pour blanchiment d'argent (chef d'accusation 3 de la plainte scellée). Le second point concerne l'argent « piégé » sur le compte de dépôt, nécessitant un intermédiaire pour être blanchi. Comment l'argent

pouvait-il être ré-injecté dans le monde extérieur, en éliminant le lien direct avec SR ? Un important vendeur de drogue, Steven Lloyd Sadler, qui a coopéré avec la police, a expliqué que la meilleure solution était de passer par LocalBitcoins.com, un site web qui mettait en relation des négociants et des acheteurs de bitcoins pour une somme modique. Ce site organisait une rencontre physique entre un vendeur qui voulait se débarrasser de sa cryptomonnaie, même avec un faible taux de change, et des acheteurs disposant d'argent liquide. Sadler conclut : « Tout vendeur de Silk Road qui n'est pas sur LocalBitcoins perd beaucoup d'argent » (O'Neill, 2014). Le troisième point relatif aux opérations bancaires concerne la difficulté d'utilisation des bitcoins : la grande majorité des 150 000 acheteurs uniques de SR (selon l'acte d'accusation) n'avaient certainement pas les compétences nécessaires pour effectuer des transactions avec cette cryptomonnaie. L'enquête de police a permis d'identifier au moins deux intermédiaires, certainement parmi beaucoup d'autres, capables de soutenir leurs transactions et de les poursuivre : Robert Faiella a revendu des bitcoins sur le site web de SR (probablement sur le forum) et les a achetés par l'intermédiaire de Charlie Shrem, directeur général de The Company, une société qui avait pour but de permettre aux clients d'échanger des espèces contre des bitcoins. Ironiquement, la plainte pénale révèle que Shrem était en outre « chargé de veiller à la conformité de la société avec les lois fédérales et autres contre le blanchiment d'argent », ce qui signifie qu'il était pleinement conscient du caractère illicite des transactions sur SR. La définition de la responsabilité est ensuite étendue au service concernant tous les aspects financiers des transactions (elle lie indirectement Silk Road à la Bitcoin Foundation, puisque Shrem en est l'un des administrateurs). L'instrument de paiement décentralisé ne pouvait donc pas assumer seul le bon traitement de la transaction financière : pour fonctionner correctement, il a besoin de l'implication dynamique (donc, de la responsabilité) d'une série d'acteurs qui ajoutent des règles de conduite et performent le marché.

La deuxième dimension concerne l'infrastructure technique du site, qui est devenue de plus en plus complexe afin d'assurer la confidentialité des échanges, tant vis-à-vis de la police que des cyberattaques de plus en plus fréquentes et percutantes (O'Neill, 2013). Dans cette mesure, les outils de chiffrement, les cyber-attaquants et les inspecteurs de police ont participé à la reconfiguration de l'écosystème de transaction, c'est-à-dire de la gouvernance de SR. Cependant, le bitcoin lui-même, initialement perçu par la police comme le maillon faible de la confidentialité, a résisté plus que prévu, comme le montre l'aventure malheureuse de deux universitaires (Ron et

Shamir, 2013). Leur analyse des flux de bitcoins, basée sur la non-évolution de certains portefeuilles, a été rapidement démentie par un utilisateur de bitcoins sur le forum Reddit. Cependant, comme l'ont démontré les enquêtes de police, SR a considéré que Tor et Bitcoin n'offraient pas de garanties suffisantes. SR a alors utilisé une couche renforcée de chiffrement afin de dissimuler les transactions individuelles. La plainte du FBI explique que « Silk Road envoie tous les paiements à travers une série complexe et semi-aléatoire de transactions factices [...] rendant presque impossible de relier votre paiement à tout argent quittant le site ». Ces outils de chiffrement n'étaient pas seulement destinés à échapper aux poursuites, mais aussi à résister aux cyberattaques, nombreuses, de pirates informatiques (avec plusieurs tentatives de chantage) ou de concurrents. L'attaque la plus grave, en avril 2013, par déni de service, qui a profité de vulnérabilités inconnues dans TOR, a d'ailleurs été conçue par un nouveau venu sur le marché, Atlantis. En plus des outils de chiffrement, SR, avec sa popularité croissante, avait besoin d'une large infrastructure et nécessitait d'un puissant parc de serveurs, finalement localisés par le FBI dans de multiples pays étrangers. Les nombreuses infrastructures affaiblissaient la sécurité de la plateforme, comme l'ont indiqué les commentateurs du forum ou de la presse. Ainsi, la police a ouvert une première brèche en saisissant une ferme de serveurs en Finlande. Mais cela n'a pas suffi pour trouver la cible de l'attaque par déni de service, même s'il est apparu clairement que l'infrastructure était entièrement sous le contrôle d'un acteur ou d'un groupe d'acteurs spécifiques. En effet, les traces laissées par l'utilisation de toutes ces infrastructures ne permettent pas d'identifier l'entité responsable. Le FBI avait besoin de saisir du matériel, à savoir le disque dur d'Ulbricht, pour fermer le site web. Ulbricht avait été identifié grâce à une utilisation trompeuse d'une adresse e-mail. Selon Wired, il avait été trop confiant dans la capacité du système de chiffrement de son disque dur à cacher ses activités. S'il avait utilisé des outils d'anonymisation plus puissants, ses traces auraient été plus difficiles à identifier. Mais ces traces ont été utiles pour démontrer le fonctionnement du site, et la culpabilité d'Ulbricht, une fois son identité repérée et son ordinateur saisi. SR a encapsulé divers dispositifs techniques, de la blockchain Bitcoin au serveur, en passant par des boîtes mail chiffrées, afin de réaliser des transactions. Comme nous l'avons vu précédemment à propos de l'affaire du fork, la gouvernance du marché du bitcoin est encapsulée dans des infrastructures particulières, fortement interdépendantes.

La troisième et dernière dimension nous amène aux règles spécifiques au marché SR. Comme dans tout marché numérique, la confiance était centrale pour SR, mais les biens particuliers que ce marché traitait rendaient cette question encore plus délicate. Les acheteurs se mettaient dans une situation de risque et pouvaient faire confiance (Luhman, 2000) au produit sous trois aspects : la qualité des produits, la confidentialité des échanges et la bonne exécution des transactions. Le site web proposait alors des mécanismes de confiance, comme les évaluations des vendeurs ou, comme nous l'avons vu, un tiers de confiance. Ainsi, on pouvait supposer que le service principal de SR n'était pas le commerce de produits illicites, mais la vente « d'assurances et de produits financiers (...) Le modèle économique consiste à banaliser la sécurité » (Greenberg, 2013). Ce point nous amène à un autre mode de gouvernance : par des règles et des instructions de fonctionnement, une partie d'entre elles étant formelles. Le site web de SR spécifiait les produits et services autorisés mais aussi les termes d'utilisation et les conditions de service. La revente des comptes fermés des vendeurs était, par exemple, interdite, et les administrateurs du site les fermaient s'ils en venaient à connaissance (voir O'Neill, 2014). Le site proclamait sa volonté de satisfaire ses clients, notamment à travers un forum et un dispositif de règlement des litiges (dont on ne sait malheureusement rien). Une telle organisation nécessitait beaucoup de travail et, *de facto*, du personnel : Ulbricht a donc dû engager plusieurs personnes pour des salaires conséquents. Par exemple, ChronicPain (Bearman, 2015), un ancien bénévole qui modérait le forum (et donnait des conseils gratuits sur l'utilisation des drogues), a été embauché pour s'occuper du service client, de la réinitialisation des mots de passe, de la résolution des litiges des consommateurs, etc. Le personnel interagissait par le biais d'un forum spécial anonymisé ; mais si Ulbricht savait tout sur les membres de son personnel, ce n'était en aucun cas réciproque. Cela a compliqué l'organisation du travail et l'exécution des règles, d'autant plus que le développement des concurrents a conduit SR à se rendre plus visible sur le marché. La presse (notamment Chen, 2011, largement cité) a joué un rôle important dans la popularisation du site, de sorte que divers commentateurs établissent un lien entre les articles liés à SR et la première forte croissance du bitcoin en juin 2011.

La gestion de ce commerce florissant a conduit Ulbricht à gagner lui aussi en visibilité ; il s'est adressé aux journalistes, a joué un rôle plus actif dans les forums et a remplacé son pseudonyme « Admin » par un autre plus fortement identifiant, DPR (acronyme de Dread Pirate Robert) : « Au fil du temps, l'administrateur est devenu une voix importante, le théoricien du site et le défenseur

de la liberté individuelle » (Bearman, 2015). Selon la plainte du FBI et les articles de presse, le modèle de gouvernance de SR semble classique : pyramidal, pour ne pas dire autocratique. DPR embauchait, fixait les règles, touchait des commissions, animait le forum du personnel, s'exprimait dans la presse et sur les forums. Cependant, comme cela a été dit à plusieurs reprises sur le forum, ses compétences techniques étaient limitées et avec toute probabilité, il n'était pas en mesure de mettre en place tout seul tous les aspects du dispositif. La supposée communauté d'utilisateurs, mise en avant par SR, était peu visible et ne s'est pas manifestée, si ce n'est par une vague de protestation sur les forums lors de la fermeture du site. Tous ces dispositifs étaient en fait sous le contrôle d'un despote exclusif (et guère bienveillant), Ulbricht, mais ils ont donné lieu à l'intervention de divers autres acteurs. L'action publique de la police et de la justice a contribué à définir l'organisation du dispositif, en le « forçant » à formaliser et à transformer ses règles (afin de mieux fonctionner) et à modifier son organisation. Par exemple, pour mieux protéger les acheteurs ou les vendeurs du FBI, ou pour assurer la qualité et la sécurité des transactions, SR a dû renforcer sa sécurité et multiplier les pare-feux. En outre, l'ethos collectif des participants a évolué, comme on peut le voir dans les interventions des responsables de SR dans la presse ou sur le forum Bitcoin : elle a conduit Ulbricht à assumer publiquement et profondément sa position libertaire, jusqu'à l'extrême (il semble qu'il ait cherché à maintenir son autorité à tout prix, même en suggérant un meurtre à gages ; Greenberg, 2015).

L'affaire Bitcoin-Silk Road contribue, dans l'ensemble, à montrer que la gouvernance de Bitcoin résulte d'un écosystème complexe d'acteurs et de dispositifs techniques qui, dans une perspective dynamique, fixent le rôle et la responsabilité de chacun, configurent l'exécution des transactions, modifient le fonctionnement du site et ses conditions d'utilisation. Outre les pouvoirs publics, divers intermédiaires, impliqués dans les aspects bancaires ou sécuritaires, mais aussi dans la consommation ou les usages, ont également contribué, comme nous l'avons vu, à façonner les échanges et les transactions. Enfin, le rôle central d'Ulbricht cache très probablement une organisation de la gouvernance plus complexe. Par la suite, le site a été temporairement remis en ligne sous la forme de deux avatars successifs, montrant que son existence pouvait survivre à « Dread Pirate Robert ».

5.4. La blockchain et son écosystème comme « gouvernance par l'infrastructure »

Afin d'observer la « fabrique » de la gouvernance de Bitcoin, ce chapitre a cherché à examiner comment les dynamiques structurantes de la gouvernance, telles que l'action collective et le consensus, sont co-construites et mises en lumière par des controverses telles que la modification d'une fonctionnalité technique ou l'introduction ou la suppression d'un intermédiaire ; dans le même ordre d'idées, nous avons observé comment la responsabilité et l'autorité sont créées et redistribuées entre les différents acteurs du système. L'expérience très actuelle, et pourtant déjà « historique », de Bitcoin nous permet ici quelques réflexions ultérieures sur le façonnage de la « gouvernance par l'infrastructure », cette fois au sein d'une des technologies décentralisées « à succès » et le plus controversées des dernières années, la blockchain.

Tout d'abord, les trois cas montrent qu'il est nécessaire de nuancer davantage le point « gouvernance technique vs. gouvernance par la communauté » qui a pu être soulevé par certaines études antérieures de Bitcoin et d'autres logiciels. Dans certains cas, nous avons pu observer des intermédiaires qui font partie intégrante de l'infrastructure : leur « puissance d'agir » supplante la blockchain en tant qu'arrangement technique « central » du système. En outre, derrière le protocole « purement technique » de la blockchain, les développeurs apparaissent, dans toute leur variété de rôles et d'activités pour maintenir et développer le code, ce qui permet, en suivant Simone (2004), d'étendre la conception de la notion d'infrastructure jusqu'aux activités et aux collaborations des personnes qui s'en sentent concernées. L'action de ces développeurs vis-à-vis de leur objet rappelle d'autres formes de gouvernance bien connues, celles des communautés open-source, comme l'ont montré De Filippi et Loveluck (2016) dans le cas plus récent de la controverse sur le Bitcoin XT. Cependant dans cette situation, nous voyons les développeurs impliqués dans le processus même du « soin de la blockchain ». Des événements tels que le *fork* involontaire offrent l'opportunité d'étudier comment une crise de l'ordre numérique est confrontée et résolue au sein d'une infrastructure distribuée, et d'identifier les mécanismes de gouvernance dans la réparation d'une « chose », la blockchain, qui présente des formes très particulières de vulnérabilité ; avec les tentatives de rétablissement de l'ordre suite au fork, les développeurs et acteurs de Bitcoin cherchent à « réparer la crédibilité » (pour emprunter l'expression de Sims & Henke, 2012) de Bitcoin et de la blockchain qui le sous-tend. Plus généralement, ce cas montre

que les mises à jour techniques, même les plus routinières, impliquées dans la maintenance (voir Denis et Pontille, 2012) d'une infrastructure distribuée sont « lourdes de gouvernance », en tant que processus dynamiques qui restaurent l'uniformité, la continuité, la connectivité entre les différents composants d'un système – mais aussi hiérarchisent les décisions, gèrent les conflits, s'alignent sur les normes, permettent d'éliminer les contrevenants et les maillons faibles, etc. Dans des grands ou petits gestes de soin des infrastructures, on a de la gouvernance, comme l'a bien démontré Barnes (2017) dans le contexte, seulement en apparence très différent, de l'infrastructure d'irrigation en Égypte. Les mises à jour logicielles deviennent des régulateurs des incohérences techniques – et en même temps, les conditions de succès d'une mise à jour dépendent de l'asymétrie de pouvoir inscrite dans un réseau complexe d'acteurs.

En effet, ces épisodes controversés révèlent également un certain nombre de « micro-hiérarchies » entre les développeurs, et entre les développeurs et les intermédiaires : d'une part, nous observons des situations où les intermédiaires sont sollicités par les développeurs pour aider à résoudre des problèmes ; d'autre part, certains développeurs – même parmi les développeurs reconnus comme centraux et pionniers – sont clairement « plus centraux et pionniers » que d'autres. Cela nous amène à des questions inédites concernant la distribution de l'autorité dans le système, et interroge les « points de contrôle » (DeNardis, 2014) dans un système basé sur la *blockchain*. Cela remet aussi une fois de plus en question le « manifeste de décentralisation » qui sous-tendait initialement Bitcoin, confronté à de multiples réalités de goulots d'étranglement et de tensions. Les deux aspects ramènent en force la matérialité de la *blockchain* : là où le discours idéologique/technique contribue à l'invisibilité de l'infrastructure qui « assemble » la *blockchain*, les points de contrôle et les tensions la dévoilent, en montrant la multitude d'entités et de sous-entités qui la composent et qui doivent atteindre une sorte d'alignement pour que la *blockchain* puisse continuer à exister comme une entité cohérente.

Les trois cas permettent également de nuancer la notion d' « utilisateurs » au sens large, que l'on serait tenté, par défaut, de catégoriser comme « tous ceux qui ne minent pas ». On voit comment, parfois, ils ne sont pas directement en scène, mais la représentation d'une entité mobilisée par des développeurs qui tentent d'anticiper leurs demandes ou leurs besoins, selon ce qui se reflète dans

la presse, ou sur les forums, et autres supports de conversation et de débat. Cependant, ces controverses révèlent une importante gamme de rôles pour les utilisateurs ; il y a bien sûr d'un côté les « utilisateurs lambda », ceux qui se fient entièrement aux intermédiaires, et de l'autre côté les mineurs qui, dans certains cas, ne peuvent plus être considérés comme des utilisateurs au sens traditionnel du terme, mais deviennent une puissance avec laquelle il faut compter, un « point de passage » obligatoire dans le réseau. Mais le plus intéressant du point de vue de la gouvernance, ce sont toutes les figures intermédiaires, des « utilisateurs/enseignants » qui interviennent sur les forums pour effectuer de la pédagogie sur des aspects spécifiques, aux utilisateurs qui « testent » le système dans les moments de crise, non pas pour leur avantage personnel mais pour l'améliorer.

Cette notion de « testeur » peut d'ailleurs elle-même être étendue au-delà des aspects techniques : les journalistes spécialisés « testent » pour mieux comprendre et expliquer, et la police, de son côté, explore les architectures de manière extrêmement attentive, en sondant leurs frontières et leurs limites. Comme dans d'autres projets open source, des formats de contribution extrêmement variés et spécifiques apparaissent : acteurs confrontés à une bifurcation involontaire, acteurs défiant les dispositifs de « sécurité » intégrés, acteurs-évangélistes. Dans ce continuum, on peut peut-être poursuivre dans l'identification de deux idéaux-types : d'un côté, le profil de l'utilisateur « passif » (s'appuyant sur un intermédiaire, mais ayant néanmoins besoin d'acquérir certaines compétences spécifiques, participant ainsi au travail de création et de diffusion de l'information) ; de l'autre, les figures quasi-mythiques du « premier utilisateur », comme Satoshi Nakamoto, dont l'existence même en tant que personne est douteuse mais qui alimente toutes sortes d' « histoires fondatrices » de Bitcoin, de l'utopie décentralisée aux moins savoureuses, comme l'existence d'une pyramide de Ponzi. Toutes ces figures et leurs manières de bricoler l'infrastructure Bitcoin ajoutent à la complexité de sa gouvernance, en contribuant à établir certains nœuds et goulets d'étranglement sujets à des vulnérabilités et controverses.

Enfin, notre étude fournit des exemples de dynamiques structurantes de la gouvernance en jeu dans le fonctionnement et la maintenance des échanges de bitcoins. Dans les trois cas, la discussion sur les forums en ligne peut jouer un rôle primordial à un moment donné dans la résolution d'une controverse, par exemple dans l'identification des mécanismes de sécurisation des échanges sur la

plateforme Silk Road, dans la détection d'une défaillance de service sur MtGox, ou dans la communication avec l'ensemble des acteurs impliqués dans la gestion de l'incident du fork. L'intervention des pouvoirs publics peut également jouer un rôle structurant dans la délimitation de la controverse : dans l'affaire Silk Road comme dans celle de MtGox, elle a contribué à dessiner la chaîne de responsabilité, à attribuer la responsabilité aux acteurs impliqués et à éliminer des acteurs spécifiques afin de circonscrire une arène plus légitime pour Bitcoin. L'action collective et le consensus sont également des mécanismes nécessaires à l'ordonnancement et à la maintenance de la *blockchain*. Dans l'épisode du fork involontaire par exemple, ces mécanismes ont été mobilisés pour sécuriser un accord avec des acteurs tels que les pools miniers, qui avaient manifestement une position dominante dans la configuration socio-technique en jeu – nonobstant la capacité supposée de la crypto-monnaie à défier les schémas hiérarchiques de pouvoir.

Avec ce chapitre, j'ai montré comment dans une infrastructure distribuée telle que Bitcoin, plusieurs points de vulnérabilité technique et organisationnelle du système ont pris forme comme lieux de redistribution et reconfigurations du pouvoir et de l'autorité, contribuant à forger la « gouvernance par l'infrastructure » de Bitcoin. Les cas d'étude détaillés dans ce chapitre suggèrent, entre autres, que la pratique de la gouvernance peut s'inventer au-delà de la régulation et du contrôle au sens strict ; le chapitre suivant explorera cet aspect plus en détail, en montrant comment ces pratiques « informelles » de la gouvernance peuvent parfois se substituer à des processus établis et consolidés de standardisation.

Chapitre 6. Signal, ou comment « quasi-standardiser par le code » un protocole de messagerie sécurisée

Ce chapitre présente un cas d'étude centré sur Signal, une des technologies de messagerie sécurisée et chiffrée de bout en bout les plus répandues à ce jour[54]. Ce système se compose d'un protocole de communication appelé Signal, d'une application « officielle » partageant le même nom, ainsi que d'autres applications qui adaptent le protocole Signal à leurs besoins et publics. Il évolue au sein d'un secteur, la messagerie chiffrée, qui est actuellement – notamment depuis les révélations d'Edward Snowden – très foisonnant et varié en termes d'arrangements d'architecture technique, organisation des processus de développement, et modèles d'affaires. Pour les acteurs dans le secteur de la messagerie sécurisée, se pose donc la question de comment le standardiser et/ou structurer. Le chapitre montre un cas de « gouvernance par l'infrastructure » qui a trait à cette standardisation : comment le protocole Signal est progressivement devenu un « standard informel » dans le secteur suite à un ensemble de pratiques informelles et controverses autour de son implémentation, et plus largement sa reconnaissance dans la pratique comme « quelque chose qui marche ». Il s'agit d'un travail mené en collaboration avec Ksenia Ermoshina entre 2016 et 2018.

Avec les révélations Snowden, le chiffrement des communications à grande échelle et de manière utilisable est rapidement devenu un sujet de préoccupation publique ; un nouvel imaginaire cryptographique s'installe, qui considère le chiffrement comme une condition préalable nécessaire à la formation de publics en réseau (Myers West, 2018). Parallèlement à la transformation du chiffrement en une question politique à part entière, les révélations Snowden ont catalysé des débats de longue date dans le domaine des protocoles de messagerie sécurisée. La communauté de la cryptographie (en particulier, les collectifs universitaires et de logiciels libres) a renouvelé ses efforts pour créer des protocoles de messagerie sécurisée de nouvelle génération afin de surmonter

[54] Suite à des déclarations fortement médiatisées telles que celle d'Elon Musk en début d'année 2021 (https://www.20minutes.fr/economie/2950683-20210112-use-signal-tweet-elon-musk-fait-bondir-vouloir-action-autre-entreprise) Signal a encore connu une forte augmentation de ses utilisateurs depuis que cette enquête a eu lieu.

les limites des protocoles existants, tels que PGP (Pretty Good Privacy) et OTR (Off-the-Record Messaging).

L'une des principales motivations derrière cet effort consistait à faciliter les processus d'échange et de vérification des clés[55], précédemment identifiés comme les principaux obstacles à l'adoption massive du chiffrement dans les outils de communication (Whitten & Tygar, 1999). Le plus avancé et le plus populaire de ces protocoles de nouvelle génération est actuellement le protocole Signal (anciennement appelé Axolotl), d'abord introduit par l'application de messagerie qui partage le même nom, puis adopté ou bifurqué par d'autres applications de messagerie instantanée, allant de WhatsApp et Wire à Matrix et Conversations. Bien que le protocole Signal soit largement adopté et considéré comme une amélioration par rapport à OTR et PGP, il reste officiellement non normalisé, même s'il existe un projet informel élaboré dans ce but par les créateurs du protocole, Trevor Perrin et Moxie Marlinspike.

L'introduction et l'adoption rapide de ce protocole, et les transformations subséquentes de l'écosystème de la messagerie chiffrée constituent un cas d'étude intéressant pour analyser en pratique la « gouvernance par l'infrastructure ». Comment s'opère une « normalisation de fait » dans le domaine de la messagerie sécurisée ? Que peut-on apprendre sur les modes de gouvernance existants en matière de chiffrement et sur l'histoire des organismes de normalisation traditionnels, en analysant l'approche de « normalisation par le *running code* » adoptée par Signal ? Le cas du protocole Signal dévoile une histoire de la messagerie sécurisée où les protocoles s'influencent mutuellement, s'empruntent les uns aux autres, et tentent même de revenir à leurs prédécesseurs et de les renouveler à la lumière des nouvelles normes et exigences mises en avant par Signal, telles que le *forward secrecy*[56], aujourd'hui devenue une caractéristique fondamentale pour les messageries sécurisées.

[55] Dans le domaine de la cryptographie à clé publique, l'échange de clés est la méthode par laquelle les clés cryptographiques sont échangées entre deux parties ; la vérification des clés est tout moyen permettant de faire correspondre une clé à une personne, en s'assurant que c'est bien cette personne qui utilise la clé (voir par exemple https://ssd.eff.org/en/glossary/key-verification).

[56] Le *forward* ou *future secrecy* (« secret futur ») est une fonction qui garantit que les clés de session d'un utilisateur ne seront pas compromises, même si la clé privée du serveur est compromise, et, en particulier, elle est destinée à protéger les sessions passées contre les compromissions futures des clés secrètes ou des mots de passe.

6.1. Chiffrer nos communications, un problème toujours plus « socio-politique »

Depuis les révélations Snowden, les communications chiffrées font l'objet d'un vaste débat public, parallèlement aux objectifs de confidentialité et de sécurité qu'elles cherchent à renforcer[57]. Les sciences sociales, en particulier les STS, relèvent le défi d'étudier en profondeur comment les outils de messagerie chiffrée sont conçus et développés, comment ils sont adoptés par différents profils d'utilisateurs – parfois de manière involontaire ou imprévue –, comment ils inspirent et sont inspirés par différents imaginaires, et finalement deviennent instruments et cibles de gouvernance.

On peut dire que l'anthropologue Gabriella Coleman a ouvert la voie aux chercheurs qui se consacrent à explorer la mesure dans laquelle le développement technique des applications et des protocoles, et l'ensemble des choix impliqués dans ce développement, contribuent de manière critique à donner un sens aux libertés numériques, à la manière dont elles devraient être préservées et à l'identité de leurs adversaires. Elle a, en particulier, examiné le rôle de la culture des hackers, en explorant ce que les hackers entendent par liberté et comment ils la mettent en œuvre, comme une forme d'autodétermination qui considère le libre accès à la connaissance comme une condition préalable nécessaire à l'évolution de leur « art technique » (Coleman, 2005). En outre, le travail de Coleman est particulièrement pertinent pour une étude du chiffrement basée sur les sciences sociales, car avec Alex Golub, elle a défini la « crypto-liberté » comme une forme particulière de pratique des hackers, fondée sur la conviction que cette liberté devrait principalement être préservée et encouragée sur Internet par le développement et l'utilisation de la technologie de chiffrement (Coleman & Golub, 2008).

Comme Sarah Myers West (2018) l'a récemment affirmé, le chiffrement est une question d'imaginaires concurrents. Les gens pensent au chiffrement à travers des codes (qui transposent les lettres d'un alphabet et/ou remplacent les mots) dans différents contextes sociaux, culturels et politiques. Le chiffrement a notamment construit ses différentes significations, comme elle le note, tant dans le domaine de la sécurité nationale et du secret que dans celui des systèmes

[57] Cette section reprend des éléments de l'introduction de l'ouvrage *Concealing for Freedom* (Ermoshina & Musiani, 2022).

démocratiques, où il permet la communication privée et permet d'éviter la surveillance et les sanctions sociales ou politiques potentielles. L'enquête de Myers West sur l'imaginaire du chiffrement illustre comment des technologies similaires peuvent acquérir des significations et des rôles différents dans des contextes culturels différents, d'autant plus qu'elles doivent être comprises non seulement dans un sens technique, mais aussi dans les contextes sociaux, culturels et politiques spécifiques dans lesquels elles sont utilisées. Les conclusions de Myers West sont importantes pour souligner, comme ce chapitre en fournira des exemples, que les technologies (et les technologues) ne déterminent pas de solutions universelles lorsqu'il s'agit du rôle et de l'impact du chiffrement, et que les contextes socioculturels d'utilisation sont primordiaux.

Fondant son travail sur la théorie du discours, mais faisant preuve d'une sensibilité STS indéniable en considérant le discours comme un processus contextuel, structurant et performatif de construction du sens, Isadora Hellegren (2017) souligne que le chiffrement est aussi une question d'histoire et de périodisation. La signification à multiples facettes du chiffrement évolue non seulement à travers les communautés de développeurs et d'utilisateurs, mais a également évolué au fil du temps. Comprendre comment divers acteurs ont construit des compréhensions spécifiques de la liberté en ce qui concerne des technologies comme le chiffrement est important pour les historiens de l'Internet, les hackers, les programmeurs et les décideurs politiques, car tous ces acteurs sont impliqués dans la construction de la forme, de la fonction et de la signification de la liberté sur Internet, en particulier lorsqu'il s'agit de sa relation avec l'État.

Bien que son objectif principal ne soit pas de comprendre la fabrication du chiffrement pour un usage spécifique, mais plutôt les discours sur le chiffrement dans son ensemble tels qu'ils se déploient dans les arènes politiques traditionnelles et moins traditionnelles, le récent *Crypto-Politics* (2019) de Linda Monsees est une contribution importante au développement d'une perspective de sciences sociales sur le chiffrement. Monsees utilise des méthodes d'analyse du discours pour examiner les débats post-Snowden liés au cryptage, tant aux États-Unis qu'en Allemagne, et décrit le paysage des discussions médiatiques et spécialisées sur le chiffrement comme le résultat de multiples sphères publiques et cercles d'experts, enchâssés dans des questions plus larges sur Internet et la société, telles que le contrôle des médias en réseau, surveillance et la protection des données personnelles, et tentant de donner un sens à la « sécurité diffuse »

d'aujourd'hui – un contexte où « les pratiques de sécurité dispersent les multiples insécurités et images de menaces plutôt que de les intensifier et de créer ainsi un état d'urgence » (Huysmans, 2014 : 87-88 dans Monsees, 2019 : 5). Monsees développe la notion de « publicité » (*publicness*) pour transmettre l'idée que les controverses politiques sur le chiffrement sont souvent situées en dehors des institutions politiques établies (bien que celles qui se déroulent dans des arènes politiques plus traditionnelles ne doivent pas être négligées). Dans le prolongement de travaux STS antérieurs sur le rôle performatif des controverses portant sur des phénomènes socio-techniques complexes et ouverts, elle conclut que « les controverses sur le chiffrement impliquent des idées spécifiques liées non seulement à la signification de la 'sécurité', mais aussi à la manière dont ces conceptions reposent sur des idées spécifiques concernant la citoyenneté, l'État et la vie privée » (2019 : 10), faisant écho à la perspective de Hellegren.

Plusieurs auteurs ont par ailleurs, au milieu et à la fin des années 2010, abordé la question de savoir ce que signifie être en ligne en tant qu'individu, citoyen et consommateur dans un monde qui est désormais largement conscient de l'ampleur de la surveillance dont nous faisons l'objet, et se sont concentrés, dans le cadre de cette question plus large, sur le rôle joué par le développement technique des architectures et des infrastructures de communication en ligne.

Comme l'explorent les travaux de Stefania Milan et de ses collègues (par exemple, Milan & van der Velden, 2018), nous sommes témoins d'une variété croissante de pratiques d' « activisme des données », c'est-à-dire d'un ensemble de tactiques, de résistances et de mobilisations socio-techniques qui adoptent une approche critique à l'égard de la datafication, de la collecte massive de données et de la surveillance omniprésente. L'activisme des données, tel que Milan le conceptualise, peut être compris comme une évolution contemporaine de phénomènes tels que ceux analysés par Coleman, ainsi que par Milan elle-même dans des travaux antérieurs (par exemple, 2013), comme l'activisme technologique radical et l'hacktivisme. L'activisme des données est censé représenter la « prochaine étape » de ces formes d'activisme pour le numérique et par le numérique, dans la mesure où il « s'engage explicitement dans les nouvelles formes [que] l'information et la connaissance prennent aujourd'hui, ainsi que dans leurs modes de production, remettant en question les conceptions dominantes de la datafication » (Milan & van der Velden, 2018). L'activisme des données, vu que la datafication et les utilisations des TIC à des fins

politiques différentes sont si répandues et omniprésentes, pourrait progressivement acquérir un attrait pour des communautés plus diverses de citoyens concernés, au-delà des exemples précédents d'engagement militant technologique qui semblaient (auto-)limités à la niche des experts et des technologues (ibid., 2018) ; une préoccupation largement discutée dans un certain nombre de projets de chiffrement les plus récents, y compris celui que nous analyserons plus en détail ici.

En lien avec ces travaux, le prisme conceptuel de la « justice des données » a été récemment proposé par Arne Hintz, Lina Dencik et Karin Wahl-Jorgensen (2019) pour illustrer que non seulement la citoyenneté et la possibilité d'agir citoyen dans l'Internet d'aujourd'hui sont profondément façonnées par des phénomènes tels que la collecte massive de données et la marchandisation, mais aussi que les droits et les pratiques des utilisateurs concernant la vie privée et la surveillance en ligne sont aujourd'hui conçus en termes hautement individualisés. Cela engendre ou maintient davantage un contexte d'inégalité, car, selon ces auteurs, cela transfère la responsabilité « d'engager et de négocier la citoyenneté à l'ère numérique sur les individus » (Gangneux, 2019). Comme l'illustrera notre étude de cas sur Signal, cette question est importante en ce qui concerne les technologies de cryptage et son adoption massive, car le public cible des applications de messagerie sécurisée, en particulier celles nées après Snowden, est loin de se limiter aux groupes de technophiles et d'activistes ; plusieurs projets visent une utilisation généralisée. Une majorité de la communauté technique de la cryptographie considère le confort d'utilisation comme le principal problème qui se dresse entre le souhait d'une adoption à grande échelle et sa réalisation dans la pratique ; cependant, ce positionnement a été contesté par certains chercheurs comme une « responsabilisation forcée » des utilisateurs au détriment du développement de stratégies collectives résilientes de sécurité numérique (Kazansky, 2015) et comme une « délégation » des questions techniques aux « *techies* progressistes », malgré un désir sociétal répandu de développer des technologies pour la justice sociale (Aouragh et al., 2015).

De plus, les technologies de chiffrement des communications en ligne sont en train de devenir l'un des principaux sites centraux de « gouvernance par l'architecture », riche en controverses qui concernent tour à tour leur développement, leur mise en œuvre, leur appropriation (parfois surprenante) par les utilisateurs, et les tentatives de régulation. En 2012, Jean-François Blanchette

montrait dans *Burdens of Proof* comment le chiffrement était en passe de devenir le nouveau « régime de preuve » d'un État de plus en plus numérisé, entraînant des négociations et des débats acérés sur ce que signifie apporter un témoignage fiable, identifier et mettre en œuvre les responsabilités, ou encore constituer la mémoire[58] (Blanchette, 2012 : 4). Suite aux révélations Snowden et à l'élargissement des débats liés à la surveillance de masse, des travaux interdisciplinaires en sciences de la communication et en sciences politiques ont récemment souligné que l'année 2013 n'a pas seulement révélé la nécessité d'une nouvelle réforme juridique des systèmes de renseignement et de surveillance, mais a mis en évidence « une variété de pratiques, de politiques et de discours changeants qui peuvent [...] être liés aux contestations post-Snowden » (Pohle & Van Audenhove, 2017 : 2-3). Un certain nombre de controverses socio-techniques peuvent être identifiées comme y étant liées : un exemple notable a été la controverse entre le FBI et Apple en 2015 et 2016, lorsque Apple Inc. a reçu de la part de tribunaux de district aux États-Unis plusieurs injonctions d'aider des enquêtes criminelles en cours en extrayant des données depuis des iPhones dotés de protections de sécurité cryptographiques pointues, qu'Apple elle-même ne pouvait pas briser à moins que de nouveaux logiciels spécifiques soient écrits pour que les autorités puissent contourner de telles barrières. Ce débat a notamment posé la question de savoir si, et si oui dans quelle mesure, les autorités judiciaires ou gouvernementales pouvaient contraindre les fabricants techniques à fournir une assistance pour déverrouiller des appareils protégés par des systèmes de cryptage (voir également Schulze, 2017). Des controverses telles que celle-ci ont contribué à dévoiler des facettes de l'expérience du chiffrement dans l'Internet d'aujourd'hui, et suggèrent que les questions les plus pressantes de notre époque liées au chiffrement pourraient être sociales, en plus d'être juridiques et techniques.

6.2. Messageries chiffrées : un secteur foisonnant et fragmenté

Pré-existante aux révélations Snowden, mais fortement reconfigurée par elles, la messagerie sécurisée est un écosystème de projets vivace et en constante évolution[59]. Les développeurs cherchent notamment à appliquer la technique du chiffrement de bout en bout aux systèmes de

[58] Le cas d'étude de Blanchette est par ailleurs le chiffrement/la cryptographie dans la signature numérique (et ses écueils), un contexte sensiblement différent de celui sur lequel se concentrera ce chapitre.
[59] Cette section reprend des éléments de Ermoshina, Halpin & Musiani (2016).

messagerie : parmi les outils les plus connus appartenant à cette catégorie figurent Signal, Telegram et WhatsApp, chacun ayant des motivations et des solutions différentes pour mettre en œuvre le chiffrement.

Un récent document de systématisation des connaissances sur la messagerie sécurisée affirme que le domaine a souffert de « l'absence d'un vainqueur clair dans la course au déploiement généralisé [des communications chiffrées] et de la persistance de nombreux problèmes de recherche [en informatique] non résolus », ainsi que de divergences entre les « revendications grandioses » et la sécurité réellement fournie (Unger et al., 2015). La diversité et la complexité du domaine s'expliquent en partie par la durée de vie relativement courte de plusieurs projets, pour un certain nombre de raisons, notamment des expérimentations techniques et universitaires qui n'ont pas donné les résultats escomptés ou attendus, l'incapacité à développer des modèles économiques durables, la gouvernance interne et l'incapacité à rallier une masse critique d'utilisateurs autour des applications de communication sécurisée, souvent en raison d'un manque de facilité d'utilisation. Comme on l'a mentionné, le public cible de ces applications, surtout celles nées post-Snowden, est de plus en plus fréquemment l'internaute lambda, plutôt que des publics hautement spécialisés. Dans les arènes politiques, les outils de messagerie chiffrée de bout en bout font l'objet d'un discours à double facette, sur l'autonomisation et la protection des libertés civiles fondamentales d'une part, et les allégations de liens avec le terrorisme d'autre part, ces dernières étant alimentées également par des récits antérieurs sur les technologies décentralisées et le peer-to-peer en tant qu'architectures favorisant à la fois l'autonomisation et les pratiques illégales (Musiani, 2013).

En effet, après les révélations Snowden, plusieurs entreprises, en particulier celles basées aux États-Unis, ont mis en œuvre un certain nombre de réponses organisationnelles et techniques basées sur la cryptographie, visant à restaurer la confiance des utilisateurs dans leurs services basés sur le cloud. Cette dynamique a été identifiée comme un « tournant cryptographique » ouvrant de nouveaux enjeux et questions d'un point de vue juridique et politique (Rubinstein & Van Hoboken, 2014), et est considérée comme une nouvelle phase des *Crypto Wars* des années 1990 (Froomkin & McLaughlin, 2016), où les caractéristiques cryptographiques de divers types de protocoles tiennent le rôle de micro-instruments de gouvernance car elles déterminent, à un niveau technique,

les limites et les possibilités de collaboration avec les acteurs gouvernementaux et privés. Par exemple, le chiffrement côté serveur n'offre pas les mêmes conditions que le chiffrement de bout en bout dans le cas où un « déchiffrement forcé » est exigé par les procédures d'application du droit. Les propriétés cryptographiques telles que le secret de transmission ou la non-répudiation, ainsi que la gestion des clés, définissent techniquement les termes et conditions des interactions et des échanges de données possibles avec des acteurs tiers, issus des secteurs privé et public.

Dans ce contexte, de nombreux acteurs du domaine partagent un accord tacite selon lequel le « *Double Ratchet* », le principe fondateur du protocole Signal, est actuellement le principal protocole de messagerie instantanée. Afin de mieux comprendre comment le protocole Signal interagit avec les développements antérieurs et ultérieurs des protocoles de chiffrement, il convient d'examiner les débats historiques autour de deux protocoles majeurs, qui ont en quelque sorte dominé l'écosystème pendant de nombreuses années avant Snowden : OTR (Off-the-Record, utilisé pour chiffrer les messages instantanés envoyés sur XMPP) et PGP (Pretty Good Privacy, utilisé pour chiffrer les e-mails).

Les principaux problèmes de PGP discutés dans la communauté cryptographique, dont les utilisateurs avancés sont également au courant, pourraient être résumés à deux aspects principaux : la gestion complexe des clés et l'absence de répudiation et de secret de transmission. La crise des « infrastructures à clé publique » et du concept même de clés et de signatures cryptographiques a également été soulignée par les communautés de formateurs en sécurité numérique et les ONG internationales qui promeuvent les technologies de protection de la vie privée, comme *Tactical Tech* et l'*Electronic Frontier Foundation* (voir Musiani & Ermoshina, 2017). Tout en offrant encore l'une des solutions les plus robustes sur le plan cryptographique, PGP est clairement confronté à des problèmes d'utilisabilité.

Le protocole OTR est né d'un projet de recherche à l'UC Berkeley en 2002 et a été publié pour la première fois en 2004. Le développeur d'OTR, Ian Goldberg, s'est décrit, lors de notre entretien avec lui, comme un utilisateur précoce de PGP et surtout comme un « spécialiste du courrier électronique » ; c'est son étudiant, Nikita Borisov, qui a attiré l'attention de Goldberg sur le domaine en pleine expansion des réseaux sociaux et de la messagerie instantanée, identifiant ainsi

une nouvelle faille de sécurité à combler. Dans sa description de la mission qui sous-tend OTR, Ian établit un lien entre ce protocole et les technologies préexistantes, comme un moyen de répondre aux défis qui n'étaient pas correctement traités par PGP :

> *Vos choix à l'époque étaient soit une communication complètement non protégée, ni chiffrée ni authentifiée, soit PGP, dans quel cas elle est confidentielle et authentifiée, sauf si votre clé est exposée, dans quel cas elle n'est pas confidentielle et l'authentification avec les signatures numériques conduit à la non-répudiation*[60].

Si la solution d'OTR, consistant à utiliser des clés spécifiques à chaque conversation, offrait une bonne répudiation et un bon secret de transmission, elle ne permettait pas le chiffrement des discussions de groupe, car, selon Goldberg, « c'est ainsi que fonctionnait la communication instantanée à l'époque : il fallait être en ligne au même moment » : La conception d'OTR s'inspirait de Aim et d'autres outils existants, qui nécessitaient une synchronisation. De plus, bien que populaires dans les communautés d'activistes à haut risque, les applications basées sur OTR (comme Jabber) ont été largement critiquées pour leur manque de support de multiples appareils à la fois, et pour d'autres problèmes d'utilisation.

Ces préoccupations communes ont été prises en compte par le protocole Signal, selon Goldberg : « Signal a essentiellement repris le protocole OTR et lui a ajouté des fonctionnalités de base pour le faire fonctionner dans un cadre asynchrone ». Utilisant une clé spécifique à chaque conversation, de manière similaire à OTR, il n'impose pas une gestion complexe des clés aux utilisateurs. Il a conservé les propriétés de répudiation et de secret de transmission, mais a ajouté la *forward secrecy* de sorte que les messages ne puissent être lus à aucun moment dans le futur dans le cas d'une compromission des clés (Cohn-Gordon et al., 2016). Signal a également résolu le problème de la messagerie asynchrone en autorisant des « pré-clés » à plus long terme gérées par le serveur Signal, et a proposé une messagerie de groupe mise en œuvre comme une messagerie point à point.

[60] Entretien avec Ian Goldberg, mai 2018.

Alors que le protocole Signal a entamé un dialogue avec la « tradition » des protocoles cryptographiques précédents (principalement en s'attaquant aux limites susmentionnées d'OTR et de PGP), il a rapidement attiré l'attention de la communauté cryptographique universitaire, et seules des failles mineures ont été constatées (Frosch et al., 2016). Bien que des approches alternatives aient été développées et largement déployées, comme le protocole MTProto que sous-tend l'application Telegram, ces protocoles ont développé leurs propres principes cryptographiques et ont donc reçu moins d'attention de la part de la communauté académique, bien qu'un certain nombre de bogues et de problèmes d'utilisation aient été révélés (Jakobsen et Orlandi, 2016 ; Abu-Salma et al., 2017). Il est intéressant de noter que si Signal a profondément influencé le domaine des protocoles cryptographiques, il ne s'est pas écarté des efforts précédents, mais s'est inspiré de leurs failles bien connues : c'est cette continuité qui peut expliquer en partie l'intérêt des experts en cryptographie.

Avec des variantes mineures mises en œuvre dans la très populaire messagerie WhatsApp, le noyau du protocole Signal semble en passe de remplacer clairement l'utilisation de XMPP+OTR et même de devenir une fonctionnalité compétitive pour les services de messagerie grand public (comme le montre l'adoption du protocole Signal comme option par Google Allo et Facebook Messenger). Des messageries chiffrées telles que WhatsApp, Telegram et Signal sont désormais les applications par défaut de ce type pour les utilisateurs qui se considèrent comme à haut risque. Or, des études d'utilisabilité ont montré que, bien que Signal (similaire à OTR) soit facile à configurer et à utiliser, même les utilisateurs très compétents ne parviennent pas à utiliser correctement la vérification. De plus, à l'heure actuelle, Signal est centralisé, car un seul serveur sous le contrôle de l'entreprise gère la configuration du protocole dans les déploiements les plus répandus (WhatsApp, Google Allo, Facebook Messenger, Wire).

Il existe des alternatives open-source qui prétendent utiliser le protocole Signal ou ses *forks*, comme l'application centralisée Wire, qui utilise une variation du protocole Axolotl appelé Proteus. Certaines parties du protocole Signal ont été copiées par un projet de standard de la fondation XMPP appelé OMEMO, dans le but d'être utilisées par des applications telles que Conversations et ChatSecure, ce qui a conduit à l'utilisation du « *Double Ratchet* » de Signal dans les projets fédérés. Un autre projet décentralisé appelé Matrix a réutilisé des parties du protocole

Signal pour les intégrer dans sa propre bibliothèque cryptographique appelée Olm. Bien que Signal semble être largement adopté et considéré comme une amélioration par rapport à OTR et PGP, le noyau du protocole Signal reste officiellement non standardisé[61], même si, comme on l'a anticipé plus haut, les créateurs du protocole, Trevor Perrin et Moxie Marlinspike, ont produit un projet de standard informel après une « pression communautaire » considérable [selon les mots du développeur principal de Matrix.org].

6.3. Un processus de « quasi-standardisation »

De nos entretiens, il résulte que les développeurs des protocoles de messagerie sécurisée sont très attachés aux standards, qu'ils considèrent comme « quelque chose sur lequel ils finiront par travailler », notamment pour accroître le « dialogue » entre les applications et réduire les effets de silo : « À long terme, je ne suis pas opposé à l'idée de la standardisation, c'est formidable d'avoir une référence pour l'interopérabilité » [développeur principal de Briar[62]]. La standardisation est considérée comme une référence et donc comme un instrument de communication ou de médiation important, qui aide la communauté travaillant à la sécurité des communications à se comprendre et à établir un socle de connaissances communes (comme les bibliothèques cryptographiques), et qui garantit également un développement plus fluide de nouvelles applications sur la base de protocoles normalisés.

Pourtant, les développeurs expriment un mécontentement généralisé à l'égard des organismes de normalisation existants, et ce pour plusieurs raisons. Les développeurs soulignent les transformations récentes de ces organisations, en se référant à un précédent « âge d'or » des organismes de normalisation, lorsque leur mode d'existence était plus proche de celui des communautés du logiciel libre. Nos répondants notent en particulier l'importance croissante des acteurs privés en tant que parties prenantes au sein des organismes de normalisation.

[61] La section suivante, qui explore cet aspect, est tirée de Ermoshina & Musiani (2019).
[62] Briar est une technologie de communication logicielle à code source ouvert, destinée à fournir des communications de type pair à pair, sans serveur centralisé et avec une dépendance minimale à l'égard d'une infrastructure externe. Les connexions se font par Bluetooth, WiFi ou sur Internet via Tor et toutes les communications privées sont cryptées de bout en bout (https://briarproject.org)

Mon impression de l'IETF est qu'il n'est plus la même bête qu'aux premiers jours. Il fut un temps où il s'agissait d'un groupe de personnes enthousiastes qui arrivaient à l'IETF avec une idée à moitié finie et qui disaient : 'Je veux que tout le monde soit au courant, mettons-la en forme et nous la développerons tous'. Je pense que c'est devenu un environnement beaucoup plus lent et plus contradictoire. Ce domaine a attiré plus d'argent et plus de participation des entreprises et donc, des conflits d'intérêt [développeur principal Briar].

Cette institutionnalisation des organismes de normalisation et leur éloignement progressif des communautés de développeurs et de codeurs créent un environnement moins propice aux expériences et aux projets inachevés :

Je pense que [un effacement automatisé et périodique de l'historique des messages] est quelque chose que nous allons mettre en œuvre, mais qui ne sera probablement pas standardisé parce que la communauté XMPP est très conservatrice. Je ne pense pas... qu'ils ne comprennent pas tout. C'est quelque chose que les utilisateurs veulent... alors pourquoi ?... Je ne sais pas. Ils se retrouvent dans ces trucs de la vieille école [développeur de ChatSecure].

Dans les mots de Callon (1986), la normalisation implique la « traduction » d'un protocole en tant qu'expérience sociotechnique en une pré-standard, capable d' « enrôler » et de convaincre divers agents au sein d'instances d'évaluation. La standardisation implique un travail collectif qui ouvre le « noyau dur » des auteurs de protocoles à des experts externes issus d'organismes de normalisation, dont certains sont éloignés des expériences et des besoins des utilisateurs, et de l'économie « réelle » du domaine des messageries chiffrées – un processus qui n'est guère attrayant pour certains développeurs, car il est considéré comme chronophage dans les premières phases de développement du projet :

Je ne penserais pas vraiment à soumettre quelque chose à l'IETF à un stade précoce ces jours-ci parce que je pense que cela impliquerait probablement beaucoup de travail pour convaincre d'autres personnes de permettre que cela devienne une norme... et évidemment, chacun aurait ses propres idées sur la meilleure façon de travailler [développeur principal Briar].

Au contraire, la plupart des développeurs partagent la philosophie selon laquelle ils construisent d'abord l'application, puis se concentrent sur la standardisation (et éventuellement la décentralisation) via l'utilisation de normes ouvertes :

> *J'ai travaillé avec le W3C il y a longtemps et je suis très conscient de la façon dont ils fonctionnent et du fait qu'ils peuvent avoir certaines limites. Nous voulons faire en sorte que Matrix soit suffisamment mature, solide et stable, puis nous pourrons le transmettre à une organisation de gouvernance appropriée, mais pour l'instant, il évolue encore très rapidement [développeur principal de Matrix.org]*

Dans le cas de la messagerie sécurisée, la vision prédominante est encore qu'il faut développer davantage le code et que la normalisation ne ferait que ralentir les efforts de développement existants. En fait, une nouvelle méthode de « quasi-standardisation » ou de « standardisation par l'exécution du code » est pratiquée dans le domaine des applications de messagerie chiffrée de bout en bout, autour du protocole Signal. Dans ce processus, une quasi-standardisation est définie comme « quelque chose qui fonctionne » et qui a été reconfiguré et redéployé par d'autres en testant ainsi sa validité. En ce sens, tous les déploiements du protocole Signal (par exemple Wire, WhatsApp et les applications basées sur OMEMO telles que Conversations et ChatSecure) fonctionnent comme des *crash-tests* de mise à l'épreuve pour le protocole, où le protocole est forgé par l'usage :

> *Je pense que la direction à prendre est toujours plus celle de Signal, lorsque vous construisez un système pendant un certain temps, vous reconfigurez un peu jusqu'à ce que vous pensiez avoir quelque chose qui fonctionne bien, puis vous commencez à le documenter et si d'autres personnes veulent contribuer à l'interopérabilité, vous leur parlez de la normalisation à ce stade, à un stade beaucoup plus avancé [...] Je me demande s'ils [Signal] vont penser à la normalisation à un moment donné, peut-être que l'idée est de la reporter à un stade ultérieur du projet, et non de l'éviter [développeur principal de Briar].*

Le protocole Signal est aujourd'hui considéré comme la meilleure pratique dans le domaine et devient une référence pour les autres projets en termes de confidentialité et de sécurité (par exemple, le *forward/future secrecy*). Les développeurs, même ceux qui travaillent dans des projets basés sur des architectures fédérées (par exemple Conversations) ou peer-to-peer (par exemple

Briar), considèrent *de facto* et par la pratique la solution Signal comme l'une des meilleures conceptions disponibles, même si elle n'est pas entièrement normalisée.

6.4. Une variété d'applications du protocole Signal

Le domaine des applications de messagerie instantanée a été profondément transformé par un certain nombre de mises en œuvre du protocole Signal, mais aussi par la popularité croissante d'autres outils de messagerie sécurisée, tels que Telegram, Threema ou Wickr, qui utilisent leurs propres protocoles. Le virage vers le chiffrement « de masse » a modifié le marché et entraîné des changements considérables au niveau de la gouvernance, engageant d'importants acteurs du secteur privé dans le jeu :

> *Ce qui se passe ces deux dernières années [2014-2016] est fantastique, avec un certain nombre de messageries qui apparaissent et aussi une plus grande publicité autour d'Axolotl ou de Signal... Snowden en parle aussi.... C'est donc quelque chose qui est vraiment bon pour l'industrie. Et nous avons vu que cela a déclenché même les grandes entreprises qui ont commencé à utiliser le chiffrement [développeur principal de Wire].*

L'un des *forks* les plus connus et les plus populaires du protocole Signal s'appelle Proteus et est utilisé par l'application Wire. Wire a été lancée par d'anciens développeurs de Skype, avec la volonté, selon son directeur technique, de répondre à « l'une des plus grandes lacunes existantes sur le marché, liée à la vie privée et à la sécurité ». Le principal groupe d'utilisateurs ciblé par Wire est identifié comme des consommateurs soucieux de leur vie privée :

> *Nos utilisateurs dans la première phase sont principalement des consommateurs, qui se soucient de la vie privée. Et nous espérons que de plus en plus de gens s'en soucient [...] J'aime comparer le tabagisme passif à la sensibilisation croissante à la vie privée, lorsque les gens comprennent comment les informations peuvent être utilisées à mauvais escient. C'est quelque chose qui doit être plus répandu, plus de gens doivent être conscients [directeur technique de Wire].*

Comme Wire ne s'adresse pas aux activistes ou à un public féru de technologie, mais à l'utilisateur lambda, l'une des principales préoccupations de ses développeurs était de construire une interface utilisable et d'intégrer de nouvelles fonctionnalités qui la distingueraient des autres messageries cryptées de bout en bout. Ainsi, Wire prend en charge les dessins, l'échange de GIF, les grandes discussions de groupe chiffrées de bout en bout, les appels vidéo de groupe à plusieurs participants, l'effacement des messages temporaires, le transfert de fichiers. Un certain nombre de nos interlocuteurs ont souligné l'aspect esthétique de l'interface utilisateur de Wire comme un avantage, favorisant l'adoption généralisée de Wire par rapport à Signal. Un autre argument de vente de Wire est la qualité et le chiffrement des appels vocaux, car il offre des appels vocaux cryptés de bout en bout en utilisant un protocole spécifique basé sur un codage à débit binaire constant.

6.3.1. La « quasi-standardisation » comme modèle d'affaires

Cependant, des difficultés et des tensions ont été observées autour des tentatives de Wire de réimplémenter le protocole Signal. Certaines de ces difficultés sont liées à l'absence de spécifications (documentation). Il n'existe en effet qu'un projet de spécification produit récemment, comme l'expliquent nos répondants, non sans la pression d'autres communautés de développeurs :

> *OWS [Open Whisper Systems, la société qui gère Signal] n'a pas donné la priorité à la normalisation [du protocole], à la fois parce que cela leur donnait la possibilité de le modifier et parce qu'il avait plus de valeur pour eux en tant que propriété intellectuelle. Cependant, ils viennent de terminer la normalisation d'une grande partie du protocole, [...] et je pense que, dans une certaine mesure, c'est à cause de la pression exercée par une communauté comme la nôtre [développeur principal de Matrix.org].*

Ainsi, ce manque de spécification oblige les développeurs à recoder à partir de zéro en utilisant parfois d'autres langages de programmation :

> *Le problème avec Axolotl était que si vous vouliez le construire complètement à partir des spécifications, il n'y avait pas, je dirais même volontairement, assez de documentation disponible. Mais si vous vouliez développer votre propre implémentation, vous étiez poussé ou intimidé pour avoir copié leur*

implémentation. [...] J'ai été très naïf et je suis allé voir Moxie l'année dernière en juin pour lui demander de revoir notre implémentation et de le payer très cher pour cela. Au lieu de cela, il a dit qu'on pouvait payer 1,5 million, qu'il nous aiderait à mettre en place l'implémentation. Ce qui s'est passé ensuite - il a dit qu'il allait nous poursuivre en justice […] Et puis ça s'est arrangé. Il a abandonné ses poursuites, nous avons abandonné les nôtres et nous utilisons Axolotl comme nous le faisons et comme nous le souhaitons [directeur technique de Wire]

L'un des développeurs de ChatSecure explique ce conflit comme la conséquence d'une politique de licence spécifique, qui a conduit à l'altération et à la modification des termes juridiques et des accords entre l'équipe Signal et les équipes cherchant à ré-implémenter le protocole Signal dans d'autres applications :

Le protocole Signal est une source ouverte sous licence GPL, ce qui signifie que vous ne pouvez pas l'intégrer dans un produit commercial ; c'est pourquoi OWS a obtenu de grands accords de licence de Facebook, Google et WhatsApp pour l'intégrer sans ouvrir l'ensemble de son code source. Une partie de ces accords concernait les incompatibilités avec la GPL et l'AppStore en particulier. Nous devions donc faire en sorte que certains termes juridiques soient exemptés [...] Moxie [développeur principal de Signal] a besoin de protéger ses revenus. Une partie de ses arguments avec Wire était qu'ils [Signal] n'avaient pas documenté le protocole Signal, donc il n'y avait pas de spécification ouverte, donc si vous vouliez écrire une réimplémentation compatible, vous auriez dû lire le code source, ce qui aurait créé une œuvre dérivée, qui ne vous aurait pas permis de l'utiliser commercialement parce qu'il aurait soutenu qu'il avait toujours le droit d'auteur de la majorité du travail [développeur de ChatSecure].

Les développeurs de Signal s'inquiètent de la compétence technique des développeurs tiers qui normalisent ou déploient des forks de leur protocole (« Moxie est un très bon codeur et ses standards sont très élevés », dit l'un d'entre eux) ainsi que de ne pas pouvoir mettre à jour le protocole assez rapidement en réponse aux recherches et aux bugs. Il est donc possible, pour l'équipe Signal, d'utiliser la non-standardisation du protocole comme partie intégrante de son modèle économique, où l'expertise et les spécifications nécessaires à un déploiement correct du protocole peuvent être offertes par l'équipe de Signal en tant que service :

Vous pouvez dire OK, nous allons concéder une licence pour cette technologie, ce qui ne m'intéresse pas, car j'aimerais qu'elle reste un logiciel libre. Mais vous pouvez aussi dire 'nous sommes les personnes qui comprennent cette technologie, il est logique de nous engager si vous voulez la déployer'. Si les gens construisent des systèmes au-dessus de cette technologie, ils paient quelqu'un [de l'équipe Signal] pour apporter des modifications à cette base de code [développeur principal de Briar].

Comme nous l'avons constaté lors de notre enquête auprès des utilisateurs de messageries sécurisées, et suite à l'observation de plusieurs formations sur la sécurité, les choix en matière d'open-source et de licence sont moins abordés dans les formations destinées aux utilisateurs à haut risque, car ceux-ci n'associent pas toujours l'open-source à la sécurité. L'open-source est souvent perçu comme un critère moins important dans le contexte d'une menace physique immédiate, car lorsqu'une solution propriétaire mais « efficace » et « facile à expliquer » existe, les formateurs lui donneront la priorité. Dans les contextes à haut risque avec des utilisateurs peu avertis, la tâche principale est de les aider à abandonner rapidement les outils non chiffrés ainsi que les outils développés par des acteurs dont la collaboration avec leurs adversaires est avérée. Cependant, une préoccupation importante pour les utilisateurs est celle des sources de financement et des modèles économiques des applications de messagerie chiffrée de bout en bout. C'était et c'est toujours le cas pour Signal également ; en particulier, les questions sur les modèles économiques étaient très fréquentes sur différents chats sur la cybersécurité que nous avons observé depuis septembre 2016. Les utilisateurs demandent de la transparence quant aux financements, mais montrent en même temps un certain scepticisme à l'égard des modèles de *crowdfunding* (dons) qui ne semblent pas assez durables pour qu'une application soit correctement maintenue.

Les critiques récentes adressées à Signal concernent leur dépendance au financement du gouvernement américain. Le site Surveillance Valley note par exemple :

Signal a été créé par les mêmes entités douteuses qui financent le projet Tor. L'argent provient principalement de l'organisme de capital-risque du gouvernement fédéral pour la liberté de l'Internet : Open Technology Fund, qui travaille en étroite collaboration avec le département d'État pour les changements de régime, et est financé par plusieurs reliques de la CIA ou de la

guerre froide – y compris Radio Free Asia et le Broadcasting Board of Governors[63].

La critique de Signal par le créateur de Telegram, Pavel Durov, va dans le même sens, remarquant qu'aucune application financée par le gouvernement américain n'est digne de confiance.

Plus largement, les applications centralisées de messagerie sécurisée chiffrée de bout en bout proposent différents modèles économiques, bien qu'il semble qu'aucune solution idéale n'ait encore été trouvée. Le projet de Wire consiste à proposer des services payants aux utilisateurs pour un espace de stockage supplémentaire (services de *cloud* chiffrés). Wire vise également à fournir des solutions commerciales pour le chiffrement de bout en bout de l'Internet des objets. Threema, l'une des rares applications chiffrées de bout en bout payantes, demande une contribution de deux dollars par utilisateur. Certains utilisateurs, notamment les membres de la *Privacy Week* et de la *Cryptoparty* autrichiennes (les deux principaux événements liés à la vie privée dans le pays), soulignent que c'est un avantage : « Nous utilisons tous Threema [...] Je préfère payer, au moins je suis sûr que je ne suis pas le produit » [Organisateur d'un *cryptoparty*, Autriche].

En conclusion, les choix de licence, les modèles commerciaux et la politique de l'open/close source s'avèrent être des processus socio-techniques complexes qui sont intégrés à la fois dans les interactions liées à la communauté, le contexte économique et les arrangements juridiques.

6.4. La gouvernance de la vie privée « par les protocoles » au temps du chiffrement de masse

Le protocole Signal a profondément influencé le domaine des protocoles cryptographiques en introduisant une combinaison de propriétés, telles que le *forward/future secrecy* et la non-répudiation, associées à une interface moderne, qui sont devenues un nouveau minimum requis pour une application de messagerie sécurisée, sans être un véritable standard formel. Comme le mentionne l'inventeur du protocole OMEMO, « si vous concevez un nouveau protocole de

[63] https://surveillancevalley.com/blog/government-backed-privacy-tools-are-not-going-to-protect-us-from-president-trump

chiffrement de bout en bout aujourd'hui, ou même il y a deux ans, pour la messagerie instantanée, le fait d'avoir le *forward secrecy* est simplement une bonne pratique. C'est ce que font également tous les autres systèmes de messagerie instantanée chiffrée. Signal le fait, WhatsApp le fait ».

À la lumière de l'histoire récente des communications sécurisées et des débats au sein de la communauté des développeurs, nous pouvons identifier un effet que l'on peut qualifier de « boucle de rétroaction » : stimulés par les innovations de Signal, les protocoles plus anciens ont été remis à neuf, et de nouvelles normes sont maintenant discutées dans le but d'apporter certaines de ces propriétés à une forme documentée et stabilisée.

Dans le domaine du chiffrement des e-mails, une nouvelle spécification a été proposée vers 2016, appelée Autocrypt, qui visait à faciliter la gestion des clés en plaçant les clés publiques dans les en-têtes des e-mails. Suivant la tendance consistant à mettre le chiffrement de bout en bout à la portée du grand public en déchargeant les utilisateurs de la responsabilité de la gestion des clés, Autocrypt vise à rajeunir le chiffrement des e-mails en rendant PGP plus accessible aux communautés non techniques. PGP a récemment fait son retour dans le domaine des communications instantanées, avec la croissance rapide du « chat par courrier électronique » ; par exemple, Delta.Chat, qui combine les spécifications de Signal avec celles d'Autocrypt et rPGP (une version optimisée de PGP permettant d'économiser de la mémoire).

Le protocole OTR a également été transformé et mis à jour sous l'influence de Signal : dans OTR v3, le problème de la compatibilité avec plusieurs appareils (ordinateur de bureau, tablette, mobile) a été résolu. Et la nouvelle version OTR v4, selon son auteur Ian Goldberg, comporte des fonctionnalités qui répondent spécifiquement aux lacunes de Signal.

D'autres normes ont été conçues, comme le protocole OMEMO, qui introduit l'asynchronie dans OTR et combine certaines des propriétés d'OTR et du protocole Signal, adapté pour être utilisé dans des systèmes de messagerie fédérés. Le succès de Signal a également attiré l'attention de la communauté cryptographique sur quelques problèmes non résolus dans plusieurs messageries chiffrées, tels que l'exposition des métadonnées, et d'autres questions liées à la nature centralisée de Signal et d'autres outils de messagerie instantanée populaires. Cela conduit à un certain

« renouveau » des systèmes fédérés et à la montée en puissance de solutions qui souhaitent mieux protéger les métadonnées des utilisateurs, de type mixnets ou peer-to-peer.

Enfin, un effort récent appelé MLS (pour *Messaging Layer Security*) a été lancé pour développer une norme offrant la confidentialité, l'intégrité et l'authentification des messages, et qui puisse également inclure l'asynchronie, le forward secrecy et l'évolutivité. MLS vise à offrir des possibilités de fédération entre divers protocoles de chiffrement pour l'établissement de clés, l'authentification et les services de confidentialité. MLS s'appuie sur les leçons tirées de plusieurs protocoles de sécurité antérieurs, tels que S/MIME, OpenPGP, Off the Record et Double Ratchet.

L'impact des processus de développement et de « quasi-standardisation » de Signal va au-delà d'un saut « linéaire » des protocoles anciens aux protocoles modernes. Le passage au chiffrement de masse a ébranlé la communauté de la messagerie sécurisée, suscité le renouvellement des protocoles et soulevé de nouveaux défis, dont beaucoup ne sont toujours pas résolus.

6.4.1. « Quasi-standardiser » dans un monde institutionnalisé

En analysant l'adoption de Signal en tant que « quasi-standard » ou norme *de facto*, ce chapitre a montré que, alors que le chiffrement devient une préoccupation publique beaucoup plus importante qu'il y a quelques années, plusieurs développeurs de messagerie chiffrée de bout en bout sont de plus en plus sceptiques quant aux arènes traditionnelles d'échange et de dialogue sur les standards en devenir, telles que l'IETF, la Fondation XMPP, le W3C ou le NIST, qu'ils considèrent comme moins efficaces (ou plus « compromises » avec des acteurs dominants qui brideraient l'innovation) qu'une approche basée sur le développement. Cela signifie-t-il que, en ce qui concerne l'adoption généralisée du chiffrement dans la messagerie sécurisée, nous assistons à la fin de l'ère de la normalisation ? La gouvernance de la messagerie cryptée se fera-t-elle par infrastructure et par code, par « quelque chose qui fonctionne » ?

En effet, la capacité d'un outil à séduire et à être mobilisé par un grand nombre d'utilisateurs puisque « il marche » semble être un indicateur essentiel de succès et d'adoption en tant que norme de facto. L'IETF lui-même a récemment reconnu un « tournant opportuniste » dans le domaine du

chiffrement (IETF, 2014) qui a pris de l'ampleur en 2013-2014 après les révélations de Snowden, et qui consiste en une évolution progressive de la communauté cryptographique vers un chiffrement « transparent » ou « indolore », nécessitant le moindre effort possible de la part des utilisateurs.

L'interopérabilité et les processus de normalisation *de facto* sont l'une des nombreuses dynamiques qui informent la gouvernance de l'Internet par l'infrastructure, en tant qu'activités « banales » et informelles qui co-construisent les artefacts technologiques et sont pourtant investies d'une valeur sociopolitique claire. D'autres dynamiques de ce type sont les tensions entre la centralisation, la fédération et la décentralisation des architectures techniques, ainsi que et des communautés ; la concentration du *leadership*, et les controverses entre les *leaders* officiels ou informels ; et enfin et surtout, l'ouverture du code, qui est liée à la fois à des différences géopolitiques et à la variété des modèles de menace des utilisateurs, et qui est une préoccupation d'importance variable pour les différents acteurs.

L'analyse de la manière dont les interfaces, et les protocoles et architectures sous-jacents, sont créés et « stabilisés » nous ramène à d'importantes questions relatives à la gouvernance de l'Internet. Ce chapitre se situe dans la lignée de travaux fondateurs sur la qualité infrastructurelle des protocoles Internet et des standards, tels que *Protocol Politics* de Laura DeNardis (2009). Ces travaux nous rappellent que, d'un point de vue technique, les protocoles peuvent être difficiles à saisir : ce ne sont pas du logiciel ni des artefacts matériels, mais du langage textuel et numérique, ce qui permet l'interopérabilité technique entre des dispositifs techniques hétérogènes. Les protocoles ordonnent les flux binaires qui représentent les informations et que les dispositifs numériques utilisent pour spécifier des formats de données communs, des interfaces, les conventions de réseautage et les procédures permettant l'interopérabilité entre les dispositifs qui adhèrent à ces protocoles, quel que soit leur emplacement géographique ou leur fabricant. En tant que sites de contrôle sur la technologie, les décisions intégrées dans les protocoles intègrent des valeurs et reflètent les intérêts socio-économiques et politiques des développeurs de protocoles (DeNardis, 2009 : 10), comme le montrent les processus plus ou moins codifiés et formels par lesquels les protocoles deviennent des standards et des normes, dont on a donné une illustration

dans ce chapitre. Ce chapitre illustre ce que Janet Abbate, dans une citation d'inspiration latourienne, a soutenu dans *Inventing the Internet* (2000) :

> *« Le débat sur les protocoles de réseau illustre comment les normes peuvent être de la politique par d'autres moyens (…) Les efforts visant à créer des normes (…) amènent les décisions privées des fabricants de systèmes techniques dans le domaine public ; de cette façon, les batailles entre les normes peuvent mettre en lumière des hypothèses tacites et des conflits d'intérêts. La passion même avec laquelle les parties prenantes contestent les décisions en matière de standards devrait nous alerter sur les significations profondes sous-jacentes aux écrous et boulons » (Abbate, 2000 : 179, ma traduction).*

En ce sens, les protocoles-en-tant-que-standards sont des infrastructures au sens analysé dans ce mémoire : les protocoles sous-jacents auxquels la conception des logiciels et du matériel se conforme représentent une forme d'infrastructure plus intégrée et plus invisible capable d'influencer des comportements, de mettre en œuvre des politiques publiques ou de restreindre ou étendre la liberté en ligne. Les protocoles ont une puissance d'agir qui dérive de leurs concepteurs et développeurs, et qui les rend des points de contrôle centralisé ou distribué, « inter-médiateurs » de contraintes et libertés. J'ai analysé ici comment les changements à moyen et long terme dans l'infrastructure par le biais de la normalisation, que ce soit par des moyens plus informels ou des voies plus traditionnelles telles que l'IETF, nécessite de tenir compte des attitudes des développeurs à l'égard de l'adoption par les utilisateurs, leur relation avec les institutions, ou encore leurs modèles commerciaux (ou leur absence). Le choix des développeurs de Signal de garder des composantes spécifiques de leur protocole centralisées – alors que d'autres projets fédèrent ou décentralisent bien plus l'architecture technique de leurs créations – leur fournit des leviers, des « points de contrôle » qui les positionne comme acteurs centraux dans la « gouvernance par l'infrastructure » du foisonnant secteur des messageries sécurisées.

Chapitre 7. Gouverner par les « boîtiers noirs » : surveillance et évasion numérique dans l'Internet russe

Cette quatrième et dernière étude de cas porte sur mon enquête la plus récente[64], portant sur les infrastructures destinées à la surveillance et à la censure mises en place par l'état Russe, et sur les résistances qu'elles engendrent auprès de groupes d'acteurs variés (activistes, technologues – fournisseurs d'accès à Internet notamment –, journalistes). Le chapitre porte plus particulièrement sur l'encadrement juridique, et le déploiement techno-économique, d'un ensemble de boîtiers visant des objectifs divers de surveillance et censure, notamment le contrôle des flux et la collecte de données personnelles.

L'Internet russe a récemment connu une augmentation rapide à la fois du contrôle juridique et de la centralisation de l'infrastructure technique. Son âge d'or en tant qu'espace de « demi-liberté d'expression » (Gelman, 2010), sans réglementation ni censure, semble être révolu (Oates, 2013 ; Konradova et Schmidt, 2014) : les lois adoptées ces dernières années, concernant la censure des sites web et la surveillance du trafic, façonnent le web russe selon le projet d' « Internet souverain » (Nocetti, 2015) promu par le gouvernement. Cette stratégie implique, entre autres, une forte pression pour que les infrastructures et les équipements destinés au contrôle soient fabriqués en Russie : dans un contexte d'embargo international et de politique de substitution des importations, un marché prometteur s'est ouvert pour les vendeurs russes de *middleboxes* et de solutions logicielles pour la surveillance et le filtrage du trafic.

Basé sur une enquête menée entre 2016 et 2019 avec Ksenia Ermoshina, puis avec Ksenia et Benjamin Loveluck (Ermoshina & Musiani, 2017 ; Ermoshina, Loveluck et Musiani, 2021), ce chapitre vise à explorer la florissante industrie russe de la censure et de la surveillance. Cette enquête a contribué à dévoiler des débats animés autour des technologies controversées que les

[64] Toujours en compagnie de Ksenia Ermoshina et, dans un deuxième temps, d'une équipe mixte composée de spécialistes de la culture et de la politique Russes et de spécialistes du numérique, dans le cadre du projet ANR ResisTIC (2018-2022).

acteurs de l'Internet doivent obligatoirement installer au sein de leurs infrastructures en Russie, qui sont coûteuses et complexes à mettre en œuvre, et qui soulèvent un certain nombre de préoccupations éthiques et politiques[65]. En particulier, la deuxième partie du chapitre se concentre sur deux types de « boîtiers noirs » : un type est utilisé pour la surveillance afin de collecter les métadonnées et le contenu du trafic Internet et est connu sous l'acronyme SORM (pour Système de mesures opérationnelles d'investigation). L'autre type concerne le filtrage du trafic, utilisé pour bloquer les sites web qui ont été mis sur la liste noire de Roskomnadzor (dorénavant RKN), l'organisme fédéral russe de surveillance des médias et des télécommunications.

Ces technologies de filtrage et de surveillance sont des « objets-frontière » (Star et Griesemer, 1989) d'un genre particulier. En effet, il ne s'agit pas toujours de « boîtiers » physiques clairement identifiables (bien que ce soit plusieurs fois le cas), mais plutôt d'une multitude de solutions logicielles, ainsi que d'objets techniques distribués et d'ajustements techno-juridiques qui viennent compléter les infrastructures matérielles existantes. Par ailleurs, ces *middleboxes* sont également des « boîtes noires » au sens STS, à plusieurs niveaux : d'abord en raison de leur opacité technique supposée, mais aussi en raison de leurs fonctions de filtrage et de surveillance, qui les placent dans le domaine du secret d'État et du secret commercial.

Pour cette étude, nous avons collecté trois types de matériel sur la période 2017-2019. Tout d'abord, nous avons mené 15 entretiens avec des FAI, des experts en informatique, des avocats spécialisés dans l'Internet, des vendeurs d'équipements de filtrage, ainsi que des militants anti-censure et anti-surveillance. Ces répondants ont été recrutés en plusieurs étapes. Tout d'abord, nous avons contacté des experts connus du public dans le domaine des télécommunications, de la censure et de la surveillance d'Internet et des droits numériques, rencontrés précédemment lors de divers rassemblements auxquels nous assistons et que nous observons régulièrement (par exemple, RightsCon, Internet Freedom Festival, Privacy Day, Chaos Communication Congress, etc.) Après cette première série d'entretiens, nous avons sollicité l'aide de ces experts pour nous recommander aux FAI éventuellement intéressés à participer à l'étude. Ce processus de recommandation était

[65] Certains des contenus de ce chapitre, notamment en termes de chiffres (nombre de FAI actifs, nombre de clients, coût des différents boîtiers…) sont susceptibles d'évoluer de façon très importante et rapide, à l'heure où je finalise ce manuscrit et la guerre fait rage en Ukraine depuis le 24 février 2022.

important en soi, car la communauté des FAI est relativement fermée. Les FAI à qui nous avons parlé sont principalement de petite et moyenne taille (entre 5 000 et 100 000 clients) et sont des participants actifs de forums professionnels (par exemple Nag.ru) et de chats sur l'outil Telegram. Nous nous sommes également entretenus avec des représentants de fournisseurs de solutions DPI et de filtrage, ainsi qu'avec des ingénieurs travaillant au point d'échange Internet de Saint-Pétersbourg. Les répondants ont demandé, sauf exception, à rester anonymes. L'étude a été complétée par une analyse des forums et chats dédiés aux FAI, qui ont été sélectionnés et suivis sur l'ensemble de la période. Enfin, nous avons procédé à une analyse de contenu des supports de communication produits par les éditeurs de solutions de surveillance et de censure : sites Web, présentations commerciales, supports issus de conférences professionnelles spécialisées.

Ce chapitre aborde les effets que ces objets techniques ont sur le marché des services Internet, dans un contexte de fortes contraintes techniques, politiques et juridiques, ainsi que les incertitudes et opportunités liées à leur interprétation. Les configurations ou agencements de marché (Callon, 2013) associés à ces boîtes impliquent de traduire les exigences politiques et juridiques en solutions techniques et en innovations commerciales. En effet, en l'absence de normalisation, les FAI doivent interpréter ce que l'on attend d'eux sur le plan technique, et sans soutien financier de l'État, ils doivent le plus souvent supporter seuls le coût de ces installations. Cependant, ils développent également des réponses à cette situation qui peuvent prendre différentes formes : économiques (en formant des alliances et des associations afin de partager les coûts), politico-juridiques (en mobilisant les organismes antitrust, et d'autres entités légales), ou techniques (en développant des stratégies et des astuces pour trouver un moyen de contourner les contraintes). Nous nous intéressons ainsi à l'articulation entre les exigences techno-légales, les produits proposés pour les exécuter, et les stratégies de négociation des FAI pour atténuer les implications économiques et techniques du filtrage et de la surveillance. Nous montrons enfin comment cette industrie participe à la création de « groupes et publics concernés, et ouvre de nouveaux espaces pour les controverses politiques » (Geiger et al., 2014) dans la gouvernance du marché informatique russe.

Comprendre la surveillance et la censure avec des approches au croisement entre les STS et l'économie politique contribue également à éclairer son fonctionnement en pratique et ses logiques

inhérentes, ce qui permet de déconstruire l'image trop simplifiée d'un contrôle direct par l'État via la technologie, véhiculée à souhait par le pouvoir russe lui-même. Après avoir pris en considération le DNS, la blockchain et les protocoles de chiffrement comme composantes centrales de la gouvernance par l'infrastructure dans l'Internet d'aujourd'hui, je montre avec le cas des boîtiers russes de surveillance et censure encore une autre facette de comment l'infrastructure Internet elle-même peut être utilisée pour affirmer des relations de pouvoir : je détaille comment ces boîtiers sont intégrés à (et contribuent à construire) un ensemble de relations sociales, économiques et politiques entre acteurs publics et privés et de ces derniers avec les citoyens-usagers-consommateurs de l'Internet russe, tout en présentant une image plus complexe de l'articulation entre « loi et code », et entre les décisions politiques et leur traduction en pratiques sociales, techniques et économiques, de contrainte et de résistance.

7.1. Trois niveaux de contrôle d'Internet « par l'infrastructure » en Russie

Avec près de six mille FAI sous licence aujourd'hui, et entre 3461 et 3940 FAI actifs, dont certains se sont développés à partir de réseaux locaux (*domovaya set*), l'industrie russe des FAI est dynamique. Jusqu'à récemment, ce marché était caractérisé par une forte concurrence entre les fournisseurs de services, des prix bas et une bonne qualité du matériel de réseau et des connexions, ainsi qu'une topographie spécifique basée sur plusieurs accords de *peering* avec des partenaires internationaux. Ces derniers temps, cependant, ce marché a été affecté par une centralisation progressive mais implacable, tant au niveau juridique qu'au niveau des infrastructures. Le nombre de licences délivrées pour les « services télématiques » et les « services de transfert de données » a diminué entre 2017 et aujourd'hui, respectivement de 1395 et 709. L'une des dernières initiatives gouvernementales sur l' « Internet russe autonome », par exemple, introduit la possibilité, du moins déclarée dans le texte de loi, d'un « point central de contrôle » pour tous les réseaux russes, et implique un enregistrement obligatoire de tous les points d'échange Internet et des câbles transnationaux, qui n'ont jamais été correctement documentés dans aucune des listes appartenant au gouvernement.

La « gouvernance par l'infrastructure » a ses propres spécificités en Russie. En particulier, les solutions techniques sont souvent en retard sur la réglementation, notamment en ce qui concerne la loi dite « Yarovaya », comme nous le verrons plus loin. Les récentes initiatives juridiques concernant l'Internet russe ont toujours *anticipé* la production et la certification de solutions techniques concrètes, ce qui a conduit à des périodes assez longues de vide techno-juridique, où des expérimentations et des bricolages étaient activement développés par les FAI pour faire face aux nouvelles exigences. Cette caractéristique de la réglementation russe de l'Internet a donné lieu à des critiques de la part de la communauté des FAI. Nombre de nos répondants ont qualifié ce scénario de « théâtre de la sécurité », ce qui sous-tend des motivations économiques plutôt que politiques ou techniques derrière la réglementation de l'Internet en Russie, compte tenu notamment de l'impératif de « substitution de l'importation » qui signifie que les solutions technologiques pour la mise en œuvre des nouvelles lois devaient être *made in Russia*, fabriquées en Russie.

La gouvernance du RuNet s'est développée sur plusieurs couches, avec trois principaux types de mesures adoptées depuis 1998 :

a) Mesures de surveillance dites d' « interception légale », appelées Système de mesures opérationnelles d'investigation (SORM), visant à permettre aux services gouvernementaux tels que le FSB (le successeur du KGB) d'accéder aux communications privées par téléphone et sur Internet ;

b) Réglementation du stockage des données, limitant les flux de données importants aux frontières nationales ;

c) Mesures de filtrage, restreignant l'accès à une liste croissante de sites web considérés comme extrémistes, par le biais d'une liste noire.

Ces trois couches sont interconnectées, et montrent une tendance globale à la « balkanisation » du réseau RuNet, c'est-à-dire à une hyper-localisation et à une réglementation des flux de données et de communication par l'État.

7.1.1. La « SORMisation » de la Russie : mesures de surveillance et « d'interception légale »

SORM a été mis en œuvre pour la première fois en Russie en 1998. SORM fournit une architecture grâce à laquelle les organismes d'application de la loi et de renseignement peuvent obtenir un accès direct aux données sur les réseaux commerciaux. Au cours des huit dernières années, SORM a donné lieu à de nouvelles configurations de dispositifs, et d'acteurs commerciaux les fabriquant, ce qui a eu des conséquences à long terme sur le marché des FAI. Trois générations de mesures SORM ont vu le jour. SORM-1 permet au FSB d'accéder au trafic téléphonique, y compris le trafic lié aux réseaux mobiles. SORM-2, mis en œuvre en 2005, est chargé d'intercepter le trafic IP, y compris la VoIP. SORM-3, mis en œuvre en 2014, rassemble des informations provenant de tous les moyens de communication, et offre un stockage à long terme et complet des données des abonnés.

Par rapport aux normes internationales d'interception légale, SORM donne une grande autonomie aux acteurs de la surveillance. Dans la plupart des pays occidentaux, les organismes chargés de l'application de la loi demandent un mandat à un tribunal, puis émettent un ordre d'interception légale à un opérateur de réseau ou à un fournisseur de services Internet, qui est tenu d'intercepter et de livrer les informations demandées. Le FSB n'a pas besoin de contacter le FAI en raison de l'architecture même de SORM, qui contient deux éléments principaux : l' « extracteur » (l'équipement – logiciel et matériel – qui effectue l'extraction des données) et la « station de contrôle à distance ». La station de contrôle est localisée dans le bureau régional du FSB et permet de contrôler à distance l'extracteur sans l'autorisation du fournisseur : le fournisseur ne peut pas savoir quelles données sont interceptées, analysées et transférées, et par quels moyens. Aucune décision de justice n'est nécessaire pour activer l'interception des métadonnées. En revanche, pour accéder aux enregistrements téléphoniques proprement dits, le FSB doit demander une autorisation judiciaire. Plusieurs centaines de milliers d'ordres sont distribués chaque année, selon les données officielles fournies par la Cour suprême.

Le composant le plus coûteux de SORM est l'équipement destiné au stockage des données. Cependant, chaque nouvelle génération de mesures SORM a modifié les exigences techniques : alors que pour SORM-2 les fournisseurs devaient stocker tout le trafic pendant 12 heures, SORM-3 les oblige à stocker toutes les métadonnées pendant trois ans. Ainsi, les fournisseurs doivent

changer tous leurs équipements car la mise en œuvre des systèmes SORM repose entièrement sur eux : « c'est nous qui le payons », remarque le fournisseur d'accès Internet Michael I. « Si vous ne mettez pas cet équipement, vous n'avez pas de licence et vous perdez des clients liés à l'État ». Lorsque le FSB local ou le bureau du procureur identifient des manquements, ils envoient l'information à RKN. Le FAI reçoit un avertissement, une première amende, puis si les violations persistent, sa licence peut être retirée (Soldatov & Borogan, 2013).

Les fournisseurs doivent renouveler les équipements SORM par eux-mêmes car il n'existe pas de normes certifiées sur le marché et il n'y a pas de consensus établi sur les procédures et les matériaux entre les fabricants. Par conséquent, les fournisseurs doivent s'adapter aux nouvelles exigences techniques, parfois en bricolant les anciens équipements : « Adaptez les pièces de votre système, tout d'abord... parce que lorsqu'ils publieront enfin les certificats... nous devrons à nouveau dépenser des tonnes d'argent, et nous devrons le faire, car c'est la Loi », note le fabricant *hardware* Andrei le 14 novembre 2015. Une enquête menée par Leonid Volkov, activiste, blogueur et programmeur, affirme qu' « un petit fournisseur doit consacrer environ 20 à 30% de son revenu annuel pour acheter de l'équipement SORM » (Volkov, 2016). Les deux plus grands fabricants d'équipements SORM gagnent 5 à 6 milliards de roubles (environ 40-45 millions d'euros) par an sur SORM, tandis que trois autres petits fabricants gagnent environ 1 milliard. Pour réduire leurs coûts, les petits fournisseurs achètent du SORM en tant que service auprès de leurs fournisseurs en amont.

La mise en œuvre de SORM-1 en Russie a suscité une campagne de protestation de la part des professionnels de l'informatique, des organisations de défense des droits de l'homme et des défenseurs de la liberté de l'Internet. Le premier mouvement anti-SORM a été lancé à la fin des années 1990 sous la forme d'une attaque de déni de service sur les outils d'analyse sémantique du FSB. Les activistes ajoutaient des mots-clés spécifiques à chaque courrier, tels que « bombe », « explosion », « attaque terroriste », déclenchant des alertes constantes au poste de contrôle et le surchargeant. Moscovskiy Libertarium, avec des partenaires russes et internationaux, a lancé une campagne de solidarité internationale contre SORM. Une pétition publique a été envoyée à la Cour suprême et à l'ancien président russe Boris Eltsine, lui demandant « d'user de son autorité afin

d'arrêter la mise en œuvre de SORM », un « exemple sans précédent de violation du droit à la vie privée et de la convention des droits de l'homme ». Si cette campagne n'a pas donné de résultats immédiats, quinze ans plus tard, dans l'affaire Roman Zakharov vs. Russie (2015)[66], la Cour européenne des droits de l'homme a reconnu que SORM constituait une violation de la Convention européenne des droits de l'homme, car son infrastructure technique permettait d'intercepter des communications sans autorisation judiciaire, contournant ainsi les procédures légales. La campagne anti-SORM du début des années 2000 était principalement menée par des journalistes, des militants ONG et des programmeurs, tandis que les fournisseurs étaient presque absents de la controverse, à deux exceptions près. Comme le note Sergey Smirnov, militant de Pravozashitnaya Set (Réseau des droits de l'homme) : « Les fournisseurs de services Internet sont arrivés à la conclusion que la perspective de perdre leur licence est bien pire que la nécessité de collaborer avec le FSB. Dans l'une des récentes publications sur les SORM, un agent du FSB a remarqué que dans la majorité des cas, les fournisseurs appliquent toutes les exigences sans aucune pression et font même preuve de compréhension ». L'absence de FAI dans le mouvement anti-SORM a rendu tout mouvement de désobéissance civile techniquement impossible. Afin de créer un précédent, Leonid Volkov a lancé une campagne contre le SORM-3 en 2015 ; il a lancé ce qu'on appelle « l'attaque contre SORM », un projet juridique et politique d'appel collectif au tribunal par les opérateurs et les fournisseurs, pour demander une meilleure réglementation du SORM et des équipements certifiés financés par l'État.

7.1.1.1. La loi Yarovaya : quand le droit précède (inhabituellement) la technique

Néanmoins, le développement des exigences juridiques et techniques du SORM a créé des tensions au sein de la communauté des FAI. En juin 2016, une nouvelle série de mesures de surveillance a été proposée par la représentante Irina Yarovaya : Les opérateurs télécoms russes auraient dû stocker tout le trafic passant par eux (y compris les appels, les lettres, les documents, les images et les vidéos) pendant six mois, et les métadonnées associées, comme on l'a vu plus haut, pendant trois ans. L'importance de cette affaire réside dans le fait qu'elle révèle un « écart inverse » entre

[66] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-10793%22]}

les mesures légales et les ressources financières et techniques : alors que « les gouvernements s'efforcent de suivre le rythme de l'évolution technologique, la technologie évoluant plus vite que les efforts d'élaboration des lois » (Nocetti, 2015 : 111), dans l'affaire de la loi Yarovaya, c'est l'élaboration des lois qui a dépassé le développement technologique réel du pays. En effet, une telle surveillance nécessite une infrastructure technique complexe et à plusieurs niveaux (notamment les serveurs, le réseau lui-même, les systèmes de stockage de données et les logiciels), ce qui a des conséquences considérables sur les modes de fonctionnement d'Internet et des télécommunications en Russie, notamment la qualité de la connexion, la vitesse à laquelle et les quantités de données que le réseau est capable de transférer et le prix des services Internet. Vladimir K., FAI, déclare : « La loi Yarovaya est techniquement absurde. Premièrement, il n'y a pas d'équipement nécessaire sur le marché. Deuxièmement, il est inutile de stocker des données chiffrées. Avec le même succès, nous pouvons coder un générateur de nombres aléatoires et envoyer ces données au FSB en prétendant qu'il s'agit du trafic de nos utilisateurs ».

Le problème est à la fois technique et géopolitique, car il interroge les limites de l'État-nation russe et ses capacités à mettre en place une nouvelle infrastructure indépendamment des équipements du marché occidental. Dans le cadre d'un embargo, dû aux sanctions occidentales imposées à la Russie suite à l'annexion de la Crimée en 2014, le gouvernement russe se tourne vers les entreprises nationales pour produire les équipements nécessaires. La politique de « substitution des importations » couplée à la nouvelle série de lois de surveillance a un impact important sur l'industrie informatique russe. Le PDG de MGTS (le réseau étatique de télécommunications basé à Moscou), Andrey Ershov, déclare : « Aujourd'hui, nous ne disposons d'aucun équipement permettant de mettre en pratique la 'loi Yarovaya' [...] Ainsi, la plus grande préoccupation exprimée publiquement par tous les opérateurs de télécommunications est liée au coût de ces solutions. [L'équipement] représente des dizaines de milliards de roubles ». Même l'ensemble émergent d'entreprises spécialisées dans les équipements SORM ne peut satisfaire aux exigences de la loi Yarovaya en termes d'équipements, estimés à 10,3 milliards de roubles (Kantyshev, 2016). Les fournisseurs et les opérateurs de télécommunications ont publiquement exprimé leur scepticisme à l'égard de la nouvelle loi de surveillance, soulignant que les nouvelles solutions risquent de devenir obsolètes en quelques années et exigeront de nouveaux investissements (Schepin, 2016). La presse et les sites Internet spécialisés ont montré une hausse de la

désapprobation de la loi Yarovaya parmi les professionnels de l'informatique, pour des raisons similaires. Parmi les acteurs qui critiquent la loi figurent les plus grandes entreprises informatiques russes, Mail.ru et Yandex, ainsi que les associations professionnelles RAEC (Association russe des communications électroniques) et ROCIT (Centre russe d'organisation civique pour les technologies de l'information), et même un groupe de travail pro-gouvernemental « Communications et informatique » (*Svyaz i IT*). Le forum professionnel le plus populaire des fournisseurs russes, Nag.ru, a réagi de manière créative à la loi en développant un « Yarculator », un logiciel permettant aux fournisseurs de calculer les prix des équipements nécessaires et le coût des services Internet pour les utilisateurs finaux.

La loi a été par ailleurs largement contestée par la société civile. Une pétition sur Change.org a recueilli 623 465 signatures au 8 janvier 2017. Une manifestation contre la loi a été organisée à Moscou en août 2016 et a rassemblé entre 2 400 et 4 000 personnes (Kozlov & Filipenok, 2016). De son côté, Edward Snowden a publiquement demandé à Poutine de ne pas signer la loi Yarovaya, en insistant sur ses conséquences économiques néfastes et en soulignant qu'un stockage de six mois des données est dangereux, irréalisable et coûteux. Si la loi SORM et la loi Yarovaya permettent au FSB d'accéder aux données stockées sur les serveurs russes sans en informer les propriétaires ou les fournisseurs de sites, il est plus difficile d'accéder aux services étrangers, par exemple Facebook et Twitter. Un ensemble de nouvelles mesures a donc été adopté pour reconfigurer le stockage et le transfert des données.

7.1.2. Stockage des données et restrictions des flux

Les révélations de Snowden ont attiré l'attention sur les pratiques de surveillance existantes et ont permis de comparer les SORM avec le système américain. Cependant, l'impact le plus important des révélations a concerné le rôle des services *cloud*, et les sociétés Internet américaines. En réponse, le gouvernement russe a modifié la « loi sur le stockage et la protection des données personnelles » et a reconsidéré la géopolitique des données pour prétendument garantir la « protection des données des citoyens russes contre la surveillance du gouvernement américain ».

Les chercheurs-journalistes Andrei Soldatov et Irina Borogan insistent sur le rôle qu'a joué Snowden dans cette affaire :

> *Pile au bon moment, Edward Snowden est apparu sur la scène mondiale. Le scandale de la NSA a fourni une excuse parfaite aux autorités russes pour lancer une campagne visant à soumettre les plateformes web mondiales telles que Gmail et Facebook à la législation russe – soit en exigeant qu'elles soient accessibles en Russie par l'extension de domaine .ru, soit en les obligeant à être hébergées sur le territoire russe (Soldatov & Borogan, 2013).*

La loi #242-FZ a été adoptée le 1er septembre 2014. Elle oblige les fournisseurs à « stocker les données personnelles des citoyens russes, utilisées par les services internet, sur le territoire de la Fédération de Russie ». Les fournisseurs doivent garantir l'enregistrement, la systématisation, l'accumulation, le stockage, les mises à jour, les modifications et l'extraction des données personnelles en utilisant des bases de données situées sur le territoire russe. Le non-respect de cette nouvelle loi peut entraîner le blocage total du service. Ainsi, par exemple, en novembre 2016, LinkedIn a été bloqué en Russie (y compris les applications mobiles) pour la violation des nouvelles politiques de stockage des données. Les services web sont également tenus de construire des portes dérobées permettant aux services secrets russes d'accéder aux données stockées. Un autre moyen de faire pression sur les entreprises occidentales consiste à bloquer des services web entiers parce qu'ils stockent des « informations interdites ». Ainsi, YouTube a été bloqué en Russie pour avoir hébergé une vidéo jugée extrémiste. Facebook a supprimé une page appelée Club Suicide plutôt que de voir l'ensemble de son réseau mis sur liste noire.

Plusieurs tactiques de résistance se sont développées en réponse à ces mesures de balkanisation. Une pétition adressée à Google, Facebook et Twitter leur demande de ne pas obtempérer aux demandes : « Nous ne faisons pas confiance aux services de sécurité nationaux qui sont en charge de la sécurité des données une fois que celles-ci sont en Russie. Nous demandons aux sociétés Internet de résister à cette pression en utilisant tous les moyens légaux possibles et nous sommes prêts à les soutenir ». Les développeurs ont été immédiatement concernés, car la loi s'attaquait aux instruments qu'ils utilisaient constamment, comme GitHub, ainsi qu'à leurs pratiques de stockage des données. Parmi les autres tactiques déployées, on trouve également une réorientation vers de

nouveaux produits qui éviteraient le stockage des données personnelles : « Nous essayons de créer des services qui ne stockent pas les données des utilisateurs, afin de ne pas avoir à les stocker sur nos serveurs », remarque Alexey P., développeur, directeur technique de Progress Engine ; « Nous avons certaines applications que nous créons pour la télévision, ou pour les portefeuilles électroniques, où les données sont stockées sur les serveurs de nos clients ». Il s'agit de tactiques de résistance spécifiques que nous pourrions qualifier de tactiques d' « évasion ». En fait, au lieu de contester la loi n° 242-FZ en communiquant directement avec le gouvernement russe, les citoyens essaient soit de communiquer avec les entreprises informatiques occidentales (en adressant des pétitions à Google et Facebook), soit de modifier leurs propres pratiques et activités professionnelles afin de trouver des vides juridiques ou des zones grises (par exemple, en utilisant des API pour l'autorisation ou des tiers pour le stockage des données des utilisateurs, ou en repositionnant leur produit afin de ne pas utiliser de données personnelles du tout).

Un autre pas vers la « souveraineté numérique », telle qu'elle est envisagée par l'État russe, a été fait au printemps 2016 avec un ambitieux projet, une variation étatique de l'attaque de l'homme du milieu[67] qu'on pourrait qualifier d' « État du milieu » : lors du forum *IT + Sovereignty*, la création prévue d'une certification SSL appartenant à l'État a été annoncée. Natalya Kasperskaya, membre du forum, explique :

> *Roskomnadzor et le FSB font pression pour que les certificats SSL soient délégués à des organisations gouvernementales... Nous avons maintenant une partie de l'Internet qui échappe complètement au contrôle de notre propre pays, et ce n'est pas bon. Parce que les données sont collectées au niveau mondial, par quelqu'un qui est au-delà des frontières de notre État.*

Selon nos interlocuteurs, ce projet est en fait une réponse à l'inefficacité de la loi Yarovaya et à la popularité croissante du chiffrement parmi les utilisateurs de RuNet. Alexey P. souligne : « Ils ont compris que le stockage de gigaoctets de données ne donnera aucun résultat, notamment parce qu'elles sont chiffrées.... donc, le projet de construire une attaque de l'homme du milieu au niveau gouvernemental est effrayant ».

[67] L'attaque de l'homme du milieu (HDM) ou *man-in-the-middle attack* (MITM), parfois appelée attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

7.1.3. Erreur 451 : Filtrage de sites Web et restrictions d'accès aux contenus

Une troisième série de mesures, fondée sur le filtrage, vise à contrôler l'accès des utilisateurs au contenu de sites web jugés extrémistes ou criminels. Depuis 2007, les procureurs régionaux ont mis en œuvre des décisions de justice exigeant des FAI qu'ils bloquent l'accès aux sites interdits accusés d'extrémisme, mais cela n'a pas été fait systématiquement. Afin de centraliser ces différents matériels, un « registre unique des ressources Internet contenant des informations dont la diffusion est interdite en Russie » a été créé en 2012 : tous les sites web qui entrent dans cette liste noire doivent être bloqués et trois agences gouvernementales participent à la constitution de cette liste noire. Depuis l'adoption de la loi dite Lugovoy, du nom de son proposant, le 1er février 2014, la liste inclut les sites web qui « font appel à l'extrémisme », par exemple les troubles de masse, la discorde religieuse ou interethnique, la participation à des attaques terroristes ou certains types d'événements publics.

Le 13 mars 2014, RKN a bloqué l'accès à quatre pages web : Grani.ru (une plateforme médiatique libérale en ligne), Kasparov.ru (le site de Garry Kasparov, joueur d'échecs et leader de l'opposition libérale), Ezhednevniy Zhurnal (plateforme médiatique libérale) et le blog d'Alexey Navalny (leader du mouvement anti-Poutine et blogueur réputé). RKN a déclaré que « ces sites web contiennent des appels à des activités illégales et à la participation à des manifestations de masse qui violent la loi ». La liste des pages web interdites est accessible en ligne. Au 30 septembre 2016, 41 064 pages – concernant principalement la prostitution, les jeux d'argent, les marchés noirs, les jeux de hasard et l'hébergement de torrents – étaient bloquées. Cependant, des sites d'ONG sont également présents, comme le site de Mirotvorets, une organisation pro-ukrainienne qui informe sur le conflit en Ukraine, notamment sur la localisation des troupes russes.

Le blocage se fait de trois manières : par DNS, par adresse IP ou par URL, en utilisant des techniques d'inspection approfondie des paquets (DPI). Sur le plan administratif, les fournisseurs de services d'hébergement de sites sont chargés de tenir à jour la liste noire et de communiquer

avec les propriétaires des sites interdits et les utilisateurs finaux. Maxim I., un de ces acteurs, note que

> *le blocage est très facile. Nous recevons et mettons à jour régulièrement la liste noire, deux fois par jour, et nous bloquons ceux de nos clients qui n'ont pas de chance... Nous informons notre client que son site a été ajouté à la liste noire. Ensuite, nous écoutons tout ce que le client veut dire sur le Roskomnadzor mais nous ne pouvons pas l'aider ou ignorer la demande du Roskomnadzor car dans ce cas, ils peuvent bloquer l'adresse IP du serveur, voire un pool d'adresses. Je ne parle même pas des conséquences administratives pour l'entreprise.*

Alors que les fournisseurs ont très peu de possibilités de résister au blocage des ressources figurant sur la liste noire, ils choisissent d'autres formes d'action pour exprimer leur critique de la censure d'Internet. Vladimir K., directeur du FAI CLN, remarque que lorsque les utilisateurs essaient d'accéder à une page bloquée, le FAI leur montre « le message d'erreur qui commence par une phrase : 'La lutte contre le mal n'est presque jamais une lutte pour le bien' ». Ainsi, le message d'erreur lui-même devient un espace d'expression où les fournisseurs peuvent communiquer symboliquement avec leurs utilisateurs en montrant leur rapport à la loi Lugovoy. Cependant, les systèmes de filtrage et de blocage russes sont appliqués de manière inégale d'une région à l'autre, d'un fournisseur à l'autre. Ainsi, plusieurs employés de FAI qui servent des grandes entreprises/monopoles, comme les Chemins de fer russes, confirment qu'ils n'ont pas été bloqués, comme Dmitry M. en 2014 : « Nous avons ce fournisseur dans notre entreprise, et tous les sites web de la liste noire peuvent être ouverts. Cependant, cela semble tout à fait logique, car Roskomnadzor ne peut donner aucun ordre aux Chemins de fer russes, qui possèdent ce fournisseur » (en Nossik, 2014). De plus, le filtrage ne fonctionne que partiellement, en fonction de la région, du fournisseur et de sa position sur le marché, de ses connexions avec les fournisseurs occidentaux (par exemple, les fournisseurs qui avaient un accord de *peering* avec Stockholm pouvaient accéder aux sites web de la liste noire).

Le paradoxe du filtrage consiste dans la double fracture numérique qu'il crée. Les utilisateurs les plus « politisés », familiers des ressources en ligne interdites, continueront à y accéder, en utilisant des outils spécifiques pour contourner la censure. En revanche, la majorité de la population sera incapable d'accéder à ces contenus, ne disposant pas des connaissances, des ressources et des

technologies nécessaires pour le faire. Les moteurs de recherche sont également touchés par le filtrage, renforçant ainsi la fracture : avant le blocage, les utilisateurs pouvaient découvrir accidentellement certains sites web (par exemple le blog de Navalny) grâce aux moteurs de recherche, mais après le blocage, ces sites ont « disparu » (ont été déréférencés) des résultats de recherche. Cela réduit donc considérablement toute audience potentielle et renforce l'effet d'écho-chambre en regroupant les utilisateurs qui sont déjà d'accord, comme le mentionne l'utilisateur popados : « Ces blocages ne sont pas pour ceux qui lisent et qui contourneront quoi qu'il arrive. C'est pour les visiteurs aléatoires […] qui constituent en fait la majorité. Ils vont simplement aller sur un autre site web. En ce sens, le blocage est plutôt efficace » (Nossik, 2014). Le même phénomène touche les sites torrents blacklistés, comme Rutracker, qui démontrent une baisse significative du trafic : « la majorité des utilisateurs sont juste paresseux, ils trouvent de nouvelles sources ouvertes de contenu. Le but du filtrage n'est donc pas de fermer pour tout le monde, mais pour une partie importante », explique Maxim I. Pourtant, les restrictions d'accès ne sont pas particulièrement difficiles à contourner. L'IETF note que « dans de nombreux cas, les clients peuvent toujours accéder à la ressource refusée en utilisant des contre-mesures techniques telles qu'un VPN ou le réseau Tor » (RFC 7725). Comme nous le verrons plus loin, les utilisateurs déploient à cette fin de multiples pratiques techniques, bricolages et arts de faire.

7.2. Le marché russe de la surveillance et de la censure Internet

Dans ce contexte, la régulation juridique et technique du RuNet produit un marché à part entière – et florissant – de la censure et de la surveillance, et façonne la concurrence entre les différents vendeurs de composants d'infrastructure. En ce sens, l'étude de ce marché permet d'analyser la relation entre normalisation et concurrence : même si la gouvernance du RuNet s'impose de plus en plus, l'État russe reste relativement lent en termes de certification des solutions techniques de surveillance et de censure, ce qui produit des vides techno-légaux temporaires permettant aux acteurs de ce marché de se développer. Par ailleurs, l'étude des « boîtiers » intermédiaires permet de mettre en lumière des pratiques de résistance qui se développent souvent en réponse à des techniques de filtrage et de surveillance spécifiques. Ainsi, comprendre le fonctionnement de ces

dispositifs socio-techniques permet de suivre et de comprendre la politisation des professionnels du Web.

7.2.1. Les fournisseurs d'accès Internet face au SORM : contraintes et bricolages

Après près de deux ans de discussions en raison de la complexité technique de la loi Yarovaya, et avec une pression et des critiques abondantes venant de la communauté des FAI, l'amendement du 12 avril 2018 introduit de nouvelles exigences pour la collecte des données : la condition de stockage des métadonnées pendant trois ans, mentionnée plus haut, est restée, mais la durée de stockage de tous les appels vocaux, données, images et messages texte a été réduite à 30 jours (au lieu des 90 jours initiaux), en augmentant la durée de stockage de 15% chaque année. Ces données doivent être mises à la disposition des autorités sur demande et peuvent être obtenues sans mandat ou décision de justice ; en outre, les services en ligne utilisant des données cryptées pour la messagerie, le courrier électronique ou les médias sociaux devraient permettre au FSB d'accéder à ces communications en clair. En outre, dans le contexte de la pandémie de Covid-19 et après une nouvelle itération de discussions, le 23 avril 2018, le ministère des communications a demandé un nouvel amendement à la loi Yarovaya, suggérant de reporter d'un an l'obligation pour les FAI d'augmenter la durée de stockage. Cependant, cette nouvelle réglementation a suscité de vives critiques, non seulement en raison de la portée de plus en plus étendue de la surveillance, mais aussi, comme on l'a vu, en raison des coûts élevés liés aux exigences de stockage massif des données. Lors de la conférence KROS en mai 2017, cela a été réaffirmé clairement par NORSI-TRANS, l'un des leaders du marché des solutions SORM : « Le stockage de l'ensemble du trafic Internet (…) n'est pas compatible avec les réalités économiques de notre pays. La seule solution pratique pour SORM est d'utiliser des équipements existants, avec des extensions minimales et une solution technique claire, sans canular ».

De plus, comme dans les cas précédents de SORM, le processus de certification est long et complexe. Il implique une multitude d'acteurs institutionnels, chacun étant responsable de la certification d'un composant ou de plusieurs composants du système. Le système doit être testé selon une méthodologie clairement définie qui doit d'abord être certifiée par le FSB et le ministère des communications. Ensuite, le FSB teste l'installation à l'aide d'un simulateur, et ce n'est

qu'après que le processus de certification peut commencer, ce qui prend environ 3 mois. Selon le directeur d'OrderCom, une agence de conseil juridique pour les fournisseurs de services Internet, les certifications pour SORM-3 Yarovaya ne seront pas publiées avant 2021.

Ce vide techno-juridique a déjà été utilisé par les FAI : « La légalisation de SORM-2 a pris 10 ans, les FAI ont réussi à se défendre devant les tribunaux car les équipements n'étaient pas certifiés ». Les FAI sont conscients de cette zone grise et essaient de ne pas faire d'excès de zèle afin de minimiser les coûts. En l'absence de solutions standardisées et certifiées par l'État, ils essaient autant que possible de se contenter de bricoler les infrastructures existantes. Cela signifie également que les responsabilités légales ne sont pas clairement définies. Les erreurs de configuration des boîtiers SORM sont fréquentes, ce qui met en danger les données personnelles des internautes. Le système est également sujet à la corruption. La situation est rendue particulièrement problématique par la nature sensible des données, des différentes parties impliquées et du caractère secret du processus global :

> *Nous enregistrons le trafic, mais qui sera responsable en cas de fuite ? Tout est distribué. Chaque FAI a son propre équipement. Le FAI l'achète à un fournisseur, mais il y a aussi la personne qui va installer cet équipement, et l'utilisateur final, l'agent du FSB. Donc. Il y a comme 3 parties impliquées dans le processus. Qui sera responsable en cas de fuite ? Qui se présentera au tribunal ? (un représentant de FAI à la conférence SORM, novembre 2017).*

Cependant, les exigences semblent être adaptées en fonction de la taille et du budget des FAI. Lorsque le FAI dépasse une certaine taille, il doit répondre aux exigences, mais les petits FAI n'installent pas toujours des boîtiers SORM sur leurs réseaux. Au lieu de cela, ils répondent aux demandes du FSB sur une base *ad hoc* : « Quand c'est nécessaire, le FSB nous appelle ou nous contacte par e-mail et nous demande de faire un tcpdump du trafic pour une IP spécifique, et de le partager par ftp ou quelque chose comme ça »[68] ; « Parfois ils [le FSB] viennent en personne, se branchent sur le réseau et écoutent, quand ils ont vraiment besoin d'écouter quelqu'un » [entretien avec le directeur de l'Association des FAI alternatifs]. D'autres options incluent une collaboration entre les FAI, qui peuvent décider de partager les coûts d'une solution SORM – selon le directeur d'OrderCom, cela peut représenter une réduction des coûts de 20-25%. Une autre solution, appelée

[68] https://habr.com/post/65924/

« outSORMing » en jouant sur le mot anglais *outsourcing* (délocalisation), consiste en un accord par lequel les petits acteurs peuvent acheter du trafic déjà « SORMisé » par les grands FAI. Enfin, dans certaines situations, une « course au SORM » peut avoir lieu, par laquelle des FAI éphémères sont mis en place et de nouvelles entités juridiques sont créées en cas de problèmes avec SORM.

Notre analyse des forums professionnels de FAI, tels que Nag.ru, montre une attitude très critique et quelque peu ironique des FAI de petite et moyenne taille à l'égard de SORM, et à l'heure actuelle, l'efficacité réelle de SORM est remise en question.

Figure 1. Un dessin ironique au sujet de la loi Yarovaya et ses conséquences pour les FAI, une « forêt pleine de zones d'ombre ». Source: https://www.ordercom.ru/sorm-vvod-otchetnost/copm.html

Selon une enquête des journalistes de RBC, SORM pourrait être soit absent, soit mal configuré pour 70% des FAI. En 2017, 451 dossiers pour violation de la réglementation SORM ont été déposés, selon l'analyse des données ouvertes sur les audiences des tribunaux. 196 opérateurs ont été condamnés à une amende, et 192 ont reçu un avertissement. Nos entretiens montrent que les opérateurs sont réticents à installer SORM, et ce pour quatre raisons principales. La première est d'ordre économique : pour les petits et moyens ISP, il est souvent plus facile et moins coûteux de payer des amendes (environ de 30 000 à 50 000 roubles) que d'acheter des solutions SORM. La deuxième raison est d'ordre infrastructurel – selon Mikhail Klimarev, directeur de la Société pour la protection de l'Internet :

> *Les infrastructures préexistantes sont parfois incompatibles avec les nouveaux équipements que des « institutions très compétentes » voudraient faire mettre en place par les FAI. Pour installer ces équipements, le FAI doit changer fondamentalement les architectures de réseau, et remplacer des installations très coûteuses.*

La troisième raison, qu'on a déjà brièvement mentionnée, est d'ordre technique : l'enregistrement et le stockage du trafic crypté (TLS 1.3) sont inefficaces pour les objectifs d'interception légale, car la plupart du trafic est impossible à lire. La dernière raison est d'ordre opérationnel, puisque dans la plupart des cas, lorsqu'une enquête est en cours, les agents du FSB se rendront plutôt directement chez le FAI pour demander des informations sur un client spécifique, ou ils utiliseront d'autres moyens pour recueillir des informations, par exemple les écoutes manuelles, la saisie d'équipement ou d'appareils, le piratage de comptes, etc.

Les exigences de SORM sont donc largement contestées par les opérateurs, principalement en raison des coûts financiers et des complications techniques que les FAI doivent supporter, et en raison de l'inefficacité perçue de ces exigences bureaucratiques *top-down*. Ils sont également considérés par de nombreux acteurs interrogés comme une source potentielle de corruption, d'abord en raison de l'architecture même des systèmes SORM. On se rappellera que SORM se compose de deux éléments principaux : l'un est le terminal installé dans le bureau d'un « curateur » régional du FSB qui permet un accès direct et à distance au trafic de tous les FAI dans sa juridiction

territoriale. L'autre élément est le système de stockage du trafic installé chez les ISP. Pendant longtemps, le terminal de contrôle à distance n'était pas interopérable et ne pouvait se connecter qu'aux systèmes de stockage du même fournisseur :

> *Le FAI est pris entre deux feux. Pour stocker les informations sur le client, le système de stockage installé par le fournisseur doit comprendre les commandes du terminal qui se trouve chez le FSB. Dans les premières années, chaque bureau territorial du FSB disposait d'un terminal d'un fournisseur très spécifique [tels que] Norsi-Trans à Nizhny Novgorod, Spectech à Saint-Pétersbourg, etc. Ce n'est qu'après la certification de SORM-2 que les terminaux sont devenus universels et interopérables.*

Ainsi, le manque d'interopérabilité susmentionné entre les terminaux et le reste du système a conduit, pendant plusieurs années, à un quasi-monopole d'un fournisseur spécifique sur un territoire donné. De plus, le lien entre les fournisseurs de SORM et le secteur de la Défense conduit à « l'opacité et la relative inaccessibilité du marché SORM », comme l'a décrit l'un de nos répondants, le directeur technique d'un fournisseur de solutions DPI.

Des entités telles que l'Association des FAI alternatifs tentent de mener une enquête antitrust. Son directeur déclare que

> *nous essayons de montrer que le prix de cet équipement est trop lourd, nous allons déposer une plainte collective pour contester le prix du SORM, afin que le FAS (le Service fédéral antitrust) compte précisément les parts de marché, leurs revenus, leurs dépenses... vérifie le coût des différents éléments. Certains collègues FAI ont décortiqué ces boîtes. Ils en ont déduit environ 90% des bénéfices... Yarovaya a permis à un petit groupe d'entreprises de vraiment profiter.*

C'est ainsi que naissent aussi des figures de « nouveaux résistants », de petits entrepreneurs qui ont été profondément, et négativement, affectés par le profit de quelques-uns que la loi Yarovaya a engendré.

7.2.2. Roskomnadzor et l'offensive de blocages Web

Les lois introduisant le blocage des contenus web existent depuis 2012, avec la mise en place d'une liste noire de contenus et pages web, détenue par RKN. Nos entretiens avec les FAI montrent cependant que déjà en 2008-2009, les fournisseurs recevaient des demandes des autorités pour

bloquer l'accès à des sites web spécifiques au cas par cas, à savoir les jeux d'argent et la pornographie. L'introduction d'une liste noire centralisée a rendu plus difficile pour les FAI d'ignorer les demandes et de se défendre devant les tribunaux. Toutefois, les exigences précises n'ont été publiées qu'en mars 2018 avec la loi 149-FZ article 10, qui définit les paramètres techniques des « pages de blocage » standardisées ainsi qu'un ensemble plus défini de recommandations techniques pour le filtrage des contenus et le blocage des sites web.

À proprement parler, il n'existe pas en Russie de loi qui régule la censure, mais les lois existantes sont modifiées afin d'ajouter une responsabilité administrative ou pénale pour la publication, la diffusion ou l'hébergement de contenus considérés comme « illégaux ». Au moins huit organisations différentes peuvent décider du caractère « illégal » d'un site web ou d'une page web spécifique : le service fédéral des impôts, les tribunaux de certaines villes, le procureur général, RKN, le ministère de l'intérieur, le tribunal de la ville de Moscou, le service fédéral de contrôle des drogues et RosPotrebNadzor (une entité chargée d'inspecter les questions liées à la consommation).

Ces mesures ont initialement déclenché des controverses liées à la cooptation du système de noms de domaine (DNS). En 2012, par exemple, la bibliothèque en ligne de Maksim Moshkow a été bloquée. Moshkow, un pionnier de l'Internet russe, avait été le promoteur de plusieurs projets médiatiques d'envergure qui utilisaient l'Internet dans son pays natal (par exemple Gazeta.ru) ; Lib.ru, également connu sous le nom de *Maksim Moshkow's Library*, a commencé à fonctionner en novembre 1994 et s'est avéré être la bibliothèque électronique russe la plus grande et la plus complète. La réponse de Moshkow au blocage de sa bibliothèque a été d'utiliser la vulnérabilité du mécanisme même de la censure du web et de bloquer le principal site web du ministère de la justice. Étant donné que de nombreux FAI bloquaient automatiquement toutes les adresses IP provenant de ce qu'on appelle le « A-Record » d'un DNS sur liste noire, Moshkow a simplement dû modifier le A-record de son propre site web en ajoutant l'adresse IP du ministère de la Justice. Suivant le même principe, en 2017, un certain nombre de « guérillas » basées sur les DNS ont eu lieu, notamment, le 15 mai, le blocage d'AS Revizor, du 4 au 9 juin, un certain nombre de blocages dont OK.ru, VK.com, Rostelecom, RZD, RBC, COMODO, badoo.com, booking.com, facebook.com, mail.ru et ainsi de suite, ainsi que plusieurs serveurs racines DNS. Cette fois, les

activistes ont utilisé la liste de blocage RKN comme base de leur action : ils ont acheté quelques noms de domaine « orphelins » dont l'abonnement a expiré mais qui figuraient encore dans la liste, et ont procédé à la modification de leurs A-record respectifs. Le 6 mai 2018, Leonid Evdokimov écrit « résistance numérique » en code Morse sur les graphiques des FAI bloqués en exploitant la même vulnérabilité.

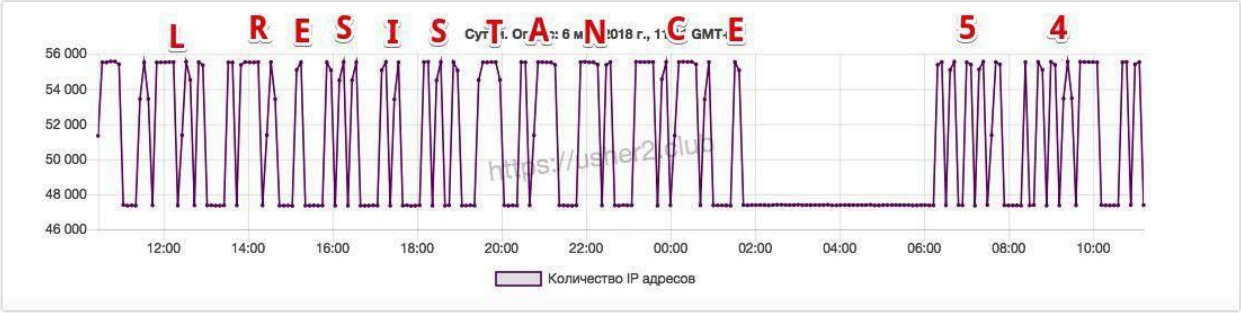

Figure 2. Le message en code Morse créé par Leonid Evdokimov (Source : https://usher2.club/)

Ces épisodes ont eu leur effet sur la réglementation et la mise en œuvre de la censure, ainsi que sur la manière dont les listes de blocage sont tenues à jour. Certaines des actions semblent même avoir été contre-productives. Par exemple, avant l'action d'Evdokimov, en avril 2018, la liste noire comptait 5136 noms de domaine orphelins qui auraient pu être utilisés pour reproduire une attaque DNS, alors que le 13 mai 2018, elle ne comptait que 204 de ces noms de domaine. Cet « effet secondaire » a été critiqué par certains de nos interlocuteurs, qui ont déclaré que les militants n'ont fait qu'aider RKN à améliorer sa gestion de la censure d'Internet.

D'autres formes de résistance impliquent les *blockpages*, placés par les FAI afin de dénoncer la censure lorsqu'une adresse particulière redirige vers un site bloqué. Comme on l'a vu plus haut, les *blockpages* étaient également utilisés pour informer les utilisateurs des raisons du blocage et des moyens de contournement, ainsi que pour exprimer une attitude critique à l'égard de la censure d'Internet et de RKN. Par exemple, certains FAI ajoutaient un lien vers la RFC 7725, une norme de l'IETF consacrée à l' « erreur 451 » (voir 7.1.3), qui est un texte particulier en soi : son nom fait référence à l'œuvre phare de Ray Bradbury *Fahrenheit 451*, alors que le deuxième paragraphe de la norme mentionne explicitement des recommandations pour utiliser Tor et le VPN afin de

contourner le blocage. D'autres FAI ont clairement affiché des déclarations critiques sur les pages de blocage. Cependant, les amendements à l'article 15.3 de la loi 149FZ, ont introduit, entre autres, un texte standardisé pour une page de blocage, ce qui a considérablement réduit la popularité de cette forme de contestation parmi les FAI.

Les activistes ont rendu la question de la censure d'Internet plus visible, notamment en rendant publiques certaines des limites et vulnérabilités des mécanismes de blocage (en cas de guérilla DNS). Les opérateurs et professionnels du web russes ont cependant dû mettre en œuvre ces mesures réglementaires, qui ont affecté leur activité, tout en remettant en cause, dans une certaine mesure, les valeurs d'ouverture qu'ils avaient pu défendre. Ils ont donc souvent adopté des stratégies différentes pour y résister et s'y adapter.

Tout comme les SORM, les « boîtes » à mettre en place sont en fait des objets hybrides et peuvent prendre différentes formes comme des scripts *faits maison* que les FAI assemblent, des solutions matérielles, des solutions basées sur le cloud ou des logiciels de blocage DPI. Les FAI peuvent donc choisir entre différentes solutions et s'appuyer soit sur le DNS, soit sur des proxy, soit sur le protocole Internet lui-même ou encore sur des techniques DPI pour filtrer et bloquer le trafic. Le directeur de SkyDNS, l'un des vendeurs proposant des solutions pour le filtrage du trafic, souligne :

> *Certains bloquaient via l'IP, d'autres via le DNS. Il y avait une sorte de vide technologique – bloquez comme vous voulez. RKN ne pouvait pas conseiller les FAI sur les solutions, de peur de tomber sous le coup des lois antitrust. Mais très vite, il y a eu plusieurs plaintes d'administrateurs de sites Web bloqués par erreur... Ils ont donc commencé à imposer le blocage par URL. Les FAI avaient l'habitude d'écrire leurs scripts de manière bricolée, mais ce n'est plus très fréquent, car ils risquent d'être pénalisés (notre entretien, 22 novembre 2018).*

Selon un FAI d'une ville de la région de Moscou (40 000 clients), le blocage manuel est devenu trop difficile à mesure que la liste de blocage s'allongeait. De plus, cette liste de blocage est souvent critiquée par les FAI en raison des multiples fautes de frappe et d'une structure désordonnée qui introduit de la confusion et entraîne des erreurs de solutions de filtrage. Une enquête informelle sur un forum de FAI montre que les méthodes les plus populaires sont le blocage d'IP et la DPI.

Dans ce contexte marqué par l'incertitude juridique et l'absence de spécifications, un marché de solutions de blocage de sites web s'est développé. Contrairement aux vendeurs de SORM, qui étaient surtout spécialisés dans le développement de solutions d'interception légale et liés aux secteurs de la défense et de la sécurité d'État, la majorité des vendeurs d'équipements de filtrage proposaient jusqu'à présent des solutions de facturation ou de contrôle parental (comme SkyDNS, Ruspromsoft ou CarbonSoft). Avec l'application progressive du blocage, les solutions de filtrage ont été introduites comme l'un de leurs services. Un plus petit nombre de sociétés, comme CyberFilter, une petite entreprise informatique offrant des solutions de filtrage, ont été créées spécifiquement pour répondre aux exigences de RKN. Nous avons identifié au moins quatorze solutions de filtrage différentes mentionnées par les FAI, soit lors de nos entretiens, soit sur des forums spécialisés. Pendant longtemps, une confusion a persisté parmi les FAI quant au choix d'un fournisseur particulier, les leaders du marché étant Carbon Reductor et SKAT selon une enquête.

Dans le but de stabiliser et d'uniformiser les procédures de blocage, et soi-disant « à la demande des FAI », RKN a procédé à un test massif de treize solutions de filtrage ou de blocage entre fin août et 2017 et fin mars 2018. Les vendeurs d'équipements destinés à la censure ont été invités à installer leur solution de blocage chez un certain nombre de FAI (entre 10 et 30 selon les équipements testés), et un laboratoire certifié a observé le fonctionnement de ces solutions pendant un mois. Le test a comparé différentes solutions de filtrage/blocage en fonction d'un certain nombre de paramètres, dont les pourcentages de contenus « extrémistes » non bloqués et d' « autres » contenus non bloqués, et a établi un classement des solutions selon la définition de « qualité » établie par ces critères. Les résultats de ces tests sont publiés sur le site web de RKN.

7.2.2.1. La controverse Revizor

Les FAI étant très nombreux, plusieurs d'entre eux ont cherché des moyens d'éviter des investissements substantiels dans les solutions de blocage/filtrage les plus coûteuses ; ainsi, le blocage entre FAI n'était pas homogène. Afin de mieux contrôler l'application uniforme de la liste noire, une autre solution technique de blocage des contenus Web a été introduite par RKN en décembre 2016, sous le label Système Automatique Revizor (AS Revizor). Les FAI ont

immédiatement perçu une connotation ironique de « Revizor » avec la pièce satirique homonyme du célèbre écrivain russe Nicolay Gogol, une comédie d'erreurs, satirisant la corruption politique étendue de la Russie impériale. L'appel d'offres pour le développement de Revizor aurait été remporté par MFI-Soft, une société également impliquée dans la production de systèmes SORM. Le coût du développement et de la production d'AS Revizor a été estimé à 84 millions de roubles.

Revizor assure l'automatisation des contrôles des FAI, sans exception, même pour les plus petits. Il se présente sous forme de boîte (contenant un routeur, un système d'exploitation intégré et un logiciel préinstallé), de machine virtuelle ou de logiciel pour Windows et Linux. Comme son code n'est pas ouvert, son fonctionnement et ses caractéristiques restent assez obscurs pour les acteurs de ce marché. Une enquête indépendante a été menée par un ingénieur pour décrire son fonctionnement réel, démontrer les failles de sécurité du système et comparer la valeur réelle de ses composants à la valeur marchande de Revizor. De plus, au-delà des problèmes de sécurité, depuis l'introduction de ce système, il y a eu quelques pannes de Revizor dues à la surcharge de la liste noire.

Avec l'ajout de Revizor et en raison des nombreux échecs de ce système, l'attribution de la responsabilité sur le marché de la censure est souvent controversée et risque de poser des problèmes. Selon Klimarev, « Supposons que je sois un petit ISP, et que j'achète le trafic pré-filtré de Rostelecom. J'installe Revizor, mais quelque chose n'est pas bloqué. Qui paie l'amende ? Rostelecom ou moi ? Rostelecom dira : 'J'ai mal configuré et mis en œuvre l'équipement au niveau local...' ». Dans ce contexte, plusieurs tendances et stratégies peuvent être identifiées sur le marché russe de la censure pour faire face aux exigences. Les vendeurs de boîtiers intermédiaires se livrent une concurrence féroce pour fournir les solutions les moins chères ou les plus efficaces, tandis que les grands FAI essaient parfois de ne pas tout bloquer afin d'attirer davantage de clients. Il peut en résulter un arrangement que l'on peut qualifier de « non-conformité dès la conception » : les vendeurs de solutions de censure commencent à faire de la publicité de systèmes intégrés qui permettent d'éviter les frais de non-blocage et de minimiser les impacts des régulateurs nationaux. Par exemple, après les blocages massifs des serveurs d'Amazon et de Google et des sites web populaires, comme effet secondaire de l' « interdiction de Telegram », l'un des fournisseurs de solutions de censure les plus populaires, Carbon Reductor, a proposé un pack qui garantissait aux

FAI la possibilité de fournir à leurs clients un accès aux plateformes populaires sans être détectés par Revizor et condamnés à une amende par RKN. Les FAI cherchent activement des moyens d'éviter de se conformer aux solutions de censure, surtout si elles impliquent des investissements substantiels de leur part, et cela fait partie de leur positionnement sur le marché.

Certains FAI s'engagent directement dans des pratiques de censure sélective afin d'en contenir les effets ou tentent de tromper le système Revizor. Selon le directeur de SkyDNS, « certains opérateurs n'appliquent la censure que sur un sous-réseau séparé, où ils installent le boîtier Revizor. Et pour leurs utilisateurs finaux, ils façonnent un autre réseau où il n'y a pas ou peu de censure ». De leur côté, les administrateurs de réseau ou les services d'hébergement se livrent à des ruses techniques qui leur sont propres ; par exemple, lorsque des adresses IP de Revizor sont identifiées, une page de blocage est envoyée en guise de réponse.

D'autres stratégies impliquent une forme de résistance juridique. Ainsi, l'organisation OrderCom apporte son soutien aux FAI qui cherchent à s'opposer aux décisions et amendes ordonnées par RKN, avec un certain succès : en 2016, 15% des décisions ont été annulées. Les FAI contestent également ce qui, selon eux, sont des erreurs dérivées de l'utilisation du système Revizor, en fournissant des copies conformes certifiées des pages bloquées. Cependant, sur 33 533 cas de décisions de justice, seuls 46 cas ont été contestés avec succès, selon une étude de Serguey Hovyadinov, un chercheur en droit et politique numériques qui a analysé les décisions de justice pertinentes entre 2012 et 2017.

7.2.3. Les coûts d'un régime de « surveillance par l'infrastructure »

L'une des principales conséquences des exigences de surveillance et de censure pour les FAI a été une augmentation de leurs coûts globaux. Selon le directeur de l'Association pour les FAI alternatifs, « Yarovaya a eu un impact substantiel [sur l'association...] [Les coûts d'équipement] sont au moins équivalents au revenu annuel d'un ISP, même sans les coûts de certification supplémentaires ». En effet, les coûts pour l'ensemble du secteur sont estimés par le FSB et le ministère des communications à environ 4,5 trillions de roubles, et par l'Union des industriels et entrepreneurs russes à 17,5 trillions.

Cela a entraîné d'importantes reconfigurations au sein du marché des services Internet, et plus particulièrement une consolidation et une centralisation croissantes des FAI commerciaux. Selon le directeur de SkyDNS,

> *nous avons vingt clients FAI qui utilisent [notre solution] Zapret ISP, et environ trois cents qui utilisent nos solutions cloud de filtrage. Nous observons une tendance : les grands, notamment Dom.Ru, absorbent les petits. Si vous avez deux ou trois mille abonnés, vous êtes un candidat sûr à l'acquisition.*

Cette situation a également entraîné une augmentation des prix des services Internet. Une étude menée auprès d'une centaine de FAI en novembre 2018 montre que 52% d'entre eux prévoient une augmentation des prix des services Internet pour l'utilisateur final ; 29% d'entre eux parlent d'une augmentation supérieure à 10%, tandis que Rostelecom montre que l'augmentation a déjà commencé à l'été 2018. Cependant, certains des FAI interrogés affirment que la loi Yarovaya elle-même n'a eu qu'un impact limité sur la hausse des prix, et expliquent cette augmentation plutôt par la crise économique et politique globale :

> *La hausse des prix est due à la crise du rouble : nous achetons des équipements à l'étranger et dépendons des taux de change des devises. Nous avons augmenté les prix de 200 % au cours des cinq dernières années, mais au bout du compte, cela ne représente qu'environ 500 roubles par mois pour un plan de base.*

Tous les fournisseurs d'accès à Internet interrogés ne sont pas d'accord sur le fait que la mise en place des « boîtes noires » a un effet direct sur le prix et la qualité des connexions Internet pour les utilisateurs russes. Selon eux, d'autres initiatives juridiques n'impliquant pas les *middleboxes* contribuent également à reconfigurer le marché en profondeur. Par exemple, la récente ordonnance n° 148 du ministère des communications oblige les FAI à fournir un « accès gratuit aux ressources socialement importantes » à partir du 1er avril 2020. La perte conséquente pour le marché des FAI est estimée à environ 200 milliards de roubles. En outre, les FAI affirment que les prix des services Internet augmentent non seulement en raison de l'équipement et de la pression réglementaire globale, mais aussi en raison de la saturation du marché et du fait qu'il est difficile pour les FAI de se développer. Le point de saturation se situe quelque part entre 2008 et 2010 selon les personnes interrogées. Ainsi, la réglementation de l'État est perçue par les FAI non pas toujours

comme le facteur clé, mais comme un obstacle supplémentaire au développement ou au maintien de leurs activités.

Un autre effet indirect probable à long terme est la menace de voir le réseau russe « coupé » de l'Internet au sens large. Le processus de centralisation a une incidence sur les relations d'échange de trafic et de transit entre les FAI : en particulier, le nombre de FAI ayant conclu des accords d'échange de trafic transnationaux diminue. Cependant, contrairement à d'autres pays qui cherchent à accroître leur souveraineté numérique (la Chine en particulier), l'infrastructure Internet russe est très étroitement liée à l'Internet mondial. Selon le directeur de SkyDNS,

> *ils essaient d'introduire des restrictions afin d'identifier certains FAI qui ont le droit de transporter du trafic transnational. MTS, TTK, NTT et d'autres... mais pour l'instant, cela ne fonctionne pas, car il y a trop d'intérêts économiques, trop d'accords internationaux et de connexions, je veux dire, en ce qui concerne les câbles, la Chine peut se permettre une balkanisation, mais pas la Russie. Nous sommes trop dépendants de l'infrastructure internationale. Cela entraînerait une dégradation catastrophique des services Internet.*

Presque tous les FAI interrogés sont d'accord avec la tendance générale à la monopolisation du service Internet par quelques grandes entreprises (à savoir Rostelecom et Dom.ru), ce qui implique davantage de dépendances infrastructurelles des petits FAI vis-à-vis des grands acteurs, comme l'obligation de leur louer des systèmes d'interconnexion, ou de payer des frais supplémentaires pour avoir le droit de connecter de nouveaux bâtiments.

7.3. La gouvernance du RuNet entre cooptations et résistances « d'infrastructure »

Un « marché de la censure et de la surveillance » florissant s'est ouvert ces dernières années pour les vendeurs russes de *middleboxes* et de solutions logicielles pour le blocage et le filtrage du trafic. Ce chapitre a analysé les débats autour de technologies controversées qui sont, grâce aux nombreuses contraintes juridiques et politiques qu'elles imposent, au cœur du marché russe de l'Internet, mais qui sont coûteuses, complexes à mettre en œuvre, et problématiques d'un point de vue éthique et politique.

Nous avons vu comment, depuis le début des années 2010, en conséquence des tensions politiques qui se sont élevées en interne et à l'étranger, la législation russe sur l'Internet s'est considérablement durcie, illustrant la volonté du gouvernement d'établir un contrôle national au sein d'une arène numérique qui lui avait jusqu'alors échappé. Ces mesures de régulation nationale du web démontrent les réponses coercitives que les autorités ont choisies face aux défis que l'Internet pose à la souveraineté, un ensemble de mesures techno-politiques et juridiques qui témoignent des efforts de la Russie pour recentrer l'Internet russe au niveau national. Dans le cadre du système politique russe, à vocation de plus en plus autoritaire, la gouvernance par l'infrastructure d'Internet prend des formes particulières, centrées sur la surveillance, la censure, l'écoute, le contrôle ; cependant, l'analyse de ces formes de gouvernance ainsi que de l'écosystème de résistances qui se déploient en conséquence et autour d'elles permet de mieux comprendre les nuances du pouvoir dans un État autoritaire à l'ère du numérique.

En effet, l'étude des infrastructures du RuNet – existantes, envisagées, souhaitées, cooptées – montre que la politique de contrôle mise en œuvre par l'État russe ne doit pas nécessairement être considérée comme suivant un modèle vertical, cohérent et hiérarchique. L'image quelque peu simpliste, que le gouvernement russe lui-même s'emploie à construire et nourrir, d'une régulation étatique qui n'a besoin que de déployer une technologie donnée pour atteindre ses objectifs de contrôle politique doit être remise en question et déconstruite. En effet, l'analyse du RuNet montre que les lois s'appliquant à l'activité en ligne sont nombreuses, variées, en constante adaptation, et leur application souvent aléatoire ou arbitraire. L'examen attentif de la législation et de son application ne montre pas une domination centralisée de l'Internet russe, mais plutôt une multiplicité de types de contrôle, partiels, fluctuants et parfois contradictoires. Comprendre la diversité des contraintes qui s'appliquent à l'Internet russe est essentiel pour comprendre les nombreuses formes de résistance, d'évasion et de contournement qui se sont développées en réaction à ces contraintes. Ces formes de résistance vont des manifestations publiques de protestation aux stratégies de contournement souterraines, intégrées aux infrastructures, en passant par toute une série de pratiques hybrides, mi-protestation, mi-arrangement technique.

La mobilisation civique russe prend notamment deux formes. La première est publique et collective, par exemple le mouvement « anti-SORM » ou les pétitions contre la loi Yarovaya. Ces

mouvements semblent avoir un impact limité, si ce n'est d'encourager la visibilité et d'attirer l'attention du public sur le problème, et même ainsi, ils restent limités à une petite partie de la population, à savoir les professionnels de l'informatique, les journalistes, les blogueurs et les militants pour les libertés de l'Internet. Cependant, au deuxième niveau, celui des tactiques d'évasion « par l'infrastructure », la mobilisation est bien plus réussie : ces techniques invisibles ou insaisissables ont un impact direct et immédiat sur les pratiques quotidiennes des utilisateurs et des professionnels de l'informatique, souvent plus que d'autres moyens de critiquer le gouvernement ou d'obtenir des changements dans la législation et la gouvernance de l'Internet. Les techniques d'évasion reposent sur un ensemble d'outils et d'arts de faire ingénieux et en constante évolution, et peuvent permettre d'accéder à ou de diffuser des contenus interdits ainsi que de poursuivre des activités économiques.

Dans ce contexte marqué par l'application des normes via un appareil techno-juridique d'une part, et différentes formes de « résistance numérique » d'autre part, il est intéressant d'observer comment la gouvernance russe de l'Internet a laissé place ces dernières années à un véritable marché de la censure et de la surveillance, qui s'inscrit dans le marché plus large des services Internet, et le remodèle en profondeur. Sur ce marché, la rationalité économique est strictement liée à l'interprétation des normes techno-juridiques, et à la capacité des acteurs à négocier, ou à être en désaccord avec, ces normes. Les FAI sont des acteurs centraux dans ce processus, devant faire face d'une part à des contraintes d'ordre juridique, mais aussi aux incertitudes liées à l'absence de certification, de normalisation et de technologie « ayant fait ses preuves », à la difficulté d'établir des responsabilités, à leur poids politique et économique relatif, etc.

La gouvernance russe de l'Internet prend de plus en plus la forme d'une bataille infrastructurelle, une dialectique entre le gouvernement, qui utilise et coopte l'infrastructure, et les utilisateurs, développeurs et fournisseurs qui la détournent et la reconfigurent, dans une co-construction constante du droit et de la technologie. Les révélations de Snowden ont certes constitué « l'excuse parfaite » pour la tentative du gouvernement russe d'imposer une approche radicale de souveraineté numérique (Nocetti, 2015). Cependant, elles sont aussi devenues d'une part un catalyseur de la mobilisation des militants des libertés numériques, non seulement pour les *power users* mais pour les pratiques quotidiennes situées des utilisateurs lambda, et d'autre part une

opportunité pour les acteurs technologiques de l'Internet russe, de se battre à la fois de l'intérieur et de l'extérieur du pays. Si les infrastructures d'Internet peuvent être assez facilement cooptées pour des objectifs politiques, elles se prêtent également à être saisies et mobilisées pour s'opposer à cette cooptation -- et, comme a pu le dire autrefois le pionnier de l'Internet David Clark, « *route around it* ».

Chapitre 8. Conclusions

Nous arrivons maintenant à la fin de ce voyage dans la gouvernance par l'infrastructure d'Internet. Tout au long de ce travail, j'ai souhaité montrer comment des « pièces » d'Internet, des composantes critiques (critiques du fait de leur rareté au sein de l'écosystème Internet, ou de leur potentiel d'« objet-frontière ») sont investies pour en faire des instruments de gouvernance, et comment cet ensemble de processus transforme aussi bien les pièces en question, que les pratiques (et les objectifs initiaux) de gouvernance.

A travers une discussion initiale des différents niveaux auxquels opère l'interaction entre infrastructures, contrôle et autorité, puis au fil des cas d'étude, on a vu comment les enjeux de gouvernance d'Internet sont souvent inscrits dans les technologies et les infrastructures elles-mêmes, dont les choix de conception, de développement et d'implémentation technique deviennent des outils stratégiques pour l'appropriation et le maintien du pouvoir, dans ses multiples facettes de contrôle, d'autorité, de régulation : comme l'a résumé de façon efficace Susan Leigh Star, « on crée des métaphores – des ponts entre différents mondes. Le pouvoir concerne quelle métaphore, la métaphore de qui, ramène ces mondes ensemble, et les maintient ainsi » (Star, 1990, ma traduction). J'ai montré comment, avec des configurations variées, la gouvernance d'Internet est une question d'alliances et de confrontations, le plus souvent mouvantes, entre de multiples acteurs, qu'il s'agisse d'institutions, d'entités provenant de la « société civile », individus ou organisations, en passant par le secteur privé. Enfin, j'ai montré comment les infrastructures sont des systèmes normatifs interagissant de façon constante et évolutive avec d'autres systèmes normatifs, qui se superposent, se confrontent et s'affrontent, qu'il s'agisse du droit ou de la loi du marché en passant par les normes, souvent *bottom-up* et partiellement implicites, façonnées par des communautés de pratique particulières.

Ce chapitre conclusif a notamment deux objectifs. En premier lieu, il s'agit de « tirer les fils » des différents cas d'étude en proposant une typologie des dispositifs et systèmes de gouvernance par l'infrastructure, qui permette d'illustrer de façon panoramique l'objectif central de ce mémoire, montrer comment des composantes d'Internent sont investies pour en faire des instruments de

gouvernance, et les effets de cette action à la fois pour ces dispositifs et pour les pratiques, et les objectifs initiaux, de gouvernance. Le reste du chapitre présentera en revanche les directions de recherche ouvertes par ce mémoire, qui incluent la relation entre la gouvernance par l'infrastructure et la gouvernance des contenus en ligne, le « dialogue » constant entre infrastructures de contrôle et de résistance qui marque l'internet d'aujourd'hui, ou encore la question de la souveraineté numérique et la mesure dans laquelle s'y déploient peut-être, comme problème public pour des acteurs différents, de nouveaux enjeux de gouvernance par l'infrastructure.

8.1. Vers une typologie des « formes d'action » de la gouvernance par l'infrastructure

Avec ce mémoire, j'ai souhaité revenir sur l'une des grandes questions des études d'infrastructure – la mesure dans laquelle les artefacts techniques « *have politics* » – en me penchant sur le cas de la gouvernance infrastructurelle d'Internet, dans ses effets systémiques, prêtant attention à ses matérialisations à des niveaux multiples (Edwards, 2003). J'ai proposé une façon de penser les différentes dimensions politiques présidant à la conception et à la mise en place des infrastructures d'Internet, mais aussi de dévoiler les manières dont le politique et les politiques s'inscrivent dans les composantes infrastructurelles de l'Internet, et sont coproduits par leur biais. En comprenant les agencements et pratiques techniques comme créateurs d'objets, de relations et de régimes politiques (Mitchell, Charbonnier & Vincent, 2018), il est possible, au croisement de la sociologie de l'action et des études de la gouvernance (voir Pinson, 2015) de penser les « formes d'action politique » de l'Internet d'aujourd'hui et de l'histoire récente.

Les cas d'étude que j'ai analysés au fil de ce mémoire montrent à quel point les outils numériques en réseau, souvent qualifiés d'immatériels ou de virtuels, possèdent toujours une matérialité « câblée et architecturée » (Jarrige et al., 2018). Cette matérialité est certes liée à du béton et à des tuyaux (Marquet, 2018 ; Chatzis *et al.*, 2017), mais elle se joue également à d'autres niveaux, encore moins visibles pour les usagers (ou tout de moins pour certains groupes d'usagers) mais porteurs de problématiques directement liées à des conceptions techniques et donc politiques. Dans

ce travail, j'ai montré comment les infrastructures informationnelles des réseaux numériques sont contraintes, propulsées par des choix et des aspects techniques qui non seulement influencent les usages, mais ont été créés, développés ou investis pour gouverner Internet. Entre le *hardware* (machinique, physique, industriel) et le *software* (logiciel, codé), ce travail appelle à une requalification des infrastructures d'Internet en rapport avec le type de prise qu'elles offrent aux acteurs de sa gouvernance, aux arrangements qu'elles contribuent à rendre possibles ou à contraindre, aux programmes politiques qu'elles se trouvent à incarner :

> *Serveurs, systèmes, plateformes, logiciels ou interfaces informatiques, tracés des routes, goudron ou signalisation : quelle est donc l'extension technique de l'infrastructure et quelles nouvelles relations instaure-t-elle avec le corps social ? Comment dès lors conçoit-on et circonscrit-on l'action des infrastructures, quand le potentiel transformateur du complexe infrastructurel – qui peut modeler et être modelé par les structures sociales – est pris en compte ? (Jarrige, Le Courant et Paloque-Bergès, 2018).*

Ce travail a interrogé conjointement les effets structurants des infrastructures, leurs échelles d'intervention, et les effets induits par leur « matérialité » hybride telle qu'on a pu la définir plus haut et dans le troisième chapitre de ce mémoire. Dans cette section conclusive du mémoire, en suivant Winner (1993) et son invitation à distinguer des genres de technologies qui permettent des genres de politiques, je souhaite apporter un complément et une récapitulation à l'approche par cas déployée lors des chapitres empiriques, afin de proposer une typologie des formes d'action inscrites dans les dispositifs et systèmes de gouvernance par l'infrastructure. En effet, ce mémoire a montré plusieurs exemples de la complexité et de la variété des processus de normalisation, de production et de gestion de l'Internet, par l'Internet : le nombre d'acteurs concernés se multiplie, les procédures deviennent plus participatives et granulaires. Ainsi, il n'est guère surprenant que plusieurs auteurs aient tenté non seulement de décrire, mais de systématiser, catégoriser et « typifier » les différentes dynamiques sociopolitiques et sociotechniques qui permettent ces processus, afin de faire avancer une évaluation critique de leur signification et impact politiques réels. Ces travaux ont en commun la priorité de développer des outils empiriques et méthodologiques permettant aux chercheurs de catégoriser la « réalité » de la théorie et des définitions liées à un processus spécifique. L'accent est souvent mis, dans ces travaux, sur la dimension procédurale dans une tentative d'interprétation, de comparaison et de mesure des différentes entités qui interviennent dans le processus.

En raison de la nature multidimensionnelle et distribuée du domaine qu'ils étudient, les spécialistes de la gouvernance de l'Internet et d'objets et dynamiques annexes se sont également engagés dans plusieurs efforts de systématisation. Par exemple, les dynamiques constitutives de la production par les pairs sur les plateformes numériques, telles que la participation en ligne et le *digital labor*, ont fait l'objet de typologies qui ont cherché à étoffer les différentes dimensions des conditions de travail en ligne (Fuchs et Sandoval, 2014), ou des entreprises sociales et « formelles » et les « publics organisés » impliqués dans des dynamiques de participation sur Internet (Fish et al., 2011). Ou encore, la typologie des processus délibératifs en ligne d'Archon Fung (2006) a montré comment ces processus s'articulent autour de trois dimensions à la fois sociales, politiques et techniques : la sélection des participants, les interactions communicatives entre acteurs et l'évaluation des « niveaux » d'autorité entre les participants (Fung, 2006). J'ai contribué pour ma part à des efforts de systématisation du champ avec Romain Badouard, Cécile Méadel et Laurence Monnoyer-Smith, en proposant un ensemble de catégories permettant une codification et une étude comparative des processus de production de normes dans la gouvernance de l'Internet, dans le but d'analyser les différentes manières dont les acteurs relèvent le défi de la multipolarité en adaptant leurs procédés de prise de décision (Badouard et al., 2012), et avec Mélanie Dulong de Rosnay, en proposant une catégorisation des plateformes de production entre pairs, dans l'objectif de démêler « en pratique » des concepts tels que l'économie du partage, la participation et les communs numériques et systématiser les facteurs qui structurent la construction de la valeur collective sur ces plateformes (Dulong de Rosnay & Musiani, 2016).

Si une approche typologique ne peut et ne doit pas remplacer – pour des raisons qu'on a cherché à souligner tout au long de ce mémoire – les efforts monographiques de dévoilement et d'analyse des détails des « pratiques situées » de la gouvernance d'Internet au cas par cas, il peut être utile d'y avoir recours temporairement dans ce chapitre conclusif pour mieux faire ressortir une vue d'ensemble de comment chacun de ces cas produit une définition de gouvernance – et différents registres et pratiques de justification de la gouvernance. Le tableau qui suit proposera cette vue d'ensemble uniquement pour un échantillon des cas qui ont été examinés lors des précédents chapitres, mais se prête à être utilisé pour la systématisation d'autres cas de « gouvernance d'Internet par l'infrastructure ».

	Enjeu de gouvernance	Type de pratique ou action	Acteurs impliqués	Technologies impliquées	Conséquences envisagées de l'action infrastructurelle	Conséquences indirectes et/ou effets secondaires de l'action infrastructurelle
Rojadirecta **Dajaz1**	Appliquer la propriété intellectuelle en ligne	Application des droits de propriété intellectuelle par le Domain Name System (DNS)	*Intellectual Property Enforcement Coordinator* (IPEC), USA *Immigration and Customs Enforcement* (ICE), USA *National Intellectual Property Rights Coordination Center* (NIPRCC) Ministère de la Justice (Department of Justice, DoJ) Opérateurs de registre DNS (ex. Verisign) Opérateurs de site web Utilisateurs	Domain Name System (DNS), l'« annuaire » d'Internet	Couper la connexion entre le nom de domaine d'un site web ciblé (car accusé de contrefaçon ou piratage) et son adresse IP correspondante Redirection de la connexion de l'utilisateur vers une page web gouvernementale expliquant la saisie. Le contenu du site web présumé en infraction étant inaccessible via son nom de domaine, les agents procèdent à la procédure de confiscation civile	Inversion de la charge de la preuve et restriction préalable Coûts élevés en cas de contestation Menace pour la liberté d'expression/ création de précédents de censure sur le Web Menace à l'universalité des noms de domaine Menace pour la sécurité d'Internet (incompatibilité avec les extensions de sécurité DNSSEC) Inefficacité (contournement ou remplacement possible, voire facile pour certains acteurs)
P2P-DNS	Construire un système de gouvernance décentralisé qui soit efficace	Construction d'une alternative décentralisée au DNS	Peter Sunde (ex-développeur, The Pirate Bay) WikiLeaks Développeurs universitaires Développeurs-entrepreneurs Utilisateurs	Domain Name System BitTorrent	Création de racine alternative, ou création du nouveau nom de domaine de premier niveau .p2p, ou remplacement du DNS par mécanisme basé sur BitTorrent Contourner ou éliminer la fort hiérarchisation du système actuel	Manque d'unicité : même nom peut faire référence à deux fichiers complètement différents, il peut être enregistré par deux entités différentes, et faire référence à des contenus complètement différents Coopération entre acteurs comme nécessaire précondition Longue coexistence entre systèmes nécessaire
Bitcoin-Fork	Préserver l'intégrité d'un système technique (et la confiance des utilisateurs)	Résolution techno-politique de la scission (fork) involontaire entre deux versions de la blockchain sous-tendant Bitcoin	Développeurs de Bitcoin (en particulier : Gavin Andresen, Vitalik Buterin, Arvind Naranayan) Utilisateurs des versions 0.7 et 0.8 du logiciel de minage bitcoind Pools de minage (en	Bitcoin Bitcoind (implémentation de Bitcoin, versions 0.7 et 0.8) BerkeleyDB (base de données) LevelDB (base de données) Canal IRC bitcoin-dev	Négociation d'une nouvelle norme pour réorganiser les opérations de Bitcoin en une seule et unique *blockchain*	Testing des défaillances du système (p. ex. avec double dépense) Choix de supporter une version de la blockchain plutôt que l'autre (à l'avantage de certains acteurs et au détriment d'autres) Centralisation humaine pour rééquilibrer

			particulier : BTCGuild, Slush)			décentralisation technique Acteur « puissant » en termes de puissance de calcul est capable à lui seul de stabiliser la controverse
Bitcoin-MtGox	Gérer la défaillance d'un intermédiaire économique et technique important	Défaillance et fermeture de MtGox	Jed McCaleb (créateur de MtGox) Mark Karpeles (racheteur de MtGox) Dwolla (e-business de transfert d'argent) Mutum Sigillum LLC (filiale de MtGox) Utilisateurs de ces services	MtGox (plateforme d'échange de bitcoins depuis 2010) Écosystème d'intermédiaires techno-économiques Bitcoin (Dwolla, filiales MtGox) Attaque par déni de service (DDoS)	Isoler un intermédiaire techno-économique défaillant de l'écosystème Bitcoin afin d'en assurer la pérennité	Incertitudes sur la gouvernance ne concernent pas le cœur du système (blockchain), mais l'un des intermédiaires/interfaces techno-économiques Difficulté de compréhension du niveau auquel se situe le problème (et tentative de la part de MtGox d'attribuer la responsabilité de sa défaillance à une faiblesse inhérente à Bitcoin) Nécessité de restaurer la confiance dans le marché, par le biais d'une confiance restaurée dans l'infrastructure qui la soutient
Protocole Signal	Adaptation d'un protocole technique à plusieurs applications	Réimplémentation du protocole de chiffrement Signal dans l'application homonyme et dans d'autres applications de messagerie sécurisée	Entreprise Open Whisper Systems (puis Signal Messenger LLC), créateurs du protocole puis de l'application Signal Développeurs du protocole Signal (en part., Moxie Marlinspike) Développeurs d'applications utilisant le protocole Signal (p.ex. Wire, ChatSecure) Autres développeurs (p.ex. Briar) Organismes de standardisation (p.ex. IETF)	Protocole de chiffrement Signal Autres protocoles de chiffrement (PGP, OTR, OMEMO) Application Signal Applications qui implémentent le protocole SIgnal (Wire, ChatSecure) Applications qui implémentent d'autres protocoles (Threema, Telegram, Briar)	Centralisation architecturelle délibérée de composantes spécifiques de leur protocole de la part de l'équipe Signal Stabilisation du protocole Signal comme un « standard de facto » dans le domaine de la messagerie sécurisée de bout en bout	« Boucle de rétroaction » : stimulés par les innovations de Signal, les protocoles plus anciens ont été remis à neuf, et de nouvelles normes sont maintenant discutées dans le but d'apporter certaines de ces propriétés à une forme documentée et stabilisée Institutions de standardisation « classiques » (p. ex. IETF) s'interrogent sur leur rôle à l'ère de la 'standardisation de facto'
SORM	Surveiller la circulation de contenus	Mise en œuvre d'un ensemble de mesures d' « interception légale » auprès de	Service de sécurité fédéral russe (FSB) Service fédéral de supervision	Deux composantes techniques : « extracteur » (équipement –	Permettre aux services gouvernementaux Russes d'accéder aux	Trop grande autonomie aux acteurs de la surveillance (station de contrôle est à

		fournisseurs d'accès à Internet sur le territoire national russe	des communications (Roskomnadzor ou RKN) Fournisseurs d'accès à Internet (FAI) Fabricants d'équipements de surveillance Professionnels de l'informatique Organisations de défense des droits de l'homme Cour suprême Utilisateurs de l'Internet russe	logiciel et matériel – qui effectue l'extraction des données) et la « station de contrôle à distance » Equipements de stockage de données et métadonnées (auprès des FAI)	communications privées par téléphone et sur Internet, à des fins de surveillances et de censure	distance, pas de décision de justice nécessaire) Coûts excessifs et imprévus pour les FAI (qui doivent changer tous leurs équipements), accroissement d'inégalités parmi les FAI selon leur taille Conséquences négatives pour les utilisateurs (qualité de la connexion, vitesse du transfert de données, prix des services Internet)
Revizor	Censurer des sites Web	Mise en œuvre d'une solution technique de blocage des contenus Web (décembre 2016, Russie)	Organisations gouvernementales/fédérales russes qui peuvent décider du caractère « illégal » d'un site ou page web : le service fédéral des impôts, les tribunaux de certaines villes, le procureur général, RKN, le ministère de l'intérieur, le tribunal de la ville de Moscou, le service fédéral de contrôle des drogues et RosPotrebNadzor (une entité chargée d'inspecter les questions liées à la consommation) Vendeurs d'équipements de filtrage (p. ex. Carbon Reductor, SkyDNS, Ruspromsoft ou CarbonSoft) FAI Utilisateurs de l'Internet russe	Revizor : solution de blocage de contenus web qui assure l'automatisation des contrôles des FAI, sans exception. Boîte contenant un routeur, un système d'exploitation intégré et un logiciel préinstallé, de machine virtuelle ou de logiciel pour Windows et Linux Code non ouvert	Mieux contrôler l'application uniforme de la « liste noire » de sites web qui publient, diffusent ou hébergent des contenus considérés comme « illégaux »	Plusieurs failles de sécurité du système démontrées Valeur réelle des composants de Revizor faible si comparée à sa valeur marchande En conséquence des échecs, attribution de la responsabilité sur le marché de la censure est souvent controversée (qui paie les éventuelles amendes ?) Stratégies de contournement et résistance possibles et répandues Arrangements de « non-conformité dès la conception » : les vendeurs de solutions de censure commencent à faire de la publicité de systèmes intégrés qui permettent d'éviter les frais de non-blocage

De cette vue d'ensemble, plusieurs idéaux-types de forme d'action de gouvernance par l'infrastructure peuvent être élaborés :

- *Répression* par l'infrastructure. Il s'agit d'un ensemble d'infrastructures dont l'objectif affiché est celui d'appliquer des mesures contraignantes pour les pratiques d'un ou plusieurs groupes d'acteurs. Les infrastructures ont été soit créées *ex nihilo*, soit reconfigurées pour ces objectifs. Le plus souvent, la responsabilité de la création de ces infrastructures et de leur mise en œuvre repose de manière importante sur les fabricants d'équipements et sur les fournisseurs de service, mandatés par des entités gouvernementales ou étatiques. Les actions exercées via ces infrastructures entraînent souvent des « effets secondaires » importants pour la stabilité et la sécurité de l'Internet ou d'une de ses composantes, notamment où la reconfiguration des fonctions de ces infrastructures mette à l'épreuve leur intégrité ou les rende plus vulnérables à des défis juridiques ou techniques spécifiques.
- *Contournement/détournement* par l'infrastructure. Dans ces cas, l'action infrastructurelle s'exerce comme réponse à la répression. Les infrastructures sont utilisées comme instrument de contournement des mesures contraignantes ; parfois elles sont créées spécifiquement, mais le plus souvent elles sont détournées ou réappropriées – il s'agit souvent des mêmes infrastructures utilisées précédemment ou parallèlement à des fins répressives, dont des groupes d'acteurs particuliers parviennent à trouver des failles ou des faiblesses. Du fait que la recherche de ces faiblesses et leur exploitation active nécessite souvent d'une expertise technique pointue, les acteurs protagonistes de ces formes d'action sont très majoritairement des professionnels de l'informatique, à la fois développeurs, industriels et entrepreneurs, occupant des rôles variés mais qui impliquent généralement la prérogative de mettre à profit leur expertise « en pratique » (opérateurs de réseau, fabricants, hackers…)
- *Standardisation* par l'infrastructure. Pour cet ensemble d'infrastructures, on peut identifier une caractéristique commune – il s'agit de technologies qui sont en mesure de devenir la norme dans un champ particulier de l'innovation sur Internet, non pas par des processus de normalisation institutionnelle, mais parce qu'un consensus informel s'établit progressivement, via les pratiques de codage et les discussions au sein de communautés spécifiques, sur leur validité comme « point de référence ». Les acteurs centraux de ces

« formes d'action » sont majoritairement des développeurs, dont les points de divergence – en termes non seulement de choix techniques, mais aussi de modèles d'affaires ou de communautés de gouvernance idéales – ressortent avec force autour des négociations pour et autour des infrastructures. Les discussions et actions autour de ce type d'infrastructures, bien que se situant largement dans le domaine de l'informel et de l' « activité quotidienne » des développeurs, ont par ailleurs des conséquences de taille par rapport à l'évolution des grandes institutions de standardisation, qui ne sont pas insensibles à ce qui se passe dans ces espaces « aux interstices » et prennent des initiatives pour construire des ponts qui les en rapprochent.

- *Réparation/maintenance* par l'infrastructure. Un quatrième et dernier groupe de démarches « par l'infrastructure » sert des objectifs de maintien ou de rétablissement de la confiance dans l'infrastructure elle-même ou de sa crédibilité, voire de mise en œuvre d'un ensemble de pratiques de réparation, de maintenance ou de « *care* » afin de rétablir une stabilité ou une qualité de l'infrastructure qui avait été compromise ou endommagée par une action précédente (Henke & Sims, 2020). Ces « formes d'action », si elles montrent la nécessité d'un large consensus afin de légitimer l'action, révèlent également et régulièrement l'existence d'acteurs « plus centraux que d'autres » dans les processus de maintenance et de rétablissement de la confiance, acteurs qui disposent généralement de ressources matérielles et logicielles importantes au sein de l'infrastructure. L'analyse de ces formes de gouvernance passe par une identification et une explicitation des composantes « techniques » et des composantes « humaines » de la confiance envers les outils numérique, et une compréhension de comment ces niveaux s'enchevêtrent.

De la « mise à l'épreuve » de cette typologie par rapport à nos cas d'étude, on retiendra notamment trois conclusions :

- Dans chaque cas ou configuration où s'opère une gouvernance par l'infrastructure, il faut conduire un travail d'identification et d'explicitation afin de comprendre ce qui, précisément, est « saisi comme infrastructure ». S'agit-il d'un élément ou d'une composante déjà identifiée et clairement établie ? S'agit-il de quelque chose qu'il faut identifier ou « infrastructuraliser » (Karasti & Blomberg, 2018) ? S'agit-il d'un élément

qu'il faut rajouter à une infrastructure par ailleurs stabilisée ? S'agit-il d'un élément à reconfigurer pour un objectif jusque-là inédit par rapport à cette infrastructure ?

- Dans chaque cas, c'est le *sens même* du mot et de la pratique de gouvernance qui change. Chacun de ces cas produit une définition de gouvernance, de pourquoi il faut gouverner, de comment on doit (ou on peut) gouverner – définition qui n'est pas surplombante mais qu'il faut tirer des cas. Comme anticipé lors de mon introduction, si ce mémoire discute constamment de *ce* qu'on fait et on étudie quand on étudie la gouvernance d'Internet, il est contre-productif de chercher à « trancher » en en donnant une seule et même définition englobante ou inclusive ; au stade actuel du développement de la gouvernance d'Internet en tant qu'arène de pratiques et domaine d'étude, il convient plutôt de noter qu'une pluralité de définitions ressortent de différents lieux – physiques, logiciels, géographiques – de l'enquête sociologique.
- Il faut cependant souligner que, même si cette démarche ne permet pas d'aboutir à une définition de gouvernance et d'Internet, elle permet d'aboutir à un ensemble de définitions qui sont, elles, très précises à chaque fois. L'exploration détaillée de plusieurs sites où les infrastructures d'Internet sont controversées, détournées, appropriées, revendiquées est *de facto* un moyen d'enquêter sur ce qu'est « Internet » et sa « gouvernance », dont les périmètres se négocient au cas par cas.

8.2. La recherche comme actrice de la gouvernance d'Internet

Le point de conclusion de la section précédente amène une autre interrogation : à quel point peut-on faire le lien entre des problèmes soulevés par les acteurs concernés par la gouvernance d'Internet au sens large, les débats publics à ce sujet, et les problématisations qui en sont faites dans le monde académique ? Au cours de ce mémoire, j'ai abordé cette question à plusieurs reprises, et il est désormais temps de réaffirmer toute son importance. Dans un domaine mouvant comme celui de la gouvernance d'Internet, ses chercheurs contribuent à le construire par leur action. En se focalisant sur tel ou tel point ou sujet, les spécialistes de gouvernance d'Internet contribuent à le faire exister comme problématique. Ils sont partie intégrante des processus de

négociation et de controverse liées à Internet et ses enjeux de pouvoir – qui, comme on l'a vu, sont performatifs, dans la mesure où ils impliquent et sont impliqués dans la création de mondes dans lesquels des modes de gouvernance spécifiques ont du sens (Ziewitz et Pentzold, 2014).

Les recherches dans le domaine de la gouvernance d'Internet sont souvent engagées dans le politique, ou adjacentes aux processus politiques. Si la « *policy-engaged research* » n'est pas née avec la gouvernance d'Internet – les recherches en urbanisme, par exemple, entretiennent un rapport étroit avec les communautés de pratique liées à leur objet – les chercheurs sur la gouvernance de l'Internet ont assez vite montré non seulement leur intention de s'attaquer à des « problèmes du monde réel », mais aussi d'être attachés à l'opportunité de contribuer à la création d'une base de résultats, de concepts et de preuves susceptibles d'informer les décisions politiques. Les chercheurs sont activement impliqués, depuis la création de ces institutions, en tant que participants aux groupes de travail de l'ICANN, ou de l'IETF (qui a une véritable « branche recherche », l'Internet Research Task Force), contribuant aux initiatives d'établissement de normes, exerçant leurs activités d'enseignement et de recherche en parallèle avec l'engagement politique, servant de conseillers aux décideurs politiques et parfois de consultants auprès de l'industrie. Ce rôle « translationnel » et pragmatique de certains chercheurs en gouvernance d'Internet trouve des échos dans l'engagement des scientifiques au sein d'autres domaines et disciplines d'actualité qui s'attaquent aux grands problèmes de la société contemporaine – l'environnement en tout premier lieu (voir De Pryck, 2022).

Le fait que cette communauté de chercheurs continue, quinze ans après sa création, à tenir la conférence annuelle de son réseau phare, le *Global Internet Governance Academic Network*, le jour qui précède l'inauguration du FGI, c'est-à-dire l'une des rencontres les plus importantes et historiques pour les praticiens de la gouvernance d'Internet, est à la fois un symbole et une incarnation régulière de cette prise de conscience. Les lieux, matériels et virtuels, où s'exerce la gouvernance d'Internet sont des points de contrôle politiques ; les recherches sur ces conflits comportent ainsi un élément normatif explicite dans la posture des chercheurs – qui commence par le choix même de ce qu'il faut étudier au sein de l'ensemble de pratiques qui constituent la gouvernance de l'Internet.

Sans surprise, les initiatives politiques ont à leur tour directement engagé des chercheurs, et commandé des travaux sur des sujets spécifiques. Par exemple, la Commission mondiale sur la gouvernance de l'Internet (*Global Commission on Internet Governance*)[69], une initiative de deux ans (2014-2016) présidée par Carl Bildt, ancien Premier ministre suédois, a piloté un réseau de recherche consultatif, international et interdisciplinaire qui a produit plus de 50 articles de recherche sur plusieurs sujets, dont la cybersécurité, la fragmentation, l'accès et l'interconnexion. Ou encore, l'UNESCO pilote depuis 2015 le projet Internet Universality Indicators[70], qui engage régulièrement des chercheurs dans l'élaboration d'un cadrage conceptuel qui puisse guider un ensemble de « bonnes pratiques » relatives à la gouvernance d'Internet, et dans l'étude de l'impact de ce cadrage dans plusieurs pays en Europe et dans le monde.

Comme je l'explique plus longuement dans l'autobiographie intellectuelle qui constitue le premier volume de ce mémoire, je suis ou j'ai été moi-même engagée dans plusieurs de ces arènes de gouvernance d'Internet, de la Commission de réflexion et de proposition sur le droit et les libertés à l'âge du numérique de l'Assemblée nationale (2014-2015) à la vice-présidence de l'Internet Society France (depuis 2017), en passant par une participation au CSA Lab, l'atelier prospectif sur le numérique et l'audiovisuel du Conseil supérieur de l'audiovisuel (2016-2018) et tout récemment, par la co-rédaction d'un rapport sur la fragmentation d'Internet pour le Panel for the Future of Science and Technology du Parlement européen (publication en juin 2022). A l'ère où de plus en plus de questions relatives à l'infrastructure technique d'Internet prennent le devant de la scène politique, il semble important que le développement de la prochaine génération d'instruments de régulation de l'Internet inclue, parmi ses acteurs, des chercheurs ayant des expertises variées dans le développement, la mise en œuvre et l'évaluation des politiques de communication dans l'intérêt du public.

Quelles conclusions « politiques, pour le politique » ce statut particulier de chercheuse et actrice dans le domaine de la gouvernance d'Internet permet-il de tirer ? En premier lieu, comme Stéphane Bortzmeyer (2019) l'a aussi souligné de son point de vue d'acteur technique, il existe des sujets qui sont en priorité plus visibles pour les utilisateurs et les utilisatrices d'Internet, du fait de leur

[69] https://www.cigionline.org/activities/global-commission-internet-governance-2014-2016/
[70] https://en.unesco.org/internet-universality-indicators/roamx-indicators

proximité avec les interfaces et les contenus, et qui sont donc non seulement plus relayés par les médias, mais aussi examinés en priorité par les législateurs lorsqu'il s'agit de « réguler Internet » : la liberté d'expression sur les réseaux sociaux, les manifestations de haine et comment les freiner, la lutte aux contenus illégaux et au piratage, ou encore les politiques de confidentialité établies par les plateformes numériques. Ces questions sont largement discutées comme objet potentiel ou actuel de régulation par les États, de plus en plus souvent en sollicitant l'aide des opérateurs techniques et des services numériques, ou parfois en opposition à ces derniers.

Cependant – ce qu'un travail de recherche tel que ce mémoire souhaite contribuer à montrer – un grand nombre de points de contrôle et de pouvoir de l'Internet résident ailleurs, échappant (ou tout de moins, ne se résumant pas) au droit national ou international et aux frontières nationales, ainsi qu'à la visibilité de la part des utilisateurs… et souvent, des régulateurs. Ces dynamiques de pouvoir et de contrôle prennent forme via la conception et le développement de l'architecture technique, ou via la variété de politiques de confidentialité ou de termes d'utilisations proposés par des acteurs privés – des instruments de gouvernance globalisés qui parfois dialoguent, parfois sont en tension avec les systèmes juridiques nationaux et internationaux ainsi qu'avec des normes culturelles régionales ou territoriales, ou établies plus ou moins formellement par des communautés spécifiques. Ces pions dans les jeux de pouvoir de l'Internet vont de l'allocation des ressources Internet critiques et du développement de protocoles jusqu'aux règles d'interconnexion Internet et l'accès du « dernier kilomètre ».

La gouvernance d'Internet présente actuellement un certain nombre de questions relatives à des domaines et des instruments de gouvernance, où l'infrastructure joue souvent un rôle clé. Ces questions sont ouvertes et mouvantes. Ainsi, si ce dernier chapitre peut avoir l'ambition de tirer des conclusions politiques de mes conclusions de recherche, il ne peut le faire qu'en proposant un court « guide » qui permette de s'orienter politiquement dans ce domaine complexe, en se posant des questions dont les réponses peuvent grandement varier selon notre rôle et notre « être parties prenantes » dans l'Internet d'aujourd'hui. Quel devrait être l'équilibre entre une gouvernance d'Internet étatique, et les modes de gouvernance globale, internationale et *multi-stakeholder*, ou encore privée, qui dépassent les frontières des États ? Quel devrait être l'équilibre entre des valeurs tels que l'autonomie individuelle, la symétrie informationnelle, l'accès à la connaissance, la vie

privée, et des modèles d'affaires qui combinent la gratuité à la rétention de l'attention et à la captation des données personnelles ? Quel devrait être l'équilibre entre l'action des États, l'action des acteurs privés, et l'initiative personnelle de l'individu dans le façonnage d'espaces d'interaction et de communication en ligne qui permettent l'expression politique et culturelle ? Quel devrait être l'équilibre entre préservation de l'anonymat au niveau de l'architecture technique de l'Internet, et la possibilité pour les autorités de remonter aux auteurs d'infractions et de délits ?

Selon les réponses que chaque utilisateur d'Internet donne à ces questions, des différentes « visions du monde » liées à Internet prennent forme, ce qui se reflète et va se refléter dans le futur dans les initiatives de gouvernance, y compris par l'infrastructure. Réprimer, contourner/détourner, standardiser, réparer ou maintenir par l'infrastructure, voilà autant de formes d'action qui contribuent à informer, co-construire, structurer le quotidien politique de l'Internet ; selon les réponses qu'on donnera aux questions ci-dessus, la stabilité et la sécurité d'Internet d'un côté, les libertés numériques de l'autre, auront des futurs politiques différents.

****

En conclusion de ce mémoire, la deuxième partie de ce chapitre présentera un certain nombre de questions clé qui ont trait à la gouvernance de et par les infrastructures Internet, qui sont à la fois des façons dont la gouvernance d'Internet elle-même est en train d'évoluer en pratique, et un début de projet pour l'étudier. Dans les pages qui suivent, je vais esquisser un agenda pour les recherches qui concernent ou peuvent concerner ces objets et ces dynamiques dans un futur proche, en montrant comment les perspectives et les cas d'étude présentés jusqu'ici fournissent une base pour « penser la gouvernance d'Internet à partir de ses infrastructures ».

8.3. La gouvernance de et par l'infrastructure se rapproche de la gouvernance des contenus

A l'heure où je commençais à écrire ce mémoire, à la fin de juin 2020, la loi dite Avia, plus précisément la « loi du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet »[71], venait d'être promulguée par le Président de la République française, après un an de discussions parlementaires acharnées et une censure, de la part du Conseil constitutionnel, de plusieurs dispositions jugées inconstitutionnelles du fait de leur atteinte « disproportionnée » à la liberté d'expression. Au centre de la polémique, la possibilité que des décisions de retrait de contenus en ligne puissent être prises par un opérateur privé sans intervention d'un juge. La loi Avia est avec toute probabilité l'exemple le plus important, dans l'actualité récente de la politique française, de comment aujourd'hui, l'une des questions les plus brûlantes de la politique par rapport à Internet est de mettre en œuvre des réponses réglementaires pour contrôler les contenus qui circulent sur Internet. Pour les décideurs, il est question d'améliorer la sécurité sur Internet, de faire face à des problèmes telles que la cyberintimidation, les discours de haine, la désinformation ou la violation du droit d'auteur, ou encore d'assurer la protection des données dans une variété de contextes.

Le moment présent, avec les nombreuses « gouvernances par l'infrastructure » qu'on a observées dans ce mémoire, ouvre une dynamique intéressante à observer pour les chercheurs en gouvernance d'Internet. En effet, pendant un temps relativement long, les questions liées à la régulation des contenus ont été traitées comme étant séparées de façon assez nette des questions propres à la régulation des couches physique et logicielle de l'Internet, et comprises notamment comme des questions de régulation des comportements et des usages des internautes. Cette régulation prenait deux formes. D'un côté, elle restait, pour la plupart, assez désincarnée des dispositifs techniques que les usagers ont à leur disposition ; si on prend l'exemple du partage de contenus dits « illégaux » explosée au début des années 2000, par exemple, la stratégie choisie par les décideurs a été de démotiver les individus à pirater en leur montrant la « bonne voie », et donc de créer des certificats susceptibles de légitimer les contenus autorisés ; on rappellera par exemple le « label PUR » proposé par l'Hadopi[72]. D'un autre côté, et à l'extrême opposé, la stratégie a été de s'attaquer à un dispositif technique, en lui-même et dans son ensemble, alors que l'objectif véritable était de s'attaquer à certains contenus supposés déviants partagés par le biais de ce dispositif ; on rappellera par exemple les tentatives, tels que la « riposte graduée », de minimiser

[71] https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b2062_rapport-fond.pdf
[72] https://www.hadopi.fr/en/node/3686

voire interdire les échanges *peer-to-peer* dans leur ensemble, en faisant l'hypothèse que les contenus partagés étaient sans doute illégaux. Cette régulation était par ailleurs très focalisée sur la responsabilité individuelle de l'internaute, sur la connaissance précise de ses actions et de leurs conséquences ainsi que des attributs et caractéristiques de ses équipements informatiques.

Avec les différents phénomènes de régulation et de modération qui ont vu le jour au cours de ces dernières années (et qui sont très bien présentés par Badouard, 2020), la gouvernance par l'infrastructure et la gouvernance des contenus se sont inexorablement rapprochées et reliées. Ceci implique l'utilisation toujours plus fréquente des infrastructures Internet comme « *proxies* » (mandataires ou intermédiaires) pour le contrôle des contenus, dans la lignée de la « délégation » du pouvoir en réseau aux machines, examinée notamment par Star (1990) et Callon (1986). Ce recours aux acteurs et actants intermédiaires de l'infrastructure Internet à des fins de contrôle des contenus est lié à plusieurs facteurs. En premier lieu, la globalisation des marchés numériques, le développement technique, et les modèles d'affaires de l'économie numérique ont réduit la capacité des institutions de contenir, ou de tirer profit de, la circulation de l'information (DeNardis & Musiani, 2016). Des stratégies de contrôle des contenus « basées sur l'infrastructure » telles que mettre fin à l'accès Internet des individus, bloquer des sites Web par le biais du DNS ou interdire le soutien financier à certains sites répondent à cette perte de contrôle (DeNardis, 2014). A ces questions se rajoute aussi l'utilisation répétée, par plusieurs gouvernements à travers le monde, des infrastructures afin de contenir la diffusion d'informations jugées sensibles (notamment en créant, avec l'aide des opérateurs de communication, des dysfonctionnements ou pannes délibérées, comme dans le cas des *kill-switch* ; Vargas-Leon, 2016). Ou encore, les mêmes technologies qui peuvent améliorer la qualité et la variété des communications entre citoyens, et de la diffusion de l'information, sont également utilisées par plusieurs acteurs étatiques pour filtrer et censurer l'information, voire pour disséminer de la désinformation (Tusikov, 2016).

Parallèlement, on voit aussi comment il sera nécessaire, dans des recherches futures, de nuancer ultérieurement la notion de « responsabilité individuelle » de l'internaute, largement considérée comme acquise dans les stratégies de régulation mentionnées ci-dessus, pour prendre en compte la multitude de leviers de pouvoir et de points de contrôle qui sont inscrits dans les intermédiaires techniques de l'Internet – des algorithmes de visibilité des plateformes aux « bulles de filtrage »

qu’ils génèrent, des systèmes de classification des moteurs de recherche aux services qui gèrent les paiements en ligne et l’échange de monnaies électroniques.

8.4. Souveraineté(s) numérique(s) par l’infrastructure

Le 19 février 2020, la présidente de la Commission européenne Ursula von der Leyen a défini la souveraineté technologique de l'Europe comme sa capacité « à faire ses propres choix, sur la base de ses propres valeurs, en respectant ses propres règles ». Souveraineté technique, souveraineté numérique, souveraineté d’Internet – surtout depuis les révélations de Snowden en 2013, ces différents termes sont de plus en plus mis en avant pour véhiculer l’idée que les États devraient réaffirmer leur autorité sur Internet et protéger leurs citoyens et entreprises des multiples défis auxquels l’auto-détermination de leur nation est confrontée dans la sphère numérique. Ils ne devraient pas le faire au moyen d’alliances supranationales ou d’instruments internationaux – qui étaient envisagés comme les principales sources normatives de la gouvernance d’Internet à l’apogée de son ère multipartite – mais en augmentant leur indépendance et leur autonomie aux niveaux technique, économique et politique. Ces dernières années, la justification de la régulation d’Internet, qui découlait auparavant de la nécessité de préserver les principes fondateurs d’un « réseau de réseaux » ouvert et libre, a fait place aux préoccupations des États quant à la sécurité de leurs populations respectives et de leurs infrastructures critiques, et par rapport à la compétitivité de leurs économies nationales.

Plusieurs spécialistes de la gouvernance d’Internet provenant de diverses disciplines ont récemment manifesté leur intérêt pour la notion de souveraineté numérique, telle qu’elle est déployée par les acteurs étatiques et non étatiques dans un certain nombre d'arènes politiques et économiques, des pays plus centralisés et autoritaires aux démocraties libérales. Cette littérature montre que le terme « souveraineté numérique » a des connotations variées selon les différents contextes nationaux, les arrangements entre les acteurs, et les ensembles concrets de pratiques qui lui sont liés (Couture & Toupin, 2019).

Les recherches existantes sur ces différentes déclinaisons du terme portent souvent sur les imaginaires passés et présents de la souveraineté numérique. Certains auteurs relient les changements discursifs du rejet cyber-exceptionnaliste de l'ingérence des États aux revendications contemporaines de souveraineté des gouvernements en matière de sécurité informatique, de gouvernance des données et de politique industrielle (par exemple, Mueller, 2019 ; Pohle & Thiel, 2019). D'autres se concentrent sur les acteurs, les arguments et les idées que sous-tendent des occurrences spécifiques du discours de souveraineté numérique, par ex. dans des pays ou des communautés particuliers (voir Ebert & Maurer, 2013). Alors que la majorité de ces recherches porte sur les revendications de souveraineté de pays autoritaires tels que la Chine (Zeng et al., 2017) et la Russie (Budnitsky & Jia, 2018), les discours les plus récents dans les pays démocratiques ont commencé à recevoir de l'attention aussi (p. ex., Gurumurthy & Chami, 2016 ; Tréguer, 2017).

Une partie substantielle des recherches sur la souveraineté numérique examine la relation entre l'État et sa dimension territoriale, et comment elle est affectée par les réseaux numériques (par exemple Limonier, 2018). La question de savoir comment assurer l'auto-détermination des États et des citoyens à l'intérieur des frontières de leur territoire national, et si cela conduit à une « re-territorialisation » voire à une « fragmentation » d'Internet est un thème central de ces travaux (par ex. Mueller, 2017). Un grand nombre de chercheurs se concentre également sur les discours et les politiques de cybersécurité afin d'évaluer les efforts des États pour assurer la sécurité des infrastructures numériques et de l'espace en ligne lié à leur territoire national (par exemple, Hansen & Nissenbaum, 2009). D'autres traitent des pratiques de surveillance des agences ou des entreprises de renseignement étrangères et de la manière dont les États cherchent à élaborer d'éventuelles contre-mesures (par exemple, Tréguer, 2017). Dans ce contexte, une attention particulière est accordée aux tentatives des États d'introduire des lois sur la localisation des données qui limitent le stockage, le mouvement et/ou le traitement des données à des zones géographiques et des juridictions spécifiques (par exemple, Panday & Malcolm, 2018).

Récemment, il y a eu quelques tentatives préliminaires pour systématiser les revendications et les définitions de souveraineté numérique, en distinguant si elles portent sur la capacité d'auto-détermination numérique des États, des entreprises ou des individus (Couture & Toupin, 2019 ;

Pohle & Thiel, 2020). Cependant, à l'heure actuelle, il y a encore un manque de recherches qui analysent systématiquement les discours et catégorisent la grande variété de dispositifs (incluant les discours institutionnels, les pratiques professionnelles et réglementaires ainsi que les structures techniques et architecturales) liés à la souveraineté numérique.

Ce qui est particulièrement intéressant dans la période post-Snowden est que l'étiquette de « souveraineté numérique », qui avant n'était proclamée et poursuivie explicitement que par des Etats dits autoritaires (Chine et Russie notamment) s'est vue ré-appropriée par plusieurs démocraties occidentales. L'Europe est un cas particulièrement intéressant avec des discours et stratégies qui sont à la fois propres aux différents pays (France et Allemagne notamment) et développés de façon coordonnée au niveau supra-national européen. Si l'étiquette est une seule, avec quelques petites variations, ce que les différents pays et gouvernements (et acteurs du secteur privé…) pensent et mettent en œuvre en se référant à elle est d'une grande variété. Or, les stratégies de « gouvernance par l'infrastructure » ont un rôle central dans ces dynamiques. Les États poursuivant des stratégies d'autonomisation, de souveraineté et d'isolement de leur Internet national sont souvent engagés dans ces usages politisés des infrastructures Internet, avec des risques associés de plus en plus évidents. Un excellent exemple est le routage Schengen, proposé au début des années 2010, c'est-à-dire l'idée de ne pas acheminer les flux de données européens via des points d'échange et des routes en dehors de l'Europe – projet qui n'a finalement pas recueilli un soutien politique suffisant, et dont le projet de « cloud européen fédéré » Gaia-X, proposé en 2019 et développé depuis, est le successeur. Les approches STS, avec leur attention aux pratiques situées et à la puissance d'agir par l'infrastructure, sont bien adaptées pour mettre ces aspects au premier plan. Ils peuvent apporter une perspective innovante sur la souveraineté numérique en examinant comment le label s'inscrit dans un certain nombre d'« infrastructures de contrôle » à plusieurs niveaux de granularité, et comment les États cherchent à les coopter comme mandataires de leur autorité.

Il me semble donc qu'une des contributions importantes qu'on pourra apporter aux études de la gouvernance de l'Internet au cours des prochaines années avec une perspective STS/études d'infrastructure sera de comprendre, d'un côté, comment différentes définitions de souveraineté numérique auxquelles aspirent, ou desquelles s'inspirent, les différents pays produisent des effets

très « matériels » : sur les infrastructures, la circulation des flux de données, la localisation géographique et la configuration technique des fermes de serveurs ou des Internet Exchange Points, etc. Il s'agira par ailleurs d'explorer comment les stratégies de souveraineté numérique, et l'image que les États en projettent à l'international, sont informées en retour par les opportunités et contraintes inscrites dans les infrastructures : comment, par exemple, ce qui se révèle possible, difficile ou impossible à mettre en œuvre d'un point de vue technique influence le projet de loi suivant, ou amène à reconsidérer certains aspects du précédent. Certains des cas d'étude dans ce mémoire montrent déjà bien ce « ballet », notamment les controverses autour de la loi Yarovaya dans le Chapitre 7.

8.5. Infrastructures de contrôle, infrastructures de résistance

Ce mémoire montre un dialogue constant d'arrangements infrastructurels. Si d'un côté, il s'agit pour ces infrastructures de servir des fonctions de contrôle, de cooptation, de concentration du pouvoir sur Internet, ou encore de développant des façons inédites de l'exercer, il s'agit d'un autre côté de développer des réponses, également « par les infrastructures », qui visent la résistance, la critique, l'évasion, souvent par le biais de bricolages ou de ruses techniques. Dans les premiers chapitres de ce mémoire, j'ai contribué à élaborer une théorie du premier type d'arrangement, en négligeant quelque peu le deuxième type. Or, ces réponses sont de plus en plus – même si à des niveaux, ou dans des dimensions, tout à fait « mundane » (Cheniti, 2009), triviales, informelles – partie intégrante de la gouvernance d'Internet. Une théorie de celle-ci qui se fonde sur ses dimensions infrastructurelles se doit de faire ressortir pleinement cet aspect, tout de moins en tant un objet sur lequel il sera nécessaire, pour les études de la gouvernance d'Internet, de se concentrer prochainement.

Comment penser les résistances qui émergent face aux emprises contraignantes qui s'exercent sur Internet ? Les travaux sur les « désobéissances » et « résistances » à la domination sont foisonnants, en histoire, en science politique, en sociologie… L'ordre institutionnel ne s'impose pas sans aménagements et arrangements dans la distribution des rôles prescrits. Dans cette perspective, les

résistances et les protestations constituent une clé d'entrée privilégiée pour analyser les organisations sociales. Les formes de résistance qui s'élaborent peuvent permettre de mettre en évidence les relations de pouvoir. Il est difficile généralement d'identifier une « résistance » cohérente et organisée (Cefaï, 2009) mais penser plutôt les résistances numériques comme une diversité de pratiques, de discours et de phénomènes (Toupin & Couture, 2021) qui incluent des arts de faire (de Certeau, 1990), des ruses (Loveluck & Holeindre, 2021), des contournements, des évasions, du piratage (Keucheyan & Tessier, 2008), des arrangements de type « nains sans géants » (Musiani, 2015b) au sein desquels on pourrait se passer de points de passage et de contrôle obligatoires…

Des formes nouvelles de protestation en ligne se développent contre les politiques gouvernementales de surveillance du web (MacKinnon, 2012). Les unes peuvent relever de la prise de parole publique et visible (voir les travaux sur le médiactivisme de Cardon & Granjon, 2014), les autres, au contraire, de l'anonymat et du brouillage (Brunton & Nissenbaum, 2015). Elles ont été, ou peuvent être, conceptualisées sur le modèle des mobilisations *off line* mais aussi selon de nouveaux modèles inspirés des figures de la navigation ; les sociologues de l'Internet se réfèrent notamment à l'exemple de la piraterie pour désigner des individus dont l'activité est plutôt de détourner les techniques (Keucheyan & Tessier, 2008).

Il est alors important de penser les résistances du Net en accordant une attention primordiale aux objets techniques eux-mêmes, aux infrastructures qui font tenir l'Internet (Bowker & Star, 1999 ; Lessig, 1999 ; Barthe, Lascoumes, Callon, 2001 ; Abbate, 2012). Dans cette perspective, la résistance prend des formes multiples et mouvantes, en permanente réinvention. Les perspectives dérivées des études d'infrastructure permettent également de montrer que les formes de résistance font aussi exister, et compter, les lieux du contrôle qu'elles identifient par leur action même.

Même dans les toutes dernières années, je suis bien sûr loin d'être la seule à essayer de penser les résistances en réseau : on retiendra notamment concepts de *data activism* (Milan, 2019), ou de *data justice* (Dencik, Hintz, Redden & Treré, 2019), présentés rapidement dans le sixième chapitre, jusqu'à l'approche de *design justice* (Costanza-Chock, 2020), qui explore la relation entre le design, le pouvoir et la justice sociale visant explicitement à remettre en cause, plutôt qu'à

reproduire, les inégalités structurelles des processus de conception technique. Pourtant, les liens entre ces façons de théoriser la « résistance par l'infrastructure » et les études de la gouvernance d'Internet ne me semblent pas encore complètement établis, alors qu'il s'agit, me semble-t-il, d'un rapprochement à effectuer afin de mieux comprendre les équilibres de pouvoir numériques de notre temps. Cet objectif compte donc parmi les objectifs que je me pose dans mon agenda de recherche futur, ce mémoire étant une synthèse de la « boîte à outils » nécessaire, et ses cas d'étude une illustration de combien le dialogue entre résistances numériques et infrastructures est étroit.

8.6. Quand l'humain se fait infrastructure (Internet) : croisements avec les études du *digital labor*

Les « petites mains de la société de l'information » (Denis & Pontille, 2012) existent depuis qu'existe la « société de l'information » (Garnham, 1998), dans l'objectif de co-construire, soutenir et maintenir son infrastructure. Cependant, l'évolution et la convergence de plusieurs phénomènes – tels que le développement des réseaux sociaux, la gouvernance algorithmique, l'utilisation de grandes masses de données (*big data*) à des fins de profilage, de recommandation et de contrôle, l'usage croissant, multiforme et *disruptive* des grandes « plateformes » numériques dans plusieurs secteurs de l'économie – entraînent des évolutions dans la qualité et la quantité du « facteur humain » dans les pratiques quotidiennes de l'Internet et les façons dont différents acteurs s'en saisissent et le co-construisent.

Notamment, des individus opérant dans les coulisses des plateformes Internet, qu'Antonio Casilli a défini comme « travailleurs du clic » (2020), se voient déléguées des tâches de plus en plus modestes et répétitives : par exemple, les « armées » de personnes employées par Google et Facebook côtoient et complémentent le travail automatisé des algorithmes afin de rechercher des sources de désinformation, ou de minimiser les résultats de recherche estimés problématiques sur la base des conditions d'utilisation des plateformes, ou selon le régime juridique de pays spécifiques (Badouard, 2020). A ces pratiques d'intégration humaine de l'activité algorithmique se rajoute une deuxième forme de « travail numérique », plus insidieuse et moins reconnaissable comme véritable pratique de travail : le fait que les utilisateurs des plateformes numériques

génèrent, souvent à leur insu, en publiant des informations relevant de la sphère personnelle, en produisant des contenus ou en cliquant sur des fonctionnalités, des « traces numériques » qui peuvent être mises en valeur et monétisées auprès de tiers par les acteurs de l'industrie du numérique (Cardon & Casilli, 2015 ; Masutti, 2020).

Cet ensemble de phénomènes – qui a été appelé, dans les années récentes, *digital labor* – me semble soulever une question qui, en complément aux travaux en socio-économie qui sont en train de le définir à la fois comme un ensemble de pratiques et comme un champ de recherche (Scholz, 2012 ; Fish & Srinivasan, 2012 ; Cardon & Casilli, 2015 ; Bucher & Fieseler, 2017 ; Tubaro & Casilli, 2019 ; Casilli, 2020), se doit d'être abordée également en lien avec l'enjeu central de ce mémoire, c'est-à-dire comment l'infrastructure Internet est régie et utilisée comme un outil de gouvernance. Plus particulièrement, ces évolutions du travail à l'ère du numérique questionnent le rôle de l'humain comme l'un des « engrenages » des technologies en réseau de demain. En 2018, une équipe interdisciplinaire de chercheurs de l'*AI Now Institute* a mis en évidence certains des défis les plus urgents dus à l'essor des technologies au croisement entre big data, algorithmes et plateformes numériques. Le rapport mentionne notamment deux points d'action, la *réflexion infrastructurelle* pour mieux comprendre et suivre les complexités de ces systèmes, et la *prise en compte du travail « caché »* ou en coulisses, qui permettrait de mieux attirer l'attention sur les formes marginalisées de travail humain dans ces systèmes (Whittaker et al., 2018). Au croisement des études d'infrastructure et des études de *digital labor*, la question centrale semble être : peut-on considérer les travailleurs du numérique en tant qu'infrastructure ? Quelles seront les implications de cette posture méthodologique et théorique ?

Pour aborder cette question, il me semble utile de re-mobiliser la notion de « *human infrastructure* » proposée en 2006 par les spécialistes de *cyberinfrastructure studies* Charlotte Lee, Paul Dourish et Gloria Mark. Cette notion, mobilisée afin d' « explorer comment les arrangements humains et organisationnels partagent des propriétés avec les infrastructures technologiques » (Lee et al., 2006), a été très récemment utilisée dans des publications relatives au travail humain que sous-tend l'intelligence artificielle (Mateescu & Elish, 2019 ; Mervich, 2020) afin de montrer à quel point est centrale, dans les processus quotidiens d'organisation et de conservation des données, l'implication humaine – de l'humain sous toutes ses facettes, au-delà des acteurs humains

plus « reconnaissables » et en vue dans les processus d'innovation, tels que les grands développeurs ou les chefs d'entreprise. Il s'agit également, au moyen d'une conceptualisation de l'humain en tant qu'infrastructure, de fournir une perspective qui permette de discuter de préoccupations éthiques critiques en ce qui concerne les conditions de travail et les problèmes épistémologiques liés à l'intelligence artificielle. En recherchant certaines des propriétés des infrastructures – relationnalité, inscription, invisibilité – auprès des humains-en-réseau, cette conceptualisation semble être prometteuse dans ses croisements avec les études du *digital labor*, dans la mesure où elle ouvre de multiples voies pour analyser et découvrir la position des humains au sein des plateformes et des algorithmes qui forment une partie toujours plus importante de l'Internet d'aujourd'hui.

8.7. Internet comme « méta-infrastructure » : quel périmètre pour sa gouvernance (et ses études) ?

A l'orée de la troisième décennie du 21e siècle, des profondes transformations de ce qu'on appelle « l'Internet » sont en cours. Son expansion est notamment en train de dépasser de façon massive le stade de la communication entre les personnes, ou entre des personnes et des données ou de l'information – le stade qui a amené au fil des années de nombreux spécialistes à parler d'Internet comme du principal « médium de masse » du nouveau millénaire (Morris & Ogan, 1996) ou d' « espace public numérique » (Stein, 2008) – pour s'étendre à des milliards d'objets de la vie quotidienne. Le « feuilleté » d'infrastructures que composent l'Internet – les couches d'infrastructure, introduites à différents moments historiques, au sein desquelles des standards et des catégories se stabilisent (Star & Ruhleder, 1994 ; Star & Lampland, 2008 ; Denis & Pontille, 2013) – s'enrichit et se complexifie par le biais de nouveaux dispositifs connectés, de nouveaux protocoles et langages qu'ils doivent parler afin de se comprendre et interagir, ainsi que de nouvelles barrières et de nouveaux obstacles.

L'Internet dit « des objets » (*Internet of Things* ou IoT en anglais ; voir Greengard, 2021 pour une contribution récente et succincte) est le plus souvent assimilé, notamment dans ses traitements médiatiques, à un certain nombre de dispositifs ménagers et d'innovations grand public, comme

les technologies portables et les voitures, et même à certains *gadgets* tels que les lunettes ou les montres « intelligentes ». Par conséquent, une grande partie des efforts exploratoires de gouvernance de l'Internet des objets a visé ces produits de consommation, ce qui a jusqu'ici donné lieu à une sous-exploration de la manière dont Internet s'est développé comme méta-infrastructure de notre quotidien.

Pourtant, comme nous l'a récemment rappelé Laura DeNardis (2020), c'est en regardant au-delà de ces applications IoT grand public qu'on trouve les évolutions les plus marquantes de ce que constitue l'Internet aujourd'hui, et de ce que ce mot pourra signifier dans un futur proche. A transformer l'Internet d'un système qui est certes doté de dimensions discrètes voir invisibles, mais qui se trouve « dans le domaine cognitif de l'utilisateur », par le biais d'interfaces telles que les écrans, en une toile de fond omniprésente de la vie quotidienne (DeNardis, 2020, p.10) sont notamment les systèmes physiques connectés qui sous-tendent désormais presque tous les secteurs industriels. Les sociétés pétrolières s'appuient sur des capteurs d'énergie connectés numériquement ; les sociétés de transport terrestre et maritime utilisent les technologies Internet pour suivre les véhicules et les colis ; les systèmes médicaux reposent de plus en plus sur des dispositifs de surveillance, de diagnostic et de traitement connectés à Internet. Les réseaux numériques sont utilisés par des entreprises en tout genre et de toute taille pour gérer le traitement des matériaux, l'optimisation des stocks et l'interconnexion entre systèmes logistiques, ce qui amène DeNardis à conclure qu'« il n'existe plus de démarcation logique entre les entreprises nativement numériques et les entreprises non-tech » (2020, p. 11). Nombre de services publics, de systèmes de contrôle du trafic et d'autres applications dites de la « ville intelligente » font désormais partie de l'écosystème Internet (Zanella et al., 2014).

La gouvernance d'Internet est susceptible de devenir de plus en plus un objet d'étude pour la sociologie de l'innovation et des techniques, en particulier pour les études d'infrastructure, à mesure que la portée des acteurs de l'infrastructure Internet s'étend à d'autres types d'infrastructures. En 2014, Larry Page prédisait que « Google construirait des aéroports et des villes » (voir p. ex. Savov, 2014), ce qui, au moins pour le moment, s'avère plus compliqué que prévu. Par ailleurs, il semble indéniable que l'influence des géants de l'Internet est en train de s'étendre : les acteurs « nativement numériques » ne limitent pas leurs activités aux logiciels, aux

contenus dématérialisés et à l'information, mais ils utilisent leur maîtrise dans ces domaines pour prendre position sur des marchés tels que le transport, la gestion des infrastructures ou les services bancaires. Alphabet, la maison mère de Google, joue un rôle d'organisateur de la mobilité ; IBM participe à la gestion des infrastructures d'approvisionnement en eau de plusieurs villes. Avec la connexion des infrastructures et des objets, l'organisation des flux physiques nécessite la maîtrise des flux d'informations. Tous ces réseaux, bien qu'utilisant souvent des technologies propriétaires, s'appuient également sur les protocoles et équipements de réseau sous-jacents d'Internet, ou s'y connectent pour des fonctions d'administration et de contrôle. Il est bon de rappeler que l'assurance, la banque, la gestion des transports sont depuis longtemps – sans doute déjà le tournant du XXe siècle – des domaines où des données standardisées circulent de façon automatique et/ou informatisée pour faciliter leur gestion (voir par exemple Campbell-Kelly, 1990 ou Yates, 1993). Cependant, les croisements qui s'opèrent actuellement entre ces différentes infrastructures et des acteurs quasi-monopolistiques de l'information et de la communication en ligne, dont le cœur de métier est de retenir l'attention et collecter des données personnelles en contrepartie de services « gratuits », posent question et seront sans doute au cœur des problématiques de recherche liées à la gouvernance au cours des prochaines années.

Depuis le début de 2020 et de la pandémie de Covid-19, ce scénario s'est enrichi de questionnements ultérieurs, ou tout de moins certaines des problématiques qui y sont liées se sont posées plus rapidement et avec plus d'acuité. En effet, la pandémie a accéléré la transition vers une « gouvernance par l'infrastructure » profondément ancrée dans la gestion de grandes masses de données. Premièrement, elle a considérablement augmenté le besoin (et la demande sociétale/politique) de résoudre ou simplifier des problèmes grâce aux technologies numériques. Cette « innovation sous la pression » a contribué à réduire les inquiétudes des citoyens et des décideurs concernant, par exemple, les risques liés à l'excès de surveillance, ouvrant la voie à des compromis concertés en matière de confidentialité (voir Kitchin, 2020). En outre, le déploiement rapide et ad hoc de technologies particulières (par exemple les applications de recherche de contacts) n'a souvent pas été précédé d'évaluations d'impact adéquates ou de consultations des parties prenantes (Madianou, 2020). Deuxièmement, la pandémie a constitué une opportunité sans précédent, pour certains acteurs, de promouvoir leurs visions de « transformations numériques » de la société (Yan et al., 2021). Créant de nouvelles perspectives de marché, elle a fonctionné

comme le banc d'essai parfait pour l'industrie technologique pour piloter et introduire de « nouvelles » solutions technologiques ; par exemple, des dispositifs intelligents pour la détection précoce des symptômes du COVID-19. La pandémie a également contribué à comprimer la courbe de diffusion de l'innovation au fil du temps (voir Rogers, 2003), en accélérant l'adoption et en raccourcissant l'intervalle normalement requis pour la transition d'une phase d'acquisition exploratoire de connaissances à l'acceptation du produit ; par exemple, les solutions de vérification de l'identité numérique dans les sites commerciaux. Enfin, forçant également les gouvernements à passer à la vitesse supérieure dans leurs processus de numérisation, la pandémie a servi de catalyseur pour inciter les décideurs à adopter ou tester des systèmes d'identification numérique, et, en dépit de plusieurs débats houleux et de controverses, elle a parfois permis aux instances politiques de venir à bout plus facilement et plus rapidement d'un certain nombre de résistances citoyennes.

Ce scénario soulève, ou va soulever à court terme, des questions « d'intérêt public » sans précédents, et aura des conséquences de taille pour la vie privée et la sécurité des utilisateurs. Il soulève également des questions importantes pour la gouvernance d'Internet et pour les chercheurs qui essaient d'en faire sens. Pour approfondir le cadre théorique et empirique proposé dans ce mémoire, deux notions qui mettent l'accent sur l'inscription des infrastructures dans le temps et dans l'espace, tout en soulignant leurs qualités évolutives et systémiques, sont particulièrement intéressantes. D'une part, la notion de zones technologiques (et plus précisément de zones infrastructurelles) de Barry (2006) permet de donner un sens aux espaces au sein desquels les différences entre pratiques, procédures et formes techniques sont réduites, et des normes communes sont établies. La notion alerte sur le « besoin d'analyse de la construction historique d'espaces politiques et économiques particuliers, et des spécificités des matériaux, des pratiques et des lieux qu'ils transforment, relient, excluent et font taire » et souligne que « la formation de zones technologiques devient critique pour la constitution d'une distinction entre les formes politiques et économiques globalisées/occidentales et les autres, *non-occidentales* » (Barry, 2006, p. 250), deux aspects qui sont étroitement liés à la démarche que sous-tend ce mémoire ainsi qu'à ses possibles développements futurs, qu'il s'agisse d'explorer la souveraineté numériques ou les résistances en ligne. D'autre part, des travaux récents sur le concept d'infrastructurisation ou « *infrastructuring* » (Blok et al., 2016 ; Karasti & Blomberg, 2018) permettent de donner du sens,

théoriquement et méthodologiquement, aux infrastructures en tant que processus, pratiques et cadres à la fois ouverts et en expansion, alors même que notre point de départ en tant que chercheurs est constitué d'études de cas d'infrastructures « limitées dans l'espace, le temps et l'organisation ». Le passage des infrastructures à l'*infrastructuring* peut permettre de rendre compte de façon plus nuancée de la manière dont un « champ est construit par l'engagement du chercheur avec le phénomène d'étude, et dans le processus, [de comment] l'objet d'enquête peut être délimité, ne serait-ce que temporairement » (Karasti & Blomberg, 2018).

En mobilisant ces notions, et d'autres encore, les études de la gouvernance de l'Internet dans un futur proche devront prendre en compte les évolutions en cours sur le périmètre et la nature même de l'infrastructure Internet, tout comme, dans un passé récent, ils ont reconnu et exploré le passage d'une gouvernance *des* infrastructures Internet à une gouvernance *par* l'infrastructure. A l'heure de l' « infrastructurisation Internet » de nos sociétés, plusieurs défis attendent – encore ! – les chercheurs STS de la gouvernance d'Internet. C'était l'espoir et l'objectif de ce mémoire, via le prisme de mes recherches, de donner un aperçu de ce qui a été fait, et de tracer un agenda pour ce qui pourrait être fait. Alors que les *Internet studies* sont actuellement – pour plusieurs bonnes raisons qui vont de la désinformation à la surveillance de masse – plutôt orientés vers l'exploration des désenchantements de l'Internet[73], je me réjouis, et je mesure la responsabilité, d'être au croisement de plusieurs conversations académiques et politiques susceptibles de contribuer à rendre notre monde connecté, d'humains et de non-humains, un peu plus ouvert et pluriel.

[73] J'emprunte cette formule à Romain Badouard (2017).

Bibliographie

Abbate, J. (2000). *Inventing the Internet*. Cambridge, MA: MIT Press.

Abbate, J. (2012). « L'histoire de l'Internet au prisme des STS », *Le temps des médias*, 18: 170-180.

Abu-Salma, R., Bonneau, J. *et al.* (2017b). Obstacles to the adoption of secure communication tools. Proceedings of the 38th IEEE Symposium on Security and Privacy. (Oakland), San Jose, CA, USA. DOI: https://doi.org/10.1109/SP.2017.65

Akrich, M. (1998). Les utilisateurs, acteurs de l'innovation. *Education permanente*, 134: 79–90

Akrich, M., Latour, B., Callon, M. (2006). *Sociologie de la traduction : textes fondateurs*, Paris, Presses des Mines.

Anand, N. (2017). *Hydraulic city: Water and the infrastructures of citizenship in Mumbai*. Duke University Press.

Anderson, N. (2012, August 29). Government admits defeat, gives back seized Rojadirecta domains. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2012/08/government-goes-0–2-admits-defeat-in-rojadirecta-domain-forfeit-case/

Aouragh, M. *et al.* (2015). Let's first get things done! On division of labour and techno-political practices of delegation in times of crisis. *The Fibreculture Journal*, (26) DOI: https://doi.org/10.15307/fcj.26.196.2015

Badouard, R. (2017). *Le désenchantement de l'internet. Désinformation, rumeur et propagande*. FYP éditions.

Badouard, R. (2020). *Les nouvelles lois du Web: modération et censure*. Paris : Seuil.

Badouard, R., Musiani, F., Méadel, C. & Monnoyer-Smith, L. (2012). Towards a Typology of Internet Governance Socio-Technical Arrangements, pp. 99-124 in Françoise Massit-Folléa, Cécile Méadel & Laurence Monnoyer-Smith (eds.) *Normative Experience in Internet Politics*, Paris: Presses de l'Ecole des Mines. http://books.openedition.org/pressesmines/586?lang=fr

Bannerman, S., & Haggart, B. (2015). Historical Institutionalism in Communication Studies. *Communication Theory*, *25*(1), 1–22. doi:10.1111/comt.12051

Baptista, I. (2019). Electricity services always in the making: Informality and the work of infrastructure maintenance and repair in an African city. *Urban Studies*, *56*(3), 510-525.

Barlow, J. P. (1996). Declaration of Independence of Cyberspace. http://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html

Barnes, J. (2017). States of maintenance: Power, politics, and Egypt's irrigation infrastructure. *Environment and Planning D: Society and Space*, *35*(1), 146-164.

Barry, A. (2006). "Technological zones", *European Journal of Social Theory*, 9(2), pp. 239-253.

Barry, A. (2020). The material politics of infrastructure. In *TechnoScienceSociety* (pp. 91-109). Springer, Cham.

Bauwens, M. (2005). The Political Economy of Peer Production. *CTheory*, 1. http://www.ctheory.net/articles.aspx?id=499

Bearman, J. (2015). "The untold story of Silk Road. Parts 1 & 2", *Wired*, June 2015.

Bellon, A. (2018). *Gouverner l'internet: Mobilisations, expertises et bureaucraties dans la fabrique des politiques numériques (1969-2017)*, Thèse de doctorat, Paris 1.

Bendrath, R., & Mueller, M. (2011). The end of the net as we know it? Deep packet inspection and internet governance. *New Media & Society*, *13*(7), 1142-1160.

Benkler, Y. (2011). WikiLeaks and the PROTECT-IP Act: A new public-private threat to the Internet commons. *Daedalus* 140(4): 154–164.

Bernards, N., & Campbell-Verduyn, M. (2019). Understanding technological change in global finance through infrastructures: Introduction to Review of International Political Economy Special Issue 'The Changing Technological Infrastructures of Global Finance'. *Review of international political economy*, *26*(5), 773-789.

Berners-Lee, T. (2019, March 12). 30 years on, what's next #ForTheWeb?. *World Wide Web Foundation.* Retrieved from: https://webfoundation.org/2019/03/web-birthday-30/.

Bygrave, L. A. and Bing, J. (eds.) (2009). *Internet governance: Infrastructure and institutions*. Oxford, England: Oxford University Press.

Blanchette, J.-F. (2011). A material history of bits. *Journal of the Association for Information Science and Technology*, *62*(6), 1042-1057.

Blanchette, J. F. (2012). *Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents*. MIT Press.

Blok, A., Nakazora, M., & Winthereik, B. R. (2016). Infrastructuring environments. *Science as Culture*, *25*(1), 1-22.

Bortzmeyer, S. (2019). *Cyberstructure. L'Internet, un espace politique*. Caen: C & F Éditions.

Boyd, D., & Hargittai, E. (2013). Connected and concerned: Variation in parents' online safety concerns. *Policy & Internet*, *5*(3), 245-269.

Bowker, G. C. (1996). "The history of information infrastructures: The case of the international classification of disease", *Information Processing & Management*, vol. 32, nº 1, p. 49-61.

Bowker, G. C., & Star, S. L. (1996). How things (actor-net) work: Classification, magic and the ubiquity of standards. *Philosophia*, *25*(3-4), 195-220.

Bowker, G. C. & Star, S. L. (1999). *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: The MIT Press.

Bowker, G. C., Baker, K., Millerand, F., and Ribes, D. (2010). Toward information infrastructure studies: Ways of knowing in a networked environment. In J. Hunsinger, L. Klastrup, and M. Allen (eds.) *International Handbook of Internet Research*. New York: Springer.

Bradshaw, S., & DeNardis, L. (2018). The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom. *new media & society*, *20*(1), 332-350.

Bradshaw, S., DeNardis, L., Hampson, F., Jardine, E., and Raymond, M. (2015). "The Emergence of Contention in Global Internet Governance." Draft Paper Presented at the 56th Annual ISA Convention New Orleans, USA, February 9th. http://web.isanet.org/Web/Conferences/New%20Orleans%202015/Archive/adf6039d-3251-4ede-a2fa-0f8701f21459.pdf

Braman, S. (2009). *Change of State: Information, Policy, and Power*. Cambridge, MA: The MIT Press.

Braman, S. (2011). Internet policy. In M. Consalvo & C. Ess (Eds.), *Handbook of Internet Studies* (pp. 137-167), Oxford: Wiley-Blackwell. doi:10.1002/9781444314861.ch7

Braman, S. (2016). Instability and internet design. *Internet Policy Review*, *5*(3). doi:10.14763/2016.3.429

Brousseau, E., Marzouki, M. & Méadel, C. (eds., 2012). *Governance, Regulation and Powers on the Internet*. Cambridge: Cambridge University Press.

Breindl, Y., & Briatte, F. (2013). Digital Protest Skills and Online Activism Against Copyright Reform in France and the European Union. *Policy & Internet*, *5*(1), 27–55. doi:10.1002/poi3.21

Brosda, C. (2015). Orientierung in der digitalen Unübersichtlichkeit. Zur medienpolitischen Relevanz der Kommunikationswissenschaft. In M. Emmer & C. Strippel (Eds.), *Kommunikationspolitik für die digitale Gesellschaft* (pp. 25–40). Berlin: Freie Universität Berlin, Institut für Publizistik- und Kommunikationswissenschaft. doi:10.17174/dcr.v1.3

Brunsson, N. & Jacobsson, B. (eds., 2000). *A World of Standards*. Oxford: Oxford University Press.

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: A user's guide for privacy and protest*. Cambridge, MA: The MIT Press.

Bucher, E., & Fieseler, C. (2017). The flow of digital labor. *New media & society*, *19*(11), 1868-1886.

Budnitsky, S. & Jia, L. (2018). "Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance", *European Journal of Cultural Studies*, 21, 594–613. https://doi.org/10.1177/1367549417751151

Buterin, V. (2013). "Bitcoin Network Shaken by Blockchain Fork", *Bitcoin Magazine*, https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448

Callon, M. (1986). "The Sociology of an Actor-Network: The Case of the Electric Vehicle", in Michel Callon, John Law and Arie Rip (eds.), *Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World*, London, Macmillan Press, pp. 19-34.

Callon, M. (2013). Pour une sociologie des controverses technologiques. *Sociologie de la traduction: Textes fondateurs*, 135-157.

Callon, M., Lascoumes, P. and Barthe, Y. (2009). *Acting in an Uncertain World. An Essay on Technical Democracy*. Cambridge, MA: The MIT Press.

Campbell-Kelly, M. (1990). *ICL: a business and technical history*. Cambridge : Cambridge University Press.

Cardon, D. (2015). Surveiller sans punir. La gouvernance de Wikipédia. In Lionel Barbe, Louise Merzeau, Valérie Schafer (éds.). *Wikipédia, objet scientifique non identifié*, Nanterre, Presses universitaires de Paris Ouest, 15-39.

Cardon, D., & Casilli, A. (2015). *Qu'est-ce que le digital labor?*. Paris: Ina.

Cardon, D., & Granjon, F. (2014). *Médiactivistes*. Paris : Presses de Sciences Po.

Carnino, G., & Marquet, C. (2018). Les datacenters enfoncent le cloud: enjeux politiques et impacts environnementaux d'internet. *Zilsel*, (1), 19-62.

Carruthers, B. G., & Uzzi, B. (2000). Economic sociology in the new millennium. *Contemporary Sociology*, *29*(3), 486-494.

Casilli, A. A. (2020). *Schiavi del clic: perché lavoriamo tutti per il nuovo capitalismo?*. Feltrinelli Editore.

Cavoukian, A. (2006). *The 7 foundational principles: Implementation and mapping of fair information practices.* Toronto, Canada: Information and Privacy Commissioner of Ontario. Retrieved from https://www.privacyassociation.org/media/presentations/11Summit/RealitiesHO1.pdf.

Cavoukian, A. (ed.). (2010). Special Issue: Privacy by design: The next generation in the evolution of privacy. *Identity in the Information Society* 3(2).

Cefaï, D. (2009). Comment se mobilise-t-on? L'apport d'une approche pragmatiste à la sociologie de l'action collective. *Sociologie et sociétés*, *41*(2), 245-269.

Chander, A. and Le, U.P. (2014). "Breaking the Web: Data Localizaton vs. the Global Internet," *UC Davis Legal Studies Research Paper Series*, No. 378, April 2014

Chatzis, K., Jeannot, G., November, V. et Ughetto, P. (eds., 2017). *Les métamorphoses des infrastructures, entre béton et numérique*, Bruxelles, Peter Lang.

Chen, A. (2011). The Underground Website where you can buy any drug imaginable, *Gawker*, 6 January 2011, http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

Cheniti, T. (2009). *Global Internet Governance in Practice. Mundane Encounters and Multiple Enactments*. Unpublished DPhil Thesis, University of Oxford.

Christou, G., & Simpson, S. (2007). Gaining a Stake in Global Internet Governance: The EU, ICANN and Strategic Norm Manipulation. *European Journal of Communication*, *22*(2), 147–164. doi:10.1177/0267323107076765

Cohn-Gordon, K., Cremers, C. and Garratt, L. (2016). On post-compromise security. In Computer Security Foundations Symposium (CSF), 2016 IEEE 29th, pages 164–178.

Coldewey, D. (2010, November 29). Peter Sunde seconds the idea of an alternative root DNS. TechCrunch. Retrieved from http://techcrunch.com/2010/11/29/peter-sunde-seconds-the-idea-of-an-alternative-root-dns/

Coleman, E. G. (2005). *The social construction of freedom in free and open source software: Hackers, ethics, and the liberal tradition*, PhD Thesis, Chicago, IL: The University of Chicago.

Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, 8(3), 255–277

Colemans, J. et Dupret, B. (eds., 2018). *Ethnographie du raisonnement juridique*. LGDJ, lextenso éditions.

Collins, R. (2006). Internet governance in the UK. *Media, Culture & Society*, *28*(3), 337–358. doi:10.1177%2F0163443706061686

Costanza-Chock, S. (2020). *Design justice: Community-led practices to build the worlds we need*. Cambridge, MA : The MIT Press.

Courmont, A., & Le Galès, P. (2019). *Gouverner la ville numérique*. Paris : PUF.

Couture, S. & Toupin, S. (2019). "What does the notion of "sovereignty" mean when referring to the digital?", *New Media & Society*, 21, 18. https://doi.org/10.1177/1461444819865984

Cristofoletti, R. (2015). Privacidade e Regulamentação do Marco Civil da Internet: registros e preocupações [Privacy and Regulation of the Civil Framework of the Internet: records and concerns]. *Revista ECO-Pós*, *18*(3), 213–229. doi: 10.29146/eco-pos.v18i3.2150

Crocker, S., Dagon, D., Kaminsky, D., McPherson, D. D., and Vixie, P. (2011). Security and other technical concerns raised by the DNS filtering requirements in the PROTECT IP Bill [White paper]. *Domain Incite*. Retrieved from http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

Curran, J., Fenton, N., & Freedman, D. (2012). *Misunderstanding the Internet*. London: Routledge. doi:10.4324/9780203146484

Daly, A., & Thomas, J. (2017). Australian internet policy. *Internet Policy Review, 6(1)* doi:10.14763/2017.1.457

de Certeau, M. (1980). *Arts de faire : l'invention du quotidien,* Paris, Gallimard.

Dehghan, S. (2012). "Iran Clamps down on Internet use." *The Guardian*, January 5.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations, 18*(3), 339-361.

De Filippi, P. & Loveluck, B. (2016). The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. *Internet Policy Review*, 5(3). DOI: 10.14763/2016.3.427

de Fornel, Michel (1994). 'Le cadre interactionnel de l'échange visiophonique', *Réseaux*, 64: 107-132.

de La Chapelle, B., & Fehlinger, P. (2016). Jurisdiction on the internet: from legal arms race to transnational cooperation. Global Commission on Internet Governance, Paper Series, n° 28. https://www.cigionline.org/sites/default/files/gcig_no28_web.pdf

Delmas-Marty, M. (2012). "The Internet: disrupting, revealing and producing rules". In Massit-Folléa, F., C. Méadel & L. Monnoyer-Smith (eds.), *Normative Experience in Internet Politics*, Paris, Presses des Mines.

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge, MA: The MIT Press.

DeNardis, L. (2010, September). *The privatization of Internet governance*. Yale Information Society Project Working Paper Draft. Paper presented at Fifth Annual GigaNet Symposium, Vilnius, Lithuania.

DeNardis, L. (2012). “Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance,” *Journal of Information, Communication & Society*, 15 (3): 1-19.

DeNardis, L. (2012b). “Governance at the Internet’s core: The geopolitics of interconnection and Internet Exchange Points (IXPs) in emerging markets, *Proceedings of TPRC 2012*, en ligne, http://dx.doi.org/10.2139/ssrn.2029715

DeNardis, L. (2013). The emerging field of Internet governance. In W. Dutton (ed.) *Oxford handbook of internet studies*. Oxford, England: Oxford University Press

DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven, CT and London: Yale University Press.

DeNardis, L. (2020). *The Internet In Everything: Freedom and Security in a World with No Off Switch*. New Haven, CT: Yale University Press.

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770. doi:10.1016/j.telpol.2015.04.003

DeNardis, L. & Musiani, F. (2016). Introduction: Governance by Infrastructure, in Musiani, F., Cogburn, D. L., DeNardis, L. & Levinson, N. S. (2016, eds.). *The Turn to Infrastructure in Internet Governance*, New York: Palgrave Macmillan (pp. 3-21).

DeNardis, L., Cogburn, D., Levinson, N. S., & Musiani, F. (Eds.). (2020). *Researching internet governance: Methods, frameworks, futures*. Cambridge, MA: The MIT Press.

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. *Information, Communication & Society*, *22*(7), 873-881.

Dencik, L., Hintz, A., & Carey, Z. (2017). Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom. *New Media & Society*, *20*(4), 1433–1450. doi:10.1177/1461444817697722

Denis, J., & Pontille, D. (2012). Travailleurs de l’écrit, matières de l'information. *Revue d'anthropologie des connaissances*, *6*(1), 1-20.

Denis, J., & Pontille, D. (2013). Une infrastructure élusive. Aménagements cyclables et troubles de la description dans OpenStreetMap. *Réseaux*, 2-3 (n°178-179), 91-125.

De Pryck, K. (2022). *GIEC. La voix du climat*, Paris, Presses de SciencesPo.

DiMaggio, P., Hargittai, E., Neuman, W. R., & Robinson, J. P. (2001). Social implications of the Internet. *Annual Review of Sociology*, *27*(1), 307-336.

Dulong de Rosnay, M. & Musiani, F. (2016). Towards a (de) centralisation-based typology of peer production. *Triple C : Communication, Capitalism & Critique*, *14*(1), 189-207.

Dutton, W. H. (2018). Networked publics: multi-disciplinary perspectives on big policy issues. *Internet Policy Review*, *7*(2). doi:10.14763/2018.2.795

Ebert, H. & Maurer, T. (2013). “Contested Cyberspace and Rising Powers”, *Third World Quarterly*, 34, pp. 1054–1074. https://doi.org/10.1080/01436597.2013.802502

Edwards, P. (2003). “Infrastructure and modernity: Force, time, and social organization”, in T.J. Misa, P. Brey et A. Feenberg (eds.), *The History of Sociotechnical Systems: Modernity and Technology*, Cambridge, The MIT Press, pp. 185-226.

Elkin-Koren, N. (2012). Governing Access to User-Generated Content: The Changing Nature of Private Ordering in Digital Networks. In Brousseau, E., Marzouki, M., Méadel, C. (eds.), *Governance, Regulations and Powers on the Internet* (pp. 318-343). Cambridge: Cambridge University Press.

Epstein, D. (2013). The making of institutions of information governance: The case of the Internet Governance Forum. *Journal of Information Technology*, *28*(2), 137–149.

Epstein, D. (2015). “Duality squared: On structuration of Internet governance.” In *Produsing Theory in a Digital World*, edited by Rebecca Ann Lind, 41–56. New York: Peter Lang Publishing.

Epstein, D., Katzenbach, C. & Musiani, F. (2016). Doing internet governance: practices, controversies, infrastructures, and institutions. *Internet Policy Review*, *5*(3). doi:10.14763/2016.3.435

Epstein, D., Nisbet, E. C., & Gillespie, T. (2011). Who’s Responsible for the Digital Divide? Public Perceptions and Policy Implications. *The Information Society*, *27*(2), 92-104. doi: 10.1080/01972243.2011.548695

Ermoshina, K. (2016). *Au code, citoyens : Mise en technologie de problèmes publics*, Thèse de doctorat en socio-économie de l’innovation, MINES ParisTech.

Ermoshina, K., Musiani, F. & Halpin, H. (2016). « End-to-end encrypted messaging protocols: An overview, » in F. Bagnoli et al. (eds.), *Proceedings of the Internet Science Third International Conference*, INSCI 2016, Florence, Italy, 12–14 September, Berlin, Springer, 2016, pp. 244–254. DOI: https://doi.org/10.1007/978-3-319-45982-0_22

Ermoshina, K. & Musiani, F. (2017), “Migrating Servers, Elusive Users : Reconfigurations of the Russian Internet in the Post-Snowden Era”, *Media and Communication* 5(1), pp. 42-53

Ermoshina, K., & Musiani, F. (2019). “Standardising by running code”: the Signal protocol and de facto standardisation in end-to-end encrypted messaging. *Internet Histories*, *3*(3-4), 343-363.

Ermoshina, K. & Musiani, F. (2022). *Concealing for Freedom: The Making of Encryption, Secure Messaging, and Civil Liberties*, Manchester, UK: Mattering Press.

Eubanks, V. (2018). *Automating Inequality. How High-Tech Tools Profile, Police and Punish the Poor*. New York: St Martin’s Press.

Feenberg, A. (1999). *Questioning Technology*, Routledge, London.

Felten, E. (July 2006) 'Nuts and Bolts of Network Neutrality', Woodrow Wilson School of Public and International Affairs, Princeton University. Accessed at http://itpolicy.princeton.edu/pub/neutrality.pdf.

Fish, A., Rosado Murillo L. F., Nguyen, L., Panofsky, A. & Kelty, C. M. (2011). Birds of the Internet, *Journal of Cultural Economy*, 4:2, 157-187. http://kelty.org/or/papers/Fish-Birds-2011.pdf

Fish, A., & Srinivasan, R. (2012). Digital labor is the new killer app. *New Media & Society*, *14*(1), 137-152.

Flanagan, M., Howe, D. C., & Nissenbaum, H. (2008). Embodying values in technology: Theory and practice. *Information technology and moral philosophy*, *322*.

Flyverbom, M. (2011). *The Power of Networks: Organizing the Global Politics of the Internet*. Cheltenham, UK: Edward Elgar Publishing.

Flyverbom, M. (2016). Disclosing and concealing: internet governance, information control and the management of visibility. *Internet Policy Review*, 5(3). DOI: 10.14763/2016.3.428

Frau-Meigs, D., Nicey, J., Palmer, M., Pohle, J., & Tupper, P. (Eds.) (2012). *From NWICO to WSIS: 30 Years of Communication Geopolitics - Actors and Flows, Structures and Divides*. Bristol: Intellect Books. doi:10.1177/0267323113476942b

Froomkin, A. M. (2000). "Wrong turn in cyberspace: Using ICANN to route around the APA and the Constitution." *Duke Law Journal 50* (1).

Froomkin, D. & McLaughlin, J. (2016). "FBI vs. Apple establishes a new phase of the crypto wars", The Intercept, February 26 2016 Available at: https://theintercept.com/2016/02/26/fbi-vs-apple-post-crypto-wars.

Frosch, T., Mainka, C., Bader, C., Bergsma, F., Schwenk, J. and Holz, T. (2016). How secure is TextSecure? In European Symposium on Security and Privacy (EuroS&P), pp. 457–472.

Fuchs, C., & Sandoval, M. (2014). "Digital workers of the world unite! A framework for critically theorising and analysing digital labour". *tripleC: Communication, Capitalism & Critique*, *12*(2), 486-563.

Fuller, M. (ed., 2008). *Software Studies: A Lexicon*. Cambridge, MA: The MIT Press.

Fung, A. (2006). Varieties of Participation in Complex Governance, *Public Administration Review*, 66 (s1), 66-75. http://www.archonfung.net/papers/FungVarietiesPAR.pdf

Galloway, A. R. (2004). *Protocol: How control exists after decentralization*, Cambridge, MA, The MIT Press.

Galperin, H. (2004). Beyond Interests, Ideas, and Technology: An Institutional Approach to Communication and Information Policy. *The Information Society*, *20*(3), 159–168. doi: 10.1080/01972240490456818

Gangneux, J. (2019). Book Review: Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society*. Cambridge, UK: Polity Press. Information, Communication and Society, 22 (14): 2211-13.

Garnham, N. (1998). Information society theory as ideology: A critique. *Loisir et société/Society and Leisure*, *21*(1), 97-120.

Geere, D. (2010, December 10). Peter Sunde starts peer-to-peer DNS system. *Wired Magazine*. Retrieved from http://www.wired.co.uk/news/archive/2010–12/02/peter-sunde-p2p-dns

Geiger, S., Harrison, D. Kjellberg, H. & Mallard, A. (2014), *Concerned Markets. Economic Ordering for Multiple Values*. Cheltenham and Northampton: Edward Elgar

Geist, M. (2001). Fair. Com: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP. *Brooklyn Journal of International Law., 27,* 903.

Gelman, V. (2010, March 9) "Lovushka polusvobody" // "The trap of a 'half-freedom'[of speech]". Retrieved from *Slon.ru* http://slon.ru/russia/lovushka_polusvobody-310531.xhtml

Ghosh, R. (ed. 2005). *Collaborative Ownership and the Digital Economy*, MIT Press, 2006.

Gill, L., Redeker, D., & Gasser, U. (2015). *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*(Research Publication No. 2015–15). Cambridge, MA: The Berkman Center for Internet & Society at Harvard University. Retrieved from http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552582

Gillespie, T. (2010). "The Politics of 'Platforms'," *New Media & Society*, 12(3): 347-364.

Gillespie, T. (2014). The relevance of algorithms. In T. Gillespie, P. Boczkowski, and K. Foot (eds.) *Media Technologies*, pp. 167-194. Cambridge, MA: MIT Press.

Gillespie, T., Boczkowski, P. and Foot, K. (eds., 2014), *Media Technologies: Essays on Communication, Materiality and Society*. Cambridge: MIT Press.

Goldsmith, J. and Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford, England: Oxford University Press.

Graeber, D. (2011) *Debt : The First 5000 Years*. New York, NY, Melville House.

Graham, S., & McFarlane, C. (2014). *Infrastructural lives*. Taylor & Francis.

Greenberg, A. (2013). "Meet The Dread Pirate Roberts, The Man Behind Booming Black Market Drug Website Silk Road**",** *Forbes*, 3 August 2013 http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/#346f8d58190c

Greengard, S. (2021). *The Internet of Things*. Cambridge, MA: MIT Press.

Grimmelmann, J. (2007). Don't Censor Search, 117 Yale Law Journal Pocket Part 48, http://yalelawjournal.org/forum/dont-censor-search

Griset, P. (1992). L'Évolution des télécommunications intercontinentales au XXème siècle. *History and Technology, an International Journal*, *8*(3-4), 231-245.

Gurumurthy, A. & Chami, N. (2016). "Internet governance as "ideology in practice" – India's "Free Basics" controversy", *Internet Policy Review*, 5.

Hagendijk, R. & Irwin, A. (2006). "Public deliberation and governance: engaging with science and technology in contemporary Europe." *Minerva*, 44 (2).

Hall, W., Madaan, A., O'Hara, K. (2020). "Web observatories: Gathering data for internet governance", in DeNardis, L., Cogburn, D., Levinson, N. S., & Musiani, F. (Eds.), *Researching internet governance: Methods, frameworks, futures*. Cambridge, MA: The MIT Press, pp. 123-144.

Halpern, C., Lascoumes, P., Le Galès, P. (2014). *L'instrumentation de l'action publique : controverses, résistances, effets*. Presses de Sciences Po.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Harvey, P. (2012). "The topological quality of infrastructural relation: An ethnographic approach", *Theory, Culture, and Society*, *n*° 29, vol. 4-5, pp. 76-92.

Harvey, P., Bruun Jensen, C. et Morita, A. (eds., 2016). *Infrastructures and Social Complexity: A Companion*, New York, Routledge.

Hellegren, Z. I. (2017). A history of crypto-discourse: encryption as a site of struggles to define internet freedom. *Internet Histories*, *1*(4), 285-311.

Henke, C. R., & Sims, B. (2020). *Repairing infrastructures: the maintenance of materiality and power*. Cambridge, MA: The MIT Press.

Higgins, V. et Larner, W. (2010). *Calculating the social: Standards and the reconfiguration of governing*, New York, Palgrave Macmillan.

Hintz, A. (2005). "Activist media in global governance: Inputs and outputs of the World Summit on the Information Society (WSIS)." Paper presented at the RE:activism conference, Budapest, Hungary.

Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, *5*(3). doi:10.14763/2016.3.424

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society*. Cambridge, UK: Polity Press.

Hoang, N. P., Niaki, A. A., Dalek, J., Knockel, J., Lin, P., Marczak, B., Polychronakis, M. (2021). How Great is the Great Firewall? Measuring China's {DNS} Censorship. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 3381-3398).

Hofmann, J., Katzenbach, C., & Gollatz, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society, 19 (9).*

Huysmans, J. (2014). *Security Unbound: Enacting Democratic Limits. Critical Issues in Global Politics*. London and New York: Routledge.

Izal, M., Urvoy-Keller, G., Biersack, E. W., Felber, P. A., Al Hamra, A., & Garces-Erice, L. (2004). Dissecting bittorrent: Five months in a torrent's lifetime. In *International Workshop on Passive and Active Network Measurement* (pp. 1-11). Springer, Berlin, Heidelberg.

Jacobs, E. (2011) Bitcoin: A Bit Too Far? *Journal of Internet Banking and Commerce*, 16 (2).

Jakobsen, J. and Orlandi, C. (2016). On the CCA (in)security of MTProto. In Proceedings of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, pp. 113–116.

Jarrige, F., Le Courant, S., & Paloque-Bergès, C. (2018). Infrastructures, techniques et politiques. *Tracés. Revue de Sciences humaines*, (35), 7-26.

Jasanoff, S. (ed., 2004). *States of knowledge: the co-production of science and the social order*. Abingdon: Routledge.

Jørgensen, R. F. (2020). "Researching Technology Elites: Lessons Learned from Data Collection at Google and Facebook", in DeNardis, L., Cogburn, D., Levinson, N. S., & Musiani, F. (Eds.), *Researching internet governance: Methods, frameworks, futures*. Cambridge, MA: The MIT Press, pp. 169-184.

Johnson, D. R., & Post, D. G. (1997). "And how shall the net be governed? A meditation on the relative virtues of decentralized, emergent law." In B. Kahin and J. H. Keller (eds.) *Coordinating the Internet*, 62–91. Cambridge, MA: MIT Press.

Jouët, J. (2000). Retour critique sur la sociologie des usages. *Réseaux*, *18*(100), 487-521.

Kamara, I., & Kosta, E. (2016). Do Not Track initiatives: regaining the lost user control, *International Data Privacy Law*, *6*(4), 276-290.

Kantyshev, P. (2016, September 4) "Rostehu Nuzhno 10,3 Milliarda Rubley na Razrabotky Paketa Yarovoj" ["Rostech Needs 10.3 mlrds of Rubles to Develop Yarovaya Law"] Retrieved from *Vedomosti*, http://www.vedomosti.ru/technology/articles/2016/09/05/655653-rostehu-zakona-yarovoi

Karasti, H., & Blomberg, J. (2018). "Studying infrastructuring ethnographically", *Computer Supported Cooperative Work*, *27*(2), pp. 233-265.

Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Scandinavian Journal of Social Theory*, *15* (1), pp. 23-36.

Kazansky, B. (2015). Privacy, responsibility, and human rights activism. *The Fibreculture Journal* (26) DOI: https://doi.org/10.15307/fcj.26.195.2015

Kelty, C. (2005). Geeks, social imaginaries, and recursive publics. *Cultural Anthropology*, *20*(2), 185-214.

Kerr, A. & Musiani, F. & Pohle, J. (2019). Communication and internet policy: a critical rights-based history and future. *Internet Policy Review*, *8*(1). https://doi.org/10.14763/2019.1.1395

Keucheyan, R., & Tessier, L. (2008). Présentation. De la piraterie au piratage. *Critique*, (6), 451-457.

Kirschenbaum, M. G. (2008). *Mechanisms: New Media and the Forensic Imagination,* Cambridge, MA, The MIT Press.

Kitchin, R. (2020). Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity*, *24*(3), 362-381.

Kitchin, R., & Dodge, N. (2011). *Code/space: Software and everyday life*, Cambridge, MA: The MIT Press.

Klein, H. (2002). ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy. *The Information Society*, *18*(3), 193-207. https://doi.org/10.1080/01972240290074959

Kleinwächter, W. (2000). ICANN between technical mandate and political challenges. *Telecommunications Policy*, *24*(6-7), 553-563.

Knoespel, K. et Zhu, J. (2008). "Continuous materiality through a hierarchy of computational code", *Théorie, Littérature, Epistémologie*, n° *25*, pp. 235-247.

Konradova, N. & Schmidt, H. (2014), "From the utopia of autonomy to a political battlefield: towards a history of the "Russian Internet", in M.S. Gorham, I. Lunde, & M. Paulsen (eds.), *Digital Russia. The Language, Culture and Politics of New Media Communication,* London and New York: Routledge

Kopel, K. (2013). Operation seizing our sites: How the federal government is taking domain names without prior notice. Berkeley Technology Law Journal 28(4): 859–900.

Kozlov, V., & Filipenok, A. (2016, August 9). Miting protiv zakona Yarovoy v Moskve sobral neskolko tysyach chelovek [Meeting against Yarovaya law gathered several thousand people]. RBC. Retrieved from http://www.rbc.ru/politics/09/08/2016/57aa0a259a79470ed51332fd

Lampland, M. & Star, S. L., *Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life*, Ithaca, NY: Cornell University Press, 3–24.

Larkin, B. (2013). “The politics and poetics of infrastructure”, *Annual Review of Anthropology*, *n*° 42, pp. 327-343.

Lascoumes, P., & Serverin, E. (1986). Théories et pratiques de l’effectivité du droit. *Droit et société*, *2*, 127.

Latour, B. (1988) The Pasteurization of France. Cambridge, MA: Harvard University Press.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. *Shaping technology/building society: Studies in sociotechnical change*, *1*, 225-258.

Latour, B. (2000). The Berlin key or how to do words with things, in Graves-Brown, P. (ed.) *Matter, materiality and modern culture*. London: Routledge, pp.10-21.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford, England: Oxford University Press.

Latour, B., Lemonnier, P. (eds., 1994). *De la préhistoire aux missiles balistiques. L’intelligence sociale des techniques*, Paris, La Découverte.

Latzko-Toth, G. (2010). *La co-construction d'un dispositif sociotechnique de communication: le cas de l'Internet Relay Chat*. Thèse de doctorat, Université du Québec à Montréal.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice*, *5* (4), 379-393.

Law, J. (2009). Actor network theory and material semiotics. In B. Turner (ed.), *The New Blackwell Companion to Social Theory* pp. 141–158. Hoboken, NJ: Wiley-Blackwell.

Lee, C. P., Dourish, P., & Mark, G. (2006, November). The human infrastructure of cyberinfrastructure. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work* (pp. 483-492).

Le Fessant, F. (2009). « Les réseaux sociaux au secours des réseaux pair-à-pair », *Défense nationale et sécurité collective*, 3 : 29-35.

Leonardi, P. (2010). “Digital materiality? How artifacts without matter, matter”, *First Monday*, n°15.

Lessig, L. (1999). *Code: And Other Laws Of Cyberspace*. New York: Basic Books.

Levinson, N. (2002). “Internet governance and institutional change.” *The Tocqueville Review/La Revue Tocqueville 23* (2): 125–41.

Levinson, N. S., & Marzouki, M. (2015). Internet governance institutionalization: process and trajectories. In *Global Governance Facing Structural Changes* (pp. 17-35). Palgrave Macmillan, New York.

Limonier, K. (2018). *Ru.net: géopolitique du cyberespace russophone*. Editions L’Inventaire.

Litvinenko, A. (2021). Re-Defining Borders Online: Russia’s Strategic Narrative on Internet Sovereignty. *Media and Communication*, *9*(4), 5-15.

Löblich, M., & Karppinen, K. (2014). Guiding Principles for Internet Policy: A Comparison of Media Coverage in Four Western Countries. *The Information Society*, *30*(1), 45–59. https://doi.org/10.1080/01972243.2013.855688

Löblich, M., & Wendelin, M. (2012). ICT policy activism on a national level: Ideas, resources and strategies of German civil society in governance processes. *New Media & Society*, *14*(6), 899–915. https://doi.org/10.1080/01972243.2013.855688

Loconto, A. & Busch, L. (2010). "Standards, techno-economic networks, and playing fields: Performing the global market economy", *Review of International Political Economy*, 17(3): 507–536.

Loveluck, B., & Holeindre, J. V. (2021). Politiques du hacking : enquête sur les ruses numériques. *Quaderni*, (2), 9-24.

Luhman, N. (2000). Familiarity, Confidence, Trust: Problems and Alternatives. In Gambetta, D. (ed.) *Trust: Making and Breaking Cooperative Relations*, University of Oxford, pp. 94-107.

Lynn, S. (2002, February 24). "President's report: ICANN—The case for reform". The Internet Corporation for Assigned Names and Numbers (ICANN). Marina del Ray, CA. http://archive.icann.org/en/general/lynn-reform-proposal-24feb02.htm

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2). https://doi.org/10.1177/2053951714541861

Mabi, C., & Massit-Folléa, F. (2013). La gouvernance des biens communs. Du climat à Internet, premières leçons d'une comparaison. *Communication. Information médias théories pratiques*, *31*(2).

MacKinnon, R. (2012). The netizen. *Development*, *55*(2), 201-204.

Macq, H. & Jacquet, V. (2018). S'engager dans un cyberparti. Internet et militantisme au sein du parti pirate belge [To engage in a cyberparty: Internet in the Belgian Pirate Party Membership]. *RESET*, *7*. doi:10.4000/reset.1102

Madianou, M. (2020). <? covid19?> A Second-Order Disaster? Digital Technologies During the COVID-19 Pandemic. *Social media+ society*, *6*(3), 2056305120948168.

Mager, A. (2012). Algorithmic ideology: How capitalist society shapes search engines. *Information, Communication & Society*, *15*(5), 769-787.

Mager, A. (2017). Search engine imaginary: Visions and values in the co-production of search technology and Europe. *Social Studies of Science*, *47*(2), 240-262.

Malcic, S. (2016). The problem of future users: how constructing the DNS shaped internet governance. *Internet Policy Review*, 5(3). DOI: 10.14763/2016.3.434

Malcolm, J. (2008). *Multi-Stakeholder Governance and the Internet Governance Forum*. Wembley, WA: Terminus Press.

Mallard, A., Méadel, C. & Musiani, F. (2014). "The paradoxes of distributed trust: peer-to-peer architecture and user confidence in Bitcoin", *Journal of Peer Production*, n°4.

Mansell, R. (2012). *Imagining the Internet: Communication, Innovation, and Governance*. Oxford, UK: Oxford University Press.

Mantelero, A. (2013). The EU proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review* 29(3): 229–235.

Marcus, G. E. (2012). "Multi-sited ethnography: Five or six things I know about it now", in *Multi-sited ethnography*, London: Routledge, pp. 24-40.

Maréchal, N. (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication, 5*(1), 29–41. doi:10.17645/mac.v5i1.808

Marino, M. C. (2020). *Critical code studies*. Cambridge, MA: The MIT Press.

Markham, A. N., & Baym, N. K. (Eds.). (2008). *Internet inquiry: Conversations about method*. Sage Publications.

Marquet, C. (2018). Ce nuage que je ne saurais voir. Promouvoir, contester et réguler les data centers à Plaine Commune. *Tracés. Revue de Sciences humaines*, (35), 75-98.

Marsden, C. T. (2017). *Network neutrality: From policy to law to regulation*. Manchester: Manchester University Press.

Masutti, C. (2020). *Affaires privées : Aux sources du capitalisme de surveillance*. Caen: C & F Éditions.

Mateescu, A., & Elish, M. C. (2019). *AI in context: The labor of integrating new technologies*. Data & Society Report.

Mathiason, J. (2008). *Internet Governance: The New Frontier of Global Institutions.* London: Routledge. doi:10.4324/9780203946084

Maurer, B., Nelms, T. C., and Swartz, L. (2013). "When perhaps the real problem is money itself": the practical materiality of Bitcoin. *Social Semiotics*, 23(2): pp. 261-277.

Meier-Hahn, U. (2015, February 5). Internet Interconnection: Networking in Uncertain Terrain [Blog post]. *RIPE Labs*. Retrieved from https://labs.ripe.net/Members/uta_meier_hahn/internet-interconnection-networking-in-uncertain-terrain

Merrill, K. (2016). Domains of Control: Governance of and by the Domain Name System, in Musiani, F., Cogburn, D. L., DeNardis, L. & Levinson, N. S. (2016, eds.). *The Turn to Infrastructure in Internet Governance*, New York: Palgrave Macmillan (pp. 89-106).

Mervich, C. (2020). *The Human Infrastructure of Artificial Intelligence*. Master's thesis, University of Twente.

Meyer, T. (2012). Graduated Response in France: The Clash of Copyright and the Internet. *Journal of Information Policy*, *2*, 107–127. doi:10.5325/jinfopoli.2.2012.0107

Milan, S. (2013). *Social movements and their technologies: Wiring social change*, Berlin: Springer.

Milan, S. (2015). From social movements to cloud protesting: the evolution of collective identity. *Information, Communication & Society*, *18*(8), 887–900. doi:10.1080/1369118x.2015.1043135

Milan, S. (2019). Acting on data (fication). In Stephansen, H. C., & Treré, E. (Eds.). (2019). *Citizen media and practice: Currents, connections, challenges*. Routledge, pp. 212-226.

Milan, S. & ten Oever, N. (2017). Coding and encoding rights in internet infrastructure. *Internet Policy Review*, 6(1). DOI: 10.14763/2017.1.442

Milan, S., & van der Velden, L. (2018). Reversing Data Politics: An Introduction to the Special Issue. *Krisis: Journal for contemporary philosophy*, *2018*(1), 1-3.

Miller, C. C. (2012). "As Violence Spreads in Arab World, Google Blocks Access to Inflammatory Video." *New York Times*, September 17, 2012.

Mitchell, T., Charbonnier, P., & Vincent, J. (2018). Étudier les infrastructures pour ouvrir les boîtes noires politiques. Entretien avec Timothy Mitchell. *Tracés. Revue de Sciences humaines*, (35), 209-228.

Mitrou, L., and Karyda, M. (2012). EU's Data Protection Reform and the right to be forgotten—A legal response to a technological challenge?, Proceedings of the 5th International Conference of Information Law and Ethics.

Monsees, L. (2019). *Crypto-Politics. Encryption and Democratic Practices in the Digital Era*. Abingdon and New York, Routledge.

Morris, J. and Davidson, A. (2003). "Policy Impact Assessments: Considering the Public Interest in Internet Standards Development", 31st Research Conference on Communication, Information and Internet Policy, http://www.cdt.org/publications/pia.pdf

Morris, M., & Ogan, C. (1996). The Internet as mass medium. *Journal of Computer-Mediated Communication*, *1*(4).

Mueller, M. L. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: MIT Press.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge: MIT Press.

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779-801.

Mueller, M., & Badiei, F. (2020). Inventing Internet Governance: The Historical Trajectory of the Phenomenon and the Field. In DeNardis, L., Cogburn, D., Levinson, N. S., & Musiani, F. (Eds.) *Researching internet governance: Methods, frameworks, futures*. Cambridge, MA: The MIT Press, 59-83.

Mueller, M. L., Kuehn, A., & Santoso, S. M. (2012). Policing the network: Using DPI for copyright enforcement. *Surveillance & Society*, *9*(4), 348–364.

Muir, S. (2011). "Multisited ethnography", in Southerton, D. (ed.) *Encyclopedia of Consumer Culture*, London: Sage, http://dx.doi.org/10.4135/9781412994248.n375

Musiani, F. (2012). Caring About the Plumbing: On the Importance of Architectures in Social Studies of (Peer-to-Peer) Technology. *Journal of Peer Production*, 1.

Musiani, F. (2013). Dangerous Liaisons? Governments, companies and Internet governance, *Internet Policy Review*, 2(1), DOI: 10.14763/2013.1.108

Musiani, F. (2015). Practice, Plurality, Performativity and Plumbing: Internet Governance Research Meets Science and Technology Studies. *Science, Technology and Human Values*, *40*(2): 272-286.

Musiani, F. (2015b). *Nains sans géants : Architecture décentralisée et services Internet*. Paris : Presses des Mines.

Musiani, F. (2016). Alternative technologies as alternative institutions: The case of the domain name system. In *The turn to infrastructure in Internet governance* (pp. 73-86). Palgrave Macmillan, New York.

Musiani, F. (2018). L'invisible qui façonne. Etudes d'infrastructure et gouvernance d'Internet, *Tracés*, 35, pp. 161-176.

Musiani, F. (2020). Science and Technology Studies Approaches to Internet Governance: Controversies and Infrastructures as Internet Politics. In DeNardis, L., Cogburn, D., Levinson, N. S., & Musiani, F. (Eds.) *Researching internet governance: Methods, frameworks, futures*. Cambridge, MA: The MIT Press, pp. 85-104.

Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. S. (Eds.) (2016). *The turn to infrastructure in Internet governance*. New York: Palgrave-Macmillan. doi:10.1057/9781137483591

Musiani, F. & Ermoshina, K. (2017). « What is a Good Secure Messaging Tool? The EFF Secure Messaging Scorecard and the Shaping of Digital (Usable) Security », *Westminster Papers in Communication and Culture*, 12 (3), pp. 51-71.

Musiani, F., Mallard, A. & Méadel, C. (2017/8). Governing What Wasn't Meant to Be Governed: A Controversy-Based Approach to the Study of Governance in Bitcoin. In M. Campbell-Verduyn (ed.), *Bitcoin and Beyond*, Routledge, pp. 133-156.

Musiani, F., Méadel, C. & Mallard, A. (2015). "Bitcoin". In Méadel, C. & Musiani, F. (eds.), *Abécédaire des architectures distribuées*, Paris: Presses des Mines, pp. 43-47. https://books.openedition.org/pressesmines/2110

Musiani, F., Paloque-Bergès, C., Schafer, V. & Thierry, B. G. (2019). *Qu'est-ce qu'une archive du Web?*. Marseille: OpenEdition Press

Musiani, F. & Schafer, V. (2018). "Governance, an issue ranging from the Internet to digital technology." *Annales des Mines*, 4. http://www.annales.org/edit/enjeux-numeriques/2018/resumes/decembre/02-en-resum-FR-AN-decembre-2018.html

Musiani, F. & Schafer, V. (2021). "Global Governance: A Short History of Debates Born With the Telegraph and Popularized by the Internet", *in* G. Balbi, N. Ribeiro, V. Schafer, C. Schwarzenegger (eds.), *Digital Roots: Historicizing Media and Communication Concepts of the Digital Age*, De Gruyter Oldenbourg, p. 117-136.

Myers West, S. (2018). Cryptographic imaginaries and the networked public. *Internet Policy Review*, 7 (2). DOI: 10.14763/2018.2.792

Nakamoto, S. (2008). "Bitcoin: A peer-to-peer electronic cash system". https://bitcoin.org/bitcoin.pdf

Naranayan, A. (2015). "Analyzing the 2013 Bitcoin fork: centralized decision-making saved the day", Freedom To Tinker Blog, July 28, 2015, https://freedom-to-tinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork-centralized-decision-making-saved-the-day/

Negro, G. (2017). *Internet in China*. London: Palgrave Macmillan.

Nelms, T. C. (2016). Alt. economy: strategies, tensions, challenges, *Journal of Cultural Economy*, 9(5), p. 507-512.

Nissenbaum, H. (2001). How computer systems embody values. *Computer, 34*(3), 119–120. doi:10.1109/2.910905

Nocetti, J. (2015). Russia's 'dictatorship-of-the-law' approach to internet policy. *Internet Policy Review, 4*(4). DOI: 10.14763/2015.4.380

Nossik, A. (2014, March 19) "Dyryavoe sito censury". ["Leaky strainer of censorship"] Retrieved from http://dolboeb.livejournal.com/2652283.html

Nye, J. S. (2014). *The regime complex for managing global cyber activities* (Vol. 1). USA: Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University.

Oates, S. (2013), *Revolution Stalled. The Political Limits of the Internet in the Post-Soviet Sphere.* Oxford University Press

Ohm, P. (2009). "The Rise and Fall of Invasive ISP Surveillance," University of Illinois Law Review; University of Colorado Law Legal Studies Research Paper No. 08-22.

O'Neill, P. H. (2014). "The final confessions of a Silk Road kingpin", *DailyDot*, January 22, 2014, http://www.dailydot.com/crime/silk-road-confession-steven-sadler-nod/

O'Rourke, C., & Kerr, A. (2017). Privacy Shields for Whom? Key Actors and Privacy Discourses on Twitter and in Newspapers. *Westminster Papers in Communication and Culture, 12*(3). doi:10.16997/wpcc.264

Oudshoorn, N. and Pinch, T. (2005}. *How users matter: The co-construction of users and technology*, Cambridge, MA: The MIT Press.

Padovani, C. (2004). The World Summit on the Information Society: Setting the Communication Agenda for the 21st Century? An Ongoing Exercise. *International Communication Gazette, 66*(3–4), 187–191. doi:10.1177/0016549204043604

Padovani, C., & Santaniello, M. (2018). Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system. *International Communication Gazette*, *80*(4), 295–301. doi:10.1177/1748048518757114

Padovani, C., & Shade, L. R. (2016). Introduction to the Special Issue: Gendering Global Media Policy: Critical Perspectives on "Digital Agendas". *Journal of Information Policy*, *6*(1), 332–337. doi:10.5325/jinfopoli.6.2016.0332

Panday, J. & Malcolm, J. (2018). "The Political Economy of Data Localization", *Partecipazione e conflitto,* 11, pp. 511–527.

Paré, D. (2003). *Internet Governance in Transition: Who is the Master of This Domain*, Oxford: Rowan and Littlefield.

Passeron, J. C., & Revel, J. (2005). Penser par cas. Raisonner à partir de singularités. In Passeron, J. C., & Revel, J. (eds.), *Penser par cas*, Paris : Editions de l'EHESS, pp. 9-44.

Pavan, E. (2012). *Frames and Connections in the Governance of Global Communications: A Network Study of the Internet Governance Forum*. Lanham, MD: Lexington Books.

Pelizza, A. (2016). Developing the Vectorial Glance: Infrastructural inversion for the new agenda on governmental information systems, *Science, Technology and Human Values,* 41(2): 298-321.

Pierson, J. (2012). Online privacy in social media: a conceptual exploration of empowerment and vulnerability. *Communications & Strategies*, 88, 99–120

Pinson, G. (2015). Gouvernance et sociologie de l'action organisée. Action publique, coordination et théorie de l'État. *L'Année sociologique*, 65, 483-516.

Pohle, J. (2016). Multistakeholder governance processes as production sites: enhanced cooperation "in the making", *Internet Policy Review*, 5(3). DOI: 10.14763/2016.3.432

Pohle, J. (2018). The Internet as a global good: UNESCO's attempt to negotiate an international framework for universal access to cyberspace. *International Communication Gazette, 80*(4), 354–368. doi:10.1177/1748048518757140

Pohle, J., Hösl, M., & Kniep, R. (2016). Analysing internet policy as a field of struggle. I*nternet Policy Review*, *5*(3).

Pohle, J., & Thiel, T. (2020). "Digital sovereignty", *Internet Policy Review*, *9*(4).

Pohle, J., & van Audenhove, L. (2017). Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change. *Media and Communication, 5*(1), 1-6. doi:10.17645/mac.v5i1.932

Ponte, S., Gibbon, P. & Vestergaard, J. (eds., 2011). *Governing through Standards: Origins, Drivers and Limitations*, New York, Palgrave Macmillan.

Ponterotto, J. G. (2006). Brief note on the origins, evolution, and meaning of the qualitative research concept thick description. *The Qualitative Report*, *11*(3), 538-549.

Powell, A., & Cooper, A. (2011). Net neutrality discourses: comparing advocacy and regulatory arguments in the United States and the United Kingdom. *The Information Society*, *27*(5), 311–325. doi:10.1080/01972243.2011.607034

Proulx, S. (2009). 'L'intelligence du grand nombre : la puissance d'agir des contributeurs sur Internet – limites et possibilités', *7ème colloque du chapitre français de l'ISKO, Intelligence collective et organisation des connaissances*, Lyon, 24-26 juin 2009. http://pro.ovh.net/~iskofran/pdf/isko2009/PROULX.pdf

Puppis, M. (2010). Media Governance: A New Concept for the Analysis of Media Policy and Regulation. *Communication, Culture & Critique, 3*(2), 134–149. doi:10.1111/j.1753-9137.2010.01063.x

Raboy, M., Landry, N., & Shtern, J. (2010). *Digital Solidarities, Communication Policy and Multi-stakeholder Global Governance: The Legacy of the World Summit on the Information Society*. New York: Peter Lang.

Raymond, M. & DeNardis, L. (2015). "Multistakeholderism: Anatomy of an inchoate global institution." *International Theory* 7, 3: 572–616.

Roberts, P. (2014). "If This Is Cyberwar, Where Are All the Cyberweapons?", Technology Review, January 27, 2014. Available at http://www.technologyreview.com/news/523931/if-this-is-cyberwar-where-are-all-the-cyberweapons/

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York, NY: Free Press.

Ron, D., and Shamir, A. (2013). "Quantitative Analysis of the Full Bitcoin Transaction Graph", BT - Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5

Rubinstein, I & van Hoboken, J. (2014). "Privacy and security in the cloud: Some realism about technical solutions to transnational surveillance in the post-Snowden era." NYU School of Law, Public Law Research Paper No. 14–46, Available at: https://ssrn.com/abstract=2443604.

Russell, A. L. (2003, August). The W3C and its Patent Policy Controversy: A Case Study of Authority and Legitimacy in Internet Governance. Paper presented at the TPRC conference, 2003. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2056900

Russell, A. (2012). "Histories of Networking vs. the History of the Internet", Paper presented at the SIGCIS Workshop, Copenhagen, Denmark, October 7, 2012.

Sargsyan, T. (2016). The privacy role of information intermediaries through self-regulation. *Internet Policy Review*, 5(4). DOI: 10.14763/2016.4.438

Sarikakis, K. (2004). Ideology and policy: Notes on the shaping of the Internet. *First Monday, 9*(8). doi:10.5210/fm.v9i8.1167

Savov, V. (2014). "Larry Page wants a Google 2.0 that will build cities and airports, report says", The Verge, 18 septembre 2014. https://www.theverge.com/2014/9/18/6375233/larry-page-wants-a-google-2-0-that-will-build-cities-and-airports

Schaar, P. (2010). Privacy by Design. *Identity in the Information Society*, 3(2) : 267-274.

Schafer, V. (2015). Part of a whole: RENATER, a 20-year old network within the Internet. *Technology and Culture* 50(2): 217–235.

Schafer, V., Le Crosnier, H. & Musiani, F. (2011). *La neutralité de l'Internet, un enjeu de communication*. Paris: CNRS Editions/Les Essentiels d'Hermès.

Schepin, A. (2016, August 1). Irkutskie Operatory Svyazi O Nedostatkah Paketa Yarovoy [ISPs from Irkutsk: On the drawbacks of Yarovaya Package]. IRK. Retrieved from https://www.irk.ru/news/articles/20160801/package

Schmidt, S. K. et Werle, R. (1998). *Coordinating Technology: Studies in the International Standardization of Telecommunications*. Cambridge and London: The MIT Press.

Scholz, T. (2012). *Digital labor: The Internet as playground and factory*. Routledge.

Schulze, M. (2017). Clipper meets Apple vs. FBI: a comparison of the cryptography discourses from 1993 and 2016. *Media and Communication*, *5*(1), 54-62.

Schwemer, S. F. (2021). Location, location, location! Copyright content moderation at non-content layers. In *The Routledge Handbook of EU Copyright Law* (pp. 378-395). Routledge.

Seltzer, W. (2011). "Exposing the Flaws of Censorship by Domain Name," *IEEE Security and Privacy*, 9(1), pp. 83-87.

Simone, A. (2004). People as infrastructure: Intersecting fragments in Johannesburg. *Public culture*, *16*(3), 407-429.

Sims, B., & Henke, C. R. (2012). Repairing credibility: Repositioning nuclear weapons knowledge after the Cold War. *Social Studies of Science*, *42*(3), 324-347.

Soldatov, A., and Borogan, I. (2015). *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*. New York: PublicAffairs.

Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*: New Haven, CT: Yale University Press.

Star, S.L. (1999). The ethnography of infrastructure, *American Behavioral Scientist*, 43(3), p. 377-391.

Star, S. L. (1990). Power, technology and the phenomenology of conventions: on being allergic to onions. *The Sociological Review*, *38*(1_suppl), 26-56.

Star, S. L. and Griesemer, J. (1989). Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39', *Social Studies of Science*, 19 (3): 387-420.

Star, S. L. & Lampland, M. (2009). "Reckoning with Standards", in Lampland, M. & Star, S. L., *Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life*, Ithaca, NY: Cornell University Press, 3–24.

Star, S. L. and Ruhleder, K. (1994). "Steps towards an ecology of infrastructure: Complex problems in design and access for large-scale collaborative systems." *Proceedings of the Conference on Computer Supported Cooperative Work*. Chapel Hill, NC. ACM Press, New York: 253–264.

Stein, L. (2008). Speech without rights: The status of public space on the Internet. *The Communication Review*, *11*(1), 1-23.

Stevenson, S. (2009). Digital Divide: A Discursive Move Away from the Real Inequities. *The Information Society*, *25*(1), 1–22. 10.1080/01972240802587539

Subra, P. (2016). *Géopolitique locale. Territoires, acteurs, conflits*, Paris, Armand Colin.

Ten Oever, N., Milan, S., & Beraldo, D. (2020). « Studying Discourse in Internet Governance through Mailing-List Analysis ». In DeNardis, L., Cogburn, D., Levinson, N. S., & Musiani, F. (Eds.) *Researching internet governance: Methods, frameworks, futures*. Cambridge, MA: The MIT Press, pp. 213-229.

Timmermans, S. & Berg, M. (2003). *The gold standard: The Challenge of Evidence-Based Medicine and Standardization in Health Care*, Philadelphia, Temple University Press.

Toupin, S., & Couture, S. (2021). Introduction: qu'est-ce que la résistance numérique?. *Revue Possibles*, *45*(1), 10-19.

Tréguer, F. (2017). Intelligence Reform and the Snowden Paradox : The Case of France. *Media and Communication*, *5*(1). doi:10.17645/mac.v5i1.821 Available at https://hal.archives-ouvertes.fr/hal-01481648/

Trompette, P. & Vinck, D. (Eds., 2009). Retour sur la notion d'objet-frontière, *Revue d'anthropologie des connaissances*, 3(1).

Tsing, A. L. (2011). *Friction: An ethnography of global connection*. Princeton University Press.

Tubaro, P., & Casilli, A. A. (2019). *Micro-work, artificial intelligence and the automotive industry*. Journal of Industrial and Business Economics, 1-13.

Tusikov, N. (2016). *Chokepoints: Global Private Regulation on the Internet*. University of California Press.

Unger, N., et al. (2015). SoK: Secure messaging. In: 2015 IEEE Symposium on Security and Privacy, 232–49. IEEE. DOI: https://doi.org/10.1109/SP.2015.22

Van Audenhove, L., Vanwynsberghe, H., & Mariën, I. (2018). Media Literacy Policy in Flanders – Belgium: From Parliamentary Discussions to Public Policy. *Journal of Media Literacy Education*, *10*(1), 59–81. doi: 10.23860/jmle-2018-10-1-4

Van Eeten, M. (2017). "Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity." *Digital Policy, Regulation and Governance* 19 (6): 429–48.

Van Eeten, M. & Mueller, M. (2013). "Where is the governance in Internet governance?" *New Media & Society,15 (5):* 720–36.

Vargas-Leon, P. (2016). Tracking Internet shutdown practices: Democracies and hybrid regimes. In Musiani, F. et al., *The Turn to Infrastructure in Internet Governance* (pp. 167-188). Palgrave Macmillan, New York.

Velasco, P. R. (2016). Sketching Bitcoin: Empirical Research of Digital Affordances. In Kubitschko, S. and Kaun, A. (eds.) *Innovative Methods in Media and Communication Research*, Springer International Publishing, pp. 99-122.

Villegas, M. G., & Lejeune, A. (2011). La sociologie du droit en France: de deux sociologies à la création d'un projet pluridisciplinaire?. *Revue interdisciplinaire d'études juridiques*, *66*(1), 1-39.

Volkov, L. (2016) "Don't Move Personal Data to Russia!" Retrieved from Change.org https://www.change.org/p/facebook-google-twitter-don-t-move-personal-data-to-russia

von Arx, K. G. and Hagen, G. R. (2002). Sovereign domains: A Declaration of independence of ccTLDs from foreign control. *Richmond Journal of Law and Technology* 9: 4–8.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, *26*(1), 23-30.

Weber, R. H. (2011). The *Right to Be Forgotten:* More Than a Pandora's Box?. JIPITEC, Vol. 2. Available at https://www.jipitec.eu/issues/jipitec-2-2-2011/3084

Weinberg, J. (2011). "Governments, privatization, and privatization: ICANN and the GAC." *Michigan Telecommunications and Technology Law Review 18,* 1.

West, C. and Zimmerman, D. H. (1987). Doing gender. *Gender & Society*, *1*(2), 125-151.

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., & Schwartz, O. (2018). *AI Now report 2018*. AI Now Institute at New York University.

Whitten, A. and Tygar, J. D. (1999) Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Usenix Security.

Winner, L. (1980). "Do artifacts have politics?", *Daedalus* 109: 121–136.

Winner, L. (1986). Myth information: Romantic politics in the computer revolution. In *Philosophy and technology II* (pp. 269-289). Springer, Dordrecht.

Woolgar, S., & Neyland, D. (2013). *Mundane governance: Ontology and accountability*. Oxford University Press.

Wu, T. S. (1997). "Cyberspace sovereignty? The Internet and the international system." *Harvard Journal of Law and Technology 10* (3): 647–66.

Wu, T. S. and Yoo, C. (2007). "Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate", *Federal Communications Law Journal*, 59(3).

Yan, Z., Gaspar, R., & Zhu, T. (2021). How humans behave with emerging technologies during the COVID-19 pandemic?. *Human behavior and emerging technologies*, *3*(1), 5.

Yates, J. (1993). Co-evolution of information-processing technology and use: Interaction between the life insurance and tabulating industries. *Business History Review*, *67*(1), 1-51.

Yoo, Y. (2012). "Digital materiality and the emergence of an evolutionary science of the artificial", in P. Leonardi, B. A. Nardi, J. Kallinikos (eds.), *Materiality and organizing: Social interaction in a technological world*, pp. 134-154.

Yoo, C. S. & Blanchette, J.-F. (2015). *Regulating the Cloud: Policy for Computing Infrastructure*, Cambridge, MA, The MIT Press.

Zalnieriute, M., & Milan, S. (2019). Internet Architecture and Human Rights: Beyond the Human Rights Gap. *Policy & Internet, 11*(1), 6–15. doi:10.1002/poi3.200

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, *1*(1), 22-32.

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". *Politics & Policy, 45*(3), 432–464. doi:10.1111/polp.12202

Ziewitz, M. (2016). Governing Algorithms: Myth, Mess, and Methods. *Science, Technology and Human Values, 41*(1): 3-16.

Ziewitz, M. and Pentzold, C. (2014). In Search of Internet Governance: Performing Order in Digitally Networked Environments. *New Media & Society, 16*(2): 306-322.

Zittrain, J. (2008). *The future of the Internet—and how to stop it*. New Haven, CT: Yale University Press.

Zittrain, J. and Edelman, B. (2003). Internet filtering in China. *Internet Computing, IEEE* 7(2): 70–77.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London, UK: Profile Books.

Zuckerberg, M. (2019, March 30). The Internet needs new rules. Let's start in these four areas. *The Washington Post*. Retrieved from: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

Zuckerman, E. (2010). « Intermediary Censorship », in Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace, Cambridge, MA*: The MIT Press, pp. 71-86.