Infrastructures d'internet, gouvernance et libertés citoyennes

Francesca Musiani

INFRASTRUCTURES D'INTERNET, GOUVERNANCE ET LIBERTÉS CITOYENNES

Un ensemble d'intérêts économiques et politiques se tourne aujourd'hui vers l'infrastructure Internet en tant qu'instrument pour aborder des controverses, voire des conflits, socio-techniques diversifiés, survenant à la fois hors ligne et en ligne. Cet article propose plusieurs illustrations pour comprendre comment les infrastructures d'Internet sont utilisées à des fins de gouvernance, de manières qui affectent ou sont susceptibles d'affecter les droits humains et les libertés citoyennes.

Francesca MUSIANI
Chargée de recherche CNRS
Directrice adjointe, Centre Internet et Société

Un ensemble d'intérêts économiques et politiques se tourne aujourd'hui 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[1].

1 - Francesca Musiani, Derrick L. Cogburn, Laura DeNardis et Nanette S. Levinson, *The turn to infrastructure in Internet governance*, New York, Palgrave-Macmillan, 2016.

Au sein des infrastructures Internet, on peut observer comment un certain nombre de dynamiques liées aux droits humains et aux libertés citoyennes – ayant trait, par exemple, à la liberté d'expression et à la censure, ou à la protection de la vie privée et la 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 ou de données, 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[2]. 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. Cet article montre, à travers plusieurs exemples, comment les infrastructures d'Internet sont utilisées à des fins de gouvernance de manières qui affectent ou sont susceptibles d'affecter les droits humains et les libertés citoyennes.

COUPURES D'INTERNET : LES *KILL-SWITCH*

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

2 - Anupam Chander et Uyen P. Le, « Breaking the Web: Data Localizaton vs. the Global Internet », *UC Davis Legal Studies Research Paper Series*, No. 378, April 2014.

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, au 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.

MÉDIATION ET MODÉRATION DES CONTENUS

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[3]. 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

3 - Romain Badouard, *Les nouvelles lois du Web : modération et censure*, Paris, Seuil, 2020.

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 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 ? À 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[4] 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[5] ».

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 citoyennes.

DROIT À L'OUBLI

Google a également été au centre d'une controverse importante, qui revient régulièrement à ce jour, sur la mise en œuvre,

4 - 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.

5 - Claire Cain Miller, « As Violence Spreads in Arab World, Google Blocks Access to Inflammatory Video », *New York Times*, September 17, 2012.

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[6] », 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[7]. Cependant, dans la pratique, 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[8], 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[9]. Alors que le Règlement général sur la protection des données (RGPD)[10] 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, du lien entre infrastructures Internet et gouvernance et ses conséquences pour la définition et la protection

6 - Alessandro Mantelero, « The EU proposal for a General Data Protection Regulation and the roots of the "right to be forgotten" ». *Computer Law & Security Review* 29(3), 2013, pp. 229–235.

7 - Rolf H. Weber, « The Right to Be Forgotten: More Than a Pandora's Box? », *JIPITEC*, Vol. 2, 2011. Available at https://www.jipitec.eu/issues/jipitec-2-2-2011/3084

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

9 - Lilian Mitrou et Maria Karyda, « 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, 2012.

10 - https://eur-lex.europa.eu/eli/reg/2016/679/oj

des libertés civiles est la pertinence croissante des approches dites de « protection de la vie privée dès la conception », ou *privacy by design* (PbD)[11]. 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, associant 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, 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[12]. La protection de la vie privée est de plus en plus intégrée aux infrastructures.

*
* *

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 ont été introduites dans l'infrastructure technologique, pour la plupart, dans un objectif de préservation, de « bon » fonctionnement et de sécurité du « réseau des réseaux ». Cependant, et notamment durant la dernière décennie, les infrastructures Internet sont investies par une variété d'acteurs afin de faire de la « politique par d'autres moyens »[13]. On se trouve donc à observer deux « couches »

11 - Ann Cavoukian, Special Issue: « Privacy by design: The next generation in the evolution of privacy », *Identity in the Information Society* 3(2), 2010 ; Seda Gürses, Carmela Troncoso et Claudia Diaz, « Engineering privacy by design », *Computers, Privacy & Data Protection*, 14(3), 2011, p. 25 ; Ann Cavoukian, « Understanding how to implement privacy by design, one step at a time », *IEEE Consumer Electronics Magazine*, 9(2), 2020, pp. 78-82.

12 - https://eur-lex.europa.eu/eli/reg/2016/679/oj#d1e3063-1-1

13 - Bruno Latour, *The Pasteurization of France*, Cambridge, MA: Harvard University Press, 1988, p. 229.

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 humains et des libertés citoyennes en ligne ■