Être souverain en 2030 : la gouvernance des infrastructures numériques

Gilles Babinet, Théophile Lenoir

Dans Revue internationale et stratégique 2020/2 N° 118 , pages 147 à 153
Éditions IRIS éditions

ISSN 1287-1672
ISBN 9782200933340
DOI 10.3917/ris.118.0147
Date de mise en ligne : 01/07/2020

Être souverain en 2030 : la gouvernance des infrastructures numériques

Gilles Babinet
Conseiller sur les questions numériques à l'Institut Montaigne.
Théophile Lenoir
Responsable du programme Numérique à l'Institut Montaigne.

À mesure que les sociétés se numérisent, il est manifeste que, sur plusieurs plans, les États perdent de leur souveraineté. Entre de nombreux exemples, ils dépendent de systèmes étrangers pour le stockage de données essentielles, pour la réalisation de cartographies, pour l'offre de services tels que la gestion du trafic, pour la mise en place de nouveaux systèmes éducatifs, ou encore pour la création des infrastructures logicielles de défense. De nombreux travaux ont été menés sur ce qu'est la souveraineté à l'heure du numérique[1], mais nous sommes encore loin d'un consensus sur la question. Si une prise de conscience commence à poindre en Europe, elle est, sur bien des plans, loin d'aboutir à la mise en œuvre de politiques publiques efficaces.

Un certain nombre de domaines posent en effet question en matière de souveraineté : la sécurité, le droit, l'économie, la fiscalité et la monnaie. Pour chacun d'entre eux, les États ont eu l'habitude d'édicter des règles votées démocratiquement et s'appliquant de manière contraignante. Cette autorité semble désormais remise en cause : la présence physique de la police ou de l'armée ne garantit plus la sécurité des citoyens et des entreprises dont les

1. Notons, en France et entre autres, le rapport de la Commission d'enquête sur la souveraineté numérique du Sénat, « Le devoir de souveraineté numérique », n° 7, tome 1, 1er octobre 2019.

systèmes d'information sont attaqués ; le droit peine à encadrer les dernières avancées technologiques qui changent le champ des possibles ; le modèle économique des entreprises numériques échappe parfois à la compréhension de ce que constitue un monopole, etc.

Dès lors, à horizon de dix ans, faut-il tenter de réaffirmer le modèle d'autrefois – c'est-à-dire, le monopole de l'autorité par l'État démocratique –, ou bien est-il envisageable pour l'État de repenser ce que cela signifie d'être souverain ? Nous nous pencherons ici sur cette seconde éventualité, en nous appuyant sur deux cas qui aident à comprendre les enjeux de la décennie qui s'ouvre : la régulation du développement des réseaux de cinquième génération (5G) d'une part, et celle des manipulations de l'information d'autre part. L'État peinera en effet à rester souverain tant qu'il imposera aux acteurs numériques de prendre des mesures derrière des portes closes. Il doit ainsi s'appuyer sur la compétence des acteurs privés pour créer des règles efficaces à l'ère du numérique en imposant, pour ce faire, des principes de transparence aux acteurs numériques, et en développant une expertise numérique pour s'assurer du respect de ces règles. Dans ce modèle, l'État ne se positionne donc plus au-dessus, mais à côté des entreprises, qui l'aident à atteindre ses objectifs.

La 5G : « Pour accéder au marché européen, il faudra accepter nos règles »

Les acteurs numériques sont des entreprises dont une partie de l'expertise repose sur l'exploitation de données. Si cette définition semble très large – quel modèle d'entreprise aujourd'hui ne repose pas, au moins en partie, sur l'exploitation de données ? –, elle permet néanmoins d'identifier une série d'enjeux communs à l'ensemble de ces services : la transparence relative au traitement des données.

La 5G est emblématique de cet état de fait. Dans la mesure où l'ensemble des systèmes économiques et sociaux sont désormais interconnectés par des technologies numériques, il est fondamental d'avoir l'assurance que ces infrastructures essentielles à la circulation des données sont sûres, exemptes de l'immixtion d'acteurs tiers, qu'il s'agisse d'États, d'organisations privées ou de tout autre type d'acteur. C'est le débat qui occupe et continuera d'occuper de nombreux gouvernements vis-à-vis de Huawei. Deux questions sont ainsi posées : et si, parmi les millions de lignes de code optimisant le réseau, il en existait une qui permettait de faire une copie de toutes les informations qui transitent sur le réseau sur un serveur en Chine ? Pire encore, et si la Chine avait la capacité d'arrêter le fonctionnement normal du réseau à distance ?

Face à ces risques, il est nécessaire de trouver une solution pour que l'État puisse garantir la sécurité de l'information des acteurs nationaux. Pour atteindre son objectif d'assurer la sécurité des citoyens, l'État doit être prudent. En effet,

s'il retarde significativement le déploiement des réseaux en rendant obligatoire l'utilisation d'équipements développés par des acteurs de confiance, il prend le risque de ralentir plus encore le développement technologique du pays. Et les conséquences d'un retard technologique, tant pour l'économie nationale que pour la sécurité de l'information domestique, ne sont pas à négliger.

Dès lors, est-il possible pour l'État d'atteindre cet objectif de sécurité ? Dans le secteur de l'aéronautique, les constructeurs parviennent à fabriquer des avions sécurisés malgré leur dépendance à des acteurs étrangers pour le montage de certaines pièces et le développement de logiciels. Dans le cas de la 5G, la Commission européenne propose une approche de minimisation des risques en s'adressant en partie aux opérateurs. Il s'agit de mettre en place une série de procédures que les acteurs étrangers et domestiques doivent respecter : évaluer les profils de risques des fournisseurs et répartir leur rôle sur le réseau en conséquence ; éviter toute dépendance majeure à un seul acteur ; travailler étroitement avec les opérateurs pour renforcer les exigences de sécurité, etc. Ainsi, de manière schématique, cette approche vise à s'assurer qu'un opérateur n'utilise pas de matériel évalué « à risque » – pour une série de raisons, parmi lesquelles le pays d'origine de l'équipementier et sa place dans le jeu géopolitique – dans des zones stratégiques où se trouvent, par exemple, un ministère ou un industriel essentiel au fonctionnement de la nation. Comme l'affirme le commissaire européen au Marché intérieur, Thierry Breton : « Pour accéder au marché européen, il faudra accepter nos règles »[1].

> Il est nécessaire de trouver une **solution** pour que l'État puisse **garantir** la **sécurité** de l'**information** des acteurs nationaux

Réguler côte à côte : la modération des contenus

Peut-on, à un horizon de dix ans, s'inspirer de cette logique dans d'autres secteurs ? Les débats autour de la modération des contenus, et en particulier de la lutte contre les campagnes de manipulation de l'information, apportent une perspective intéressante. Dans ce cas, la souveraineté est menacée par deux types d'acteurs : les acteurs étrangers qui tentent de manipuler l'opinion

1. Gabriel Grésillon, Derek Perrotte et Nicolas Barré, « Thierry Breton : "Pour accéder au marché européen, il faudra accepter nos règles" », *Les Échos*, 7 janvier 2020.

nationale, et les réseaux sociaux eux-mêmes, qui limitent la capacité des États de contrôler la circulation d'informations en ligne. Une fois intermédié par les réseaux sociaux, l'espace informationnel devient en effet international, et permet donc à des acteurs étrangers, avec des moyens raisonnables, de s'immiscer dans des débats nationaux. Ce fut notamment le cas lors des dernières élections présidentielles états-unienne et française et, dans une moindre mesure, lors des élections européennes de 2019. Plus récemment, lors de la crise du coronavirus, le groupe de travail East StratCom au sein du Service européen pour l'action extérieure (SEAE) a mis en garde les responsables européens concernant la présence de messages d'influence pro-Kremlin en ligne. Si les effets de ces contenus étrangers sur les attitudes des citoyens n'ont, à ce stade, jamais été démontrés, cela ne fait aucune différence pour l'État, qui doit empêcher ces perturbateurs extérieurs de semer le trouble dans les débats nationaux. Cette question demeurera centrale pour les régimes démocratiques au cours de la décennie qui s'ouvre.

Les **États** doivent s'armer de **compétences numériques** fortes pour être certains que ceux qui développent des services **respectent** les **règles**

Afin de comprendre la manière dont ces acteurs utilisent les réseaux sociaux pour arriver à leurs fins, les États sont obligés de s'en remettre aux plates-formes numériques, bien que celles-ci soient réticentes à l'idée de supprimer des contenus à la demande des États. Effectivement, décider de ce qui est vrai ou faux, acceptable ou non, fait entrer ces plates-formes – qui veulent attirer des utilisateurs de tous bords politiques – dans un jeu auquel elles n'ont aucun intérêt à prendre part.

Comme démontré par l'étude de l'Institut Montaigne, « Désinformation : dépasser la modération des contenus »[1], le gouvernement français a fait fausse route en voulant modérer les contenus sans passer par la case infrastructure. Cette étude compare les lois allemande et française de modération des contenus – notamment la désinformation et les contenus haineux – afin de proposer des pistes de solutions pour contourner le débat épineux entre sécurisation de l'espace en ligne et liberté d'expression. En France, le premier réflexe a été de demander aux plates-formes, à la suite d'une procédure judiciaire, de supprimer

1. Voir « Désinformation : dépasser la modération des contenus », Institut Montaigne, 14 novembre 2019.

les contenus manifestement faux. Or, cette approche s'avère insuffisante pour faire face à l'échelle et à la rapidité avec laquelle les informations circulent, mais aussi pour limiter les tentatives d'immixtion dans les débats précédant les élections françaises. Le problème fondamental n'est, en effet, pas tant que des informations fausses circulent sur Internet, mais que des mécanismes en ligne permettent de leur donner une substance disproportionnée. Et c'est en ce sens que Camille François défend l'approche ABC pour contrer les manipulations d'information : surveiller les *actors*, *behaviors* et *content*[1]. Pour cela, il importe de se tourner vers l'infrastructure sur laquelle les informations circulent. Sous cet angle, la question de la souveraineté est similaire à celle posée dans le cas de la 5G : pour trouver la solution, il est nécessaire de déterminer les informations auxquelles nous avons collectivement besoin d'avoir accès afin de limiter la capacité d'acteurs étrangers d'intervenir dans l'espace informationnel national. Autrement dit, les États ont besoin de la compétence des réseaux sociaux, qui sont les mieux placés pour identifier les acteurs, les comportements et les contenus à observer.

En France, l'État avait souhaité réaffirmer sa souveraineté en se plaçant au-dessus des plates-formes, en leur demandant de supprimer les contenus qu'il juge problématiques. À moyen terme, une autre manière de procéder consisterait à se placer à leurs côtés, en leur demandant l'accès à une partie de l'infrastructure, c'est-à-dire aux informations qui lui permettraient de comprendre ce qui est problématique, et ainsi parvenir à trouver des solutions adaptées.

La transparence sans la naïveté

Toutefois ne faut-il pas être naïf : un mécanisme doit exister afin de s'assurer que les acteurs numériques coopèrent efficacement. Pour cela, à un horizon de dix ans, et ce, en débutant le plus rapidement possible, les États doivent s'armer de compétences numériques fortes pour être certains que ceux qui développent des services respectent les règles – dans notre exemple, communiquer des informations utiles pour limiter la capacité d'acteurs extérieurs d'intervenir dans les débats nationaux. Mettre l'accent sur des obligations de moyens n'exclut pas des pénalités en cas de dispositifs insuffisants ou non alignés avec les principes édictés par l'État. Mais ce qui importe est que l'État puisse mieux comprendre les enjeux des plates-formes pour définir des règles efficaces, c'est-à-dire des règles qui lui permettent d'atteindre ses objectifs souverains (objectif de sécurité, de cohésion sociale, etc.), pour ensuite demander à ces mêmes plates-formes de les respecter. C'est tout le sens, en France, du rapport

1. Camille François, « Actors, Behaviors, Content: A Disinformation ABC », Transatlantic Working Group, 20 septembre 2019.

de la mission de régulation des réseaux sociaux[1] ou encore du livre blanc britannique sur les contenus problématiques en ligne[2].

Notons que cette logique fonctionne dans une série de domaines pour lesquels le traitement des données a lieu à l'intérieur des entreprises, par exemple le cas des risques de discrimination par les algorithmes. On se trouve à nouveau dans une situation où des services développés par des acteurs privés posent question sur le respect des principes de l'État : que se passe-t-il si un système d'intelligence artificielle utilisé pour le recrutement discrimine une population donnée, alors que la loi française l'interdit ? Pour faire respecter son principe de non-discrimination de manière efficace, la meilleure solution qui se présente à l'État est de s'appuyer sur les compétences des entreprises, qui sont les plus à même de tester leurs produits pour vérifier s'ils discriminent ou non. Cependant, afin de ne pas tomber dans la naïveté, l'État doit développer lui-même une expertise pour définir un cahier des charges – quelle est la meilleure méthode pour procéder aux tests ? – et être en mesure de vérifier, lorsque c'est nécessaire, que ces tests sont bien menés, que les ressources dédiées en interne sont suffisantes et, si ce n'est pas le cas, de sanctionner.

D'ici à 2030, l'**État** devra affirmer une **nouvelle** forme de **souveraineté** pour **protéger** ses citoyens

Quelques règles simples seraient donc à généraliser au sein des institutions publiques pour remplir cet objectif à horizon 2030 :

- *Accroître l'expertise au niveau politique* : pour l'instant, le cas de la France montre que les élus ne sont pas suffisamment à l'aise avec ces sujets[3], ce qui ne permet pas d'avoir des débats publics de qualité, à un moment où les nuances sont essentielles pour ne pas aboutir à la mise en place de systèmes de contrôle soit trop autoritaires, soit trop naïfs. Les chantiers consécutifs à horizon 2030 sont nombreux et immenses, et comprennent, entre autres, la refonte du cadre de l'*antitrust*, une redéfinition des doctrines de sécurité nationale et européenne, ou encore l'élaboration d'un plan d'action pour penser dès aujourd'hui l'éducation de demain ;

1. Rapport de la mission « Régulation des réseaux sociaux – Expérimentation Facebook », « Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne », mai 2019.
2. Department for Digital, Culture, Media and Sport, « Online Harms White Paper », 8 avril 2019-12 février 2020.
3. « Le numérique à l'Assemblée nationale : où en est-on ? », Institut Montaigne, 27 novembre 2018.

– *Augmenter la compétence de la fonction publique* : il s'agit là d'une étape indispensable afin d'être en mesure de travailler efficacement avec les plates-formes numériques, tout en comprenant les intérêts, ainsi que les possibilités et les limitations technologiques. Les compétences des régulateurs sont nécessaires pour envisager une politique d'audit par exemple (voir ci-dessous), et de manière générale pour accroître l'autonomie et la résilience de l'État ainsi que pour créer des feuilles de route ambitieuses ;
– *Définir les* stress-tests *et l'« auditabilité » externe comme un modèle référent* : à l'instar de ce qui a été fait dans les mondes comptable et financier, l'État doit demander aux acteurs numériques davantage de transparence et être en mesure de vérifier la véracité des informations analysées. C'est la voie qui lui permettra de développer une nouvelle forme de souveraineté reposant sur le respect de règles édictées par l'État, avec le concours de l'expertise numérique.

□

Rarement les États auront été confrontés à un changement de paradigme aussi net : d'un monde où la souveraineté s'exprimait essentiellement par le territoire, nous passons à une ère où les données et l'expérience utilisateur permettent de structurer des offres tout à fait crédibles d'alternatives aux services des États. La menace se caractérise surtout par le fait que ces acteurs privés cherchent de plus en plus à affaiblir les États pour disposer d'un accès le plus direct possible au consommateur, dont la part citoyenne ne les intéresse finalement pas. D'ici à 2030, l'État devra affirmer une nouvelle forme de souveraineté pour protéger ses citoyens. ■