Qui exerce l'autorité dans l'espace numérique ?

Marc Watin-Augouard

Qui exerce l'autorité dans l'espace numérique ?

in X. LATOUR (dir.), *L'autorité et la sécurité : l'exemple de la gendarmerie nationale* , Université Côte d'Azur, 2021

GENERAL D'ARMEE (2S) MARC WATIN-AUGOUARD
Chercheur associé au Centre de recherche de l'École des officiers de la Gendarmerie nationale
Fondateur du Forum International de la Cybersécurité (FIC)
Responsable de la majeure « Souveraineté numérique et cybersécurité » de l'Institut des Hautes Études de Défense Nationale

Résumé : Le substrat numérique innerve notre société. L'hyperconnexion, portée notamment par la 5G, va marquer la prochaine décennie, en attendant une nouvelle rupture technologique avec l'informatique quantique. L'État est remis en cause dans ses fondements historiques par la porosité des frontières et l'action des multinationales du numérique, le GAFAM. Dans ce contexte, se posent la question de la souveraineté et donc de la gouvernance. L'ONU devrait avoir un rôle majeur mais les divisions entre les États qui veulent une gouvernance du numérique et ceux qui veulent une gouvernance sur le numérique mettent en évidence une divergence profonde sur les libertés et notamment la liberté d'expression. Les conventions régionales, quelle que soit leur intérêt n'ont qu'un rayonnement spatial limité, même si la Convention de Budapest relative à la cybercriminalité inspire directement ou indirectement la législation de plus de 150 Etats. L'Europe peut jouer un rôle majeur, en proposant une « troisième voie » entre la marchandisation du net et son exploitation collectiviste. La présidence française du Conseil de l'Union européenne est une opportunité pour sortir d'un étau qui ne respecte pas les valeurs qu'il faut défendre dans le substrat numérique. Les acteurs privés sont de plus en plus présents, en imposant leurs technologies, leurs normes et, partant, leur mode de société. Sans doute faut-il associer tous les acteurs publics et privés dans une gouvernance qui conjuguent les capacités de chacun. Tel est l'ambition de l'Appel de Paris, lancé le 12 novembre 2018 lors du Forum sur la Gouvernance de l'Internet (FGI). Sans une telle association qui place l'humain au cœur de la transformation numérique le risque est grand de voir le substrat numérique devenir un vecteur d'asservissement alors qu'il a été conçu par ses fondateurs comme un espace de liberté.

Mots-clés : gouvernance ; souveraineté numérique ; ONU ; Union européenne ; coopération public-privé ; Appel de Paris

L'espace numérique est improprement ainsi dénommé, en raison des sources utopistes qui ont influencé sa création et son essor. La Déclaration d'indépendance du cyberespace, prononcée en 1996 par John Perry Barlow, a sans aucun doute promu l'idée selon laquelle l'espace numérique était un espace « à part », pouvant être distinct des espaces physiques (terre, mer, air) et échapper aux règles qui les régissent, organisent les activités humaines qui s'y déploient. L'espace numérique est, en vérité, un substrat qui irrigue, innerve tous les espaces au sein desquels nous vivons. Il est « tout pour tous, partout, pour tout, en tout » et devrait accélérer sa pénétration avec le déploiement de technologies de rupture, notamment avec le déploiement de la 5G, de l'intelligence artificielle et de l'informatique quantique. L'hyperconnexion donne tort aux « anarchistes » de la Silicon Valley qui rêvaient d'un espace échappant à toute contrainte, à toute régulation. Mais comment appréhender l'autorité dans l'espace numérique ? Dans le monde réel, l'autorité est indissociable de l'État de droit. Elle est codifiée dans ses fondements, dans sa matérialité. Elle confère un droit de commander, d'obtenir l'obéissance, de sanctionner. Elle s'exerce dans la verticalité. Dans l'espace numérique, les paradigmes sont remis en cause : l'autorité traditionnelle doit composer, s'inscrire dans un système maillé, par construction acentrée. La fin de l'utopie marque notre temps, car on ne peut être « ailleurs » dans un substrat qui pénètre désormais nos propres corps. La transformation numérique remet en cause les fondements traditionnels de l'État, sous les coups de boutoir de multinationales qui entendent dominer le monde. Pour autant, les États s'emparent du net, ne serait-ce que parce qu'on leur demande de faire preuve d'autorité pour créer une ordre public protecteur des personnes physiques et morales et parce qu'ils sont en quête d'une souveraineté, d'une autonomie stratégique. Mais ils ne peuvent, seuls, atteindre cet objectif et doivent inscrire leur intervention dans une gouvernance « multiacteurs ».

***

I. L'État en quête d'autorité

A l'exception des États-Unis, les États n'ont pas pris au début la mesure de la transformation numérique, croyant sans doute qu'elle créait un monde « à part ». En France, le gouvernement a même tourné le dos à internet, jusqu'aux Universités d'été d'Hourtin (1997), préférant le choix du Minitel. L'utopie des pionniers a montré ses limites (A), tandis que les nouveaux usages ont fragilisé les bases traditionnelles de l'Etat

(B). Pour autant, il doit retrouver son autorité, ne serait-ce que pour assurer la sécurité des personnes et des biens face aux prédateurs (C). Le retour de l'État passe par une coopération multi-acteurs sans laquelle il n'est pas possible de mettre en œuvre une gouvernance de l'espace numérique.

A. La fin de l'utopie

Si la Rand Corporation, *think tank* lié au Pentagone, a contribué à la conception du réseau internet, son véritable essor est dû à l'extraordinaire concentration de grandes universités, de centres de recherche, d'entreprises et de startups au sein de ce que l'on appellera, en 1971, la Silicon Valley[1]. Si l'on ajoute les très nombreuses communautés hippies qui vivent un « néocommunalisme » en prônant l'amour et le partage gratuit, toutes les composantes sont réunies pour allier le rêve et la réalité, créer un réseau distribué permettant de communiquer sans frontière. Joseph Carl Robnett Licklider, psychologue, physicien (acousticien) et mathématicien, dirige un réseau de chercheurs, les *ARPA's Contractors* et rédige à leur attention le « *Memorandum pour les membres et affiliés du réseau d'ordinateurs intergalactiques* ». Ce titre est révélateur de la pensée du moment qui veut concilier rigueur scientifique et idéal. Entre la première connexion reliant quatre universités, en 1969, et l'année 1996 qui marque l'influence du tandem Clinton-Gorre, le libertarisme fondateur s'érode, à la vitesse développement du nombre d'ordinateurs reliés et du déploiement des « autoroutes de l'information ». Si l'on peut gérer par consensus un réseau de quelques dizaines d'abonnés, les conditions ne sont plus les mêmes lorsque John Perry Barlow lance le chant du signe de l'utopie par sa Déclaration d'indépendance d'internet[2] . Un seul extrait suffit à mesurer l'écart entre ce qui était espéré et ce que nous vivons aujourd'hui : « *Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Au nom du futur je vous demande à vous du passé de nous laisser tranquilles. Vous n'êtes pas*

[1] Le terme est alors anachronique, car le vocable « internet » n'est usuel qu'à partir de 1983, lorsque sont adoptés les protocoles TCP/IP qui permettent le routage et l'adressage de nos échanges.

[2] John Perry Barlow, cofondateur de *l'Electronic Frontier Foundation*, *Déclaration d'indépendance du Cyberespace,* Davos, 9 février 1996. La Déclaration d'indépendance du cyber espace est une réponse à la promulgation, la veille, du *Telecommunications Act* et du *Communications Decency Act* par Bill Clinton.

les bienvenus parmi nous. Vous n'avez pas de souveraineté là où nous nous rassemblons » […].

Internet devrait, selon l'auteur, être en dehors du monde réel et échapper ainsi à toute manifestation de la souveraineté des Etats. *« Nous n'avons pas de gouvernement élu et nous ne sommes pas près d'en avoir un, aussi je m'adresse à vous avec la seule autorité que donne la liberté elle-même lorsqu'elle s'exprime. Je déclare que l'espace social global que nous construisons est indépendant, par nature, de la tyrannie que vous cherchez à nous imposer. Vous n'avez pas le droit moral de nous donner des ordres et vous ne disposez d'aucun moyen de contrainte* […] ». A en croire l'auteur, la puissance publique serait impuissante dans le cyberespace. Elle n'aurait ni autorité morale, ni autorité physique sur les internautes, citoyens d'un « autre monde ». Si beau que soit le texte, il est aujourd'hui totalement décalé au regard d'une réalité marquée par la pénétration d'internet dans la vie réelle.

Déjà, dans la décennie qui encadre la Déclaration, la gouvernance de l'internet se construit, certes selon un modèle associatif, mais avec des liens étroits avec l'administration américaine. Ainsi vont être fondés l'*Internet Society* (ISOC 1992), en charge des normes, protocoles et infrastructures techniques, le *World Wide Web Consortium* (W3C 1994), organisme de standardisation du web, puis l'*Internet Corporation for Assigned Names and Numbers* (ICANN 1998). Ces organismes sont des associations de droit californien ; elles pourraient sembler être distinctes du gouvernement américain. Dans les faits il n'en est rien. L'exemple de l'ICANN est topique : cette association gère les noms de domaine ou, plus exactement, les liens entre les noms de domaine et l'adresse Internet Protocol (IP) correspondante[3]. C'est une fonction particulièrement stratégique qui, jusqu'au 1er octobre 2016, était placée sous la tutelle du Département du Commerce (DoC) américain.

Cette régulation « souple » se suffit à elle-même, tant qu'internet est « américain » et que ses utilisations demeurent « professionnelles ». Mais le développement du web et, au début des années 2000, l'apparition des ordiphones et des réseaux sociaux, conduisent les Etats à être plus interventionnistes, alors que le nombre d'un milliard d'internautes vient d'être dépassé. Mais ils le font dans un contexte qui les fragilise.

[3] Il traduit une URL en adresse IP et inversement, à la manière d'un Bottin du téléphone qui met en relation un nom et un numéro de téléphone.

B. La remise en cause de l'État

Le substrat numérique remet en cause la notion d'État, avec le sens que lui donnait Carré de Malberg : « *Communauté d'hommes, fixée sur un territoire propre et possédant une organisation d'où résulte pour le groupe envisagé dans ses rapports avec ses membres une puissance suprême d'action, de commandement et de coercition* » [4].

Internet vient heurter la souveraineté par son maillage (presque) sans frontière, sauf pour les Etats qui recherchent une « balkanisation » du cyberespace[5]. Le pouvoir de battre monnaie est contrarié par les cryptoactifs qui, dans le sillage du bitcoin veulent concurrencer les monnaies officielles[6]. Le pouvoir de créer le droit est concurrencé, voire écarté, par les normes d'origines externes la plupart anglo-saxonnes, qui sont subies à défaut d'avoir été inspirées. L'exemple des clauses générales d'utilisations (CGU) qui sont inscrites dans les contrats de service des GAFAM est particulièrement explicite, dans la mesure où elles font autorité dans la relation avec le client, tout en étant contraires au droit interne. « Code is law », selon Lawrence Lessig, soulignant ainsi l'autorité de l'algorithme qui se substitue aux formes classiques d'autorité pour dire ce que l'on doit faire ou ne pas faire, accepter ou refuser : *« Ce régulateur, c'est le code : le logiciel et le matériel qui font du cyberespace ce qu'il est. Ce code, ou cette architecture, définit la manière dont nous vivons le cyberespace. Il détermine s'il est facile ou non de protéger sa vie privée, ou de censurer la parole. Il détermine si l'accès à l'information est global ou sectorisé. Il a un impact sur qui peut voir quoi, ou sur ce qui est surveillé. Lorsqu'on commence à comprendre la nature de ce code, on se rend compte que, d'une myriade de manières, le code du cyberespace régule »* [7].

Le pouvoir de lever l'impôt est lui-même contrarié par la stratégie de multinationales du numériques, peu enclines à payer leur part, là où elles n'ont pas d'établissement stable mais où elles réalisent de substantiels bénéfices. La France a su faire preuve d'autorité, lâchée par la plupart des Etats européens - qui s'étaient pourtant concerté au

---

[4] CARRE DE MALBERG, Contribution à la théorie générale de l'État (1921).

[5] La Russie avec Runet (2019), la Chine avec la « Muraille électronique de Chine », l'Iran, la Corée du Nord, etc.

[6] Souvent dénommés à tort « cryptomonnaies », car ils n'offrent aucun des caractéristiques des monnaies.

[7] LAWRENCE LESSIG, *Code is Law-On liberty in cyberspace*– Harvard Magazine, janvier 2000

Sommet de Tallinn, en septembre 2017 -, sanctionnée par les Etats-Unis, jusqu'à ce que l'OCDE lui donne raison[8] [9].
Le pouvoir de rendre justice est contrarié par l'extra-territorialité de nombreux contentieux de nature pénale, civile ou commerciale. Il suffit de se reporter sur les clauses relatives aux litiges, contenues dans les CGU des GAFAM, pour constater que le juge californien est toujours déclaré compétent, sauf lorsque le juge français manifeste son autorité[10].
Enfin, le pouvoir de faire la guerre est accaparé par des groupes non étatiques, non dépourvus de tout lien avec les Etats qui les hébergent. Ces groupes remettent en cause les principes qui fondent le droit des conflits armés, même si leur action se situe dans « l'infra guerre ».
Fragilisés par le développement de l'espace numérique, les Etats, en retrait jusque dans les années quatre-vingt-dix, cherchent à regagner une marge d'autonomie afin de ne pas abandonner leur autorité.

C. Les États s'emparent du Net

Plusieurs raisons motivent l'intérêt de l'État pour internet : c'est un espace de souveraineté interne et externe, un espace de compétition, un espace de confrontation, voire de conflictualité puisque la croissance de la cybercriminalité, dans ses manifestations paroxystiques, peut devenir un enjeu de défense.

Si la cybercriminalité est entrée dans le code pénal français avec la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, la loi Godfrain (1988) marque la première prise de conscience par le Parlement des risques qui s'attachent à ce que l'on qualifie aujourd'hui de cyberattaque. Depuis 2001 au moins, la plupart des lois relatives à la sécurité comportent un volet cyber. Le droit pénal est sans doute celui qui illustre le mieux l'autorité régalienne, par les obligations ou les interdits qu'il contient. L'autorité de l'État se manifeste dans l'espace numérique, notamment en raison du nombre croissant de personnes physiques et morales victimes de prédateurs. L'État-providence redevient État-gendarme, parce que sa légitimité serait en

[8] Par la loi du 24 juillet 2019 portant création d'une taxe sur les services numériques.
[9] Les tractations entre les 140 pays engagés ont permis d'arriver, en octobre 2021, à un compromis définitif (136 pays favorables) sur un taux minimal de 15 % et vise une mise en œuvre en 2023.
[10] TGI Paris, Que Choisir c/ Twitter, 7 août 2018, TGI Paris, Que Choisir c/ Google inc. , 12 février 2019,
TGI Paris, Que Choisir c/Facebook, 9 avril 2019, Tribunal Judiciaire de Paris, Que Choisir/ iTunes et Apple Music 24 juin 2000

cause en cas d'impuissance. Or, l'espace numérique connaît une double migration : celle des prédateurs, d'une part, qui ont compris qu'ils n'ont jamais été aussi près de leurs victimes, ni aussi éloignés de leurs victimes ; ils ont donc intérêt à glisser du champ du matériel à celui de l'immatériel. Certains États, d'autre part, qui viennent des « banderilles numériques » sur des États tiers, plus discrètes que la « politique de la canonnière », car plus difficiles à attribuer et donc à dénoncer sur la scène internationale. Face à l'aggravation des effets des cyberattaques, le seuil de l'agression armé est approché. L'État est obligé de faire preuve d'autorité s'il veut préserver sa souveraineté. C'est notamment une stratégie de cyberdéfense, civile et militaire, qui lui permet de protéger contre les cybermenaces les organes essentiels à la vie de la Nation. Dans la phase la plus haute dans le spectre, la lutte informatique offensive (LIO) est la manifestation la plus forte en signification si l'on considère que l'autorité implique de ne pas subir. Mais il s'agit là aussi d'une question de souveraineté.

Dans le monde réel, traditionnel, la souveraineté a été fondée sur les traités de Westphalie qui ont organisé la souveraineté interne et externe des États en deçà ou au-delà des frontières. Cette approche westphalienne demeure pertinente, mais elle est soumise à l'épreuve de la transformation numérique. Les frontières n'existent que pour les États et non pour les prédateurs. Pour les premiers, elles ne sont pas un rempart mais un obstacle. Pour les seconds, elles jouent un rôle de protection contre le droit de suite des États victimes. Si la criminalité internationale a toujours nécessité - au moins depuis la création d'Interpol, en 1929 – une coopération internationale appelant une « coopération des autorités », la cybercriminalité accentue cette exigence en raison de la volatilité et du caractère transfrontière des actions malveillantes. C'est dire si l'exercice de l'autorité dans l'espace numérique passe par des alliances (OTAN) ou par une action à l'échelle de l'Europe. Par exemple, la portée et la puissance du règlement général sur la protection des données à caractère personnel (RGPD) serait faible si l'État français ne partageait pas avec les 26 autres États-membres une même vision, une même stratégie, une même forme d'action en cas de transgression des règles protectrices de la vie privée des citoyens, notamment lorsqu'elles ont pour origine un État situé en dehors de l'Union européenne.
Mais il faut aller au-delà de l'Europe, si l'on veut que chaque État puisse exercer son autorité dans l'espace numérique, dans le respect des règles de droit international. La quête d'une gouvernance de l'espace

numérique témoigne d'une volonté, affichée avec plus ou moins de bonne foi, par les Etats qui aspirent à un cyberespace sécurisé.

***

II. La quête d'une gouvernance

L'État ne peut seul exercer l'autorité dans l'espace numérique. Un espace sans frontière appelle une gouvernance élargie. L'ONU est un cadre intéressant par sa dimension planétaire, mais ses efforts sont limités dans leurs résultats (A). Les Conventions régionales ont le mérite de rassembler, mais elles manquent d'universalité (B). L'Europe, quant à elle, devrait avoir une influence à la hauteur de sa puissance économique, à condition qu'elle soit politiquement unie (C). Enfin, les acteurs privés, très présents au cœur de la transformation numérique, ne peuvent être tenus à l'écart, tout en étant encadrés, ce qui justifie une gouvernance multi-acteurs, telle qu'elle est ambitionnée par l'Appel de Paris (D).

A. L'ONU face à la division du cybermonde

La montée en puissance d'Internet a été principalement encadrée par les États-Unis, soit directement, soit par le biais d'associations *ad hoc,* de droit californien. De ce fait, la domination américaine s'est fait sentir, notamment au début des années 2000. La résolution 56/183, du 21 décembre 2001, de l'Assemblée générale de l'ONU, marque sans doute le début d'une contestation de l'autorité américaine sur l'espace numérique. A cette occasion est institué le Sommet mondial sur la société de l'information (SMSI) qui a pour objectif de mieux associer les États et la société civile. Dans les conclusions du Sommet de Tunis (2005) on peut lire « *Nous réaffirmons les principes énoncés pendant la phase de Genève du SMSI, en décembre 2003, selon lesquels l'Internet est devenu une ressource publique mondiale et sa gouvernance devrait constituer l'une des priorités essentielles de la société de l'information. La gestion internationale de l'Internet devrait s'opérer de façon multilatérale, transparente et démocratique, avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales. Elle devrait assurer une répartition équitable des ressources, faciliter l'accès de tous et garantir le fonctionnement stable et sécurisé de l'Internet, dans le respect du multilinguisme ».*

Dans ce cadre, il est créé un Forum pour la Gouvernance de l'Internet (FGI) qui se réunit chaque année. Instance de dialogue, le FGI n'a pas de pouvoirs normatifs, mais il contribue à apaiser les tensions. Dès lors qu'Internet est planétaire, les regards se tournent naturellement vers l'ONU. Mais les résultats sont mitigés, pour ne pas dire faibles.
La première tentative de gouvernance mondiale a lieu à Dubaï (3-12 décembre 2012), à l'occasion du Sommet de l'Union internationale des télécommunications (UIT) qui se tient en vue d'une première révision du Traité portant Règlement des Télécommunications internationales (RTI), issu de la Conférence administrative télégraphique et téléphonique internationale de Melbourne (CAMTT- 24/11- 9/12 1988). A cette occasion se manifeste la fracture du monde en deux blocs : celui qui veut une gouvernance « de » l'internet et celui qui veut une gouvernance « sur » l'internet. Les seconds partagent avec les premiers le souhait de garantir le bon fonctionnement du système, mais ils se distinguent par leur volonté de contrôler les contenus véhiculés sur le web et leurs auteurs. Excès d'autorité jugent les démocraties qui renoncent à signer le document final. Cet échec regrettable met en exergue les limites que les démocraties entendent apporter au contrôle des Etats et donc à leur autorité. La seconde tentative s'appuie sur les groupes d'experts gouvernementaux (GGE), mis en place par l'ONU, en vue de trouver les solutions de droit international garantissant la paix dans le cyberespace. Si un accord est trouvé en 2013 et en 2015, quant à l'applicabilité du droit international existant, les suites sont un échec (2017), lorsqu'il faut descendre dans la granularité, et sont mitigées (2021) avec la concurrence de l'Open Ended Working Group (OEWG) initié par les Russes. De tous ces travaux se dégagent 11 normes non contraignantes pour engager un comportement responsable des États dans le cyberespace. Dans ces conditions, l'ONU n'apparaît pas encore comme le leader encadrant l'autorité dans l'espace numérique. Faut-il alors se situer à l'échelle des conventions régionales ?

B. Des conventions régionales trop limitées dans leur champ d'application spatiale

Les conventions régionales peuvent-elles faire autorité ? Plusieurs accords comprennent des dispositions relatives à l'espace numérique, soit à titre principal, soit parmi les domaines qu'elles couvrent. Dans l'ordre chronologique on peut citer : l'Organisation de la Coopérations de Shangaï (OCS 2001), la Convention de Budapest du Conseil de

l'Europe sur la cybercriminalité (2001), la Convention du Commonwealth (2002), la Convention des Pays arabes du Caire (2010), la Convention de Malabo des pays de l'Union Africaine (2014). S'agissant de la première, il n'est pas étonnant qu'elle ne soit point en mesure de servir de modèle, dès lors qu'en sont membres la Russie, la Chine, le Pakistan et qu'ont le statut d'observateur l'Afghanistan, la Biélorussie et l'Iran…comment dialoguer sur l'autorité avec des Etats qui nient les principes démocratiques ? Les accords du Commonwealth et du Caire ne semblent pas être déterminants au vu de leur faible ou inexistante matérialisation. Plus intéressante est la Convention de Budapest qui vient de célébrer ses 20 ans, avec la publication, le 17 novembre 2021, d'un 2e Protocole additionnel. Cette convention a été ratifiée par 66 Etats, dont tous les Etats européens (sauf l'Irlande…) ; 20 Etats ont fondé leur législation sur la Convention, tandis que près de 50 s'en inspirent. C'est dire si le texte a une portée qui dépasse le ressort du Conseil de l'Europe. Parce qu'ils ont aujourd'hui leur propre instrument (la Convention de Malabo), les Etats africains commencent à ratifier un texte qui prend ainsi plus de poids. La Convention de Budapest est contraignante. Elle a un effet direct sur les règles de droit pénal et de procédure pénale des Etats signataires, permettant à chaque Etat d'exercer son autorité dans le respect de la souveraineté des autres, tout en rendant plus efficace la lutte contre la cybercriminalité. Malgré cette force, la Convention n'est pas ratifiée par la Russie, la Chine, Cuba, l'Iran, etc., autant dire qu'elle ne produit aucun effet sur les Etats d'où proviennent nombre de cyberattaques. Si pertinente soit-elle, la Convention de Budapest ne porte que sur la lutte contre la cybercriminalité. L'Union européenne peut-elle apporter une réponse plus globale, certes limitée dans l'espace, mais ayant une influence dépassant ses frontières ?

C. L'Union européenne, une « troisième voie » ?

L'Union européenne peut-elle affirmer son autorité dans un monde bipolaire marqué par un antagonisme Chine/USA ? Il convient de remarquer que l'UE a d'abord considéré l'espace numérique au travers du Marché commun devenu Marché unique. La défense du consommateur est le fil conducteur qui se manifeste au travers de ses règlements et directives[11]. Aujourd'hui se dessine une Europe de la

[11] Directive cadre 002/21/CE (directive « cadre » Paquet Telecom) du Parlement européen et du Conseil du 7 mars 2002 ;

cybersécurité, sous l'impulsion de Thierry Breton[12]. Cette Europe a des ambitions en termes d'autonomie stratégique mais elle veut principalement ne pas subir pour manifester son autorité, sans laquelle celle des États-membres serait imparfaite. Pour cela, il faut que l'Europe ait un discours unitaire, alors qu'elle est parfois tiraillée en raison d'approches divergentes. C'est notamment le cas en ce qui concerne la relation avec les États-Unis, la dépendance ne semblant pas un obstacle, en particulier pour l'Europe du nord et certains États à l'est. Si l'Europe fait bloc, elle peut exercer une autorité qui bénéficie par effet de cascade aux Etats membres. L'exemple du RGPD est particulièrement révélateur. Une fois entré en vigueur, il a contraint les pays du monde, désireux de partager des données à caractère personnel, à respecter le principe d'adéquation. Le Japon a ainsi signé

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) Futur règlement e-privacy ;
Règlement (UE) No 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE *Règlement e-idas ;*
Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union ;
Règlement (UE) n°679/2016 relatif à la protection des données à caractère personnel RGPD ;
Directive (UE) du Parlement européen et du Conseil du 11 décembre 2018 instituant un code européen des communications électroniques.

[12] Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européenne ainsi que l'évaluation de la nécessité d'améliorer leur protection ;
Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI ou NIS sur OSE, FSN) ;
Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (créée en 2004) et à la certification (*Cybersecurity Act*) ;
Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres ;
Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres ;
Stratégie UE en matière de cybersécurité pour la décennie du 16 décembre 2020 ;
Centre de cybersécurité de Bucarest (Commission 20 avril 2021) ;
Unité conjointe de cybersécurité (Commission 23 juin 2021).

un accord avec l'UE. Les États-Unis n'ont pas tenu compte de l'arrêt de la Cour de Justice de l'Union européenne (CJUE) déclarant illégal l'accord *Privacy Shield*[13]. Le même texte, porté par un seul Etat, n'aurait pas, à n'en point douter, produit le même effet, eut la même autorité. L'Union renforce donc l'autorités Etats membres. Le même mécanisme devrait s'observer avec les prochains règlements (*Digital Services Act*, *Digital Market Act*, *Digital Governance Act*, *e-evidence*). A l'heure où la France exerce la présidence du Conseil de l'Union européenne (PFUE), la voix de l'Europe doit être entendue, la voie de l'Europe doit être tracée, faute de quoi notre continent est appelé à devenir une « colonie du monde numérique », selon la formule de la sénatrice Catherine Morin-Desailly[14]. L'autorité est tributaire de capacités juridiques mais aussi technologiques, car derrière la technique se profile la norme, derrière la norme les usages, derrière les usages un modèle de société. Cela explique pourquoi l'Europe, dans son programme pour une Europe numérique, a fixé cinq objectifs spécifiques qui correspondent à des domaines politiques clés : calcul à haute performance, intelligence artificielle, cybersécurité et confiance, compétences numériques avancées, déploiement et meilleure utilisation des capacités numériques[15]. Les technologies ne sont pas seulement un soutien de l'autorité, mais elles la conditionnent. En témoignent les propos du président Vladimir Poutine, devant des étudiants russes, le 1 er septembre 2017 : « *L'intelligence artificielle représente l'avenir non seulement de la Russie, mais de toute l'humanité. Elle amène des opportunités colossales et des menaces imprévisibles aujourd'hui, celui qui deviendra le leader dans ce domaine sera le maître du monde. Et il est fortement indésirable que quelqu'un obtienne un monopole dans ce domaine ».*

Les capacités ne peuvent se développer sans une coopération public/privé. Serait-elle une clé de l'autorité dans l'espace numérique ?

D. Le secteur privé et l'autorité dans l'espace numérique

[13] Arrêt Data Protection Commissioner/ Facebook inc. et Maximillian Schrems (affaire. C 311-18) Le 16 juillet 2020,

[14] CATHERINE MORIN-DESAILLY, Rapport n°443 fait au nom de la Commission des affaires européennes sur l'union européenne, colonie du numérique, Sénat 20 mars 2013.

[15] Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique (période 2021-2027).

Les États sont tributaires des acteurs privés dans l'espace numérique. Un seul exemple suffit à illustrer cette dépendance : pour venir à bout du *botnet Retadup*, l'action de la gendarmerie est partie d'une alerte lancée par Avast, offreur d'antivirus. Sans cette entreprise, l'État n'aurait jamais connu cette cyberattaque, sinon trop tard[16]. L'autorité de l'Etat repose donc sur l'échange d'informations, mais chacun reste dans son rôle. Il y a lieu toutefois de s'interroger sur certaines initiatives qui, au-delà d'une coopération aboutissent à une substitution, lorsque le privé entend lui-même exercer l'autorité. A l'initiative de Microsoft, 34 multinationales, dont Facebook et ABB, ont signé le 17 avril 2018 un *Cybersecurity Tech Accord* destiné à lutter contre les attaques informatiques. Le texte ambitionne d'être la première étape d'une « Convention de Genève du numérique ». Mais est-ce à un groupe privé que revient la mission de « *s'opposer aux cyberattaques contre les citoyens et les entreprises »,* alors que c'est la mission première des États ? Plus préoccupante est l'attitude des plateformes, au premier rang desquelles les réseaux sociaux. En s'appuyant sur des algorithmes qu'elles ont conçus, elles s'arrogent le droit de dire le bien et le mal, de prononcer des exclusions, des suspensions qui portent atteinte à la liberté d'expression. La lanceuse d'alerte Frances Haugen a mis en évidence devant l'Assemblée nationale et le Sénat les pratiques de Facebook. Les réseaux sociaux doivent contribuer à la régulation des contenus qu'ils véhiculent (ce que le futur règlement DSA veut encadrer), mais doivent-ils pour autant se substituer à l'autorité légitime, celle du juge ? Un équilibre doit être trouvé. C'est l'ambition de l'Appel de Paris, lancé le 12 novembre 2018 par le président Emmanuel Macron, lors du Forum sur la gouvernance de l'Internet (FGI), à l'UNESCO. Si la gouvernance de l'internet appelle une coopération multipartite, elle ne saurait en aucun cas remettre en cause l'autorité de l'État. Celle-ci ne se partage pas mais peut être renforcée par des apports externes, notamment issus d'acteurs privés.

***

Le substrat numérique ne se distingue plus des espaces physiques. Pour autant, il met en évidence des spécificités. Plus que dans le monde réel, l'autorité est dépendante des technologies et de ceux qui les mettent en œuvre. L'État est fragilisé par l'émergence d'un monde

[16] Réseau d'ordinateurs zombies, agissant sur plus de 1340000 ordinateurs compromis démantelé en 2019.

apparemment sans frontière. Pour autant, son intervention est plus que jamais nécessaire car, sans lui, le risque est grand de voir l'emporter la loi du plus fort. L'autorité n'est pas alors la manifestation du rapport du fort au faible, mais la protection du plus faible face aux prédateurs, les cybercriminels ou les États sans scrupule. C'est aussi la protection de la « cybersouveraineté » du citoyen, de sa sphère d'intimité menacée par des acteurs « sans foi ni loi », animés par les lois du marché et souvent désireux de substituer aux États pour imposer leurs propres règles, leur propre vision du monde. Aussi paradoxal que cela puisse sembler, l'internet « sans frontière » va donner à la puissance publique, à son autorité, un nouveau fondement. Mais l'État gendarme du XXIe siècle ne pourra concevoir son rôle selon les principes qui ont guidé son action aux XIXe et au XXe siècles. Aujourd'hui, l'heure est venue d'ajouter la « distribution » à la déconcentration et à la décentralisation. Cette distribution est la conséquence du réseau maillé, tel qu'il a inspiré internet. Le maillage des acteurs est une condition du maintien de l'autorité dans l'espace numérique. L'État doit être le connecteur et l'arbitre. C'est à cette condition qu'il sera avec tous ses partenaires le garant d'un espace numérique ordonné et protecteur de tous. La gendarmerie nationale, fondatrice du Forum international de la cybersécurité (FIC), vient de créer un commandement de la gendarmerie du cyberespace (COMCYBEGEND). Son ambition est bien de contribuer à la construction d'une nouvelle approche de l'autorité, au plus près du terrain, conjuguant le régalien avec un partenariat multiacteurs. Un exemple parmi d'autres qui témoigne de la nécessité de refonder l'autorité avec le recours à d'autres méthodes.