Dossier bibliographique E DELIB 12 sept. 2024

- Bertrand BRUNESSEN, « La souveraineté numérique européenne : une pensée en acte ? », in *RDT Eur, Revue trimestrielle de droit européen*, 2021

- Jean-Philippe DEROSIER, « Les limites du concept de souveraineté numérique », in *La souveraineté numérique : le concept, les enjeux,* Mare et Martin, 2018

- Samuele FRATINI, « Quels sont les modèles de mise en œuvre de la souveraineté numérique ? », Entretien, Sciences po, Chaire digital, Governance and Sovereignty, juin 2024

- Thierry MÉNISSIER, « Les formes imparfaites de la souveraineté numérique ». Séminaire « Société & souveraineté », IPhiG & PACTE, UGA, Grenoble, Déc. 2020

- Marc MOSSÉ, « Le numérique et le retour de la souveraineté », in *La souveraineté numérique : le concept, les enjeux,* Mare et Martin, 2018

- Pierre-Yves QUIVIGER, « Une approche philosophique du concept émergent de souveraineté numérique », in *La souveraineté numérique : le concept, les enjeux*, Mare et Martin, 2018

- Dominique ROUSSEAU, « Réflexions introductives sur le concept de souveraineté numérique », in *La souveraineté numérique : le concept, les enjeux*, Mare et Martin, 2018

- Pauline TURK, « La "souveraineté numérique" : un concept pertinent en droit constitutionnel ? », in *La souveraineté numérique : le concept, les enjeux*, Mare Martin, 2018

- Pauline TURK, « Définition et enjeux de la souveraineté numérique », Cahiers français, mars avril 2020

- Christian VALLAR, « La souveraineté numérique : rapport de synthèse », in *La souveraineté numérique : le concept, les enjeux*, Mare et Martin, 2018

+ Pauline TURK, *La souveraineté européenne*, Pouvoirs, n° 190, 2024

RTD Eur. 2021 p.249

La souveraineté numérique européenne : une « pensée en acte » ?

Brunessen Bertrand, Professeure à l'Université Rennes I, responsable de l'Axe intégration européenne (IODE UMR 6262)

Une disruption de plus à mettre au crédit du numérique : le thème de souveraineté européenne fait un retour inattendu dans le discours politique européen à la faveur d'une redéfinition de la politique européenne du numérique.

Plus que le numérique lui-même, c'est son ubiquité qui est, au fond, en cause, derrière l'idée de souveraineté : la souveraineté numérique concerne tout à la fois la politique de défense, la politique économique, la politique commerciale, la défense de la démocratie et des valeurs européennes, la régulation du marché intérieur, la cybersécurité. Saisis dans leur intégralité, ces différents domaines qui, à leur façon, mettent en cause l'intégrité des compétences européennes et son autonomie, finissent par constituer quelque chose de fondamental et d'existentiel pour l'Union européenne et ses États membres : son indépendance, sa capacité à garder la maîtrise de ses compétences les plus fondamentales et à appliquer les valeurs qui fondent sa raison d'être et son identité. On comprend, dans ces conditions, ce dépassement d'une idée historiquement taboue pour montrer l'urgence d'une situation qui pourrait, à terme, en annihiler les enjeux.

À cela s'ajoute aussi la prise de conscience brutale, peut-être pour la première fois, des limites de chaque État face à ces enjeux. Si la rhétorique sur l'idée d'être plus forts ensemble cherche à cimenter une forme de solidarité européenne depuis toujours, la conscience, réelle, de la plus-value liée à l'appartenance au marché intérieur n'a jamais semblé non plus un horizon indépassable, comme l'a encore confirmé le Brexit. Les avantages économiques ont toujours été soupesés à l'aune des contraintes politiques qu'implique l'appartenance à l'Union européenne et cette équation n'a rien d'une évidence dans un contexte de résurgence des populismes alimentés par l'envie de « reprendre le contrôle ». En ce qui concerne les enjeux de défense et de sécurité, la question n'a jamais pu être dissociée, par les États membres, de celle de la relation transatlantique et n'a donc jamais fait l'objet d'une approche européenne proprement autonome. Pour la première fois, le numérique a créé une réelle rupture, par la prise de conscience, commune à tous les États membres, de leur incapacité individuelle à exister, défendre leurs valeurs, leur modèle, leur économie et leurs citoyens, seuls dans le cyberespace : la domination économique des plateformes américaines et chinoises, la puissance technologique des États-Unis et de la Chine ont révélé, sous un angle assez cruel, l'impuissance du soft power européen à exister et défendre ses choix, et ce constat est plus cinglant encore à l'échelle nationale. Face aux campagnes de désinformation et de manipulation de l'opinion pour déstabiliser les démocraties européennes, aux cyberattaques des infrastructures sociales essentielles, à l'impuissance des économies à lutter contre la puissance de marché des plateformes, à la captation des données des citoyens et des industries européennes et à un retard technologique devenu évident, le sentiment d'impuissance individuelle des États membres semble avoir brisé le plafond de verre de la qualification des enjeux politiques qui se jouent désormais au niveau européen. Si Paul-Henri Spaak a pu dire qu'il n'y avait « que deux types d'États en Europe : les petits... et ceux qui ne savent pas encore qu'ils le sont », le numérique a provoqué la prise de conscience des États appartenant à cette seconde catégorie.

Sur un plan purement juridique, quelques précisions liminaires s'imposent : il ne s'agit pas ici de souveraineté au sens où

avait pu la définir Jean Bodin et qui conduirait à appliquer à l'Union européenne la théorie de l'État. Le terme de « souveraineté numérique » heurte les juristes et les politistes, légitimement attachés à l'intégrité du concept ; relier un microprocesseur ou les terres rares à la puissance d'État peut paraître bien hasardeux(1). La souveraineté numérique semble plutôt renvoyer à une souveraineté à l'envers, c'est-à-dire à l'idée que la souveraineté de l'État est de multiples façons mise en cause par la transition numérique et que seule l'échelle européenne peut limiter, peut-être corriger, ces atteintes. Les États sont confrontés à des plateformes numériques ou des puissances étrangères qui ont les moyens d'être non seulement leur égal, mais peut-être aussi leur supérieur et leur concurrent.

La conceptualisation de la souveraineté numérique européenne ne consiste pas à projeter la théorie de l'État(2) au niveau européen, mais à penser l'indépendance, voire la mise en capacité d'agir, « l'empowerment », de la puissance publique européenne, dans une situation mondiale dans laquelle elle n'a pas su trouver sa place : rendre aux États européens une capacité d'agir(3) dans un monde reconfiguré par le numérique. L'enjeu n'est donc pas la souveraineté européenne, ou alors une souveraineté inversée : une souveraineté numérique européenne qui rendrait aux États les moyens d'agir et leur indépendance. La mise en pouvoir d'agir des États membres dans le cyberespace passerait ainsi par l'Union européenne.

Les enjeux du numérique s'arriment en effet sur ceux de la souveraineté des États membres(4) de l'Union. On sait, depuis Carré de Malberg, que la souveraineté a plusieurs significations(5). Cette souveraineté politico-juridique de l'État qui lui donne la compétence de ses compétences et fait de l'État la puissance suprême qui n'a ni supérieur ni égal ni concurrent pourrait sembler mise en cause dans un contexte marqué par l'extraterritorialité des législations étrangères et une surveillance numérique globale par des puissances étrangères.

Les révélations d'Edward Snowden sur l'ampleur de la surveillance numérique - organisée, quotidienne, tentaculaire - de toutes les plus hautes autorités politiques européennes par les agences américaines, en particulier la NSA, et de la façon dont ces informations ont pu servir les intérêts américains ont sans doute créé une rupture dans l'inconscient européen, arrimé depuis toujours à une inaltérable alliance transatlantique. La stratégie de surveillance globale des principales puissances étrangères, aux fins de manipulations géostratégiques de l'Europe, est telle qu'elle ne peut pas ne pas affecter quelque peu au passage la puissance de l'État et sa souveraineté-indépendance. À cela, s'ajoutent les stratégies de certaines puissances étrangères, plus spécifiquement la Chine et la Russie, qui ciblent les processus démocratiques des États par de multiples campagnes de désinformation et de manipulation des opinions publiques. Ajoutons la puissance économique des géants du numérique, dont le chiffre d'affaires approche parfois les recettes fiscales étatiques, et leur accumulation de grands volumes données, qui en font des « acteurs économiques capables de rivaliser avec les États »(6).

La souveraineté au sens politico-juridique n'est pas cependant pas réellement en cause, les enjeux du numérique concernant essentiellement la capacité d'agir des États membres de l'Union avec l'avènement des cybermonnaies, le contournement des règles de fiscalité, la création de « cour suprême » ou de mesures de sécurité ou d'identification proposées par certaines plateformes numériques. Le pouvoir de marché des géants du numérique, qui tentent de capter toutes les chaînes de valeur et cherchent à imposer leurs conditions, est parfois édifiant, comme l'a encore montré, au début de l'année 2021, le bras de fer entre Facebook et l'Australie. Leurs effets « systémiques » les érigent en régulateurs de la liberté d'expression sur les espaces publics qu'ils ont créés et qui ont rendu presque obsolètes toutes les autres structures de débat public : que penser, par exemple, de la logique d'attribution d'un temps de parole équitable dans les médias à l'heure des réseaux sociaux ? Ce sont bien là quelques exemples de tentatives d'appropriation par les géants du numérique de ces « marques de souveraineté » conceptualisées par Bodin au XVI^{e} siècle, qui interrogent sur la concurrence que pourraient connaître les États dans leurs fonctions régaliennes(7).

La fondamentalité et l'ubiquité de ces bouleversements ont fait prendre à l'Europe la mesure de son impuissance, si elle se limite à ne penser son action qu'à travers son marché intérieur. Même si ce marché intérieur reste au coeur de sa stratégie de reconquête numérique, par la création d'un espace européen des données ou la conditionnalité de l'accès aux données des citoyens au respect des règles européennes, l'aveu d'impuissance est là, et suscite un mouvement d'européanisation convergent.

D'un côté, les États acceptent l'européanisation de la politique du numérique, même si celle-ci évolue sans véritable base juridique propre - le Président français allant même jusqu'à évoquer la « souveraineté européenne » dans le domaine du numérique. Les États membres acceptent aussi, de fait, d'exercer en commun des compétences nationales, que la Commission coordonne avec des « boîtes à outils » (pour la 5G, pour l'e-santé, pour la numérisation de la justice) ou des « cadres » (pour le filtrage des investissements directs étrangers). Même les parlements nationaux, par essence attachés à la souveraineté nationale qu'ils représentent, en appellent à la souveraineté numérique européenne : le Sénat français conforte régulièrement « la prise de conscience, par l'Union européenne, de l'importance des enjeux de souveraineté numérique »(8). Cette européanisation spontanée de questions relevant de compétences nationales est à mettre en lien avec l'importance des enjeux, en particulier la protection du modèle de démocratie libérale européenne, dès lors que les États européens sont désormais « dans une position de dépendance vis-à-vis des modèles américain du capitalisme de surveillance et chinois du crédit social »(9). La marge de manoeuvre européenne est alors étroite : face à la structuration binaire entre États-Unis et Chine, dans laquelle la Russie cherche aussi à prendre sa part, l'Europe cherche encore sa place au niveau mondial(10), mais elle s'est imposée sur le plan interne comme le seul niveau d'action possible.

D'un autre côté, l'Europe assume aussi la nécessaire affirmation de son identité dans cette transformation numérique. L'idée de souveraineté devient tangible et acquiert la force de l'évocation : elle s'affirme progressivement dans le discours politique, singulièrement dans le domaine numérique(11) et, même si elle ne revêt pas la signification politico-juridique qu'elle implique, son apparition dans les discours, sans être de l'ordre du performatif, n'est pas neutre non plus, d'autant qu'elle s'accompagne de mesures très stratégiques, de la cybersécurité à la politique industrielle, en passant par la cyberdéfense, la régulation des plateformes ou la gouvernance des données. L'existence précède en quelque sorte l'essence : la politique européenne du numérique existe et commence à porter ces enjeux fondamentaux, indépendamment de la façon dont on peut l'appréhender politiquement et juridiquement.

Si le terme de souveraineté apparaît, celui d'autonomie stratégique de l'Union, plus largement évoqué encore, correspond bien à la réalité et au mode de pensée européen, inscrit dans une éternelle stratégie de dépolitisation et de technicisation des enjeux. Si la revendication d'indépendance s'inscrit dans des enjeux de souveraineté, la recherche d'autonomie semble aussi être une façon dépolitisée de parler de souveraineté, un peu à la manière de la jurisprudence de la Cour de justice qui défend l'autonomie de l'Union européenne à l'égard des ordres juridiques extérieurs. L'autonomie se veut néanmoins ici « stratégique », ce qui concède au concept une dimension politique, et même, en l'occurrence, géopolitique. La stratégie est tout aussi essentielle que l'autonomie dans un contexte où le *soft power* traditionnel de l'Union européenne a montré ses limites, parfois même son irénisme. La recherche d'indépendance ne suffit pas ; le temps est peut-être venu d'affirmer une véritable puissance européenne, pour ne pas la cantonner au rôle subalterne de « colonie du monde numérique »(12). Conscientes d'être des « herbivores géopolitiques dans un monde de carnivores »(13), les institutions européennes changent de perspectives : la Commission s'affirme désormais « géopolitique » et assume de vouloir mettre fin à la « naïveté »(14). Comme l'affirme le Commissaire au marché intérieur, « nous devons être désormais un acteur autonome et stratégique. Et pour cela, nous devons nous équiper d'un arsenal de 'hard power', afin que l'Europe puisse user de son influence pour défendre sa vision du monde et défendre ses propres intérêts [...]. Ce ne sont plus seulement des mots. L'Europe se donne aujourd'hui les outils nécessaires pour s'affirmer dans la défense de ses intérêts et de ses valeurs. C'est vrai en matière de capacités technologiques de défense, c'est vrai en matière d'accès à notre marché, en matière de

désinformation, de cybersécurité, de menaces hybrides ou de souveraineté digitale »(15). Pour la première fois, le discours européen ne cherche pas à mobiliser à travers un idéal, mais par une logique de combat : la meilleure défense, c'est l'attaque. La transition numérique s'inscrit « dans un contexte de glissement des plaques géopolitiques, qui aura une incidence sur la nature de la concurrence. L'Europe se doit, plus que jamais, de faire entendre sa voix, de défendre ses valeurs et de *se battre* pour garantir des conditions de concurrence équitables. Il y va de sa *souveraineté* »(16). L'Union européenne, comme toujours, se construit surtout dans l'adversité, au travers de crises qui suscitent la prise de conscience de ses faiblesses et imposent la nécessité ; c'est toujours ainsi que l'Union parvient à trouver la force politique et les ressources juridiques pour défendre ses valeurs et son identité.

Si la notion de souveraineté est acceptée malgré tout ce qu'elle pourrait impliquer, c'est qu'il s'agit ici d'une souveraineté européenne à l'envers, qui conforte et protège la souveraineté politique des États. La souveraineté numérique européenne est la condition de la souveraineté étatique. La souveraineté numérique européenne, entendue comme la défense de l'autonomie stratégique européenne, ne se construit pas au détriment des souverainetés nationales : elle devient la condition de leur intégrité.

I - La souveraineté numérique « empowerment » : la défense de l'autonomie technologique européenne

La stratégie « Façonner l'Europe numérique » rappelle combien la capacité de garantir l'intégrité et la résilience des infrastructures de données et des réseaux est une prémisse de la souveraineté technologique européenne(17). La souveraineté numérique passe par le développement de solutions numériques européennes et l'interopérabilité des infrastructures numériques essentielles comme les réseaux 5G.

Le numérique implique le droit dans un rapport dialectique avec la technologie. L'efficacité du droit et la défense des valeurs sont devenus tributaires des enjeux technologiques. La « souveraineté technologique de l'Europe »(18) dépend ainsi, fondamentalement, de son industrie. Dans ces conditions, la politique européenne du numérique s'arrime principalement sur la politique industrielle européenne, qui n'est pas tout à fait une politique comme les autres, du fait des limites de la compétence européenne, de la symbiose des enjeux publics et privés, mais aussi du fait qu'elle est moins normative que liée à des investissements. La simple volonté politique est nécessaire, mais elle est loin d'être suffisante dans ce domaine, où il s'agit d'investissements massifs dans des nouvelles technologies dont on ne perçoit pas toujours la nécessité à court terme - les *deep tech* restant assez opaques pour beaucoup - et qui impliquent des prises de risques, par exemple, pour les technologies de rupture, qui ne font pas toujours partie de l'ADN européen. La question des investissements est donc centrale, mais la définition d'une stratégie politique aussi : la nouvelle approche de la politique industrielle européenne s'inscrit désormais dans une volonté de restaurer la souveraineté et l'autonomie stratégique européenne. Les outils juridiques de l'autonomie technologique européenne passent par deux politiques : la politique industrielle (**A**) et la politique de recherche et de développement (**B**), qui permettent de mettre en commun des intérêts publics et privés pour développer des solutions techniques européennes autonomes.

A - La politique industrielle

La politique industrielle est une compétence limitée au niveau européen, car elle correspond à une compétence d'appui et de complément de l'Union, au sens de l'article 6 TFUE. C'est aussi une politique hybride et juridiquement atypique, qui imbrique des intérêts publics et privés en s'arrimant sur l'action des autorités publiques nationales et européennes - et des acteurs privés. En droit de l'Union, la transversalité de cette politique(19) appelle une mise en cohérence avec les autres politiques européennes.

La stratégie industrielle européenne proposée en 2020 part du constat que la « future souveraineté technologique de l'Europe » dépend de ses infrastructures numériques stratégiques : au-delà des actions engagées pour la sécurité des réseaux 5G, l'objectif de la politique industrielle européenne sera de développer une infrastructure de communication quantique essentielle, conçue pour déployer une infrastructure de bout en bout sécurisée et certifiée, fondée sur la distribution quantique de clés pour protéger les principaux actifs numériques de l'UE et de ses États membres(20). La politique industrielle européenne a aussi pour objectif de soutenir le développement de technologies clés génériques qui ont une importance stratégique : la robotique, la microélectronique, le calcul à haute performance, l'infrastructure de données en nuage, les chaînes de blocs, les technologies quantiques, la photonique, la biotechnologie industrielle, la biomédecine et les nanotechnologies. Le renforcement de l'autonomie stratégique passe ainsi par l'européanisation de toute la chaîne de valeur numérique : données, cloud, technologies de processeurs de nouvelle génération, connectivité et réseaux 6G(21).

Le Plan de relance adopté en 2020 porte une attention particulière aux « deep tech ». Ces technologies concernent surtout l'informatique en nuage (le traitement des données), les technologies quantiques (qui permettent la création d'applications pratiques) et le calcul à haute performance (qui permet de traiter et d'analyser des données beaucoup plus rapidement que d'autres ordinateurs). Certains instruments du plan de relance sont fléchés de manière à financer le développement, au niveau européen, de la prochaine génération de technologies numériques (supercalculateurs, informatique quantique, chaîne de blocs, intelligence artificielle), à renforcer les capacités européennes au sein des chaînes de valeurs numériques stratégiques (notamment les microprocesseurs) et le déploiement d'infrastructures de réseau comme la 5G.

La dépendance technologique des États et de l'Union européenne aux ressources technologiques d'entreprises étrangères, soumises à l'extraterritorialité du Cloud Act américain, soulève évidemment des questions sur les capacités industrielles européennes : le contrat signé par le Heath Data Hub français(22) avec Microsoft ou le contrat du ministère de l'Intérieur avec la société Palantir, liée à la CIA, voire même celui de Doctolib (qui a été choisi pour la gestion des rendez-vous vaccinaux en France) avec Amazon (AWS), soulève évidemment des questions sur l'intégrité des données (personnelles, notamment de santé, ou des services de renseignements français), au regard des programmes de surveillance américains. Dans ces contrats, c'est bien l'absence de cloud européen en mesure de proposer des services suffisamment perfectionnés qui a été déplorée (et non l'absence de services de cloud français). La dépendance technologique se renforce aussi par les effets de réseaux ainsi créés et l'absence d'interopérabilité entre les infrastructures de stockage, qui rend difficile le changement de prestataire de services de cloud. La question qui se pose aujourd'hui pour le cloud se posera demain pour les deep tech et l'IA.

L'enjeu d'une infrastructure de cloud européen pour la souveraineté numérique européenne. La faiblesse des services de cloud européens rend les États et l'Union dépendants de solutions techniques étrangères, qui limitent l'effectivité de la protection des droits fondamentaux : les difficultés se posent, que ces entreprises stockent ces données sur le territoire européen (du fait de l'application de législation extraterritoriales étrangères, en particulier le *Cloud Act* américain) ou qu'elles transfèrent des données à l'étranger, l'affaire *Schrems II* ayant montré que les données des citoyens européens pouvaient être transmises à des autorités étrangères dont les règles en matière de protection des données ne respectent pas les exigences européennes. Si les affaires mettent surtout en cause le droit américain, la question se posera *a fortiori* pour les entreprises chinoises (les BATX), du fait des lois adoptées par la Chine en matière de cybersécurité et de renseignement qui contraignent les entreprises chinoises à coopérer avec les autorités publiques. La création d'un cloud européen est donc un enjeu de souveraineté face auquel l'Union semble impuissante : il ne paraît pas possible, en l'absence d'un cloud européen suffisamment performant, d'imposer juridiquement une localisation européenne des données qui interdirait le recours à des responsables de traitement soumis à une législation extra-européenne, malgré les souhaits émis par certains parlements nationaux(23). L'effectivité du droit passe par l'existence de certaines technologies, ce qui pose la question

de la politique industrielle européenne.

La création d'une plateforme européenne pour les données. Une alliance franco-allemande, soutenue par la Commission, a fait émerger une approche commune pour un cloud européen. Lancée en novembre 2020, une plateforme européenne pour les données est en cours de construction au sein du projet Gaia-X(24), porté par des industries, les gouvernements français et allemand et la Commission, avec l'objectif clair de défendre une souveraineté numérique européenne en matière de données. Cette infrastructure européenne doit permettre des services d'hébergement qui garantissent le respect des règles juridiques européennes. Parmi les conditions de participation à Gaia-X, les entreprises doivent respecter des principes de sécurité et transparence. Un tempérament notable : cette plateforme européenne est ouverte à toutes les entreprises, même étrangères, sous réserve qu'elles déclarent le lieu de stockage des données et clarifient l'application de lois étrangères(25). Alors que ce cloud européen devait, à l'origine, être limité aux entreprises non soumises à des lois étrangères, il sera finalement ouvert aux entreprises soumises à de telles lois extraterritoriales, dès lors qu'elles le déclarent de façon transparente. Cela suscite quelques interrogations sur le degré de protection de la souveraineté numérique européenne.

B - La politique de recherche et de développement : les partenariats publics-privés

Entreprises communes dans le cadre de partenariats public-privé. Les exemples américains et chinois illustrent bien, chacun à leur manière et toutes choses égales par ailleurs, cette imbrication du public et du privé pour l'émergence des nouvelles technologies. La puissance des entreprises numériques américaines résulte du soutien dont elles ont amplement bénéficié(26) par le biais de la DARPA(27). Sans avoir de DARPA européenne, la conscience de la nécessité de renforcer les liens entre la recherche et l'industrie passe aussi par la politique de recherche. Pour mettre en commun les moyens de développer la recherche, la Commission créée des initiatives technologiques conjointes (ITC), qui sont ensuite déclinées en programmes ciblés sous la forme juridique d'entreprises communes(28). Par le biais de partenariats publics-privés, les autorités publiques européennes participent au financement d'entreprises communes sur lesquelles elles disposent d'un droit de regard, tout en les laissant déterminer librement leurs stratégies commerciales(29).

Les règlements établissant les entreprises communes organisent les modalités de contrôle de la Commission (par exemple, des contrôles de performance), ainsi qu'un contrôle budgétaire : les entreprises communes sont directement responsables devant l'autorité de décharge en ce qui concerne l'exécution du budget(30).

La politique de recherche et de développement européenne cherche donc aussi, à sa mesure, à contribuer à ces partenariats publics-privés. Les programmes cadres de recherche (établis en fonction des stratégies politiques européennes) se concrétisent d'abord par la création de plateformes technologiques européennes(31), qui doivent aiguiller la Commission dans la définition d'une politique d'innovation technologique et permettre de flécher les investissements publics et privés. Ces programmes se concrétisent ensuite par la mise en place d'initiatives technologiques conjointes (ITC)(32), qui appellent à leur tour la création d'entreprises communes pour leur mise en oeuvre(33). Les entreprises communes sont donc des partenariats conclus entre le secteur public (la Commission seule ou en association avec des États selon les cas) et l'industrie, et parfois des laboratoires de recherche. Les entreprises communes sont ainsi créées par des règlements du Conseil et fondées sur l'article 187 TFUE, selon lequel « l'Union peut créer des entreprises communes ou toute autre structure nécessaire à la bonne exécution des programmes de recherche, de développement technologique et de démonstration de l'Union ».

Certaines entreprises communes, comme EuroHPC, s'inscrivent dans un modèle qui associe les États membres, l'Union (représentée par la Commission) et l'industrie (la European Technology Platform for High Performance Computing

Association - ETP4HPC - et la Big Data Value Association - BDVA). La Commission a proposé de réajuster les missions de cette entreprise commune dans un projet de règlement du 18 septembre 2020 (34), afin de permettre l'émergence des espaces européens de données, des nouvelles solutions de cloud et d'IA.

L'approche commune pour le déploiement des réseaux à très haute capacité. La connectivité, assurée par les infrastructures à fibre optique et 5G, est au coeur de la transformation numérique. La répartition des compétences entre l'Union européenne et les États est parfois tempérée par une coordination européenne régulée par de la *soft law*, à l'image des « boîtes à outils ». La question de l'accès au spectre radioélectrique pour la 5G, qui se pose en lien avec les questions de sécurité et de résilience des réseaux 5G (35), illustre l'européanisation de l'exercice d'une compétence nationale à travers des formes de coordination. Au niveau législatif européen, un cadre est fixé par le code des communications électroniques européen (36) et une décision sur les ultra-hautes fréquences, qui fixent des délais pour l'autorisation de l'utilisation du spectre radioélectrique pour les réseaux 5G. En vertu de leurs compétences nationales, les États membres doivent accorder aux opérateurs l'accès au spectre radioélectrique. Pour accélérer le déploiement des réseaux et coordonner l'assignation des radiofréquences, la Commission a adopté une recommandation (37) pour que les États membres constituent une boîte à outils de bonnes pratiques (pour le 30 mars 2021). La recommandation va cependant au-delà d'une simple coordination, car elle formule des orientations sur ces bonnes pratiques : la Commission cherche ainsi, par du droit souple, à faciliter le déploiement des réseaux, en incitant les États à simplifier les procédures d'autorisation, à mettre en place un point d'information unique au sein des administrations nationales, à étendre l'accès aux infrastructures existantes pour l'installation des éléments de réseau. La multiplicité des procédures en manquement engagées par la Commission en 2021 contre les insuffisances dans la transposition du code européen des communications électroniques montre toute l'importance stratégique de ces questions.

Initiative pour un système spatial européen indépendant de communications. Si les enjeux de la connectivité passent parfois par de la *soft law*, elle passe aussi par d'autres voies, comme le montre la volonté de créer une infrastructure européenne souveraine, à travers une constellation de satellites, pour fournir un accès à internet à haut débit. Une initiative européenne a été engagée en ce sens en 2020, dans le cadre du programme de télécommunications par satellite de l'Union européenne (GOVSATCOM) (38). L'objectif est de réfléchir à la faisabilité d'un réseau européen de communication par satellites, qui pourrait passer par un partenariat public-privé.

II - La souveraineté numérique et la défense de l'autonomie stratégique européenne

La cybersécurité est essentielle pour la souveraineté numérique européenne. La cybersécurité renvoie, au sens de la loi européenne sur la cybersécurité, aux actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces. Les cybermenaces étant elles-mêmes définies comme tout événement ou toute action potentiels susceptibles de nuire ou de porter atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes (39).

Les cyberattaques sont le fait d'individus et d'entités parfois très liés à des autorités publiques étrangères (40), qui peuvent déstabiliser gravement le fonctionnement démocratique (perturbation des processus électoraux) ou les services essentiels à la vie de la nation. Elle peut relever de formes classiques de cybercriminalité ou, de plus en plus, de formes sophistiquées de cyberespionnage par des puissances étrangères. La récente multiplication des cyberattaques (41) a révélé l'insuffisante protection des infrastructures publiques ; en France, en 2020, 20 % des rançongiciels étaient dirigés contre des activités essentielles de services publics de collectivités territoriales et 11 % contre les établissements de santé.

Du point de vue de la souveraineté, la conception de ces cyberattaques semble évoluer vers des formes de cyberespionnage

ciblant des menaces très stratégiques : il existe ainsi une « nouvelle tendance particulièrement préoccupante, qui consiste à prendre pour cible des infrastructures critiques au travers d'actions de cartographie des réseaux et de prépositionnement d'implants informatiques dont les objectifs restent difficilement identifiables. Il pourrait s'agir soit d'opérations de reconnaissance en vue de préparer des actions de sabotage avec un impact significatif sur la sécurité nationale, soit d'actes d'intimidation visant à influencer immédiatement la posture des États ciblés dans un contexte de tensions géopolitiques » (42).

La cyberattaque du logiciel SolarWinds, qui a permis à des pirates informatiques, soutenus par des États, d'espionner pendant des mois des administrations dans le monde (aux États-Unis, en Europe (43), en Asie), ainsi que des grandes entreprises, notamment américaines (par exemple, Microsoft et ses services de cloud Microsoft Azur), a révélé l'ampleur des vulnérabilités. À l'occasion d'une mise à jour d'un logiciel (Orion de SolarWinds), une porte dérobée (*backdoor* appelée ici Sunburst) a été insérée dans le code source du logiciel SolarWinds : cette intrusion n'a été détectée que plusieurs mois après par la société de sécurité de FireEye. Parmi les agences et départements d'États américains affectés figurent le Pentagone, les départements d'État du Commerce, de la justice, du Trésor, de la Sécurité intérieure, l'Administration nationale des télécommunications et de l'information (NTIA). Plus encore, cette cyberattaque s'est doublée d'une attaque par rebond, sur les réseaux, de la société de cybersécurité Fire Eyes. Le vol et la destruction de données, peut être aussi le ciblage d'infrastructures essentielles, qui rappelle des cyberattaques comme celle de NotPetya, montre que l'enjeu dépasse la cybercriminalité « ordinaire » et concerne un espionnage à grande échelle par des puissances étrangères. La structuration et l'ampleur de ces cyberattaques confirment aussi l'hypothèse d'une implication d'autorités étatiques par un gouvernement étranger (la Russie est particulièrement ciblée (44)), peut-être même plusieurs. Ces cybermenaces posent ainsi des défis nouveaux pour la défense des souverainetés nationales des États dans l'Union.

Le cadre législatif européen prévoit des mesures internes pour protéger les capacités de cybersécurité et garantir une cyberrésilience (**A**). Les institutions ont aussi cherché à renforcer, sur le plan externe, les outils de la politique de défense pour se donner les moyens d'une véritable cyberdéfense européenne (**B**).

A - La cybersécurité européenne

La cybersécurité dépend certes de solutions technologiques (45), mais elle dépend aussi, fondamentalement, d'une régulation des comportements humains, que le droit peut chercher à encourager ou à contraindre : la « cybersécurité n'est pas qu'une question liée à la technologie, mais une question pour laquelle le comportement humain est tout aussi important » (46). C'est pourquoi le droit de l'Union cherche à encourager les administrations, les entreprises et les citoyens à adopter une « hygiène informatique », c'est-à-dire des mesures simples, de routine, qui, lorsqu'ils les mettent en oeuvre et les effectuent régulièrement, réduisent au minimum leur exposition aux risques liés aux cybermenaces. La régulation juridique des comportements a donc une place essentielle dans les questions de cybersécurité.

La stratégie de cybersécurité européenne du 16 décembre 2020, qui s'inscrit dans l'Union de la sécurité (47), privilégie une double approche de la cybersécurité : une approche législative transversale de la cybersécurité (**1**), qui a vocation à être complétée par des approches sectorielles de la cybersécurité, dans des domaines comme l'énergie, les services financiers, les transports ou la santé. Les enjeux de cybersécurité concernent aussi la sécurité des réseaux de communications, en particulier la 5G (**2**). Au-delà des réseaux 5G, l'enjeu va rapidement être, pour l'Union européenne, de développer une infrastructure de communication quantique et ainsi déployer une infrastructure de bout en bout sécurisée et certifiée, fondée sur la distribution quantique de clés, pour protéger les principaux actifs numériques de l'UE et de ses États membres (48).

1 - Le cadre législatif horizontal de la cybersécurité

Le cadre européen de certification de cybersécurité a été établi par le *Cybersecurity Act* de 2019(49). Ce cadre européen de certification de cybersécurité établit un ensemble de règles, d'exigences techniques, de normes et de procédures qui s'appliquent à la certification ou à l'évaluation de la conformité de produits et de services liés aux technologies de l'information et des communications (TIC)(50). Le *Cybersecurity Act* prévoit ainsi les principales exigences pour les « schémas européens de certification de cybersécurité », permet la reconnaissance et l'utilisation, dans tous les États membres, des certificats de cybersécurité européens(51), et des déclarations de conformité de l'Union européenne pour les produits, services ou processus TIC. Il pose des principes fondamentaux comme celui de sécurité, dès la conception (*security by design*) et sécurité par défaut.

La méthode est cependant progressive : le cadre européen s'appuie d'abord sur des schémas nationaux et internationaux existants, et sur des systèmes de reconnaissance mutuelle pour créer les conditions d'une évolution vers les schémas européens de certification de cybersécurité.

Un schéma européen de certification de cybersécurité a pour objectif de protéger les données : la certification tend à protéger les données (stockées, transmises ou traitées) contre le stockage, le traitement, l'accès ou la diffusion, la destruction, l'altération accidentels ou non autorisés au cours de l'ensemble du cycle de vie du produit, service ou processus TIC. L'objectif est d'identifier les dépendances et vulnérabilités connues, de garder une trace des données, fonctions ou services qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui. Il s'agit aussi de rétablir rapidement la disponibilité des données et des services après un incident.

Le règlement prévoit plusieurs niveaux d'assurance des schémas européens de certification, élémentaire, substantiel ou élevé, en fonction du niveau de risque associé à l'utilisation prévue du produit ou service et des répercussions d'un incident. Le niveau d'assurance élémentaire minimise les risques élémentaires connus d'incidents et de cyberattaques : l'évaluation porte simplement sur un examen de la documentation technique. Le niveau substantiel minimise les risques de cybersécurité connus, et le risque d'incidents et de cyberattaques émanant d'acteurs aux aptitudes et aux ressources limitées. Les évaluations sont un peu plus substantielles et comprennent au moins un examen prouvant l'absence de vulnérabilités connues du public et des vérifications démontrant que les produits, services ou processus mettent correctement en oeuvre les fonctionnalités de sécurité nécessaires. Enfin, le niveau élevé minimise le risque que des cyberattaques de pointe soient menées par des acteurs aux aptitudes solides et aux ressources importantes. L'évaluation est donc encore renforcée : elle passe non seulement par le contrôle de l'absence de vulnérabilités connues du public et la mise en oeuvre des fonctionnalités de sécurité nécessaires, au niveau de l'état de l'art, mais, en plus, une évaluation de leur résistance à des attaques menées par des acteurs compétents (tests de pénétration).

La sécurité des réseaux et systèmes d'information. La directive SRI(52) établit des mesures pour la sécurité des réseaux et des systèmes d'information dans l'Union(53) : l'idée est d'élever la capacité de ces réseaux à résister à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement.

La directive structure aussi la gouvernance de ces enjeux de sécurité. Elle a mis en place un groupe de coopération pour l'échange d'informations entre les États membres, ainsi qu'un réseau des centres de réponse aux incidents de sécurité informatique (réseau des CSIRT), pour permettre une coopération opérationnelle rapide.

Sur les règles juridiques, la directive SRI établit des exigences en matière de sécurité et de notification pour les opérateurs

de services essentiels (identifiés par chaque État membre, ce sont des entités publiques ou privées qui fournissent un service essentiel au maintien d'activités sociétales et/ou économiques critiques(54)) et pour les fournisseurs de service numérique (places de marché en ligne, services d'informatique en nuage et moteurs de recherche). Par une harmonisation minimale, laissant aux États membres la possibilité d'adopter un niveau de sécurité plus élevé, elle pose des obligations de gestion des risques, de notification des incidents pour les opérateurs de services essentiels (OSE) et les fournisseurs de service numérique.

L'application de cette directive a mis en évidence de nombreuses insuffisances : faible niveau de résilience cybernétique des entreprises, manque de cohérence de la résilience entre les États membres et les secteurs concernés, faible niveau de connaissance commune de la situation et absence de réponse commune aux crises. En outre, le manque de clarté du champ d'application de la directive (identification des OSE par les États membres) a entraîné des différences nationales importantes dans son application. Par exemple, certains grands hôpitaux peuvent ou non relever du champ d'application de la directive selon les qualifications retenues au niveau national. Enfin, une certaine inefficacité du régime de surveillance a été constatée : les États membres n'ont pas réellement appliqué les sanctions prévues pour les entités qui n'avaient pas mis en place des exigences de sécurité ou n'avaient pas signalé les incidents. À tout cela s'ajoute encore un problème de coopération et de confiance mutuelle entre les États membres qui n'ont pas toujours partagé leurs informations, ce qui affaiblit l'efficacité des mesures de cybersécurité.

La proposition de directive SRI 2(55) élève le niveau d'harmonisation européenne et cherche à opérer un changement systémique et structurel : l'idée est de couvrir un champ matériel plus large avec une surveillance plus ciblée sur les grands acteurs clés. La proposition élargit le champ d'application de la directive actuelle en ajoutant de nouveaux secteurs en fonction de leur importance pour l'économie et la société(56). Fondamentalement, la proposition élimine la distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques : les entités seraient classées en fonction de leur importance et divisées, respectivement, en catégories essentielles et importantes, avec des régimes de surveillance différents : le texte distingue les « entités essentielles » et les « entités importantes » atteignant des seuils spécifiques dans un grand nombre de secteurs. La directive s'appliquerait donc à certaines entités *essentielles* publiques ou privées opérant dans des secteurs de l'annexe I (énergie ; transports ; banques ; infrastructures des marchés financiers ; santé ; eau potable ; eaux usées ; infrastructures numériques ; administration publique et espace) et à certaines entités *importantes* opérant dans les secteurs de l'annexe 2 (services postaux et de courrier ; gestion des déchets ; fabrication, production et distribution de produits chimiques ; production, transformation et distribution de denrées alimentaires ; fabrication et fournisseurs numériques). Les micro et petites entités sont exclues du champ d'application de la directive, à quelques exceptions(57).

La proposition cherche aussi à renforcer la confiance des autorités publiques nationales et des entreprises pour encourager le partage d'informations (assistance mutuelle, mécanismes d'évaluation par les pairs). Elle prévoit, par exemple, un cadre pour la divulgation coordonnée des vulnérabilités et exige des États membres qu'ils désignent des CSIRT pour servir d'intermédiaires de confiance et faciliter l'interaction entre les entités déclarantes et les fabricants ou fournisseurs de produits TIC et les services de TIC.

La résilience des entités critiques. Une directive de 2008 prévoit une protection des « entités critiques », c'est-à-dire des systèmes indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens(58) : elle s'applique aux secteurs de l'énergie, des transports, des services bancaires, des infrastructures de marchés financiers, de la santé, de l'eau potable et des eaux usées, des infrastructures numériques, des administrations publiques et de l'espace.

La directive prévoit des obligations pour les États membres, notamment de prendre certaines mesures visant à garantir la fourniture, sur le marché intérieur, de services essentiels au maintien des fonctions vitales de la société et des activités économiques, en particulier d'identifier les entités critiques et de leur permettre de renforcer leur résilience et d'améliorer leur capacité à fournir ces services sur le marché intérieur. Elle établit aussi des règles de surveillance et une supervision spécifique des entités critiques présentant une importance particulière pour l'Europe.

La proposition de révision cherche à améliorer la résilience des entités critiques, qui fournissent des services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales (59), et à la mettre en cohérence avec la directive SRI 2, en écho à l'interdépendance entre les activités physiques et numériques. L'idée est que les autorités compétentes désignées en vertu de la directive sur la résilience des entités critiques et celles désignées en vertu de la directive SRI 2 prennent des mesures complémentaires et échangent des informations sur la résilience cybernétique et non cybernétique. L'objectif est aussi que les entités particulièrement critiques dans les secteurs essentiels, au sens de la directive SRI 2, soient également soumises à des obligations plus générales de renforcement de la résilience pour faire face aux risques non cybernétiques.

2 - La sécurité des réseaux 5G

La « future souveraineté technologique de l'Europe » dépend de ses infrastructures numériques stratégiques (60). Les réseaux 5G constituent une infrastructure numérique stratégique, car ils sont au coeur de tous les enjeux économiques, démocratiques et sociétaux : la cybersécurité des réseaux 5G est « essentielle non seulement pour protéger nos économies, nos sociétés et nos processus démocratiques » : la « dépendance de nombreux services critiques à l'égard des réseaux 5G rendrait les conséquences de perturbations systémiques et généralisées particulièrement graves » ; « garantir la cybersécurité des réseaux 5G revêt donc une importance stratégique pour l'Union, à l'heure où le nombre de cyberattaques ne cesse de croître et alors que ces attaques, plus sophistiquées que jamais, émanent d'une grande variété d'acteurs malveillants, en particulier des acteurs étatiques ou soutenus par un État extérieurs à l'UE » (61). L'enjeu est le déploiement d'un réseau 5G hautement sécurisé, alors que se profile déjà l'horizon des réseaux 6G.

Le rapport du groupe SRI, daté de 2019, sur les risques liés à la cybersécurité des réseaux 5G, souligne que la principale différence de la 5G avec les cybermenaces sur les réseaux existants porte sur la nature et l'intensité des impacts de ces menaces : « la dépendance accrue des fonctions économiques et sociétales à l'égard des réseaux 5G pourrait aggraver considérablement les conséquences négatives potentielles des perturbations » (62). L'intégrité et la disponibilité des réseaux 5G sont des enjeux fondamentaux, dès lors que les cyberattaques peuvent atteindre des services de sécurité publique, d'urgence, de santé, des activités gouvernementales, etc. Les auteurs de ces cyberattaques peuvent avoir des profils et des motivations variés (du hacker individuel, motivé par des considérations financières ou un désir de notoriété, au « groupe hacktiviste », cherchant à atteindre les organisations auxquelles il s'oppose, en passant par les « groupes de criminels organisés », les cyberterroristes et l'espionnage industriel), mais ce sont surtout celles qui sont le fait d'acteurs étatiques ou soutenus par un État qui sont potentiellement les plus attentatoires à la souveraineté étatique, puisque leurs motivations sont politiques et qu'ils ont les moyens d'atteindre des cibles critiques (63) : « ils représentent les acteurs les plus sérieux et les plus susceptibles de constituer une menace, car ils peuvent avoir la motivation, l'intention et surtout la capacité de mener des attaques persistantes et sophistiquées contre la sécurité des réseaux 5G. La combinaison de la motivation, de l'intention et d'une capacité de haut niveau permet aux États de perpétrer des attaques qui peuvent être très complexes et avoir un impact majeur sur les services essentiels pour le grand public, détériorant la confiance dans les technologies mobiles et les opérateurs » (64). Les cyberattaques conduites par des États étrangers peuvent être renforcées par l'aide d'un initié, qui renvoie à une personne travaillant pour le compte d'un opérateur de réseau mobile ou d'un fournisseur de réseau mobile et qui cherche à servir les intérêts d'un acteur étatique. Plusieurs États membres ont

identifié certains pays comme représentant une « menace cybernétique particulière pour leurs intérêts nationaux, sur la base du mode opératoire antérieur des attaques de certaines entités ou de l'existence d'un programme cybernétique offensif d'un État tiers donné à leur encontre »(65).

On évoque souvent l'architecture technologique décentralisée de la 5G, qui élargit les possibilités pour les cyberattaques, du fait que certaines fonctions des coeurs de réseaux peuvent être intégrées en périphérie. À cela s'ajoute le recours accru aux logiciels qui, à l'occasion de leurs mises à jour, peuvent être la cible de malwares. L'importance des logiciels dans les équipements 5G a aussi pour effet de confier un rôle majeur aux opérateurs de réseaux mobile dans la gestion de la sécurité lors du déploiement du réseau. Ces spécificités technologiques renforcent « la dépendance des opérateurs de réseau mobile à l'égard de fournisseurs tiers et au rôle de ces derniers dans la chaîne d'approvisionnement 5G », aussi, dans ce contexte « d'exposition accrue aux attaques facilitées par des fournisseurs tiers, le profil de risque individuel des fournisseurs » a une importance toute particulière(66).

La marge de manoeuvre européenne en matière de sécurité des réseaux 5G reste étroite, dès lors que les questions de sécurité nationale relèvent, au sens de l'article 4 TUE, de la seule responsabilité des États membres. Le Conseil européen ayant souhaité une « approche concertée » en matière de sécurité des réseaux 5G(67), la Commission(68) a sollicité des évaluations nationales des risques pour coordonner cette évaluation au niveau européen. L'« approche européenne commune » repose sur cette coordination au sein du groupe de coopération SRI (composé de représentants des États membres, de la Commission et de l'ENISA) pour analyser les risques et vulnérabilités des réseaux 5G, qui a donné lieu à une boîte à outils pour la cybersécurité de la 5G en 2020(69).

Les conclusions de la boîte à outils recommandent aux États membres d'évaluer avec soin les profils de risque des fournisseurs et d'appliquer des restrictions pour les fournisseurs à haut risque. Ces restrictions peuvent aller jusqu'à exclure certains fournisseurs si cela est nécessaire. Les opérateurs sont aussi incités à recourir à plusieurs fournisseurs pour éviter une dépendance trop marquée à l'égard d'un seul(70).

Un faisceau d'indices permet d'évaluer les risques des fournisseurs, le principal étant la possibilité que le fournisseur soit soumis à des interférences provenant d'un État tiers(71). L'interférence d'États tiers est renforcée par l'existence de liens étroits entre le fournisseur et le gouvernement de ce pays, par la législation du pays tiers, « en particulier lorsqu'il n'existe pas de contrepoids législatif ou démocratique, ou en l'absence d'accords de sécurité ou de protection des données entre l'UE et le pays tiers donné »(72), par « les caractéristiques de l'actionnariat du fournisseur », et, enfin, « la capacité du pays tiers à exercer toute forme de pression, y compris en ce qui concerne le lieu de fabrication de l'équipement »(73). Ces caractéristiques ont conduit à poser la question du recours aux entreprises chinoises pour fournir les infrastructures nécessaires au déploiement de la 5G, notamment Huawei.

Les États ont ainsi adopté des législations protégeant la sécurité nationale selon différentes modalités. La loi française du 1er août 2019 prévoit que l'exploitation sur le territoire national des appareils permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile est soumise à une autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale. Le Premier ministre doit refuser l'autorisation prévue à l'article L. 34-11 s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale. Pour cela, il doit prendre en considération, pour l'appréciation de ce risque, le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un État non membre de l'Union européenne. La décision rendue sur cette loi, dite « anti-Huawei », par le Conseil constitutionnel français, le 5 février 2021(74), confirme la constitutionnalité du dispositif d'autorisation administrative d'exploitation des équipements de réseaux 5G(75).

Si la Commission ne peut qu'accompagner la mise en oeuvre de cette approche européenne de cybersécurité de la 5G (76), **elle reste en mesure d'agir sur d'autres terrains qui ont une incidence sur la sécurité de la chaîne d'approvisionnement 5G.** Les « mesures stratégiques contribuant à garantir la souveraineté et l'avance technologiques de l'UE dans le développement futur des technologies de réseau » (77) doivent maintenir une chaîne d'approvisionnement et de valeur dans le domaine de la 5G pour éviter toute forme de dépendance à long terme. Pour cela, les institutions européennes peuvent agir en renforçant les règles techniques et organisationnelles en matière de sécurité des communications électroniques ou encourager la normalisation, et ainsi promouvoir des spécifications techniques permettant d'atteindre les objectifs en matière de sécurité et d'interopérabilité. Des mécanismes de certification 5G peuvent aussi être envisagés dans le cadre européen de certification en matière de cybersécurité.

D'autres outils peuvent compléter cette stratégie d'autonomie européenne des réseaux 5G (et favoriser la diversification des fournisseurs d'équipements 5G), comme la mobilisation des instruments de défense commerciale pour lutter contre les distorsions du marché de l'offre de la 5G résultant de dumping ou de subventions, l'application des règles de concurrence pour maintenir une ouverture des marchés de fourniture de matériel et de logiciels 5G. Les règles de passation des marchés publics dans le domaine des réseaux 5G peuvent aussi contribuer à ces objectifs, en intégrant ces exigences de sécurité lors de l'attribution de marchés publics en rapport avec les réseaux 5G. La Commission envisage aussi d'appliquer le cadre de l'UE pour le filtrage des investissements directs étrangers pour les actifs clés pour la 5G, en contrôlant les IDE non seulement sur les actifs de réseau sensibles, mais, plus largement, sur toute la chaîne de valeur de la 5G. Les autres instruments de la politique de cybersécurité européenne, ainsi que ceux qui se mettent en place dans la politique de cyberdéfense peuvent aussi contribuer à la sécurité des réseaux 5G.

B - La cyberdéfense

Dans son discours sur l'état de l'Union, en 2017, le président de la Commission affirmait que « les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars ». De fait, la cyberdéfense est devenue progressivement le cinquième champ d'intervention opérationnel de la défense européenne.

L'émergence d'une politique de cyberdéfense européenne. La prise de conscience européenne en matière de cyberdéfense a été quelque peu tardive : ce n'est véritablement qu'en 2007, avec la cyberattaque visant l'Estonie et, en 2008, avec le conflit entre la Russie et la Géorgie, que l'ampleur des enjeux liés aux cyberattaques sur les questions de défense collective a été révélée, confirmée régulièrement par les attaques contre les infrastructures en Ukraine. De cette prise de conscience résulte une stratégie de cybersécurité européenne proposée en 2013 (78), qui a fait émerger le cyberespace comme le cinquième domaine opérationnel de la politique de défense et a ouvert la voie au développement des capacités de cyberdéfense.

La cyberdéfense présente des caractéristiques propres, en particulier le fait que les frontières entre le domaine civil et militaire s'estompent dans le cyberespace. Mais l'action de l'Union européenne en matière de cyberdéfense se heurte aussi aux difficultés générales de la politique européenne de défense, qui reste tributaire des souverainetés nationales et des conceptions différentes de ces enjeux (79), qui rendent difficile l'émergence d'une « cyberpuissance européenne » (80). L'Union européenne peine à raisonner de manière autonome, tant les liens avec l'alliance atlantique (81) restent un marqueur fort de la défense européenne.

La relation UE-OTAN en matière de cyberdéfense. La déclaration commune de Varsovie, du 8 juillet 2016, par l'UE et l'OTAN (82), a établi une coopération dans le domaine de la cybersécurité et de la cyberdéfense, notamment dans le

contexte des missions et opérations, ainsi que dans le cadre du renforcement des capacités de cyberdéfense, de la recherche et de la technologie. Un arrangement technique signé le 10 février 2016, entre l'équipe d'intervention en cas d'urgence informatique de l'UE (CERT-UE) et la capacité OTAN de réaction aux incidents informatiques (NCIRC), facilite le partage d'informations pour la prévention des cyberattaques. De nombreuses mesures de coopération ont ainsi été adoptées pour lutter contre les menaces hybrides et assurer la cyberdéfense (exercices communs, promotion de la recherche, formations et partage d'informations).

Les enjeux de souveraineté européenne. Le constat est aujourd'hui unanime : « différents États - la Russie, la Chine et la Corée du Nord, entre autres, mais aussi des acteurs non étatiques (y compris des organisations criminelles) inspirés, employés ou soutenus par des États, des agences de sécurité ou des entreprises privées - ont été impliqués dans des actes de cybermalveillance à visée politique, économique ou de sécurité comprenant des attaques contre des infrastructures critiques, des activités de cyberespionnage, la surveillance de masse de citoyens de l'Union, la participation à des campagnes de désinformation, la diffusion de maliciels (Wannacry, NotPetya, etc.), ainsi que la limitation de l'accès à l'internet et du fonctionnement de systèmes informatiques » ; ces activités « mettent en péril la démocratie, la sécurité, l'ordre public et l'autonomie stratégique de l'Union »(83).

L'Union et les États membres sont ainsi confrontés à des menaces étatiques de grande ampleur(84) « prenant la forme de cyberattaques politiques d'État » : « des capacités de cyberdéfense offensive sont utilisées contre les États membres de l'Union à une échelle sans précédent »(85), induisant une situation parfois qualifiée de « cyberguerre froide »(86). Aux côtés des formes plus « ordinaires » de cybercriminalité, l'enjeu pour la souveraineté étatique vient du fait qu'un grand nombre de cyberattaques sont dirigées, en violation du droit international, par des puissances étrangères ou avec leur appui.

La Commission européenne, qui se veut « géopolitique », affirme aujourd'hui vouloir « changer de paradigme » pour l'autonomie stratégique de l'Union européenne et repenser la place de l'Europe dans le monde. Au-delà du *soft power* caractéristique d'une Europe « naïve », l'Union doit devenir « un acteur autonome et stratégique » par l'adoption d'un « arsenal de hard power » à même de lui permettre de défendre sa vision du monde et ses propres intérêts : capacités technologiques de défense, lutte contre la désinformation et les menaces hybrides, cybersécurité, et souveraineté numérique(87).

De nombreux projets de coopération structurée permanente portent sur des questions de cyberdéfense. En décembre 2020, un accord politique a permis de confirmer la création d'un Fonds européen de défense qui doit permettre le financement de technologies de rupture en matière militaire(88) et contribuer à l'autonomie stratégique européenne (même si la participation d'États tiers à ce Fond est possible).

Boîte à outils cyberdiplomatique de l'Union. La « boîte à outils cyberdiplomatique » est conçue pour définir une réponse diplomatique commune de l'Union européenne face aux cyberattaques(89). Cette réponse repose sur une gradation de mesures qui va de la simple coopération et dialogue diplomatiques à des mesures préventives contre les cyberattaques et des sanctions. La stratégie de cybersécurité adoptée en décembre 2020 confirme cette réponse diplomatique aux cyberattaques. Elle cherche à renforcer la coordination de la cyberdéfense et la coopération et la constitution des capacités de cyberdéfense.

La cyberdiplomatie européenne permet également l'adoption de mesures restrictives dans le cadre de la PESC, sur le fondement d'un règlement et d'une décision (PESC) 2019/797 du 17 mai 2019(90) qui établissent un cadre pour des mesures restrictives ciblées visant à dissuader et contrer les cyberattaques ayant des effets importants qui constituent une

menace extérieure pour l'Union (91) ou ses États membres (92). Les cyberattaques sont des actions non autorisées qui concernent l'accès aux systèmes d'information, les atteintes à l'intégrité d'un système d'information ou des données, ou l'interception de données. Ces cyberattaques constituent une menace pour les États membres si elles portent atteinte aux systèmes d'information en ce qui concerne les infrastructures critiques (93), les services nécessaires au maintien d'activités sociales et/ou économiques critiques (94), les fonctions critiques des États (95), le stockage ou le traitement des informations classifiées ou les équipes d'intervention d'urgence mises en place par les pouvoirs publics.

Adoption de mesures restrictives contre des cyberattaques. Le Conseil a pris des mesures restrictives en juillet 2020 (96) en matière de cyberattaques : les huit personnes et quatre entités et organismes (chinois, nord-coréen et russes) responsables de cyberattaques qui ont été inscrites sur la liste des personnes et entités ou organismes sanctionnés se voient opposer une interdiction de voyager vers l'UE et un gel des avoirs. L'UE a ainsi identifié six personnes physiques et trois entités ou organismes comme responsables de cyberattaques, comme la tentative de cyberattaque contre l'Organisation pour l'interdiction des armes chimiques (OIAC) et les cyberattaques connues sous les noms de « WannaCry » (97), de « NotPetya » (98) et de « Operation Cloud Hopper » (99).

Parmi les individus sanctionnés, il est assez notable, du point de vue de la souveraineté, de souligner que figurent des membres des services de renseignements russes, identifiés comme des agents de soutien en matière de renseignement humain au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU). Quatre agents russes ont ainsi participé à la cyberattaque contre l'OIAC, aux Pays Bas, en avril 2018. Si elle avait abouti, cette cyberattaque aurait compromis la sécurité du réseau et les travaux d'enquête en cours sur les armes chimiques. Parmi les entités sanctionnées, on trouve aussi le Centre principal pour les technologies spéciales de la Direction principale de l'état-major général des forces armées de la Fédération de Russie, reconnu responsable de cyberattaques en 2017 (« NotPetya », contre un réseau électrique ukrainien), constitutives d'une menace extérieure pour l'Union ou ses États membres en ce qu'elles ont rendu les données inaccessibles dans un certain nombre d'entreprises de l'Union en ciblant les ordinateurs avec des *ransomwares* et en bloquant l'accès aux données, entraînant, entre autres, des pertes économiques importantes. La confirmation de la participation d'entités et d'agents russes à ces cyberattaques renforcent les enjeux de souveraineté numérique européenne de la cyberdiplomatie. La souveraineté numérique doit renforcer la « résilience européenne », c'est-à-dire sa capacité à résister aux chocs.

III - La souveraineté numérique « résilience » : la défense des valeurs européennes

A - La défense du modèle de démocratie libérale

Les enjeux du numérique sur les démocraties sont considérables, car ils révèlent de nouvelles vulnérabilités qui posent, en particulier, la question de la manipulation des opinions publiques et de la protection de l'intégrité des élections : la protection à définir passe donc à la fois par la lutte contre des multiples formes de désinformation et de manipulation de l'opinion publique, afin d'influencer le résultat des élections, et contre les cyberattaques qui peuvent cibler des infrastructures électorales critiques. Le plan d'action européen de 2018 contre la désinformation (100) précise que les campagnes de désinformation, en particulier celles menées par des pays tiers, font souvent partie d'une guerre hybride (101) comprenant des cyberattaques et le piratage de réseaux. La stratégie pour l'Union de la sécurité de 2020 insiste aussi sur la dimension hybride des attaques menées par des acteurs étatiques qui combinent cyberattaques, dommages causés aux infrastructures critiques, campagnes de désinformation et actions de radicalisation du discours politique.

Le numérique pose aussi d'autres enjeux démocratiques fondamentaux, comme le microciblage et la publicité politique, qui peuvent très largement contribuer à ces formes de manipulation (à l'image de l'affaire *Cambridge Analytica*), mais qui concernent sans doute un peu moins directement des enjeux de souveraineté numérique que les opérations qui sont le fait

de puissances étrangères.

Le constat est passablement inquiétant : les acteurs étatiques étrangers « déploient de plus en plus des stratégies de désinformation visant à influencer des débats sociétaux, à introduire des clivages et à interférer avec les processus de prise de décision démocratiques »(102). En 2018, une trentaine d'États avaient déjà recours à ces stratégies de désinformation, mais la Russie, dont la doctrine militaire passe ouvertement par le contrôle de l'information, était identifiée comme la principale menace pour l'Union européenne ; les cyberattaques russes sont « systématiques, bénéficient d'importantes ressources et se distinguent par leur ampleur des activités menées par d'autres pays. Eu égard à leur caractère coordonné, à leur niveau de ciblage et à leurs implications stratégiques, les activités de désinformation de la Russie font partie d'une menace hybride plus vaste qui fait appel à divers outils et leviers, ainsi qu'à des acteurs non étatiques ». L'attention portée aux cyberattaques russes ne doit pas faire oublier que d'autres pays tiers « assimilent rapidement les méthodes russes et déploient également des stratégies de désinformation »(103).

En 2020, deux États font l'objet d'une préoccupation particulière : la Russie et la Chine(104), même si d'autres États contribuent très largement aux cyberattaques contre les démocraties, comme la Corée de Nord ou la Turquie(105).

Lutte contre les cyberattaques contre les infrastructures électorales critiques. Ces cyberattaques peuvent d'abord passer par des intrusions ciblées pour collecter des informations sensibles et organiser des fuites (pratiques de « hack and leak », c'est-à-dire de piratage et de divulgation, qui peuvent avoir lieu avec ou sans falsification de ces informations), et la perturbation de systèmes informatiques (notamment d'entreprises de radiotélédiffusion ou de commissions électorales)(106). Les élections démocratiques sont devenues la cible de ces cyberstratégies malveillantes, comme la campagne de l'élection présidentielle américaine de 2016, qui a fait l'objet de « hack and leak operation » (HLO) par les services de renseignement russes. Les processus électoraux sont protégés comme infrastructures critiques dans le cadre du filtrage des investissements directs étrangers(107), du recueil sur la cybersécurité des technologies électorales(108) et sont intégrés dans la révision de la directive SRI, qui devrait permettre de lutter contre les opérations de « hack and leak »(109).

Il faut, à l'évidence, aller au-delà : un mécanisme européen pour renforcer « la résilience des processus électoraux », à travers le réseau européen de coopération en matière d'élections, est envisagé pour rassembler des expertises et échanges de bonnes pratiques, en lien avec le groupe de coopération SRI pour la sécurité des réseaux et des systèmes d'information et le système d'alerte rapide de l'UE.

La lutte contre les opérations d'influence et les ingérences étrangères. Les plateformes numériques et les réseaux sociaux sont une voie privilégiée pour les ingérences étrangères cherchant à manipuler l'opinion publique et influencer les résultats des élections, et ainsi porter atteinte à l'intégrité des processus électoraux : ces ingérences passent par la prise de contrôle de comptes de médias sociaux, l'utilisation de comptes de médias sociaux commandés par des robots (*bots*).

Il existe de multiples formes de désinformations, définies comme « des contenus faux ou trompeurs diffusés avec l'intention de tromper ou dans un but lucratif ou politique et susceptibles de causer un préjudice public »(110). La Commission distingue, dans cette pluralité de stratégies de désinformation, deux formes d'ingérences particulièrement attentatoires pour la souveraineté numérique : les « opérations d'influence » qui renvoient à des « efforts coordonnés déployés par des acteurs nationaux ou étrangers pour influencer un public cible, au moyen d'une série de moyens fallacieux, notamment la suppression de sources d'information indépendantes, combinée à de la désinformation », et les « ingérences étrangères dans l'espace de l'information, qui ont souvent lieu dans le cadre d'une opération hybride plus large », définies comme « des efforts coercitifs et trompeurs déployés par un acteur d'un État étranger ou des agents de celui-ci

dans le but d'entraver la formation et l'expression libres de la volonté politique des individus »(111). L'ingérence électorale des puissances étrangères est une menace particulièrement forte pour les démocraties, comme l'ont montré les inquiétudes autour des élections au Parlement européen de 2019, qui ont aussi donné lieu à des activités de désinformation constantes de la part de sources russes pour déstabiliser et influencer le processus électoral(112), malgré les précautions prises par les institutions(113).

Bien conscientes des enjeux démocratiques fondamentaux des opérations d'influence et des ingérences étrangères depuis 2015(114), les institutions européennes cherchent cependant encore des moyens de les contrer. La commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE) du Parlement européen, procède à des travaux et auditions sur ces sujets. Le groupe de travail East Stratcom, au sein du service européen pour l'action extérieure, est une cellule de communication stratégique à destination de l'Europe orientale, qui conduit le projet *EUvsDisinfo*. Ce projet cherche, depuis 2015, à anticiper et répondre aux campagnes permanentes de désinformation de la Russie touchant l'Union européenne, ses États membres, ainsi que les pays situés dans leur voisinage commun. Son objectif est d'éclairer et permettre la compréhension des opérations de désinformation du Kremlin : par une analyse étendue de données et des médias, EUvsDisinfo recense et diffuse, sur sa base de données, les cas de désinformation provenant des médias pro-Kremlin dans l'Union(115), et analyse les nouvelles pratiques de désinformation. Une partie importante de l'activité de ce groupe de travail porte sur l'ingérence électorale.

Un travail de lutte contre les contenus de désinformation élaborés et propagés par des sources russes, en vue d'élections et de référendums organisés dans l'UE, a été entrepris : aux campagnes de désinformation sur la guerre en Syrie, sur la destruction de l'appareil du vol MH17 dans l'est de l'Ukraine, sur l'utilisation d'armes chimiques dans l'attaque de Salisbury(116), succède aujourd'hui une vague de désinformation sur la pandémie de Covid-19 et la campagne vaccinale(117). La Russie et la Chine lancent désormais « des opérations d'influence et des campagnes de désinformation ciblées sur la Covid-19, visant à saper le débat démocratique, à exacerber la polarisation sociale et à améliorer leur propre image »(118).

Le *Digital Services Act* devrait contribuer à donner aux autorités publiques européennes des moyens de lutter contre ces manipulations. La lutte contre la manipulation devrait aussi passer par la sanction financière des entreprises qui participent à des opérations d'influence ou à des activités d'ingérence étrangère. Des enjeux commerciaux alimentent, en effet, la manipulation des médias sociaux, avec l'émergence d'entreprises spécialisées dans l'acquisition de faux comptes ou « de faux engagements, de manière à amplifier artificiellement tel ou tel récit concernant des questions politiques particulières et à exploiter des divisions existantes au sein de la société »(119).

B - La défense du bien commun

Les monnaies virtuelles posent, avec une grande acuité, la question de leur régulation par les autorités publiques, du fait des risques que pose cette « privatisation monétaire »(120) pour la stabilité financière et, plus largement, la souveraineté monétaire européenne. Mais la captation, par les plateformes numériques, des attributs de la souveraineté concerne aussi d'autres prérogatives de puissance publique, comme le contrôle juridictionnel du respect des droits fondamentaux dans les activités numériques.

1 - La souveraineté monétaire européenne

Les monnaies virtuelles suscitent une méfiance des autorités publiques(121), parfois inversement proportionnel à

l'engouement qu'elles semblent susciter dans des transactions décentralisées, émancipées de toute médiation étatique, à travers des technologies de registres distribués comme la *blockchain*. Dès lors, il est tentant de voir dans cette appropriation par des personnes privées d'un domaine, par essence, régalien, un contournement de la souveraineté de l'État. La première bataille est une question de qualification, les institutions publiques rejetant celle de monnaie pour évoquer, par une forme de mystification volontairement inquiétante, la notion de « crypto actifs ».

Les enjeux de la qualification des monnaies virtuelles ou crypto-actifs ou « écran-monnaie » (122) **sont multiples**. Sans entrer dans des considérations trop approfondies, on peut rappeler l'opposition entre plusieurs théories qui cherchent à établir le critère de la qualification juridique de la monnaie : avec la théorie étatiste (souvent critiquée pour reposer sur une assimilation entre monnaie et monnaie ayant cours légal), la notion de monnaie est arrimée sur celle d'État, avec la théorie sociologique sur la confiance qu'elle suscite : ainsi, la « théorie sociologique rompt la filiation avec l'État et minimise l'importance de la souveraineté » (123), en qualifiant de monnaie, au fond, ce qui est socialement accepté comme monnaie dans les échanges. À cette théorie, on oppose l'idée de « tiers garant », qui peut être représenté par l'État (124) ou, plus largement, par des institutions publiques garantes de la stabilité monétaire. C'est ainsi qu'émerge une troisième théorie dans la doctrine, la théorie « institutionnelle » (125), qui repose sur l'idée que la confiance dans une monnaie repose sur l'existence d'un cadre institutionnel qui garantit la stabilité des prix en en faisant une réserve de valeur. La théorie institutionnelle dissocie les crypto-actifs de l'État, mais les arrime à la puissance publique en fondant la confiance qu'ils suscitent sur les institutions garantes de la stabilité monétaire ; ainsi conçu, « l'écran-monnaie ne signifie aucunement que le marché ait pris l'ascendant sur l'autorité » (126).

Si l'on accepte la qualification de monnaie virtuelle (en la dissociant de celle de monnaie ayant cours légal), comme semble le faire la Cour de justice (127) et le législateur européen (128), l'enjeu reste de penser leur régulation dans un cadre territorialement et conceptuellement délicat à appréhender, du fait de la nature décentralisée de la technologie des registres distribués. Les questions de stabilité financière sont fondamentales, mais d'autres enjeux, comme la lutte contre le blanchiment d'argent ou le financement du terrorisme, le sont tout autant. Le *Digital Finances package* cherche à clarifier l'application des règles européennes existantes aux crypto-actifs (129), sur la base d'une classification des différentes catégories de crypto-actifs qui distingue cryptomonnaies des jetons ou « token » : d'une part, pour les crypto-actifs déjà régis par la législation européenne (130), il s'agit de mettre à jour ces règles avec l'émergence des technologies distribuées par un « régime pilote » pour les infrastructures de marché qui font ou souhaitent tester des transactions sur instruments financiers sous forme de crypto-actifs (131). D'autre part, pour les actifs numériques non réglementés (crypto-actifs, jetons utilitaires et *stablecoins*, qui sont des jetons se référant à un ou des actifs et jetons de monnaie électronique), une proposition de règlement définit un nouveau régime (132), qui cherche à saisir assez largement tous les services qui leur sont liés (133).

L'enjeu pour la souveraineté monétaire concerne surtout la régulation de certains *tokens* (134) **: les jetons liés à des actifs de référence (les « stablecoins ») utilisés à des fins de paiement**. Les *stablecoins* ou « jetons de valeur stable » regroupent les jetons de monnaie électronique et les jetons se référant à des actifs. Ce sont des actifs numériques dont le but est de conserver une valeur stable, ce qui les rend plus utiles pour les paiements (contrairement aux crypto monnaies qui sont très volatiles). Cet enjeu de souveraineté monétaire est pris au sérieux par les institutions européennes (135) et les autorités nationales. Le gouvernement français évoque régulièrement les risques de perte de souveraineté liés aux monnaies virtuelles privées, et notamment aux crypto-actifs utilisés à des fins de paiement, comme les *stablecoins* qui prétendent offrir une valeur stable : ainsi, « l'émergence des global *stablecoins* (au premier rang desquels le projet Libra) soulève des enjeux inédits en termes de souveraineté (monétaire, économique, juridique, numérique et fiscale), du fait de leur usage potentiellement massif » (136).

L'Union européenne cherche à réguler (137) tous les services liés à ces actifs numériques non réglementés (crypto-actifs, jetons utilitaires et *stablecoins*) (138) et envisage de nouvelles obligations pour les prestataires de services de crypto-actifs (obtention d'un agrément), ainsi que pour les émetteurs de crypto-actifs (publication d'un livre blanc précisant les informations essentielles sur les actifs numériques), les émetteurs de jetons se référant à des actifs (agrément, gouvernance, conflits d'intérêts, informations sur le mécanisme de stabilisation, etc.), les émetteurs de jetons de monnaie électronique et les fournisseurs de services de crypto-actifs (exigences prudentielles et organisationnelles, traitement des plaintes, etc.). Les institutions cherchent aussi à organiser des mécanismes de surveillance efficaces au niveau national, voire européen, pour les émetteurs de *stablecoins* d'importance significative, qui seront sous le contrôle de l'Autorité bancaire européenne.

Une autre réponse, envisagée par les autorités publiques, semble être la création de monnaies virtuelles souveraines, c'est-à-dire de monnaies numériques qui pourraient avoir cours légal : ainsi, la Chine, qui a limité l'usage des cryptomonnaies, teste un yen numérique. La Commission et la BCE semblent amorcer un premier pas en ce sens, avec une déclaration commune sur l'euro numérique (139). Parmi les avantages associés à un euro numérique, la BCE met en avant, notamment, l'indépendance stratégique de l'UE (140).

La question des monnaies se pose avec d'autant plus d'acuité qu'elle est portée par une plateforme comme Facebook avec le Diem (anciennement appelé Libra) qui, en plus d'un système de cryptomonnaie, applique des systèmes d'identification virtuelle et, désormais, un système de protection para-juridictionnel des droits fondamentaux sur sa plateforme.

2 - La protection juridictionnelle des droits fondamentaux

La protection des droits fondamentaux suscite beaucoup de questions, en particulier le respect de la vie privée et de la liberté d'expression. Le *Digital Services Act* prévoit une pluralité de dispositions pour les plateformes qui présentent des risques systémiques.

Les plateformes numériques attachées à l'autorégulation semblent avoir voulu anticiper la question de la régulation des contenus pour mieux la maîtriser. Après différentes affaires qui ont posé avec acuité la question de la modération des contenus sur les grandes plateformes de réseaux sociaux, Facebook a créé un Conseil de surveillance pour garantir la liberté d'expression des utilisateurs, à travers une procédure d'appel permettant de contrôler les décisions de suppression de contenus sur ses plateformes.

Les premières décisions du Conseil de surveillance, rendues le 28 janvier 2021, annulent plusieurs décisions de Facebook : certaines mesures de suppression étaient fondées sur les Standards de la communauté en matière de discours haineux (141) ou en matière de personnes et d'organisations dangereuses (142). Le Conseil de surveillance a aussi annulé la décision de Facebook de supprimer une publication affirmant que l'hydroxychloroquine était un traitement pour le Covid-19, en vertu des Standards de la communauté en matière de violence et d'incitation (143).

Si cette instance n'est, à l'évidence, ni un organe juridictionnel ni un tribunal arbitral, il n'est pas inintéressant de souligner que le Conseil de surveillance cherche à légitimer ses solutions au regard de standards et instruments internationaux de protection des droits de l'homme. Ses décisions affirment, par exemple, l'applicabilité des Principes directeurs des Nations unies (PDNU) ou du Pacte international relatif aux droits civils et politiques. Elles citent aussi la pratique du Comité des droits de l'homme des Nations unies et les travaux du Rapporteur spécial des Nations unies sur la promotion et la protection de liberté d'opinion et d'expression.

Allant plus loin, l'appréciation des restrictions à la liberté d'expression s'inspire des méthodes juridictionnelles classiques,

en évoquant le contrôle de la nécessité et de la proportionnalité de l'atteinte. Ainsi, dans certaines décisions, le Conseil de surveillance évoque l'existence de mesures moins restrictives de la liberté d'expression que la suppression d'un contenu : ainsi, Facebook disposerait de nombreux moyens moins restrictifs que la suppression d'un contenu comme le fait de contextualiser davantage certaines publications. De la même façon, le Conseil de surveillance a souligné les problèmes de légalité, de cohérence, de clarté et d'intelligibilité des règles de Facebook en matière de désinformation et de préjudice imminent : certaines règles posées par Facebook seraient ainsi trop vagues, contraires aux normes internationales relatives aux droits de l'homme ou mentionnées de façon disparate.

L'affaire la plus attendue était à l'évidence celle du 5 mai 2021 relative à la suspension du compte de D. Trump(144), parfois comparée, de façon un peu surprenante, aux États-Unis à l'affaire *Marbury v. Madison* par la presse américaine(145). Facebook avait demandé au Conseil de surveillance si sa décision du 7 janvier visant à interdire l'accès de M. Trump à la publication de contenus sur Facebook et Instagram pour une durée indéterminée le 7 janvier dernier était opportune. Analysant la nécessité, l'adéquation et la proportionnalité de l'atteinte à la liberté d'expression, le Conseil de surveillance confirme que la sanction est proportionnée à l'infraction commise par D. Trump : les deux publications litigieuses de D. Trump du 6 janvier 2021(146) enfreignent gravement les Standards de la communauté Facebook et les Règles de la communauté Instagram. En alimentant de façon injustifiée l'idée de fraude électorale et des appels à l'action, D. Trump avait créé les conditions d'un risque sérieux de violence. La publication des contenus litigieux, qui légitiment des actes de violence, interviennent à un moment où il existait un risque clair et immédiat de préjudice. La violation des règles de Facebook par D. Trump est d'autant plus grave que, en tant que président des États-Unis, ses publications ont une forte influence. La gravité des infractions justifie donc la décision de Facebook de suspendre le compte de D. Trump.

Appliquant une sorte de principe de légalité des délits et des peines, le Conseil de surveillance juge cependant la suspension indéfinie du compte de D. Trump vague et « arbitraire » car non prévue par les règles de la plateforme. Les sanctions prévues par les règles de Facebook prévoient la suppression de contenus, l'imposition d'une période de suspension assortie de délais précis, ou encore la désactivation permanente d'une page ou d'un compte, mais pas une « suspension indéfinie ». Le Conseil en conclut que Facebook doit établir préalablement des sanctions nécessaires et proportionnées pour répondre aux infractions graves de ses règles relatives au contenu.

Facebook avait aussi souhaité obtenir du Conseil de surveillance des « observations ou des recommandations sur les suspensions à suivre lorsque l'utilisateur concerné est un dirigeant politique ». Dans son avis consultatif sur les politiques, le Conseil de surveillance se révèle peu disert, si ce n'est qu'il n'estime pas utile de distinguer entre les dirigeants politiques et les autres utilisateurs influents, soulignant que tout utilisateur influent peut contribuer à des risques sérieux de préjudice.

Ces quelques rapides éléments montrent que, malgré toutes les limites de l'analogie, si le Conseil de surveillance semble chercher une forme de légitimité quasi juridictionnelle, Facebook cherche surtout à définir sa propre légalité à travers les conditions générales d'utilisation incarnées par les « standards de la communauté » définis unilatéralement par la plateforme, en attendant, pourquoi pas, la création d'un « Parlement facebook » puisque la plateforme, après avoir créé un espace public, une identité numérique, une monnaie, un bloc de légalité et une « Cour suprême », pourrait bien, après tout, être tentée d'aller au bout de sa logique inspirée d'un singulier statomorphisme. Le développement de ces formes de légitimation des plateformes pourrait poser, à terme, la question de l'intégrité des fonctions régaliennes étatiques. L'insuffisance de l'auto-régulation apparaît ainsi de façon assez évidente, et l'apport du *Digital Services Act* se révèle fondamental.

On mesure ainsi comment, de façon ubiquitaire, le développement des activités numériques affecte les prérogatives régaliennes des États. La souveraineté numérique, si elle existe, renvoie donc à une souveraineté à l'envers : elle aurait pour objet de préserver, peut-être de restituer, les prérogatives souveraines des institutions publiques nationales, ou européennes selon les cas. Au regard de l'évolutionnisme permanent du numérique, de ses usages et de ses technologies, il est difficile de conclure précisément sur la question de la souveraineté numérique européenne. Cette réflexion pose malgré tout une question fondamentale sur l'identité européenne : l'Union européenne cherche-t-elle à incarner une Europe puissance ou recherche-t-elle simplement une forme de résilience ? En d'autres termes, la souveraineté numérique européenne se limite-t-elle à renforcer sa capacité à encaisser les chocs ou est-elle l'occasion pour l'Union européenne d'affirmer une réelle identité politique ?

Mots clés :
DROIT ET LIBERTE FONDAMENTAUX * Généralités * Protection * Dualité
INFORMATIQUE * Internet * Cloud computing * Développement et sécurisation * Politique européenne numérique * Souveraineté numérique européenne

(1) Le Président du Conseil européen a pourtant souligné combien l'approvisionnement en ressources critiques, comme les terres rares ou les microprocesseurs, sont « essentiels pour notre souveraineté numérique » (L'autonomie stratégique européenne est l'objectif de notre génération - Discours du président Charles Michel au groupe de réflexion Bruegel, 28 sept. 2020).

(2) A.-T. Norodom, Être ou ne pas être souverain, en droit, à l'ère numérique, *in* C. Castets-Renard, L. Rass-Masson, V. Ndior (dir.), *Enjeux internationaux des activités numériques, Entre logique territoriale des États et puissance des acteurs privés*, Larcier, 2020.

(3) Le rapport sénatorial de G. Longuet, en 2019, définit « la souveraineté numérique - capacité de l'État à agir dans le cyberespace - dans ses deux dimensions : la faculté d'exercer une souveraineté dans l'espace numérique, qui repose sur une capacité autonome d'appréciation, de décision et d'action dans le cyberespace - et qui correspond, de fait, à la cyberdéfense ; et la capacité de garder ou restaurer la souveraineté de la France sur les outils numériques, afin de pouvoir maîtriser nos données, nos réseaux et nos communications électroniques ».

(4) A. Blandin-Obernesser (dir.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016 ; P. Türk et C. Vallar (dir.), *La souveraineté numérique, le concept, les enjeux*, Mare & Martin, 2018.

(5) R. Carré de Malberg, *Contribution à la théorie générale de l'État*, Dalloz, 2003, Réimpression des éditions de 1920 et 1922.

(6) Rapport sénatorial de G. Longuet, préc.

(7) La commission des affaires européennes du Sénat français, soulignant « l'importance des enjeux de souveraineté

numérique », insiste sur « la double menace, pour les États européens et l'Union, que représentent, en matière d'autonomie stratégique, d'une part, la rivalité d'acteurs étatiques, par exemple via l'existence de législations extraterritoriales comme le Cloud Act, et d'autre part, la position dominante d'acteurs privés américains, et dans une moindre mesure chinois, susceptibles, en s'appuyant, notamment, sur la masse considérable de données qu'ils détiennent, d'entrer en concurrence avec les États dans leurs fonctions régaliennes » (Avis politique sur la politique européenne en matière de données et la souveraineté numérique européenne, 19 nov. 2020, p. 7).

(8) Commission des affaires européennes du Sénat français, Avis politique relatif au programme de travail de la Commission européenne pour 2021, 13 janv. 2021, p. 4.

(9) Le Sénat français a récemment dénoncé les choix politiques qui « cultivent une forme de complaisance vis-à-vis des géants du numérique extra-européens, plaçant nos démocraties libérales entre le modèle du capitalisme de surveillance à l'américaine et celui du crédit social chinois. Leur justification ne tient qu'au fait que les pays européens pâtissent d'un déficit d'offre en matière d'infrastructures et technologies de données, résultat d'une politique industrielle et de règles de concurrence inadaptées à l'ère numérique » (Proposition de résolution européenne du Sénat français du 21 oct. 2020 pour une localisation européenne des données personnelles).

(10) « Les équilibres entre puissances placent aujourd'hui l'Europe, et la France, dans une position bien particulière. Pour les États-Unis, il s'agit d'affirmer une souveraineté mondiale, forts de la création du net à l'origine libertarien - mais financé par la Défense, au prix de l'acceptation des monopoles - pourtant si contraires à la pratique historique des États-Unis -, et d'une chasse permanente et mondiale aux talents et aux pépites - puisque « le gagnant prend tout ». Pour la Chine et la Russie, l'affirmation de souveraineté se décline de façon différente, plus défensive et parfois plus subtile » (Rapport G. Longuet précité sur la souveraineté numérique de 2019).

(11) « Au cours des prochaines années, le virage numérique s'accélérera encore et aura des répercussions considérables. Nous devons nous assurer que l'Europe sera souveraine sur le plan numérique et obtiendra sa juste part des avantages découlant de cette évolution » (Conseil européen, Un nouveau programme stratégique 2019-2024, 20 juin 2019).

(12) C. Morin Desailly utilise la même image (« L'Union européenne, colonie du monde numérique ? », rapport de la commission des affaires européennes du Sénat, n° 443, 2013).

(13) Selon le mot de Frank-Walter Steinmeier, cité par Maxime Lefebvre, « Europe puissance, souveraineté européenne, autonomie stratégique : un débat qui avance pour une Europe qui s'affirme », Question d'Europe, n° 582, févr. 2021.

(14) T. Breton, Discours devant la sous-commission sécurité et défense du Parlement européen - 25 juin 2020.

(15) *Ibid.*

(16) Communication de la Commission, *Une nouvelle stratégie industrielle pour l'Europe*, 10 mars 2020 COM(2020) 102 final, p. 1 (nous soulignons).

(17) Communication de la Commission, 19 févr. 2020, *Façonner l'avenir numérique de l'Europe*, COM(2020) 67 final.

(18) Communication de la Commission, 19 févr. 2020, *Une stratégie européenne pour les données*, COM(2020)66 final.

(19) L'art. 173, § 3, TFUE, organise la transversalité de la politique industrielle européenne, en prévoyant que les toutes les politiques européennes doivent contribuer à la réalisation des objectifs de cette politique.

(20) Communication de la Commission, *Une nouvelle stratégie industrielle pour l'Europe*, 10 mars 2020 COM(2020) 102 final, p. 13.

(21) Conclusions du Conseil européen extraordinaire, 1er et 2 oct. 2020.

(22) B. Bertrand, Polyphonie dans l'appréciation du recours à une solution technique américaine pour la Plateforme Health data Hub : le Conseil d'État et l'art de la fugue, JCP, 30 nov. 2020.

(23) Proposition de résolution européenne du Sénat français du 21 oct. 2020 pour une localisation européenne des données personnelles.

(24) Une association à but non lucratif de droit belge dont les statuts ont été signés le 15 sept. 2020 à Bruxelles.

(25) Des discussions sont, par exemple, en cours avec Microsoft, qui propose des services de cloud avec Azur, en cause dans l'affaire *Health Data Hub*.

(26) V. par ex. M. Mazzucato, *L'État entrepreneur. Pour en finir avec l'opposition public privé*, Fayard, 2020.

(27) Agence pour les projets de recherche avancée de défense (Defense Advanced Research Projects Agency : DARPA).

(28) V. le document de la Commission « Report on European Technology Platforms and Joint Technology Initiatives : Fostering Public-Private R&D Partnerships to Boost Europe's Industrial Competitiveness », 10 juin 2005, SEC(2005) 800.

(29) Cour des comptes européenne, Rapport annuel sur les entreprises communes de l'UE pour l'exercice 2018 (2019//C426//01).

(30) Le Parlement européen et le Conseil sont responsables des procédures annuelles relatives au budget et à la décharge. V. les Rapports annuels de la Cour des comptes européennes sur les entreprises communes de l'UE et du 12 nov. 2020 pour l'exercice 2019.

(31) Les plateformes technologiques européennes servent à l'identification des besoins en matière de recherche et à l'organisation de programmes de recherche (« agendas stratégiques de recherche »).

(32) Les initiatives technologiques conjointes sont des partenariats public-privé qui associent des investissements privés et publics (nationaux et européen).

(33) Par exemple, ARTEMIS, qui porte sur les systèmes intégrés (composants informatiques spécialisés affectés à une tâche spécifique), et ENIAC, sur la nanoélectronique, ont finalement été fusionnées en une seule entreprise commune : ECSEL (Composants et systèmes électroniques pour un leadership européen).

(34) COM(2020) 569 final2020/0260.

(35) V., sur la boîte à outil élaborée par les États membres avec la Commission et l'Agence de l'UE pour la cybersécurité (ENISA) définissant des mesures d'atténuation.

(36) Dans le prolongement des enjeux de connectivité mis en évidence par le code des communications électroniques européen, dont le délai de transposition expirait le 21 déc. 2020 (Dir. 2018/1972 du 11 déc. 2018). V. aussi la dir. 2014/61 sur la réduction des coûts du haut débit.

(37) Recommandation de la Commission du 18 sept. 2020 concernant une boîte à outils commune de l'Union pour réduire le coût de déploiement des réseaux à très haute capacité et assurer un accès au spectre radioélectrique 5G en temps utile et dans des conditions favorables aux investissements, afin de favoriser la connectivité pour soutenir la reprise économique après la crise Covid-19 dans l'Union, C(2020) 6270 final.

(38) L'objectif de ce programme est de fournir des capacités de communication sécurisées aux missions et opérations critiques pour la sécurité et la sûreté gérées par l'Union européenne et ses États membres, y compris les acteurs nationaux de la sécurité et les agences et institutions de l'UE.

(39) Règl. (UE) 2019/881 du 17 avr. 2019, art. 2, JOUE du 7 juin 2019.

(40) Selon l'ANSSI, « la moitié de ces attaques sont le fait de seulement 5 groupes distincts », ce qui montre leur professionnalisation : malgré cela, ils restent « difficilement identifiables, souvent hors de portée des mécanismes d'entraide pénale internationale, voire, dans certains cas, protégés par des États » (Cybersécurité : faire face à la menace, la stratégie française, 18 févr. 2021, p. 7).

(41) Les cyberattaques par rançongiciels ont été multipliées par 4 en France entre 2019 et 2020, passant de 54 à 192.

(42) *Cybersécurité : faire face à la menace*, La stratégie française, 18 févr. 2021, p. 8.

(43) L'administration fédérale allemande a confirmé qu'elle était concernée. L'OTAN et le Parlement européen pourraient avoir été ciblés.

(44) Cette attaque pourrait être le fait du groupe APT29, qui est lié aux services de renseignement russes (SVR). La société de sécurité n'a pas confirmé ce lien, qui ne se fonde, jusqu'à présent, que sur les similitudes entre Sunburst et un autre malware développé par des pirates informatiques russes. La Chine ou la Corée du Nord pourraient aussi être en cause.

(45) La stratégie française passe ainsi par le développement de « solutions souveraines identifiées comme clé pour notre autonomie stratégique » (Cybersécurité : faire face à la menace, la stratégie française, 18 févr. 2021, p. 13).

(46) Règl. (UE) 2019/881 du 17 avr. 2019, consid. 8, JOUE du 7 juin 2019.

(47) Communication de la Commission, *Stratégie de l'UE pour l'Union de la sécurité*, 24 juill. 2020, COM(2020) 605 final.

(48) Communication de la Commission, *Une nouvelle stratégie industrielle pour l'Europe*, 10 mars 2020 COM(2020) 102 final, p. 13.

(49) Règl. (UE) 2019/881 du 17 avr. 2019, JOUE du 7 juin 2019.

(50) Le texte définit un « produit TIC » comme un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information, un « service TIC » comme un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information, et, enfin un « processus

TIC » comme un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance.

(51) Un certificat de cybersécurité européen atteste qu'un produit TIC, service TIC ou processus TIC a été évalué en ce qui concerne sa conformité aux exigences de sécurité spécifiques fixées dans un schéma européen de certification de cybersécurité.

(52) Dir. (UE) 2016/1148 du 6 juill. 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JOUE 2016, n° L 194, p. 1.

(53) Entendus comme tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, ces systèmes renvoient aussi aux données numériques stockées, traitées, récupérées ou transmises en vue de leur fonctionnement, utilisation, protection et maintenance.

(54) Les opérateurs de services essentiels sont des entités publiques ou privées qui fournissent un service essentiel au maintien d'activités sociétales et/ou économiques critiques (santé, transports, énergie, banques et infrastructures des marchés financiers, infrastructures numériques et fourniture d'eau), dès lors que la fourniture de ce service est tributaire des réseaux et des systèmes d'information et qu'un incident aurait un effet disruptif important sur la fourniture du service.

(55) 16 déc. 2020, COM(2020) 823 final.

(56) Elle laisse une certaine souplesse aux États membres pour identifier les petites entités présentant un profil de risque élevé en matière de sécurité.

(57) Ces exceptions concernent les fournisseurs de réseaux de communications électroniques ou de services de communications électroniques accessibles au public, les fournisseurs de services de confiance, les registres de noms de domaines de premier niveau (TLD) et de l'administration publique, et certaines autres entités, tel le fournisseur unique d'un service dans un État membre.

(58) Dir. 2008/114/CE du Conseil du 8 déc. 2008 concernant le recensement et la désignation des infrastructures critiques européennes, ainsi que l'évaluation de la nécessité d'améliorer leur protection, JOUE 2008, n° L 345, p. 75.

(59) 16 déc. 2020 COM(2020) 829 final.

(60) Communication de la Commission, *Une nouvelle stratégie industrielle pour l'Europe*, préc. p. 13.

(61) Communication de la Commission, 29 janv. 2020, *Sécurité du déploiement de la 5G dans l'UE -Mise en oeuvre de la boîte à outils de l'UE,* COM(2020) 50 final, p. 1.

(62) Groupe SRI, *Rapport sur l'évaluation coordonnée au niveau de l'UE des risques liés à la cybersécurité des réseaux 5G*, 9 oct. 2019, p. 12.

(63) Par exemple, les fonctions de coeur de réseau, les fonctions de gestion et d'orchestration de réseau et les fonctions de réseau d'accès.

(64) Groupe SRI, Rapport sur l'évaluation coordonnée au niveau de l'UE des risques liés à la cybersécurité des réseaux 5G, 9 oct. 2019, p. 13. Par exemple, des États ou des acteurs soutenus par des États peuvent provoquer une panne à grande échelle ou une perturbation importante des services de télécommunications en exploitant des fonctions non documentées ou en attaquant des infrastructures critiques interdépendantes (par exemple, l'alimentation électrique).

(65) Groupe SRI, rapport préc., p. 14.

(66) *Ibid.*

(67) Concl. du 22 mars 2019.

(68) Recomm. 2019/534 sur la cybersécurité des réseaux 5G du 26 mars 2019, JOUE 2019, n° L 88, p. 42.

(69) Groupe SRI, Cybersécurité des réseaux 5G, Boîte à outils de l'UE : mesures destinées à atténuer les risques, 29 janv. 2020.

(70) *Ibid.*

(71) Le rapport SRI précise que « si l'accès direct d'un acteur de la menace à la chaîne d'approvisionnement des télécommunications ou son influence sur celle-ci peut faciliter considérablement son exploitation à des fins malveillantes et rendre l'impact de ces actions nettement plus grave, il convient également de noter que les acteurs ayant un niveau élevé d'intention et de capacités, comme les acteurs étatiques, chercheront à exploiter les vulnérabilités à n'importe quel stade du cycle de vie des produits fournis par n'importe quel fournisseur » (NIS Cooperation Group, Rapport de 2019 préc., p. 22).

(72) Dans ce contexte, plusieurs États membres attribuent un profil de risque plus élevé aux fournisseurs qui sont sous la juridiction de pays tiers menant une politique cybernétique offensive.

(73) Groupe SRI, Rapport de 2019 préc., p. 22

(74) Décis. n° 2020-882 QPC du 5 févr. 2021, *Société Bouygues télécom*, AJDA 2021. 306 ; *ibid.* 680, note C. Broyelle. V. les QPC transmises par le Conseil d'État à propos de la loi n° 2019-810 du 1er août 2019 dite « anti Huawei » (CE 18 nov. 2020, n° 442120, Lebon ; AJDA 2021. 774), en particulier les dispositions de la loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.

(75) B. Bertrand, J. Sirinelli, Entre cybersécurité et régulation économique, le Conseil constitutionnel valide la loi « anti Huawei », JCP, 15 mars 2021.

(76) Essentiellement en assurant un suivi par des rapports sur l'état d'avancement de la mise en oeuvre de la boite à outils, en juill. 2020 et déc. 2020, qui soulignent les enjeux pour l'achèvement de l'application de ces mesures : les États doivent ainsi veiller à ce que les risques identifiés soient atténués de manière satisfaisante et coordonnée, notamment en vue de réduire au minimum l'exposition aux fournisseurs à haut risque et d'éviter la dépendance à l'égard de ces derniers.

(77) Communication de la Commission, 29 janv. 2020, *Sécurité du déploiement de la 5G dans l'Union, Mise en oeuvre de la boîte à outils de l'UE,* COM(2020) 50 final, p. 10.

(78) Communication conjointe de la Commission et de la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité, 7 févr. 2013, « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé » (JOIN(2013)0001). V. aussi le Cadre stratégique de cyberdéfense de l'Union européenne du 18 novembre 2014, les concl. du Conseil du 10 févr. 2015 sur la cyberdiplomatie, et l'évaluation de la stratégie de cybersécurité de l'Union européenne en 2013 (document de travail des services de la Commission du 13 sept. 2017 « Assessment of the EU 2013 Cybersecurity Strategy » (SWD(2017)0295).

(79) G. Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, Palgrave Macmillan, 2016.

(80) D. Deschaux-Dutard, L'Union européenne, une cyberpuissance en devenir ? Réflexion sur la cyberdéfense européenne, Rev. internationale et stratégique 2020/1, n° 117, p. 18.

(81) V. Joubert et J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de

l'OTAN et de l'UE », Hérodote, n° 152-153, 2014/1-2.

(82) Concl. du Conseil sur la mise en oeuvre de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du Traité de l'Atlantique Nord (6 déc. 2016, doc. 15283/16 ; 5 déc. 2017, doc. 14802/17).

(83) Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI).

(84) « Le nombre de cyberattaques continue d'augmenter. Ces attaques sont plus sophistiquées que jamais, proviennent de sources très diverses à l'intérieur et à l'extérieur de l'UE et ciblent des domaines dont la vulnérabilité est maximale. Des acteurs étatiques ou soutenus par un État sont souvent impliqués et visent des infrastructures numériques essentielles, comme les principaux fournisseurs de services en nuage » (Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité du 24 juill. 2020, COM/2020/605 final).

(85) Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI).

(86) Cette notion de « cyberguerre froide » désigne « un état du cyberespace dans lequel les États se munissent d'un arsenal cybernétique - tant défensif qu'offensif - et recourent - souvent indirectement, via des acteurs non étatiques - à des cyberattaques dans le cadre de manoeuvres de déstabilisation, sans franchir le seuil qui caractériserait une cyberguerre ouverte » (D. Deschaux-Dutard, L'Union européenne, une cyberpuissance en devenir ? Réflexion sur la cyberdéfense européenne, *op. cit.*, p. 18).

(87) T. Breton, « Repenser notre sécurité : vers l'autonomie stratégique de l'Europe - discours au Parlement Européen », Discours devant la sous-commission sécurité et défense du Parlement européen le 25 juin 2020.

(88) Thierry Breton évoque ainsi des solutions d'*edge computing* permettant une agrégation des données des drones militaires, des technologies spatiales (récepteurs de positionnement par satellites d'*encryption* militaire utilisant Galileo PRS, capteurs optiques militaires pour petits satellites, des solutions de Big Data pour la surveillance par satellites), des technologies de surveillance et de détection des menaces cyber, un réseau crypté tactique et militaire (T. Breton, « Repenser notre sécurité : vers l'autonomie stratégique de l'Europe », *op. cit.*).

(89) V. les concl. du Conseil du 19 juin 2017 relatives à un cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance (« boîte à outils cyberdiplomatique »). V. aussi la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 13 sept. 2017 « Résilience, dissuasion et défense : doter l'Union européenne d'une cybersécurité solide » (JOIN(2017)0450).

(90) Règl. (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, JOUE 2019, n° L 129 I, p. 1 ; Décis. (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, JOUE n° L 129 I, p. 13.

(91) Les cyberattaques constituant une menace pour l'Union sont, notamment, celles qui sont dirigées contre ses institutions, organes et organismes, ses délégations auprès de pays tiers ou d'organisations internationales, ses opérations et missions organisées dans le cadre de la politique de sécurité et de défense commune et ses représentants spéciaux.

(92) Les cyberattaques constituant une menace extérieure sont, notamment, celles qui ont leur origine ou sont menées à l'extérieur de l'Union, utilisent des infrastructures situées à l'extérieur de l'Union, sont menées par toute personne physique ou morale, toute entité ou tout organisme établi ou agissant à l'extérieur de l'Union, ou sont menées avec l'appui, sur les instructions ou sous le contrôle de toute personne physique ou morale, entité ou organisme agissant à l'extérieur de l'Union.

(93) Ce sont les infrastructures indispensables au maintien des fonctions vitales de la société, ou à la santé, la sûreté, la sécurité et au bien-être économique ou social des citoyens.

(94) Cela concerne, en particulier, les secteurs de l'énergie, des transports, des activités bancaires, des infrastructures des marchés financiers, de la santé, de l'approvisionnement en eau potable et sa distribution, des infrastructures numériques et tout autre secteur essentiel pour l'État membre concerné.

(95) En particulier dans les domaines de la défense, de la gouvernance et du fonctionnement des institutions, y compris pour ce qui est des élections publiques ou de la procédure de vote, du fonctionnement de l'infrastructure économique et civile, de la sécurité intérieure et des relations extérieures, y compris dans le cadre de missions diplomatiques.

(96) Décis. PESC du Conseil 2020/1127 du 30 juill. 2020 modifiant la décis. (PESC) 2019/797 concernant des mesures restrictives à l'encontre des cyberattaques menaçant l'Union ou ses États membres JOUE n° L 246, p. 12 ; et Règl. d'exécution 2020/1125 du Conseil du 30 juill. 2020 modifiant le règl. 2019/796 concernant des mesures restrictives à l'encontre des cyberattaques menaçant l'Union ou ses États membres JOUE 2020, n° L 246, p. 4.

(97) « WannaCry » est une cyberattaque qui a perturbé des systèmes d'information dans le monde entier, en les ciblant au moyen d'un rançongiciel et en bloquant l'accès aux données. Les systèmes d'information d'entreprises présentes dans l'Union, y compris des systèmes d'information relatifs à des services nécessaires à la maintenance de services et d'activités économiques essentiels au sein des États membres, en ont été affectés.

(98) « NotPetya » est une cyberattaque qui a rendu des données inaccessibles dans un certain nombre d'entreprises au sein de l'Union, de l'Europe au sens large et du monde entier, en ciblant les ordinateurs au moyen d'un rançongiciel et en

bloquant l'accès aux données.

(99) L'opération « Cloud Hopper » a ciblé les systèmes d'information de sociétés multinationales sur six continents, y compris des entreprises situées dans l'Union, et a obtenu un accès non autorisé à des données commercialement sensibles.

(100) Communication du 5 déc. 2018, *Plan d'action contre la désinformation*, JOIN(2018) 36 final.

(101) Cadre commun en matière de lutte contre les menaces hybrides : une réponse de l'Union européenne, JOIN(2016)18final.

(102) Communication du 5 déc. 2018, *Plan d'action contre la désinformation*, JOIN(2018) 36 final, p. 3. Ces stratégies visent non seulement des États membres, mais également des pays partenaires du voisinage oriental, ainsi que du voisinage méridional, du Proche-Orient et d'Afrique

(103) Plan d'action contre la désinformation, *op. cit.*, p. 4.

(104) Communication de la Commission relative au plan d'action pour la démocratie européenne, 3 déc. 2020, COM/2020/790 final.

(105) V. les travaux et auditions de la Commission INGE du 2 févr. 2021 (Commission spéciale du Parlement européen sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation).

(106) Plan d'action contre la désinformation, *op. cit.,* p. 3.

(107) Le règl. (UE) 2019/452 du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union (JOUE 2019, n° L 79 I, p. 1) qualifie les infrastructures électorales d'infrastructures critiques susceptibles d'être prises en compte pour apprécier si les effets d'un investissement direct étranger sont susceptibles de porter atteinte à la sécurité ou à l'ordre public.

(108) Groupe SRI, Compendiumon Cyber Security of Élection Technology, CG Publication 03/2018, juill. 2018.

(109) Plan d'action pour la démocratie européenne, *op. cit.*

(110) *Ibid.*

(111) *Ibid.*

(112) Rapport sur la mise en oeuvre du plan d'action contre la désinformation [JOIN(2019) 12 final du 14 juin 2019)].

(113) Malgré l'anticipation des institutions européennes : v. la recommandation de la Commission sur les réseaux de coopération électorale, la transparence en ligne, la protection contre les incidents de cybersécurité et la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement européen, C(2018)5949.

(114) Le Conseil européen a commencé à évoquer la menace que représentent les campagnes de désinformation en ligne à partir de 2015 et a mandaté la haute représentante pour lutter contre les campagnes de désinformation de la Russie. Cela a donné naissance à la *task force East Strat.*

(115) Depuis 2019, EUvsDisinfo étudie et informe aussi la désinformation diffusée dans les Balkans occidentaux et dans le voisinage sud de l'UE.

(116) Plan d'action contre la désinformation, *op. cit.*

(117) Communication conjointe de la Commission européenne et du haut représentant intitulée « Lutter contre la désinformation concernant la Covid-19 - Démêler le vrai du faux », JOIN(2020) 8 final.

(118) Plan d'action pour la démocratie européenne, *op. cit.*

(119) *Ibid.*

(120) F. Martucci, Réflexions sur la notion de monnaie légale à l'heure de l'écran-monnaie : rétablir l'autorité face au marché, E. Carpano et G. Marti (dir.), *Démocratie et marché dans l'Union européenne*, Bruylant, 2021, spéc. p. 265.

(121) Banque de France, « Les dangers liés au développement des monnaies virtuelles : l'exemple du Bitcoin », Focus n° 10, 5 déc. 2013.

(122) F. Martucci propose la notion d'« écran-monnaie » pour décrire « les instruments monétaires dématérialisés dont il n'est possible de concrétiser l'existence que par le truchement d'un écran » (F. Martucci, Réflexions sur la notion de

monnaie légale à l'heure de l'écran-monnaie : rétablir l'autorité face au marché, *op. cit.,* spéc. p. 263).

(123) *Ibid.*

(124) « La monnaie ne se laisse pas dissoudre dans l'analyse économique standard. Car, pour remplir sa fonction d'actif financier ou d'instrument de paiement, elle doit nécessairement instituer une communauté de cocontractants [...]. Et, ce qui soude cette communauté de croyants ne dépend pas de la conviction individuelle de chacun de ses membres. En dépit des fantasmes contemporains de monnaie autoréférentielle, il n'y a pas et il ne peut y avoir de monnaie sans un tiers garant de sa valeur. Ce tiers a été, jusqu'à ces dernières années, en Europe et encore aujourd'hui dans la plupart des pays, incarné par l'État, qui, au travers de sa banque centrale, est l'ultime gardien de la qualité des relations monétaires » (A. Supiot, Homo juridicus. *Essai sur la fonction anthropologique du Droit*, Seuil 2005, coll. Point Essai, p. 159).

(125) A. Sáinz de Vicunna, Institutional Theory of Money, *in* M. Giovanoli et D. Devos (dir.), *International Monetary and Financial Law : The Global Crisis*, Oxford University Press, 2010, p. 517-532 cité par F. Martucci, Réflexions sur la notion de monnaie légale à l'heure de l'écran-monnaie : rétablir l'autorité face au marché, *op. cit.*, p. 269.

(126) F. Martucci, Réflexions sur la notion de monnaie légale à l'heure de l'écran-monnaie : rétablir l'autorité face au marché, *op. cit.*, p. 276.

(127) CJUE, 22 oct. 2015, aff. C-264/14, *Hedqvist*, D. 2015. 2251 ; Rev. crit. DIP 2020. 669, étude M. Audit ; RTD com. 2016. 830, obs. D. Legeais ; RTD eur. 2016. 77, obs. D. Berlin. T. Bonneau, Analyse critique de la contribution de la CJUE à l'ascension juridique du bitcoin, Liber amicorum Blanche Sousi, *L'Europe bancaire et financière,* 2016, RB éd., p. 295.

(128) La directive relative à la prévention de l'utilisation du système financier, aux fins du blanchiment de capitaux, définit les monnaies virtuelles comme « les représentations numériques d'une valeur qui ne sont émises ou garanties ni par une banque centrale, ni par une autorité publique, qui ne sont pas nécessairement liées non plus à une monnaie établie légalement et qui ne possèdent pas le statut juridique de monnaie ou d'argent, mais qui sont acceptées comme moyen d'échange par des personnes physiques ou morales et qui peuvent être transférées, stockées et échangées par voie électronique » (dir. (UE) 2015/849 du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, art. 3, JOUE 2015, n° L 141, p. 73).

(129) Les crypto-actifs sont définis comme la représentation numérique d'une valeur ou de droits pouvant être transférée et stockée de manière électronique, au moyen de la technologie des registres distribués ou d'une technologie similaire.

(130) Les actifs numériques assimilables à des instruments financiers relèvent, par exemple, de la législation européenne sur les marchés de valeurs mobilières.

(131) Proposition de règlement sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, COM(2020) 594 final.

(132) Proposition de règlement sur les marchés de crypto-actifs, COM(2020) 593.

(133) Notamment les fournisseurs de portefeuilles de conservation, les échanges de crypto-actifs, les plateformes de négociation de crypto-actifs et les émetteurs de crypto-actifs.

(134) Un « jeton utilitaire » est une catégorie d'actif numérique destiné à fournir un accès numérique à un bien ou à un service, disponible sur la DLT, et uniquement accepté par l'émetteur de ce jeton. Il existe une grande variété de *tokens* qui peuvent permettre d'accéder à un service ou faciliter les paiements.

(135) Communication de la Commission sur une stratégie en matière de finance numérique pour l'UE, 24 sept. 2020, COM(2020) 591 final.

(136) Réponse du ministère de l'Économie (publiée dans le JO Sénat du 11 mars 2021, p. 1634) dans le cadre des débats parlementaires relatifs au « Développement des monnaies numériques et perte de souveraineté » qui ont eu lieu au Sénat français.

(137) Proposition de règlement sur les marchés de crypto-actifs, COM(2020) 593.

(138) Notamment les fournisseurs de portefeuilles de conservation, les échanges de crypto-actifs, les plateformes de négociation de crypto-actifs et les émetteurs de crypto-actifs.

(139) La déclaration conjointe de la Commission européenne et de la Banque centrale européenne sur leur coopération en matière d'euro numérique, le 19 janv. 2021, confirme que ces institutions réfléchissent aux enjeux politiques, juridiques et techniques de l'introduction éventuelle d'un euro numérique.

(140) BCE, *Rapport sur l'euro numérique*, oct. 2020.

(141) Dans le cas 2020-002-FB-UA, le Conseil de surveillance annule la suppression d'une publication évoquant le manque de réaction face au traitement réservé aux musulmans ouïgours en Chine, par rapport aux réactions violentes qu'ont suscitées les caricatures en France. En revanche, le Conseil de surveillance a maintenu la décision de Facebook de supprimer une publication utilisant le mot russe (« taziks ») pour décrire les Azéris qui, selon les affirmations de l'utilisateur, n'avaient pas d'histoire par rapport aux Arméniens (Cas 2020-003-FB-UA).

(142) Le Conseil de surveillance a annulé la décision de Facebook de supprimer une publication contenait une citation attribuée à Goebbels (Cas 2020-005-FB-UA).

(143) Cas 2020-006-FB-FBR.

(144) Cas 2021-001-FB-FBR.

(145) « Cet arrêt rappelle l'arrêt monumental rendu en 1803 par la Cour suprême des États-Unis dans l'affaire *Marbury v. Madison*, une affaire qui a établi le principe de responsabilité du pouvoir judiciaire sur les pouvoirs exécutif et législatif » (https://www.cnbc.com/2021/05/05/facebook-oversight-boards-trump-decision-was-marbury-v-madison-moment.html).

(146) Le 6 janv. 2021, au cours du dépouillement des votes du collège électoral et des violentes émeutes et de l'assaut du Capitole de Washington, le président Donald Trump a publié deux contenus : au cours de l'insurrection, il a diffusé une vidéo sur Facebook et Instagram dans laquelle il affirme : « Je comprends votre douleur. Je sais que vous vous sentez blessés. On nous a volé cette élection. C'était une victoire écrasante et tout le monde le sait, surtout nos adversaires. Mais il faut rentrer maintenant. Nous devons retrouver la paix. Il faut que la loi et l'ordre règnent. Nous devons respecter nos forces de l'ordre. Nous ne voulons aucun blessé. C'est une période difficile, inédite, où de tels évènements surviennent, où ils ont pu nous la voler à tous, à moi, à vous, à notre pays. C'était une élection frauduleuse, mais nous ne pouvons pas entrer dans leur jeu. Nous devons retrouver la paix. Alors rentrez chez vous. Nous vous aimons. Vous êtes exceptionnels. Vous avez vu ce qu'il s'est passé. Vous avez vu la manière dont les autres sont traités, à quel point ils sont mauvais et diaboliques. Je sais ce que vous ressentez. Mais rentrez chez vous et rentrez en paix ». Facebook a supprimé cette publication pour avoir enfreint son Standard de la communauté sur les individus et organismes dangereux.

Ensuite, alors que la police sécurisait le Capitole, D. Trump a publié une déclaration écrite sur Facebook : « Ce sont des choses et des évènements qui arrivent quand une immense victoire électorale est si peu cérémonieuse et si vicieusement arrachée à de grands patriotes qui ont été mal et injustement traités pendant si longtemps. Rentrez chez vous en paix et avec amour. Souvenez-vous de ce jour pour toujours ! ». Facebook a supprimé cette publication pour avoir enfreint son Standard de la communauté sur les individus et organismes dangereux. Facebook a également bloqué la fonction de publication de M. Trump sur Facebook et Instagram pendant 24 heures avant d'étendre la suspension « jusqu'à nouvel ordre et pour au moins les deux prochaines semaines jusqu'à ce que la transition pacifique du pouvoir soit terminée ».

Les limites du concept de souveraineté numérique

Par Jean-Philippe Derosier,
Professeur agrégé des facultés de droit à l'Université Lille II – Droit & Santé, membre du CRD&P EA 4487 (ERDP), Directeur scientifique du ForInCIP et de la revue Jurisdoctoria, auteur du blog La Constitution décodée[1]

À l'instar de tout concept, on ne peut donner du concept de « souveraineté numérique » qu'une définition stipulative. Celle-ci pourrait être trouvée dans la formulation de Pierre Bellanger[2], spécialiste de souveraineté numérique et qui a indiqué qu'elle est « la maîtrise de notre destin sur les réseaux informatiques. C'est l'extension de la République dans cette immatérialité informationnelle qu'est le cyberespace »[3]. Une telle définition, proposée par un expert du numérique et de sa souveraineté, mérite-t-elle d'être discutée, qui plus est par un juriste ?

Oui, si l'on commence par demander si elle peut correspondre à la souveraineté numérique *juridiquement* entendue. Mais alors, d'autres interrogations émergent. Que signifie « *juridiquement* » dans cette assertion ? Est-il *nécessaire* de définir la souveraineté numérique juridiquement ? Est-il seulement *possible* de définir la souveraineté numérique juridiquement ?

---

1. L'auteur, qui assume seul la responsabilité de ces lignes, remercie Basak Acar, étudiante du Master 2 Droit de la sécurité et de la défense, pour l'aide dans la recherche bibliographique

2. P. Bellanger, *La souveraineté numérique*, Stock, Paris, 2014. Voir également, du même auteur, « De la souveraineté numérique », in *Le Débat* 2012/3 (n° 170), pp. 149 à 159.

3. « La souveraineté numérique : ce dossier qui effraie Hollande et Valls », in *Le Point*, 13 janvier 2016, http://www.lepoint.fr/politique/emmanuel-berretta/la-souverainete-numerique-ce-dossier-qui-effraie-hollande-et-valls-13-01-2016-2009389_1897.php, consulté le 25 avril 2017.

Quant au « juridique », d'abord indiquons qu'il s'agit là de ce qui a trait à l'ordre normatif qu'est le droit, donc aux normes (juridiques) positives et à leur validité, leur application et leur organisation. Le droit a pour particularité de régler lui-même sa propre production : est donc « juridique » ce que le droit lui-même pose comme tel[4].

Quant au « nécessaire », ensuite remarquons que dans la loi pour une République numérique[5], entrée en vigueur le 7 octobre 2016, l'article 29, introduit par amendement parlementaire en première lecture à l'Assemblée nationale[6], dispose que :

« Le Gouvernement remet au Parlement, dans un délai de trois mois à compter de la promulgation de la présente loi, un rapport sur la possibilité de créer un Commissariat à la souveraineté numérique *rattaché aux services du Premier ministre, dont les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège. Ce rapport précise les moyens et l'organisation nécessaires au fonctionnement du Commissariat à la souveraineté numérique. »*[7]

Le droit positif semble ainsi se saisir de la souveraineté numérique, à des fins précisément juridiques. Le Commissariat à la souveraineté numérique, qui pourrait être juridiquement établi et rattaché à une institution juridiquement établie par la Constitution, le Premier ministre, pourrait se voir confier des missions juridiques, telles que concourir à l'exercice de « la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège ». En effet, soit cette souveraineté nationale et les droits et libertés en question ne relèvent pas eux-mêmes du droit, auquel cas l'étude pourrait s'arrêter ici. Soit, ce qui

4. On souscrit ici à la méthodologie normativiste et, au-delà de ce rappel, on se permet de renvoyer, pour de plus amples détails, aux travaux de Kelsen, principalement et à ce que l'on a pu écrire par ailleurs.
5. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* du 8 octobre 2016.
6. Amendement, n° CL129, Assemblée nationale, 6 janvier 2016.
7. On peut également mentionner le décret n° 2016-66 du 29 janvier 2016 instituant un commissaire à l'information stratégique et à la sécurité économique (*JORF* du 30 janvier 2016) : ledit commissaire est notamment associé à la définition et la mise en œuvre des politiques publiques dans le domaine de la souveraineté numérique (article 2).

paraît plus vraisemblable au point qu'on le considérera comme admis, ils en relèvent et, dans ce cas, on peut se demander s'il existe un lien entre la dénomination dudit commissariat et les missions qui lui sont confiées. En d'autres termes, il est bien nécessaire de chercher à définir la souveraineté numérique du point de vue juridique.

Cela est-il alors seulement possible enfin ? Oui, mais difficile et subtil. En effet, le concept juridique de souveraineté numérique soulève des difficultés en tant que concept « néo-générationnel », ou concept « 2.0 » ! (I), tandis que sa dimension « bidimensionnelle » (ou 2.2 ?) révèle ses subtilités (II).

1. Les difficultés d'un concept néo-générationnel

En tant que concept néo-générationnel, la souveraineté numérique n'est pas forcément récente mais supposerait, pour être pensée, de dépasser les modèles classiques[8]. Celui de l'État, certes (2), mais d'abord celui du droit lui-même, pensé selon le modèle hiérarchique de la « pyramide des normes » (1).

a. Dépasser le modèle pyramidal

Le numérique lui-même est un réseau, plaçant tous ses utilisateurs en interaction constante. Le penser en droit, à partir de la souveraineté numérique, requiert alors de dépasser le modèle pyramidal classique, de la théorie de la hiérarchie des normes élaborée par l'École de Vienne. Cela impose d'évoluer vers les théories du réseau, où les systèmes juridiques sont eux-mêmes en interaction : c'est généralement à cette méthodologie que souscrivent ceux qui proposent des réflexions sur la souveraineté numérique.

La théorie d'un droit qui ne fonctionnerait plus exclusivement selon le modèle pyramidal kelsénien mais qui rejoindrait un fonctionnement « en réseau » a été initialement développée par les Professeurs François Ost et Michel van de Kerchove. Son élaboration part du constat que le modèle pyramidal est aujourd'hui insuffisant pour « rendre compte à lui seul de la

8. On renvoie, pour d'autres développements sur ce sujet, à P. Türk, « La souveraineté de l'État à l'épreuve d'internet », in *RDP* 2013/6, pp. 1489 et s.

complexité croissante de la réalité juridique »[9], car il reposerait sur une trop grande simplicité. Dès lors, « pour faire bref, trois hypothèses essentielles se dégagent : sans disparaître, la hiérarchie révèle ses limites – discontinuité, inachèvement, alternance – où la subordination cède partiellement la place à la coordination et à la collaboration ; sans perdre toute vigueur, la linéarité se relativise et s'accompagne fréquemment de phénomènes de bouclage ou d'inversion dans l'ordre des relations ; l'arborescence se dilue, dans la mesure où la multiplicité des foyers de création du droit ne peut pas toujours être dérivée d'un point unique et souverain »[10]. Afin d'illustrer leur propos, les auteurs s'arrêtent alors sur l'exemple de la construction européenne : « l'Europe ne représente pas comme un étage supérieur de notre construction juridique […]. Elle interfère à tous les niveaux de notre vie quotidienne et transforme en profondeur nos ordres juridiques. Or, c'est la thèse qu'on soutient, le "modèle européen" s'inscrit malaisément dans l'ordonnancement hiérarchique des pouvoirs, de même qu'il ne relève guère des techniques réglementaires classiques. C'est dire que son intrusion progressive dans les systèmes juridiques nationaux contribue fortement à la diffusion de la logique régulatoire propre aux figures en réseau »[11].

---

9. F. Ost et M. Van de Kerchove, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Publications de l'Université de St Louis, Bruxelles, 2002, p. 49. Soulignons bien que les auteurs ne proposent pas de renoncer au système pyramidal, mais de le compléter par la figure du réseau.

10. *Ibidem*, p. 50.

11. *Ibidem*, p. 65. Sur cette figure du réseau à propos de la construction européenne, cf. également R. Tinière, « L'accélération de la constitutionnalisation de l'Europe : prémices de la création d'un État fédéral européen ou structuration accrue de l'espace européen ? », in *Politeia* n° 8 (2005), pp. 303 à 315 ; ainsi que, où le réseau est évoqué en propos conclusifs, R. Medhi, « La "double hiérarchie" normative à l'épreuve du projet de traité établissant une Constitution pour l'Europe », in *Les dynamiques du droit européen en début de siècle. Études en l'honneur de Jean-Claude Gautron*, Pédone, Paris, 2004, pp. 461 et 462. La figure d'un « droit en réseau » a été étudiée à l'aune de nombreux autres exemples, parmi lesquels celui de la loi belge attribuant compétence universelle aux tribunaux belges pour juger de certains crimes, cf. A. Bailleux, « L'histoire de la loi belge de compétence universelle. Une valse à trois temps : ouverture, étroitesse, modestie », in *Droit et société* n° 59 (2005), pp. 107 à 136. L'auteur décèle, dans cette loi, « un mouvement d'*ouverture* de la pyramide étatique aux réalités d'un monde en réseau qui ne se satisfait plus d'une production traditionnelle du droit » (p. 109),

Cela soulève néanmoins une première difficulté, celle de la validité. En effet, selon quel critère, dans ces nouveaux modèles, le droit est-il valide, existe-t-il ? Cette construction théorique part d'une hypothèse parfaitement discutable, qui est admise et non vérifiée : la « simplicité » de la construction pyramidale serait « insuffisante » pour expliquer la réalité juridique contemporaine. De plus, elle correspond davantage à une analyse de sociologie juridique et non à une construction théorique expliquant le droit positif : en étudiant le rôle et l'influence d'acteurs dans la production du droit (non pas d'organes habilités à produire des normes mais bien d'acteurs exerçant une influence sur les contenus normatifs), les tenants de cette construction théorique étudient et expliquent une façon de créer des contenus normatifs et non pas comment le droit est valide ou comment il est appliqué. En ce sens, cette construction théorique ne constitue pas, « à l'heure actuelle, une alternative à la théorie de la hiérarchie des normes, mais une régression vers un empirisme naïf. Elle n'explique pas plus, mais moins »[12].

b. Dépasser le modèle étatique

De même, penser la souveraineté numérique, en droit, requiert de dépasser l'État[13] et de « penser global »[14], en lien direct avec la théorie du

évoquant même « un réseau normatif sans frontière » (p. 113), et arguant du fait que « les organisations non gouvernementales jouèrent un rôle fondamental dans la promotion de la loi […] ; cette ingérence des ONG au sein du pouvoir législatif est tout à fait caractéristique d'une production du droit en réseau qui consacre une écriture à plusieurs mains de la règle » (p. 127).

12. O. Pfersmann, « La production des normes : production normative et hiérarchie des normes », in D. Chagnollaud, M. Troper (dir.), *Traité international de droit constitutionnel*, Dalloz, Paris, tome 2 : *Distribution des pouvoirs*, 2012, p. 526 ; cf. également O. Pfersmann, « Contre le pluralisme mondialisationnaliste, pour un monisme juridique ouvert et différencié », in M. Senn, B. Winiger (dir.), *Recht und Globalisierung*, *Archiv für Rechts- und Sozialphilosophie*, Beiheft n° 121, pp. 140 et 141.

13. C'est ce que propose Dominique Rousseau. Outre sa contribution, on renvoie à « Dominique Rousseau : "Le numérique signe la fin du droit des États" », *Libération,* 21 septembre 2015.

14. D. G. Post, « Governing Cyberspace », in *Wayne Law Review* 1996 (Vol. 43, No. 1), pp. 155 à 171.

droit en réseau. Cela impose ainsi de dépasser la dimension nationale en prenant en compte d'autres acteurs, tous liés par le réseau. Les utilisateurs du numérique, les opérateurs économiques, GAFA et autres, les acteurs du contrôle du numérique sont alors parties prenantes et il faut prendre en compte leur intervention, leur action et presque leur domination dans le monde numérique, donc leur (forme de) souveraineté numérique.

De plus, la souveraineté numérique peut, voire doit être pensée au niveau de l'Union européenne. Cependant, selon les canons juridiques classiques, cette dernière n'est pas souveraine[15].

Cela soulève alors une seconde difficulté quant à l'identification de ces acteurs, du point de vue du droit. La question n'est pas de savoir selon quel phénomène humain ils ont été créés (réunion d'individus qui avaient en commun un projet d'entreprise, par exemple), mais bien selon quels critères peuvent-ils être identifiés en droit et bénéficier, ainsi, du *droit* d'agir sur la scène juridique. *Google* est une société internationale au poids majeur dans le monde numérique, mais n'existe qu'en vertu du droit et des États.

À l'heure actuelle, ces acteurs existent tous en vertu de critères directement ou indirectement étatiques, l'État étant la source du droit garantissant l'accès au réseau, permettant la création d'opérateurs économiques (sociétés commerciales ou autre), offrant une régulation du réseau. C'est parce qu'il y a des normes constitutionnelles qu'il peut y avoir des lois et des règlements sur leur fondement, permettant de créer ces acteurs. Et l'on retrouve le modèle pyramidal. C'est toujours parce qu'il y a des constitutions, instituant des États, que ces derniers peuvent, selon leurs règles constitutionnelles, agir sur la scène internationale et créer des institutions, telles celles de l'Union européenne. Et l'on retrouve le modèle étatique.

Par conséquent, dépasser ce modèle revient à nier l'existence même de ces acteurs. Cela pourrait s'inscrire également dans une volonté de souscrire à une démocratie numérique, qui pourrait être le prolongement

15. Sur ce sujet long et épineux, on s'autorise à renvoyer aux travaux que l'on a publiés sous le titre *Les limites constitutionnelles à l'intégration européenne*, LGDJ, Paris, coll. Bibliothèque constitutionnelle et de science politique, 2015, notamment le dernier chapitre.

d'une démocratie constitutionnelle, le numérique signant la fin du droit des États.

Cela ne fait que repousser la difficulté car il faut alors déterminer comment penser la démocratie et la Constitution en dehors du cadre étatique. Certes, le célèbre article 16 de la Déclaration des droits de l'homme et du citoyen de 1789 ne vise pas l'État mais « toute société ». Cependant, au-delà du fait que ce ne sont là que des mots et non des concepts, selon l'analyse ici développée, « toute société » qui s'organise à partir d'une Constitution s'érige en État, car il n'y a pas d'autre source normative de Constitution que de source étatique.

On retombe alors sur le même écueil rencontré à propos de la théorie du droit en réseau : le dépassement du modèle pyramidal et du modèle étatique ne correspond pas à une progression, mais à une régression. Il remet en cause l'existence même des acteurs, ne permettant plus de les identifier, et l'existence même du droit, ne permettant plus d'en cerner la validité. Dès lors, par ce dépassement, on peut difficilement étudier le droit en général et définir le concept juridique de souveraineté numérique, en particulier. Cela suffit-il à en remettre en cause l'existence ?

2. Les subtilités d'un concept bidimensionnel

Le concept de souveraineté numérique, juridiquement entendu, peut être perçu dans deux dimensions : le numérique dans la souveraineté (1) ou la souveraineté dans le numérique (2).

a. Le numérique dans la souveraineté

Le numérique peut constituer un instrument d'exercice de la souveraineté, en étant alors une forme de prolongement de la démocratie, voire un moyen de l'exercer. En effet, il est venu au renfort de révolutions, que l'on a alors qualifiées de « révolutions 2.0 »[16] : il fut ainsi un vecteur de souveraineté. Il s'agit même de la souveraineté à l'état pur : le constituant

16. Sur ce sujet, en lien avec la souveraineté numérique, cf. P. Türk, « La souveraineté de l'État à l'épreuve d'internet », préc.

au sens propre du terme, c'est-à-dire celui qui établit la (première ou nouvelle) constitution intervient en dehors de tout État puisqu'il veut faire la révolution, renverser l'État pour en ériger un nouveau.

De même, il peut intervenir dans l'exercice de la démocratie, par des moyens de vote électronique, d'intervention législative grâce au numérique, au contrôle du pouvoir grâce à Internet[17]. Le numérique permet une participation citoyenne, à travers des pétitions citoyennes récoltées sur Internet et, plus généralement, un rapprochement entre le peuple, les institutions et les élus qui les composent. Les sites des institutions politiques constituent une plateforme de leur communication. Il est ainsi possible de visualiser la séance publique (de l'Assemblée nationale et du Sénat) en direct, d'avoir accès au compte rendu des débats quelques heures après leur tenue, de lire les décisions du Conseil constitutionnel ou du Conseil d'État sans attendre qu'un compte rendu en soit dressé dans la presse. L'accès à l'ensemble du droit, des débats publics et politiques devient direct et immédiat. Ceci vient indéniablement au renfort de la démocratie en rapprochant l'électeur de son élu et réciproquement : le citoyen-spectateur *de* la vie publique se transforme peu à peu en en citoyen-acteur *dans* la vie publique, pouvant librement s'exprimer, dire ce qu'il pense d'une action de son élu et de son action en général.

Parallèlement, de nouveaux mécanismes institutionnels viennent renforcer cela. D'une part, l'Assemblée nationale a mis en place, sur son site Internet, une possibilité de réagir aux études d'impact des projets de loi qui lui sont soumis en premier lieu. Cette possibilité est consacrée par les textes, résultant de l'article 83, al. 2 RAN selon lequel « *les documents qui rendent compte de l'étude d'impact réalisée sur un projet de loi soumis en premier lieu à l'Assemblée […] sont mis à disposition par voie électronique, afin de recueillir toutes les observations qui peuvent être formulées* ». Accessible à tous depuis Internet, il n'est pas besoin d'être électeur, national, concerné

17. Sur ce sujet, on renvoie aux travaux du colloque qui s'est tenu à Toulon, le 10 novembre 2016, sur *La démocratie connectée : ambitions, enjeux, réalité* (dans le même cadre des journées décentralisées de l'AFDC) et dont les travaux seront prochainement publiés. On peut mentionner, brièvement, les divers sites institutionnels qui référencent des données renforçant la transparence (publication sur le site des assemblées de la réserve parlementaire, du nom des collaborateurs, etc., publication sur le site de la HATVP) et les sites issus d'initiatives privées et citoyennes.

par la loi et son impact pour pouvoir déposer une contribution, ce que l'on peut faire depuis n'importe quel appareil connecté n'importe où dans le monde[18] : le numérique, dans sa mise en œuvre, dépasse effectivement les frontières. De même, le recueil des soutiens citoyens à une proposition de loi déposée par un cinquième des parlementaires, sur le fondement de l'article 11 de la Constitution, en vue de l'organisation d'un *referendum*, se fait « sous forme électronique », selon l'article 5 de la loi organique prise pour l'application dudit article[19].

D'autre part, certains textes ont pu faire l'objet d'une consultation directe lors de leur préparation : il ne s'agit plus, alors, de la seule étude d'impact, mais bien du texte lui-même, son auteur (le Gouvernement ou un parlementaire) s'engageant à tenir compte des avis récoltés. Ce fut d'abord le cas pour la proposition de loi créant de nouveaux droits en faveur des malades et des personnes en fin de vie[20]. Le Gouvernement a également procédé à de telles consultations, à deux reprises, sur le projet de loi pour une République numérique et celui sur Égalité et citoyenneté. Deux sites Internet leur ont été respectivement dédiés, permettant de recueillir plus de 8 500 contributions et près de 150 000 votes sur le premier, avant que le projet de loi ne soit déposé à l'Assemblée nationale, ce qui a permis de l'enrichir « d'une partie des remarques provenant des différents contributeurs que le Gouvernement a jugée utile de prendre en

18. Ce n'est là qu'une supposition : à regret, l'auteur de ces lignes n'a pas sillonné l'ensemble des chemins de la planète pour s'assurer de la véracité de cette hypothèse…
19. Loi organique n° 2013-1114 du 6 décembre 2013 portant application de l'article 11 de la Constitution, *JORF* du 7 décembre 2013 page 19937.
20. Déposée par les députés A. Claeys et J. Leonetti, elle est devenue la loi n° 2016-87 du 2 février 2016 créant de nouveaux droits en faveur des malades et des personnes en fin de vie, *JORF* du 3 février 2016. Ouverte du 2 au 16 février 2015 sur le site de l'Assemblée nationale, la consultation semble avoir été un succès au regard du nombre de contributions recueillies (11 922). Toutefois, on peut constater que de très nombreuses d'entre elles sont similaires et on suppose qu'elles ont été orchestrées par des associations militantes soutenant ou, au contraire, s'opposant à ces nouveaux droits, pour le moins polémiques au sein de l'opinion publique. De plus, les parlementaires à l'initiative de cette proposition de loi étant eux-mêmes à ce point impliqués dans le sujet depuis de nombreuses années, on doute que leurs positions, déjà bien arrêtées, puissent être altérées par de nouvelles contributions.

compte »[21]. Le système était différent quant au second : la consultation a été ouverte après son dépôt à l'Assemblée nationale et pendant que les rapporteurs procédaient à son examen. L'objectif était de « nourrir le débat parlementaire », étant précisé que « les élus restent souverains et prennent leurs décisions en toute autonomie »[22]. L'utilité en termes de communication fut indéniable, mais, en termes d'impact sur la production législative, elle est bien plus questionnable… mais était-ce là son objectif ? Point trop n'en faut…

Le numérique devient ici un prolongement et un exercice de la souveraineté.

b. La souveraineté dans le numérique

La souveraineté numérique peut également signifier – peut-être même davantage – un contrôle dans et sur le numérique. Que faut-il alors entendre par « contrôle » ? Il peut avoir deux significations.

Ce peut être soit un contrôle signifiant domination, nationale ou supranationale. Et il ne peut alors y avoir qu'une seule entité souveraine, du moins à son propre égard, co-existant, le cas échéant, avec d'autres entités souveraines. Cependant, même cela, c'est difficile car la pluralité de souveraineté ne permet pas une domination et un contrôle total. C'est ce que soulignait Kelsen qui, lui-même, détruisait le concept de souveraineté, en soutenant qu'en droit, il ne pouvait être pensé car c'était la domination d'un État sur tous les autres[23]. En l'espèce, cela conduit, *a minima*, à une fermeture des réseaux, à l'instar de la Chine, à travers des protocoles de chiffrement numérique nationaux. Et ce n'est pas sans porter atteinte aux « droits et libertés que la République protège » (en référence à l'article 29

21. Projet de loi pour une République numérique, Assemblée nationale, n° 3318, enregistré le 9 décembre 2015, extrait de l'exposé des motifs, p. 4.
22. Extrait du site « Égalité et citoyenneté. Le projet de loi », https://www.egalite-citoyennete-participez.gouv.fr, consulté le 13 juillet 2016.
23. H. Kelsen, « Les rapports de système entre le droit interne et le droit international public », in *RCADI* n° 14 (1926-IV), pp. 227 à 331 et, du même auteur, *Das Problem der Souveränität und die Theorie des Völkerrechts. Beitrag zu einer reinen Rechtslehre*, Mohr, Tübingen, 1920.

SCIENCES PO, Chaire digital, Governance and Sovereignty

[ENTRETIEN] QUELS SONT LES MODÈLES DE MISE EN ŒUVRE DE LA SOUVERAINETÉ NUMÉRIQUE ? PAR SAMUELE FRATINI

11 juin 2024

©tete_escape

Propos recueillis par Luca Lefevre

Quelles sont les différences fondamentales entre la souveraineté en général et la souveraineté numérique ?

Le concept traditionnel de souveraineté est très différent de la manière dont il est utilisé dans les domaines de la gouvernance numérique. La souveraineté traditionnelle est une caractéristique des États internationalement reconnus qui exercent une autorité suprême sur un territoire, tandis que la souveraineté numérique est une stratégie efficace visant à étendre l'autorité de l'État sur les infrastructures numériques dans un contexte mondial. La souveraineté numérique est davantage une stratégie qu'un pouvoir entièrement détenu par un État.

Si l'on considère que la souveraineté est l'autorité suprême de l'État sur son territoire, la première distinction est que l'espace numérique n'est pas un territoire réel mais une infrastructure mondiale. Pourtant, il est de plus en plus souvent décrit comme un espace ou un territoire afin de le rendre accessible au contrôle de l'État. Deuxièmement, les États-nations ne sont pas l'autorité suprême sur l'infrastructure numérique. Dans la grande majorité des cas, notamment dans

l'Union européenne, en Russie et en Chine, la souveraineté numérique a été proposée comme une sorte de stratégie défensive visant à accroître l'autorité de l'État sur les infrastructures numériques et en particulier sur les technologies numériques étrangères, c'est-à-dire les technologies américaines.

Enfin, la souveraineté numérique est liée à la concurrence géopolitique ; la poursuite de la souveraineté numérique ne peut être dissociée de l'équilibre des pouvoirs existant dans le monde. Elle s'inscrit dans un moment de démondialisation, où les dynamiques existantes sont de plus en plus contestées dans tous les secteurs, et où le secteur numérique ne fait pas de différence.

Quelle est la différence entre la définition de la souveraineté numérique en Europe et en Russie ou en Chine ?
Il s'agit de modèles extrêmement différents, mais qui ont un point commun : ils sont apparus comme une stratégie défensive face à une hégémonie américaine perçue dans le secteur technologique. Ils sont apparus à des périodes différentes en appliquant des solutions différentes, mais ils sont tous liés par la nécessité perçue d'être plus autonome face aux États-Unis. C'est vrai à différents niveaux mais, à mon avis, il s'agit d'un trait commun.

Hormis ce point, elles relèvent toutes de modèles différents de souveraineté numérique. La première caractéristique est que ces trois entités politiques ont commencé à poursuivre la souveraineté numérique en mobilisant des étiquettes différentes. Elles parlent, par exemple, de « souveraineté technologique » ou de « souveraineté Internet » à trois moments historiques différents. L'Union européenne et la Russie ont commencé à parler de souveraineté numérique au début des années 2010, tandis que la Chine a commencé à le faire à la fin des années 90.

L'expansion de l'Internet et du World Wide Web en Chine a été considérée dès le départ comme une sorte de problème de sécurité nationale. Cela s'explique en partie par un modèle de souveraineté différent : en Chine, la frontière entre les entreprises privées et les autorités publiques n'est pas aussi nette qu'en Europe, par exemple. Il s'agit d'une différence essentielle, car la stratégie de souveraineté numérique en Chine n'est pas caractérisée par la nécessité pour l'État de réaffirmer son contrôle sur l'infrastructure numérique, parce que le cyberespace n'a jamais été imaginé comme apatride en Chine. Il a toujours été guidé et orienté par le parti communiste chinois. La souveraineté numérique était davantage orientée vers l'arène internationale, car elle était considérée comme une question de sécurité nationale et, comme la Chine se considérait comme une sorte de puissance anticolonialiste, elle a manifesté le besoin d'être souveraine, en particulier face à l'expansion de la technologie américaine et des valeurs américaines qui y sont liées. À partir de la fin des années 90, nous avons pu observer une constellation d'initiatives telles que le Great Firewall ou le soutien au multilatéralisme dans les organismes internationaux, qui caractérisent l'approche chinoise de la gouvernance numérique en tant que question territoriale.

Certaines caractéristiques du modèle chinois ont été partiellement intégrées dans le modèle russe, mais nous avons généralement tendance à oublier que l'approche russe de l'internet était assez libérale jusqu'au début des années 2010. En 2010, ils ont proposé le terme « Internet souverain », ce qui signifie que l'Internet et le cyberespace, en général, sont de plus en plus considérés comme une sorte de champ de bataille. Ils ont commencé à suivre trois directions :

1. Un filtrage rigoureux des contenus, à la fois par un filtrage direct sur les plateformes numériques, en particulier les plateformes nationales russes, et par l'exclusion directe des opérateurs étrangers.

2. Exigences strictes en matière de localisation des données. Les entreprises étrangères sont obligées de stocker une grande partie de leurs données en Russie et de les remettre aux autorités russes si elles en font la demande.

3. La Russie s'est également engagée dans une campagne continue de désinformation dans de nombreux pays occidentaux – le cas américain est le plus connu, mais ce n'est pas le seul, et ceci est particulièrement intéressant et important avant les élections européennes.

Ces trois trajectoires ont été de plus en plus cristallisées dans un ensemble de lois établies. Par exemple, la « loi Yarovaya[1] » et d'autres lois ont mis cette stratégie en pratique. Il s'agit donc plus ou moins de la stratégie russe.
Dans le cas de l'Union européenne, les débats ont également commencé au début des années 2010, mais au niveau national. Un exemple remarquable est celui de la France où, en 2012, la souveraineté numérique était déjà un sujet, en particulier avec des personnalités comme Bellanger[2] et d'autres qui ont commencé à parler de la mise en œuvre de la souveraineté numérique comme une sorte de tentative d'émancipation de l'Europe par rapport à l'Amérique. Il y a également eu une sorte de débat en Allemagne, mais il était davantage lié à une marque de droite radicale et non à une stratégie nationale accueillie par l'ensemble du spectre politique. Le véritable tournant a été les révélations de Snowden. Par exemple, en termes de gouvernance de l'internet, nous considérons qu'il existe une « gouvernance de l'internet post-Snowden » parce que l'Europe a commencé à comprendre comment ces technologies ont été militarisées par les États-Unis. Ensuite, la souveraineté numérique a été de plus en plus décrite comme la capacité de l'Europe à agir librement et de manière autonome dans l'espace numérique, et c'est devenu l'objectif derrière un grand nombre de politiques européennes telles que le GDPR ou aussi la loi la plus récente sur l'IA. Il existe aujourd'hui une véritable volonté d'être libre de choisir son propre destin dans l'espace numérique. Par conséquent, la souveraineté numérique devient une composante stratégique d'une grande politique européenne plus large, à savoir l'autonomie stratégique.
Quel rôle joue le cloud souverain dans la détermination de la souveraineté numérique ?
Le cas de la Russie est l'un des exemples les plus évidents, mais ces tentatives prennent des formes différentes dans le monde entier. Je n'ai peut-être pas mentionné que la souveraineté était composée de différents éléments. La trajectoire est, bien sûr, d'être libre d'agir dans l'espace numérique, mais cet objectif est atteint grâce à plusieurs composantes.

Par exemple, l'idée de pouvoir développer sa propre technologie est appelée souveraineté technologique. Un autre exemple est la possibilité de disposer d'une main-d'œuvre qualifiée pour gérer la technologie, ce que l'on appelle la souveraineté en matière de compétences. L'une de ces composantes est la souveraineté en matière de données, c'est-à-dire la capacité d'un État-nation à exercer son contrôle sur la manière dont les données sont collectées, stockées et utilisées tout au long du cycle de vie du flux de données.

Pour y parvenir, certaines entités politiques, en particulier la Russie, la Chine et l'Union européenne, ont commencé à recourir à des structures de gouvernance traditionnelles pour exercer leur contrôle. Cette structure de gouvernance traditionnelle est la juridiction de l'État. L'idée inhérente est que si vous pouvez prendre ces données et les stocker dans votre juridiction, vos lois s'appliqueront à ces données, vous permettant ainsi d'échapper à d'autres juridictions menaçantes.

Cependant, il est important de ne pas limiter et réduire la capacité à exercer un contrôle sur les flux de données à la seule dimension territoriale. Par exemple, les États-Unis exercent un degré élevé de souveraineté sur les données sans recourir à la juridiction territoriale. En 2018, ils ont introduit le USA CLOUD Act, qui permet aux autorités étatiques d'accéder à des bases de

données privées en cas d'urgence nationale. En fait, ils militarisent leurs entreprises, et le contrôle des données passe par des circuits privés plutôt que par le territoire.
Ainsi, bien que le cloud souverain soit important, il ne constitue pas un bouclier total contre toutes les menaces, ni le seul moyen d'exercer un contrôle sur les données. La souveraineté des données n'est pas séparée des autres composantes de la souveraineté numérique. Elle peut également révéler les faiblesses de l'État. Par exemple, le projet GAIA-X de l'Union européenne, qui vise à développer un cloud souverain, témoigne d'un manque de clarté stratégique. Dans un premier temps, la réponse semblait être qu'un cloud souverain ne devait être entretenu que par des entreprises européennes, Amazon étant exclu. Cependant, par la suite, la filiale européenne d'Amazon a été réincorporée, ce qui rend le concept de souveraineté flou.

Cette situation est également liée à la capacité de développer ses propres infrastructures numériques et à la vulnérabilité au lobbying. En Suisse, en 2022, les autorités fédérales ont tenté d'établir un cloud souverain pour l'administration publique, qui a finalement été confié, en 2023, à cinq entreprises étrangères, quatre américaines et une chinoise. Cela montre que malgré les meilleures intentions, de telles tentatives sont soumises à la capacité réelle de développer l'infrastructure et à l'influence du lobbying étranger.

La question importante est donc la suivante : que peut-on attendre de la souveraineté des États en ce qui concerne les grandes entreprises ? Une solution peut-elle être trouvée en soutenant les entreprises locales plutôt qu'en luttant contre les entreprises américaines et chinoises ? Du côté européen, il s'agit d'une distinction cruciale. D'autres superpuissances comme la Chine et les Etats-Unis ont suivi la stratégie de développement de leurs propres entreprises nationales. Toutefois, dans l'Union européenne, certaines observations doivent être prises en compte.

On observe une sorte de double mouvement dans la relation entre les États et les entreprises. D'une part, on assiste à une exclusion croissante des entreprises liées à des États perçus comme des menaces, comme l'affaire TikTok aux États-Unis et partiellement dans l'UE, ou l'interdiction des entreprises occidentales en Chine et en Russie. D'autre part, les États tentent de plus en plus d'exercer un contrôle sur les entreprises nationales. La répression chinoise contre les grandes entreprises technologiques est un cas célèbre où l'État a tenté de renforcer son contrôle sur les entreprises, causant des dommages économiques.

Aux États-Unis, sous les administrations Trump et Biden, des auditions du Congrès ont demandé aux PDG des grandes entreprises technologiques si leur travail était fonctionnel pour les intérêts américains. Ce double mouvement s'explique par le fait que les entreprises mondialisées doivent répondre à différents pays, ce qui fait qu'elles ne sont que partiellement nationales. Les entreprises chinoises, par exemple, doivent se conformer à la fois aux exigences chinoises et internationales.

En ce qui concerne l'Europe, un secteur privé plus puissant avec des champions nationaux pourrait promouvoir les intérêts européens et exporter des normes européennes. Toutefois, le marché unique européen se heurte à des obstacles qui empêchent une intégration complète, ce qui empêche les entreprises nationales de se développer et d'alimenter l'innovation. L'effet Bruxelles a permis à l'UE d'exporter ses normes dans le monde entier parce que les entreprises américaines opérant en Europe ont adopté ces normes. Par conséquent, s'il est essentiel de développer un secteur numérique national avec des champions nationaux, il convient de peser soigneusement les risques d'exclusion des opérateurs américains, car cela pourrait compromettre le succès des normes européennes à l'échelle mondiale.

Que peut-on attendre de la souveraineté des Etats face aux grandes entreprises ? La solution peut-elle être trouvée dans le soutien aux entreprises locales plutôt que dans la lutte contre les

entreprises américaines et chinoises ? Si les entreprises sont nationales (notamment aux Etats-Unis), quelles sont les raisons de ne pas favoriser l'autorégulation pour atteindre la souveraineté numérique ?

Nous avons l'habitude de penser qu'une entreprise est née dans un certain pays, qu'elle y a son siège et que ses intérêts sont alignés sur ceux du pays. Le premier point est que ce n'est pas tout à fait exact.

Le deuxième point est que le degré de pénétration des technologies numériques dans notre vie quotidienne s'est accru au fil du temps. Cela signifie que les grandes entreprises numériques ont désormais non seulement des obligations commerciales, mais aussi des obligations sociales et politiques. La Chine et les États-Unis sont tous deux préoccupés par le degré d'indépendance de leur secteur privé et tentent, de différentes manières, de rétablir leur contrôle sur ces entreprises.

C'est ce qui distingue le moment actuel de la période initiale d'expansion des technologies numériques. Nous sommes aujourd'hui dans un moment de régulation parce que les technologies numériques se sont déjà répandues et ont pénétré notre vie quotidienne. Il existe une sorte de consensus non écrit selon lequel nous nous dirigeons vers une réglementation plus stricte.

N'est-il pas paradoxal de lutter à la fois pour la souveraineté numérique à l'échelle mondiale et d'assister à un retour de la régulation ?
C'est logique, mais comme la réglementation, par définition, n'est pas neutre, certains pays ont essayé d'imposer et d'exporter leurs normes. En conséquence, d'autres États ressentent le besoin de contrer ces normes étrangères par leurs propres réglementations nationales. Cette dynamique signifie que la réglementation engendre souvent d'autres réglementations.

Un modèle basé sur l'État, s'il était européen et incluait donc le respect des droits fondamentaux, ne serait-il pas la solution optimale pour l'UE ?
Plusieurs observations peuvent être faites sur ce point. La première est que les modèles que nous avons proposés (*ndlr dans l'article*) sont, par définition, mutuellement exclusifs. Ils peuvent avoir des caractéristiques communes, mais ils se rapportent à des dimensions différentes.
Par exemple, la première distinction est que l'Union européenne n'est pas un véritable État. Concrètement, cela signifie que l'Union européenne ne peut pas centraliser la gouvernance numérique comme le fait la Chine sans porter atteinte à la concurrence économique interne ou à d'autres domaines. La première observation porte donc sur la structure même de l'Union européenne.

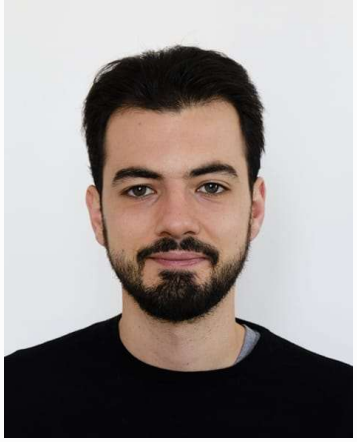
La deuxième observation est que l'Union européenne dispose d'un vaste marché intérieur unique, mais qu'il n'est que partiellement intégré en raison de barrières culturelles, linguistiques et juridiques. Il n'est même pas aussi grand que le marché chinois. La Chine, modèle étatique par excellence, dispose d'un vaste marché intérieur qui lui permet de développer ses propres entreprises en interne, puis de les exporter à l'échelle mondiale. Un degré élevé de centralisation de la gouvernance numérique dans l'Union européenne entraverait considérablement ce processus.

Le dernier constat est que l'Union européenne se différencie en défendant les droits fondamentaux dans l'espace numérique. Une solution basée sur l'État ne serait pas compatible avec le modèle de gouvernance multipartite, qui est appliqué différemment dans le monde. Si la gouvernance est trop centralisée entre les mains de l'État, les intérêts et les compétences d'autres secteurs, tels que le secteur privé, le monde universitaire et les experts techniques, seront plus facilement négligés. Par conséquent, l'Union européenne devrait continuer à promouvoir ses propres intérêts souverains dans l'espace numérique tout en restant démocratiquement représentative de chaque groupe sociétal touché par la numérisation.

Dernier point, l'Union européenne est dans un processus d'intégration continue. L'intégration progresse face à des défis globaux comme la pandémie ou la transition numérique. Ces défis et d'autres défis connexes, comme celui de l'environnement, exigent que l'Union européenne fasse progresser son identité, non seulement pour orienter sa stratégie, mais aussi pour construire cette identité. Si l'Union européenne cessait de développer son propre modèle de gouvernance numérique, qui est le modèle fondé sur les droits fondamentaux, elle capitulerait devant d'autres États-nations établis comme la Chine et les États-Unis. Par conséquent, puisqu'il s'agit d'une question d'intégration européenne, l'Union européenne devrait promouvoir son propre modèle.

---

[1] Les lois yaroyava sont un ensemble de textes fédéraux adoptés en Russie en 2016. L'objectif déclaré est de renforcer les capacités de l'État dans la lutte contre le terrorisme. Ces lois permettent notamment au service de sécurité intérieure FSB d'accéder aux données des messageries en ligne, y compris les données cryptées.
[2] Voir par exemple : Bellanger, Pierre. » De la souveraineté numérique « , *Le Débat*, vol. 170, no. 3, 2012, pp. 149-159.



Samuele Fratini *est doctorant en sciences sociales au département des communications, des interactions et des constructions culturelles de l'université de Padoue et à l'institut des médias et du journalisme de l'université de la Suisse italienne de Lugano. Il a publié un article avec Emmie Hine, Claudio Novelli, Huw Roberts et Luciano Floridi intitulé « Digital Sovereignty : A Descriptive Analysis and a Critical Evaluation of Existing Models« , qui propose une classification en quatre modèles de mise en œuvre de la souveraineté numérique.*

Les formes imparfaites de la souveraineté numérique

Thierry Ménissier

Les formes imparfaites de la souveraineté numérique

Thierry Ménissier

Conférence dans le cadre du séminaire « Société & souveraineté », IPhiG & PACTE, UGA, Grenoble, 11 décembre 2020 ; texte à paraître dans un volume collectif dirigé par Thomas Boccon-Gibod & Alban Mathieu.

Résumé :

Dans cette contribution, nous confrontons la notion philosophique et politique de souveraineté à la réalité des technologies numériques. En apparence, telle qu'elle est héritée de son histoire en Europe, cette notion ne peut ni décrire adéquatement ni encadrer normativement les réalités de la socialité et de l'économie numériques. Pourtant, de nombreux acteurs semblent vouloir la conserver, faute de pouvoir réinventer une notion valable sur les plans descriptif et normatif. Nous proposons d'admettre l'hypothèse que, pensée d'après son origine intellectuelle dans la tradition de philosophie politique moderne, la souveraineté se dit en plusieurs sens. Elle n'est pas seulement "institutionnelle", mais également "populaire" et "nationale". Comment apparaissent les réalités du pouvoir social numérique (les communautés d'usagers) et les relations géopolitiques de l'économie numérique à la lumière de ces différentes acceptions de la notion de souveraineté ?

Mots-clés : souveraineté, Etat, nation, peuple, pouvoir constituant, numérique.

Abstract:

In this contribution, we confront the philosophical and political notion of sovereignty with the reality of digital technologies. On the face of it, as inherited from its history in Europe, this notion can neither adequately describe nor normatively frame the realities of sociality and the digital economy. However, many actors seem to want to keep it, because they cannot reinvent a notion that is both descriptive and normative. We propose to admit the hypothesis that, thought according to its intellectual origin in the tradition of modern political philosophy, sovereignty is said in several senses. It is not only "institutional", but also "popular" and "national". How do the realities of digital social power (user communities) and the geopolitical relations of the digital economy appear in the light of these different meanings of the notion of sovereignty?

Keywords: sovereignty, state, nation, people, constituent power, digital.

***

Dans cette contribution[1], nous souhaitons poursuivre notre réflexion en philosophie politique sur la relation entre l'action des nouvelles technologies sur l'activité sociale-humaine et les concepts hérités de la modernité[2]. La souveraineté représente un de ces concepts, et fait même partie des plus importants. Souvent, on estime de manière spontanée que la notion héritée

[1] Cet article est le fruit du travail scientifique qui est mené dans le cadre de la chaire « éthique & IA » soutenue par l'institut pluridisciplinaire en intelligence artificielle MIAI@Grenoble Alpes (ANR-19-P3IA-0003).

[2] Voir Thierry Ménissier, *La Liberté des contemporains. Pourquoi il faut rénover la République*, Grenoble, PUG, 2011 ; *Innovations. Une enquête philosophique*, Paris, Hermann, 2021.

de souveraineté ne correspond plus aux réalités technologiques et économiques contemporaines, notamment celle du numérique, de l'IA et de la *data*. Ce jugement n'est pas entièrement faux puisque par exemple, dans leur fonctionnement social habituel, ces technologies se déploient dans un espace qui, à la fois, ignore les frontières territoriales et excède les régulations nationales. A certains égards, l'économie globalisée dans laquelle se déploient les technologies innovantes a rendu obsolète l'idée héritée de souveraineté. Mais une telle position apparaît évidemment insuffisante du fait que derrière les relations des promoteurs de l'innovation – dont certains sont d'ailleurs publics : institutions directement étatiques ou entreprises patriotiquement affiliées à leur nation d'origine – se jouent des rapports de force qui s'inscrivent dans le cadre des thématiques qui furent autrefois pensées à partir de l'essor de la souveraineté nationale : lutte des acteurs pour la conquête de territoires jusqu'à la volonté hégémonique, concurrence internationale dans les investissements d'innovation, cyber-conflictualité ou cybercriminalité parfois clairement commanditée par des États souverains belliqueux. De plus, et de manière paradoxale, parmi ces acteurs, certains sont de bons connaisseurs de la réalité techno-économique contemporaine et revendiquent de pouvoir conserver le concept de souveraineté nationale ou européenne en l'associant aux adjectifs « numériques » et « digital », ce qui implique l'éventualité de le repenser partiellement.

Devant une telle situation, nous concevons notre contribution sur un double plan : d'une part, préciser ce qu'il est possible de conserver du concept hérité de souveraineté, de l'autre, déterminer dans quelle mesure les nouvelles technologies pourraient permettent de le réinventer. Afin de traiter les deux séries de questions qui émergent alors, nous voulons plus particulièrement approfondir un point particulier que l'on peut formuler ainsi : *la souveraineté se dit en plusieurs sens*. Elle n'est en effet pas seulement « institutionnelle », permettant la construction et la préservation de l'institution publique, mais elle est également « nationale » et « populaire ». Que signifient ces dimensions dans le monde numérique ? Que permettrait de penser l'idée d'une « souveraineté nationale et populaire numérique » ? Et qu'est-ce que cet angle de vue apporte à l'évolution de la notion de souveraineté en tant que principe fondamental de l'agir politique ?

La définition institutionnelle de la souveraineté

La notion de souveraineté, appréhendée de manière spontanée, paraît renvoyer à l'autorité de l'État et à la légitimité de l'Administration, à savoir, au pouvoir constituant de la politique dans sa version moderne, et à un des tout premiers pouvoirs constitués. C'est en fonction de cette double dimension étatique et administrative que la notion de souveraineté évoque la

dimension institutionnelle. Or, si ce qui apparaît spontanément évident n'est pas totalement erroné, c'est que cette dimension fait appel à une référence fondatrice de la théorie politique moderne : le concept de souveraineté désigne le pouvoir suprême de faire les lois de manière inconditionnelle, tel que Jean Bodin, juriste-philosophe angevin, l'a formulé dans le contexte socio-politique particulièrement chaotique et violent des guerres civiles (dites « guerres de religion ») qui déchirèrent le royaume de France au XVI^{ème} siècle, avant d'embraser l'Europe entière[3]. Bodin publie *Les Six livres de la République* quatre ans après le massacre de masse de la Saint-Barthélemy. Sa définition de la souveraineté est fameuse : elle est « la puissance absolue et perpétuelle d'une république »[4]. Ce qui signifie que peut être considérée comme souveraine la société politique qui choisit ses propres lois sans qu'on les lui impose, et qui, à partir de cette primauté, se trouve capable de structurer son espace propre. Formuler un ordre juridique et coercitif incontestable, où force reste toujours à la puissance publique, telle fut la solution proposée par Bodin pour sortir du chaos et de la violence.

Par suite, les caractères classiques de la souveraineté ainsi entendue sont la *toute-puissance* (le droit de mettre légitimement hors d'état de nuire les opposants) et la *perpétuité* (le fait qu'il n'y ait, sur un plan de principe, pas de terme temporel à l'existence de l'ordre qui se revendique souverain)[5]. *Mutatis mutandis*, ces caractères principaux du concept ont été validés et développés par Hobbes puis par Rousseau, à savoir par les concepteurs de l'institution républicaine moderne : tout au long de la pensée politique moderne, un véritable travail de *domestication* du premier concept de souveraineté inventé par Bodin (soit la version absolutiste de la souveraineté) a été opéré dans le sens républicain, afin de le rendre capable de porter et de garantir des libertés publiques dans le cadre de l'État de droit (soit la version de plus en plus démocratique de la souveraineté)[6]. L'histoire de la pensée politique moderne et contemporaine se confond avec un dialogue soutenu avec le concept bodinien de souveraineté, qui fut certes critiqué par les penseurs libéraux (Locke, Constant), mais au final – en tout cas sur le plan de la théorie de l'État – seulement amendé ou marginalement déformé afin de faire droit à d'autres foyers de légitimité que la seule puissance étatique (à commencer par les droits de l'Homme)[7].

---

[3] Sur ce contexte, voir par exemple Nicolas Le Roux, *Guerres et paix de religion (1559-1598)*, Paris, Belin, 2014.
[4] Jean Bodin, *Les Six livres de la république* (1576), Livre I, chapitre 8, Paris, Librairie Arthème Fayard, 1986, p. 179 sq.
[5] Sur la relation entre le pouvoir absolu et la perpétuité chez Bodin, voir Julian Franklin, *Jean Bodin et la naissance de la théorie absolutiste* [1973], trad. J.-F. Spitz, Paris, PUF, 1993.
[6] Sur l'histoire conceptuelle de la notion de souveraineté, voir Gian Mario Cazzaniga & Yves Charles Zarka (dir.) ; *Penser la souveraineté à l'époque moderne et contemporaine*, Pise-Paris, Edizioni ETS et Librairie Philosophique J. Vrin, 2001, 2 volumes.
[7] Et cela, bien que dans l'histoire de la théorie politique moderne, d'autres voies existaient pour la constitution du concept de souveraineté, permettant de construire un modèle alternatif. Par exemple, la tentative de Johannes Althusius dont la *Politica methodice digesta* parue en 1603 et conçue dans un contexte historique, social et

Or, en dépit de ce travail de transformation de la notion bodinienne, entendue en fonction de son type initial, la conception moderne de la souveraineté ne peut avoir cours dans le monde des réseaux numériques. Cette conception de la souveraineté s'exprime en effet par le pouvoir administratif et coercitif des États, par la préservation d'espaces et de biens in-appropriables de manière privative, par l'exploitation juridiquement monopolistique des ressources publiques (naturelles, patrimoniales, immobilières et mobilières), enfin par la délimitation et la préservation des frontières nationales. Or, une telle idée de souveraineté ne peut plus avoir cours dans le monde numérique, notamment parce qu'elle conçue en fonction d'une représentation de l'espace issue, du point de vue géopolitique et diplomatique, des Traités de Westphalie du XVII^{ème} siècle. Dans un espace global nécessairement transfrontalier comme celui de la circulation des *data*, dominé par les GAFAM et les BATX (qui, en tant que puissances de fait, ne sont pas des institutions publiques mais des entreprises privées), l'héritage de la conception initiale de la souveraineté est très difficile à articuler à nos nouvelles réalités. Si bien que malgré des efforts considérables, lorsqu'elle est tendue vers l'objectif qui consiste à « sauver » la conception classique de la souveraineté, la meilleure volonté des plus grands experts en science de l'informatique ne parvient qu'à un résultat mitigé sur le plan descriptif et décevant sur le plan normatif[8].

Finalement, la souveraineté appréhendée de manière institutionnelle à partir de son type théorique initial ne constitue pas un canevas pertinent pour penser la régulation des plateformes numériques par la puissance publique, en tout cas de manière conceptuellement adéquate et normativement efficace. Ne serait-ce que lorsqu'on entreprend de le décrire, le pouvoir de ces entités socio-techniques capitalistes ne correspond en rien au monde issu de la pensée politique moderne : vouloir appliquer les concepts de celles-ci aux nouvelles réalités revient à les étendre sur un lit de Procuste qui en mutile les spécificités. C'est pourquoi, si l'on adopte le point de vue de ces nouvelles réalités technologiques, on est incité à inventer une autre manière de

politique totalement différent de celui que connaissait Bodin, comprend une théorie de la souveraineté intéressante et fortement divergente de la définition bodinienne. Voir à ce propos Gaëlle Demelemestre, *Les deux souverainetés et leur destin. Le tournant Althusius-Bodin*, Paris, Éditions du Cerf, 2011.

[8] Voir à cet égard le rapport proposé par la CERNA en 2018, *La Souveraineté à l'ère du numérique. Rester maîtres de nos choix et de nos valeurs*, Commission de réflexion sur l'Ethique de la Recherche en sciences et technologies du Numérique d'Allistene, téléchargeable à l'URL : https://www.allistene.fr/publication-de-la-cerna-sur-la-souverainete-a-lere-du-numerique/ , consulté le 27 mai 2021. On relève dans ce rapport la volonté de faire coïncider les nouvelles réalités technologiques et la notion classique de souveraineté avec l'idée de maîtrise d'un espace institutionnellement délimité par les prérogatives nationales de la politique des nations, dans une conception qui reconnaît l'Etat comme la puissance exclusive pour la préservation des libertés. A côté de cet effort, on remarque également des considérations philosophiquement plus fragiles relevant de l'extension démesurée de la notion de souveraineté (« souveraineté de l'individu », « souverain bien », etc.), ce qui peut aussi traduire une forme d'usure d'une idée devenant bien trop large pour qualifier adéquatement la réalité et posséder une réelle force normative.

décrire la réalité du pouvoir suprême – mais alors il convient de faire preuve de créativité et d'imagination. C'est par exemple à la lumière d'un tel constat, que Benjamin J. Bratton a proposé le concept d'« empilement » (*stack*), qui possède des origines certes métaphoriques mais qui paraît être caractérisé par une certaine valeur en termes tant descriptifs qu'heuristiques[9].

La souveraineté se dit en plusieurs sens

Toutefois, cette approche initiale doit être complétée, car, pensée d'après son acception classique, la notion de souveraineté possède deux autres acceptions qui, au fil de l'histoire politique de la théorie moderne, sont venus amender et compléter la dimension institutionnelle. D'une part, la souveraineté dite populaire renvoie à l'action du peuple, qui, *via* son consentement, exprime dans une république ou une démocratie la force authentiquement constituante[10] ; de l'autre, la souveraineté dite nationale, non moins importante, recèle quant à elle une ambiguïté indépassable. Elle fut en effet à la fois promue à l'époque de la Révolution française par un éminent promoteur du système représentatif, l'Abbé Sieyès[11], puis lors de l'affirmation des États-nations en Europe par les tenants d'une forme de pouvoir populaire, la nation étant alors entendue comme la force émergente incarnée dans un territoire, une langue et une culture[12]. Qu'elle soit appréhendée comme une communauté d'affects sensibles exprimés à travers l'attachement patriotique fondateur des révolutions modernes[13] ou comme une « communauté imaginaire » cimentant une appartenance collective fantasmée[14], la nation représente donc elle aussi un socle fondamental pour la souveraineté. Les adjectifs « national » et « populaire » qualifient ainsi l'un et l'autre le pouvoir constituant, seule source incontestable de légitimité dans un système de l'État de droit qui, de prime abord, pouvait sembler dominé par la seule dimension institutionnelle de la souveraineté.

---

[9] Benjamin H. Bratton, *Le* Stack. *Plateformes, logiciel et souveraineté* (2016), trad. Ch. Degoutin, Grenoble, UGA Éditions, 2019.

[10] Pour comprendre l'idée de souveraineté populaire, la référence à la pensée de Rousseau s'impose (en particulier : *Du Contrat social*, I, 7 : « Du souverain », qui traite de l'engagement réciproque de co-obligation des citoyens les uns envers les autres, constituant la légitimité du domaine public). Pour une mise en contexte historique de cette idée, on peut suivre les développements de Lucien Jaume, *Le Discours jacobin et la démocratie*, Paris, Fayard, 1989.

[11] Emmanuel-Joseph Sieyès, *Qu'est-ce que le Tiers-Etat ?* (1789), préface J. Tulard, Paris, PUF, 1982.

[12] Voir pour la conception « allemande » de la souveraineté de la nation en Allemagne : Johann Gottlieb Fichte, *Discours à la Nation allemande* (1807), trad. A. Renaut, Paris, Imprimerie nationale, 1992 ; et pour la conception « française », Ernest Renan, *Qu'est-ce qu'une nation ?* (1887), présentation R. Girardet, Paris, Imprimerie nationale, 1995.

[13] Voir Philippe Raynaud, *Trois Révolutions de la liberté : Angleterre, Etats-Unis, France*, Paris, PUF, 2009.

[14] Voir Benedict Anderson, *L'imaginaire national : réflexions sur l'origine et l'essor du nationalisme* (1991), trad. P.-E. Dauzat, Paris, Éditions La Découverte, 2002.

Véritable soubassement philosophique du concept de souveraineté, cette notion de pouvoir constituant renvoie, sur le plan juridique en droit public, au moment fondateur de la Constitution[15] ; sur le plan politique, elle évoque également le moment où, dans le contexte d'un vide juridique, une force collective s'empare de fait du pouvoir et ré-institue des normes (dans ce cas, la notion de pouvoir constituant est articulée par des forces révolutionnaires)[16]. Dans ce dernier cas, la notion renvoie à l'activité directe du peuple sur la création du texte constitutionnel, cette notion de peuple, au sens politique et républicain du terme, se trouvant elle-même l'héritière d'une longue histoire à la fois théorique (philosophique, juridique, politique), éthique, sociale et imaginaire[17]. Ce qui en définitive constitue, dans la théorie politique contemporaine, le ressort du pouvoir démocratique, c'est le peuple est considéré comme le véritable auteur de la constitution[18]. Bien entendu, ce principe fondamental représente quelque chose de très délicat à réaliser dans les faits, particulièrement dans le contexte de la mosaïque européenne[19].

Dégager de tels éléments conceptuels permet-il d'élargir suffisamment la notion de souveraineté, au point de lui faire correspondre les nouvelles réalités technologiques ? Jusqu'où alors est-il possible de développer l'analogie entre la souveraineté politique et la « souveraineté numérique » ? Cette dernière expression permet-elle réellement de penser l'autonomie populaire et nationale entendue comme authentique pouvoir constituant ? Si tel n'est pas le cas, de quelle nature spécifique pourrait être le pouvoir constituant d'un « peuple numérique » ? Ou bien, faut-il tenir pour un fait avéré que l'apparition des GAFAM et BATX met radicalement et définitivement à mal les notions cardinales de nation et de peuple (au sens politique du terme), et par conséquent profondément rend profondément caduque celle de souveraineté nationale ?

La réalité sociale ou populaire du numérique, impossible pouvoir constituant

[15] Claude Klein, *Théorie et pratique du pouvoir constituant*, Paris, PUF, 1996.
[16] Antonio Negri, *Le pouvoir constituant. Essai sur les alternatives de la modernité*, Paris, PUF, 1997.
[17] Voir à ce propos, et parmi une imposante bibliographie, les contributions suivantes : Etienne Balibar, « Ce qui fait qu'un peuple est un peuple. Rousseau et Kant », *Revue de synthèse*, n° 3-4, juillet-décembre 1989, p. 391-417 ; Bruno Bernardi, *Qu'est-ce qu'une décision politique* ?, Paris, Librairie Philosophique J. Vrin, 2003 ; Philippe Crignon, « Représentation et communauté. Sur Thomas Hobbes », *Archives de Philosophie*, 2005/3, tome 68, p. 493-524 ; Déborah Cohen, *La nature du peuple. Les formes de l'imaginaire social (XVIII^e^-XXI^e^ siècle)*, Seyssel, Champ Vallon, 2010 ; Catherine Colliot-Thélène, *La Démocratie sans* demos, Paris, PUF, 2011 ; Louis Carré, « Populace, multitude, *populus*. Figures du peuple dans la Philosophie du droit de Hegel », *Tumultes*, 2013/1 n° 40, p. 89-107.
[18] Voir Pasquale Pasquino, « Constitution et pouvoir constituant : le double corps du peuple », in Pierre-Yves Quiviger, Vincent Denis & Jean Salem (dir)., *Figures de Sieyès*, Paris, Publications de la Sorbonne, p. 13-23.
[19] Voir Stéphane Pinon, « La participation populaire directe au pouvoir constituant. Regards sur le droit étranger », *Revue interdisciplinaire d'études juridiques*, 2017/1 Volume 78, p. 3-35.

Le problème est que la théorie classique du pouvoir constituant, telle que la doctrine de droit public l'a conçue, repose d'une part sur une notion d'autonomie inspirée par les philosophes classiques (Spinoza, Grotius, Locke et Montesquieu entre autres) et de l'autre sur les expériences du pouvoir constituant (théorisées par les Pères Fondateurs états-uniens puis par les Constituants français). Or, dans les deux cas, le soubassement concret du concept repose sur des formes sociales d'expression et sur des pratiques matérielles qui ne sont pas celles du pouvoir numérique d'aujourd'hui. Pour le moment, et telles qu'on peut les observer, ces dernières ne permettent pas une autonomie de ce genre.

Les particularités culturelles, sociales et économiques du nouveau monde technologique sont en effet très différentes de celles typiques de l'histoire politique constitutive de la notion de souveraineté. D'abord, sur un plan culturel, « l'utopie numérique » s'est constituée en regard d'une critique de la bureaucratie étatique et en fonction de l'hypothèse de la puissance émancipatrice du marché[20]. Ensuite, sur le plan des revendications politiques, à l'origine d'internet, l'imaginaire de la libre circulation de l'information, développée par exemple par John Perry Barlow dans le contexte de la culture hippy, a ouvert la voie à une posture libertaire et libertarienne érigeant la communauté des usagers contre le droit des États-nations, ainsi qu'on peut le lire dans la *Déclaration d'indépendance du cyberespace*[21]. Du point de vue de ce texte-symptôme, la revendication de l'extraterritorialité de l'espace numérique apparaît fondamentale, notamment dans la mesure où l'auteur vante une sorte d'autorégulation de la société selon l'éthique de la réciprocité avec les libres contributions de chacun.

De ce fait, la notion d'une souveraineté numérique a représenté dès le début d'internet un pur et simple oxymore, puisque ses concepteurs y ont vu un espace de partages et d'intérêt nouvelle formule, dans une vision à propos de laquelle, malgré le recul historique d'aujourd'hui, on n'arrive pas à savoir si elle est plutôt emprunte de naïveté, radicalement audacieuse, ou agressivement libertarienne. Dans le même temps, sur le plan économique, des acteurs nouveaux y ont vu une opportunité de produire de la valeur marchande. Les entreprises qu'on n'appelait pas encore GAFAM ont su, dès les années 1990, nourrir et stimuler le goût des consommateurs de biens technologiques et de services numériques, et par suite s'approprier le marché des données personnelles en inventant des régimes d'affaire originaux et lucratifs, en

[20] Voir par exemple Patrice Flichy, *L'imaginaire d'Internet*, Paris, La Découverte, 2001 ; Fred Turner, *Aux sources de l'utopie numérique. De la contre-culture à la cyberculture, Stewart Brand un homme d'influence* (2006), trad. L. Vannini, Caen, C&F Éditions, 2012.

[21] John Perry Barlow, *Déclaration d'indépendance du cyberespace* (1996), trad. J.-M. Mandosio in Olivier Blondeau (dir.), *Libres enfants du savoir numérique. Une anthologie du "Libre"*, Paris, Éditions de l'éclat, 2000, p. 47 à 54. Texte original notamment accessible au lien URL : https://www.eff.org/cyberspace-independence, consulté le 12/06/2021.

même temps que le système purement technique des plateformes se développait. Si bien que peu à peu, elles ont pris une place importante en termes de nombre d'usagers et de clients. Au point que Facebook et ses semblables ont engendré des « communautés » tellement fortes que les responsables peuvent aller jusqu'à imaginer revendiquer des prérogatives traditionnellement régaliennes comme celle de battre monnaie (on se souvient par exemple du projet de monnaie numérique de Facebook en 2019-2020, « Libra »).

L'existence désormais indiscutable des « communautés numériques » invite à poursuivre le questionnement de la théorie politique, et à se demander : qu'est-ce qui constitue les particularités d'une communauté comme celle d'une nation ou d'un État souverain ? Sont-ce des valeurs et des symboles partagés, un territoire occupé, une langue, une histoire, une armée ou une monnaie communes ? Bien entendu, les GAFAM ne sont ni des États ni de nouvelles formes de nations. Cela signifie qu'on ne peut les considérer comme des communautés politiques, du moins telles que nous les connaissons à travers les États-nations, sauf dans les inventions de la littérature de science-fiction[22].

En l'état actuel des pratiques numériques, et pour prendre des cas concrets, certes, Google est devenu une puissance capable de tenter d'imposer aux États ses normes techniques et ses règles juridiques de fonctionnement ; et Facebook, Instagram ou LinkedIn rassemblent des communautés très vastes, quantitativement parlant, elles-mêmes constituées de sous-groupes aussi hétérogènes les uns vis-à-vis des autres que les régions ou provinces qui composent les États contemporains. Mais aucune de ces sociétés commerciales ne peut se faire passer pour un cyber-État. Leurs usagers ne sont pas ni ressortissants nationaux ni des citoyens. Elles ne pourraient leur offrir qu'une citoyenneté sans ancrage, car au vu des pratiques numériques, il s'agit d'une souveraineté en quelque sorte « hyper-post-nationale » ou « hyper post-patriotique »[23], car elle n'est nourrie par aucune histoire longue, aucune culture approfondie susceptible de fournir des références sérieuses pour un monde partagé, aucune esthétique capable de conférer son style à une existence authentiquement vécue, enfin aucune cosmologie crédible. Aucun engagement réciproque ne vient non plus, pour les « communautés numériques », fonder une forme effective de souveraineté populaire, car aucun contrat social explicite n'est à l'origine de leur rassemblement. En fait de condition civile par les usages numériques, ce mode d'existence ne peut pas être « enraciné »[24]. Il se trouve même déraciné,

[22] Voir à ce propos le roman de Marc Dugain, *Transparence*, Paris, Gallimard, 2019.
[23] Par référence aux thématiques de la citoyenneté post-nationale notamment développées par Jürgen Habermas, (*Après l'État-nation. Une nouvelle constellation politique*, Paris, Fayard, 2000) et Jean-Marc Ferry (*La question de l'État européen*, Paris, Gallimard, 2000).
[24] Simone Weil, *L'Enracinement*, Paris, Gallimard, 1949.

Et par suite il apparaît très dangereux pour les libertés publiques tout autant que pour les privées. Par exemple, le droit à l'expression permis et encouragé par ce type d'espace, généralisé dans les pays de culture hédoniste régis par des États de droit ou non, se trouve en effet doublé par un espionnage généralisé, qui recouvre des buts évidemment commerciaux, mais également parfois, de basse politique.

Mais comme elles se fondent, et ce sur de très vastes échelles, sur les usages de ces dispositifs socio-techniques que sont les plateformes, ces sociétés commerciales peuvent se prévaloir de représenter tout à la fois des vecteurs d'échanges informationnels et communicationnels, des ensembles de pratiques et de communautés d'émotions. Tendanciellement cosmopolitiques, elles peuvent même revendiquer le développement d'affiliations effectives et fortes, sur la double base du sentiment d'identification de leurs usagers et du partage de symboles par ces derniers. Certaines fictions littéraires ont réussi à traduire de manière éloquente ces formes d'affiliation, leurs potentiels attraits pour les individus ainsi que les risques de leur développement dans le contexte des démocraties libérales pluralistes[25]. Mais ces ensembles sociaux, qui ne sont pas assimilables à des nations, émergent dans le contexte de la crise multifactorielle actuellement traversée par la politique traditionnellement définie (critiques de l'administration, défiance envers la légitimité du monopole de la coercition par l'État, sentiment de perte d'identité nationale dans le contexte de la globalisation, ou encore mise en question de la représentativité des partis et des élus). En dépit de leur affiliation (même parfois très forte jusqu'à de l'addiction), aucun des usagers des services numériques ne peut encore s'écrier « J'aime mon réseau plus que mon âme »[26]. Mais dans un tel contexte de crise de la politique, l'appartenance aux communautés numériques ne fait-elle pas perdre quelque chose à l'attachement politique aux communautés nationales ? Par suite, sous l'effet des séductions exercées par la vie numérique – on se trouve tenté de parler d'un véritable opium digital – cette appartenance ne nuit-elle pas également à l'engagement civique ?

Il est peu contestable en tout cas que les méga-entreprises du numériques tendent à éroder le pouvoir des puissances publiques[27]. Elles contraignent de fait les institutions et les

[25] Voir par exemple Robert Charles Wilson, *The Affinities*, New York, Tor Books, 2015 (*Les Affinités*, trad. G. Goulet, Paris, Gallimard, 2018).
[26] Par référence à la formule employée par Machiavel dans sa lettre du 16 avril 1527 : « J'aime ma patrie plus que mon âme ».
[27] Voir Nikos Smyrnaios, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'Internet », *Communication & langages*, 2016/2, n°188, p. 61-83.

politiques publiques à évoluer et à se redéfinir, dans tous les secteurs que l'on peut imaginer[28]. Et l'on comprend sans peine que certaines prérogatives régaliennes, au cœur du rapport de force entre les États et les entreprises d'Internet jouent un rôle décisif dans les partitions originales qui sont en train de se dessiner : par exemple, si un jour les GAFAM imposent leurs règles fiscales aux États souverains, ne pourrait-on pas imaginer qu'elles iront jusqu'à se revendiquer en meilleures représentantes de leurs usagers que ces États de leurs propres citoyens, et négocier pour eux les règles de vie collective (fiscalité, protection et sécurité sociale...) ? Véritable cas d'espèce de ce que nous avons nommé l'« innovation sauvage »[29], dans le rapport de force qui s'est établi au plan géopolitique mondial entre les deux types de puissances, il n'y a aucune limite dans la transformation du monde qui résulterait de la victoire des GAFAM. Et cela, parce que la lutte de fait engagée entre ces puissances dans le cadre de l'économie globalisée concerne également la confrontation de deux modèles radicalement différents.

Un enjeu majeur : la dynamisation des compétences numériques par la puissance publique

Les communautés apolitiques du numérique font donc courir le risque de dépolitiser l'existence humaine et l'on peut également les soupçonner de promouvoir un type de relations sociales et humaines qui prend sens au sein d'un projet de totalitarisme doux et ludique [30]. Elles stimulent des formes d'indifférence à l'égard de la chose publique qui se manifestent par plusieurs phénomènes, à la fois banals et massifs, parmi lesquels l'achat et l'usage par les particuliers de matériels et de services sans conscience de leur origine ni de leur coût social et environnemental de production ; le recours massif aux plateformes d'accès gratuit qui utilisent à des fins commerciales les informations mises en ligne, parfois implicitement, notamment *via* les techniques du marketing digital ou numérique ou e-marketing ; et corrélativement le « laisser-aller des usagers », tant à l'égard du respect des règles de savoir-vivre sur les réseaux que vis-à-vis de la sécurisation de leurs propres informations personnelles.

Il convient également de prendre en compte le phénomène social dit de l' « illectronisme » (ou illettrisme numérique). En effet, les usages du numérique, aujourd'hui massifs mais aussi peu rigoureux que peu réflexifs, sont contemporains des formes d'ignorance, voire d'une réalité d'exclusion sociale. Or, il est intéressant, dans une réflexion de philosophie

[28] Ainsi que le documentent par exemple les études réunies par Éric Brousseau, Meryem Marzouki & Cécile Méadel (dir.), *Governance, regulations and powers on the Internet*, Cambridge, University Press, 2012.
[29] Thierry Ménissier, *Innovations. Une enquête philosophique*, *op. cit*., p. 12-14, 63-70 et 108-128.
[30] Voir à ce propos Philippe Vion-Dury, *La Nouvelle servitude volontaire. Enquête sur le projet politique de la Silicon Valley*, Limoges, FYP Éditions, 2016.

politique, de se pencher de manière quelque peu approfondie sur la réalité sur ce phénomène social – pour autant que, de son côté, la souveraineté politique classique est devenue effectivement favorable à l'engagement civique à mesure que, dans les différents pays inspirés par l'esprit des Lumières[31], les citoyens acquéraient par l'instruction la maîtrise du langage et des savoirs nécessaires à l'expression publique.

Selon l'INSEE, en 2019 en France, « 15% des personnes de 15 ans ou plus n'ont pas utilisé Internet au cours de l'année, tandis que 38% des usagers manquent d'au moins une compétence numérique de base et 2% sont dépourvus de toute compétence », ainsi l'illectronisme concernait à cette date 17% de la population. Une personne sur quatre ne sait pas s'informer et une sur cinq est incapable de communiquer *via* Internet, et « les personnes les plus âgées, les moins diplômées, aux revenus modestes, celles vivant seules ou en couple sans enfant ou encore résidant dans les DOM sont les plus touchées par le défaut d'équipement comme par le manque de compétences. »[32] Or, dans le même temps, le Gouvernement français entend dématérialiser la totalité des démarches administratives d'ici 2022, ce qui augmente le problème : dans le cadre de l'e-administration, il est en effet fondamental pour chacun des citoyens de savoir utiliser les ressources numériques courantes (Internet, traitement de texte…). On affirme souvent aujourd'hui que de telles compétences sont devenues presque aussi indispensables que celles, basiques pour évoluer dans une société développée, telles que savoir lire, écrire et compter. Ne pas avoir accès à Internet ou ne pas savoir utiliser les outils numériques représente donc un réel handicap, notamment pour effectuer des démarches administratives ou encore accéder aux services publics, pouvant accroître la vulnérabilité sociale de populations potentiellement déjà fragiles. Selon la même enquête, les raisons de l'absence d'équipement à domicile apparaissent variées : le manque de compétence (41 %), le coût du matériel (32 %) ou de l'abonnement (27 %) sont les plus citées, loin devant l'absence d'offre haut-débit (5 %). Mais cette dernière raison clive vraiment le territoire : elle est citée par 13 % des non-équipés des communes rurales contre moins de 2 % dans les unités urbaines de plus de 100 000 habitants. Si 79 % des connexions filaires sont en haut-débit, ce n'est le cas que de 69 % dans les communes rurales (où on trouve 16 % de bas débit) contre plus de 80 % dans les unités urbaines de 10 000 habitants ou plus et 87 % en agglomération parisienne (où seules 5 % sont en bas-débit). Comment, parallèlement au développement du réseau et à une aide dans l'accès au matériel, contrer de tels phénomènes ?

[31] Condorcet, *Cinq mémoires sur l'instruction publique* (1791), Paris, Flammarion, 1994.
[32] Voir *Insee Première*, n°1780, octobre 2019 : *Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base*, p. 1-2.

La notion de « compétence numérique » offre une piste intéressante. *Eurostat* (direction générale de la Commission européenne chargée de l'information statistique à l'échelle communautaire) distingue quatre domaines de compétences numériques[33] : la recherche d'information (sur des produits et services marchands ou administratifs, etc.) ; la communication (envoyer ou recevoir des courriels, etc.) ; la résolution de problèmes (accéder à son compte bancaire par Internet, copier des fichiers, etc.) ; enfin, l'usage de logiciels (traitement de texte, etc.). Ces compétences sont mesurées à partir des déclarations sur le fait d'effectuer certaines tâches dans l'enquête annuelle auprès des ménages sur les technologies de l'information et de la communication, menée dans tous les pays de l'Union européenne. Chaque compétence est notée 0 (compétence nulle), 1 (basique) ou 2 (compétence plus que basique). Le non-usage d'Internet au cours de l'année impliquant la note 0 : l'échelle mesure donc une capacité pratique (liée à la possession d'un équipement et à un usage même minimal d'Internet) si l'on considère la population générale, mais une compétence si l'on se restreint aux usagers d'Internet. Elle sous-estime légèrement les compétences en « logiciels » et « résolution de problèmes » dont les critères ne nécessitent pas tous l'usage d'Internet.

Ainsi, les outils de mesure permettent de constater l'importance du développement de l'accès au numérique : en 2017, 84 % des ménages ont eu accès à Internet à leur domicile, soit deux fois plus qu'en 2006, cela, notamment sous l'effet de la tendance qui a conduit, depuis une dizaine d'années, les équipements et les usages à se faire bien plus mobiles qu'autrefois. Huit personnes sur dix de 15 ans ou plus avaient utilisé Internet au cours des trois derniers mois en 2018, le plus souvent pour envoyer des courriels et rechercher des informations. Cependant, une personne sur cinq n'a aucune capacité numérique en 2017. Les plateformes numériques et le commerce électronique se développent rapidement, mais restent minoritaires dans les secteurs concernés. En 2017, les ventes dématérialisées représentent 30 % du chiffre d'affaires des sociétés de 250 salaries ou plus ; cette part a doublé en dix ans. Parmi les activités de technologies, contenus et supports de l'information (TCSI), l'emploi et la valeur ajoutée sont particulièrement dynamiques dans les services de programmation, conseil et autres activités informatiques.[34]

Pour contrebalancer ces effets, une réflexion de fond est menée depuis plusieurs années par les sciences sociales[35], et sur le plan hexagonal des structures ont été dédiées, et des actions

[33] https://ec.europa.eu/eurostat/databrowser/view/tepsr_sp410/default/bar?lang=fr
[34] Insee, *L'économie et la société à l'ère du numérique*, édition 2019.
[35] Voir par exemple Périne Brotcorne & Gérard Valenduc, « Les compétences numériques et les inégalités dans les usages d'internet. Comment réduire ces inégalités ?, *Les Cahiers du numérique*, 2009/1 Vol. 5, p. 45-68.

engagées par la puissance publique. Ainsi, celles développées par l'Agence du numérique, service à compétence nationale dépendant du Ministère de l'Économie, de l'Industrie et du Numérique, créé par décret le 3 février 2015, et chargée de l'impulsion, de l'animation et de l'accompagnement des projets et des initiatives numériques développés dans les territoires par les collectivités publiques, les réseaux d'entreprises, les associations et les particuliers, tels que le pilotage et la mise en œuvre du déploiement du plan « France très haut débit », le pilotage et la mise en œuvre des actions du programme « Quartiers numériques », également dénommé « French Tech », et l'accompagnement des initiatives candidates à l'octroi du label du même nom, et la diffusion des outils numériques et le développement de leur usage auprès de la population. Elle comprend trois pôles responsables respectivement des 3 missions suivantes : la Mission Très Haut Débit[36], la Mission French Tech[37] et la Mission Société Numérique[38]. Les activités de la Mission Société Numérique visent explicitement à se situer au plus près des usagers-citoyens. Sa communication se veut explicitement garante des valeurs d'égalité typiquement républicaines et elle entend « faciliter l'équipement et l'accompagnement des foyers, en particulier ceux qui restent en retrait dans l'utilisation des technologies numériques (séniors, familles à revenu modeste, personnes à faible niveau d'éducation ou sans emploi…) ». Ces programmes dédiés par l'instruction numérique sont mis en œuvre en France au niveau de l'État et des Régions dans le cadre du « plan stratégique d'inclusion numérique », qui s'appuie sur la stratégie nationale « Pour une France connectée Plan national pour un numérique inclusif » élaboré entre novembre 2017 et mai 2018 sous l'égide du Secrétariat d'État au numérique[39]. La crise sanitaire lié à la pandémie de COVID-19 a enfin vu le lancement de la plateforme Solidarité numérique[40], dont le but est d'accompagner personnes en difficulté face aux outils numériques[41].

A cela s'ajoute l'action des associations et des collectifs qui luttent contre l'exclusion et la précarité numériques : nationales comme Emmaüs Connect[42], régionales comme La Mêlée[43], ou de terrain comme Travailler et Apprendre Ensemble (TAE)[44] ; et également celle des start-

[36] https://www.amenagement-numerique.gouv.fr/
[37] https://lafrenchtech.com/fr/
[38] https://societenumerique.gouv.fr/
[39] Voir le rapport de synthèse : https://www.enssib.fr/bibliotheque-numerique/documents/68347-rapports-et-recommandations-strategie-nationale-pour-un-numerique-inclusif.pdf ; et le dossier de presse (13/09/2018) : https://societenumerique.gouv.fr/wp-content/uploads/2018/09/DP_SNNIVDEF2.pdf
[40] https://solidarite-numerique.fr/
[41] Voir https://www.vie-publique.fr/en-bref/274035-solidarite-numerique-nouveau-site-pour-lutter-contre-lillectronisme
[42] https://emmaus-connect.org/exclusion-numerique/
[43] https://www.lamelee.com/
[4444] https://ecosolidaire.org/

up comme WeTechCare[45] (notamment responsable des *Cahiers de l'inclusion numérique* [46]), ou encore celle des programmes reconnus d'utilité publique tel que Solidatech[47], lui-même étant lié au réseau TechSoup Global[48], fondé en 1987, réseau international de solidarité numérique pour les organisations à but non lucratif et qui se compose de 68 partenaires en Afrique, Amérique, Asie-pacifique, Europe et au Moyen-Orient qui vise à renforcer l'impact des associations membres sur les problématiques sociétales locales et à favoriser un changement social mondial.

Vers un pouvoir numérique constituant ?

Les effets bénéfiques sur le développement de l'instruction numérique de ce type d'action sont à souligner. Il convient de les considérer en regard de l'émergence d'une « souveraineté numérique » digne de ce nom, car basée à la fois sur une réalité sociale ou populaire et sur une sensibilité à la chose publique. L'enjeu qui se dessine ici est également que les pratiques numériques, en modifiant le concept hérité de souveraineté, suggèrent un sens original pour cette notion. Trois remarques s'imposent à ce propos. Premièrement, la relation entre les programmes d'accès à internet et l'idée d'une souveraineté numérique se précise si l'on admet que les compétences numériques ne sont pas seulement « pragmatiques », en ce qu'elles permettraient une meilleure inclusion sociale et une meilleure insertion professionnelle, mais qu'elles valent comme des compétences civiques. De même, avant le numérique, savoir lire et écrire, ont constitué la base de la diffusion des idées émancipatrices et ont permis de cultiver l'esprit critique. A cette condition, il est possible de constituer comme les usagers comme un « public » (selon le concept de Dewey[49]) : l'accès aux nouveaux moyens d'expression, d'information et de communication constitue un nœud qui mêle intimement épistémologie, pédagogie, éthique et politique[50]. On pourrait dire, en reprenant la terminologie de Bernard Stiegler, que c'est dans le même *pharmakon* que se trouvent le poison et son remède[51].

Deuxièmement, il convient de souligner qu'il est nécessaire d'ouvrir pour les usagers une voie de sortie du consumérisme numérique, tant en développant le sens critique par le biais

[45] https://wetechcare.org/
[46] https://www.inclusion-numerique.fr/
[47] https://www.solidatech.fr/
[48] https://www.techsoup.global/
[49] John Dewey, *Le Public et ses problèmes* (1927), trad. J. Zask Paris, Gallimard, « Folio essais », 2010.
[50] A propos de ce nœud, voir Claude Gautier, « Le Public et ses Problèmes : le problème social de la connaissance », *Philosophical Enquiries. Revue des philosophies anglophones*, n°5, 2e semestre 2015, accessible à l'URL : http://www.philosophicalenquiries.com/numero5article3Gautier.html
[51] Voir par exemple http://arsindustrialis.org/pharmakon

d'un internet nourri de contenus complexes qu'en proposant la logique d'action émancipatrice propre au « faire » (*Making*, *Hacking*) par le biais des espaces de pratique[52]. L'expérience des Espaces publics numériques en est aujourd'hui venue aux retours d'expérience[53]. On s'accorde notamment à reconnaitre que l'acronyme « EPN » gagne aujourd'hui à être repensé en termes « espaces de pratiques numériques » (ou EPN 2.0)[54]. On ne peut pas attendre de l'institution qu'elle réinvente à elle seule le pouvoir constituant dont elle a besoin pour asseoir sa propre légitimité : si l'on veut une souveraineté 2.0 forte, il convient de libérer l'énergie du peuple ou de la nation numériques.

Troisièmement, le caractère illimité de l'espace numérique a pu inviter au développement de la posture libertaire – libertarienne, et pour concevoir les ressources de la souveraineté numérique en termes de pouvoir constituant, il est probablement nécessaire de dépasser le cadre strictement national dans lequel la modernité a conçu ce concept.

Les crises nationalistes des XIX^{ème} et XX^{ème} siècles, la montée du populisme au siècle dernier et sa résurgence dans le nôtre – deux phénomènes historiques et politiques massifs auxquels la souveraineté étatique et nationale n'a pas peu contribué – devraient donner à penser. Or, il se trouve que les tenants de ce qu'on nomme en théorie politique la perspective rationaliste sur la nation[55] fournissent ici quelques ressources : il n'y a pas de pouvoir constituant sans engagement des citoyens dans la défense de certaines valeurs, à commencer par les valeurs éthiques et politiques, bien entendu, mais également esthétiques. La pratique de l'espace numérique à l'échelle du continent européen peut engendrer, *via* des contenus culturels de qualité, un goût pour la complexité favorisant, à terme, la mobilisation de nouvelles formes de communautés civiques. Mobiliser les citoyens dans des formes de souveraineté post-nationale apparaît paradoxalement nécessaire si l'on veut fortifier ou recomposer une souveraineté numérique « populaire », foyer de légitimité pour une souveraineté de type

---

[52] Voir Michel Lallement, *L'Âge du Faire, Hacking, travail, anarchie*, Paris, Éditions du Seuil, 2015 ; ; Isabelle Berrebi-Hoffmann, Marie-Christine Bureau, Michel Lallement, *Makers. Enquête sur les laboratoires du changement social*, Paris, Éditions du Seuil, 2018.

[53] Voir par exemple ces analyses et préconisation : Agence nouvelle des solidarités actives (ANSA) et Comité Interministériel des Villes, Rapport « Espaces Publics Numériques et politique de la ville », 2011, téléchargeable à l'URL : http://observatoire-reussite-educative.fr/thematiques/numerique-et-medias/Ressources-formation-contibutions-analyse/rapports-colloques-1/etude-epn-et-politique-de-la-ville ; et Loïc Gervais, « Itinéraire d'un animateur d'espace publique numérique (EPN) », *Cahiers de l'action*, 2017/1 N° 48, p. 23-29, accessible à l'URL : https://www.cairn.info/revue-cahiers-de-l-action-2017-1-page-23.htm

[54] Voir pour une définition approfondie : https://movilab.org/wiki/Espace_de_Pratiques_Numériques ; voir également Antoine Burret, « Démocratiser les Tiers-lieux », *Multitudes*, 2013/1 n° 52, p. 89-97, accessible à l'URL : https://www.cairn.info/revue-multitudes-2013-1-page-89.htm

[55] Voir Ernest Renan, *op. cit.*, et de manière contemporaine Dominique Schnapper, *La Communauté des citoyens*, Paris, Gallimard, 1994 ; Pierre Manent, *La Raison des nations : Réflexions sur la démocratie en Europe*, Gallimard, 2006.

institutionnel. Cela apparaît d'autant plus important que dans un monde politique et civil qui n'est plus régi par des formes transcendantes d'autorité (Dieu, le roi, la République), l'idée de pouvoir souverain représente une métaphore inopérante : dans le monde social ordinaire, l'autorité est devenue purement immanente. Il n'y a plus d'autorité extraordinaire sauf en matière de religion. Le pouvoir suprême (puisque « souveraineté » vient du latin « *superus* ») repose au plan politique sur des représentations nationales devenues « locales » dans l'espace mondial. Au plan européen et dans le contexte de l'Union Européenne telle que nous la connaissons actuellement, il appartient à ceux qui peuvent en imposer la norme juridique ; au niveau des opérateurs du numérique, il obéit à ceux qui peuvent imposer à la fois le fait technique, compris dans ce termes les normes techniques et les comportements prescrits par les solutions offertes au public – sur ce point, le pouvoir obéit désormais, comme le soulignait Lawrence Lessig, aux concepteurs programmateurs employés par les firmes : « *Code is Law* »[56]. Que reste-t-il alors du pouvoir populaire ? Quel pouvoir pour ceux qui peuvent de fait s'ériger en collectifs d'usagers, communautés de valeurs animées par l'engagement de leurs membres ?

Repenser le concept de souveraineté à partir des réalités numériques ?

Si l'on veut penser un concept de souveraineté réellement applicable au régime numérique, et faire émerger une notion adéquate à la « souveraineté numérique », il apparaît peut-être intéressant d'inverser audacieusement la perspective, et d'entreprendre de repenser le concept même de souveraineté à partir du numérique. Ce que l'on attend souvent de ce concept ce n'est rien d'autre que de sanctuariser les économies nationales particulières, ce qui s'exprime, de par le monde, à travers le financement de l'innovation au strict niveau national. Mais une telle visée constitue désormais, vu le rapport de force engagé avec les États particuliers par les puissances compagnies numériques, un objectif bien trop restreint, et sans doute un réflexe qui fait manquer l'essentiel et courir le risque de perdre la partie.

Dans un tout autre ordre de faits, l'appropriation des technologies numériques laisse espérer la relocalisation du pouvoir constituant, par exemple *via* le développement de solutions de proximité (locales ou régionales) pour l'*open data*. Les EPN 2.0, dont relèvent notamment de telles pratiques d'*open data*, doivent être conçus comme des ateliers en vue de la préservation des libertés publiques. En effet, par le biais de la diffusion de la culture de la donnée, et sous l'effet de l'injonction à mettre cette dernière au service du public, peut s'opérer pour une

[56] Lawrence Lessig, « *Code is law, On Liberty in Cyberspace* », Harvard magazine, janvier 2000, accessible à l'URL https://www.harvardmagazine.com/2000/01/code-is-law-html consulté le 10/06/2021.

communauté civique ancrée dans son territoire à la fois une salutaire réappropriation de ses propres ressources et la réinvention d'une forme d'intérêt général.

La notion classique de souveraineté, comme d'autres concepts hérités de la tradition politique moderne aujourd'hui débordés par les nouvelles technologies, lorsqu'elle est étroitement interprétée, tend à masquer l'importance fondamentale des nouvelles réalités socio-techniques, surtout celles qui émergent à travers les pratiques numériques. Pourtant à ce niveau se joue peut-être l'émergence d'une souveraineté numérique populaire ou d'une nouvelle forme de souveraineté pour les communautés numériques. Les usages publics de la donnée, à savoir, la synergie des acteurs du numérique dans le sens de l'intérêt général, laissent espérer l'émergence d'un nouveau concept de régulation favorable à la démocratie, par le biais de la réappropriation locale des pratiques numériques. C'est une manière d'inventer la nouvelle Athènes, en évoquant un des grands modèles de la culture politique de l'autonomie, aux antipodes du « projet politique de la Silicon Valley » et de sa « nouvelle servitude volontaire » qui isole les usagers dans des identités illusoires[57]. La thématique que nous avons explorée dans cette contribution ne traduit pas seulement notre « futur imparfait »[58]. Elle nous invite à imaginer de nouvelles formes mentales, aujourd'hui attendues aussi bien pour guider les pratiques numériques et politiques que pour construire l'avenir avec des perspectives renouvelées.

***

Auteur

Thierry Ménissier est Professeur de philosophie politique à l'Université Grenoble Alpes, chercheur dans l'Institut de Philosophie de Grenoble (IPhiG) et responsable de la chaire « éthique & IA » au sein de l'Institut pluridisciplinaire d'intelligence artificielle (*MIAI*) de Grenoble. Ses recherches portent sur la transformation des principes de l'éthique publique et sur le sens de l'innovation technologique et sociale.

Dernières publications:

- *Innovations. Une enquête philosophique*, Paris, Éditions Hermann, 2021.
- « Les dispositifs de reconnaissance faciale, un défi pour l'éthique de l'IA », *Klesis. Revue philosophique*, n°49, 2021 [en ligne].

[57] Philippe Vion-Dury, *La Nouvelle servitude volontaire*, *op. cit.*

[58] Selon l'expression employée par Sheila Jasanoff, dans « Future Imperfect: Science, Technology, and the Imaginations of Modernity », in Sheila Jasanoff & Sang-Hyun Kim (eds.), *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*, Chicago, The University of Chicago Press, 2015, p. 1-33.

- « Un « moment machiavélien » pour l'Intelligence Artificielle. La Déclaration de Montréal pour un développement responsable de l'IA », *Raisons Politiques*, 2020/1 (n°77), p. 67-81.
- *Philosophie de la corruption*, Paris, Éditions Hermann, 2018.

Institut de Philosophie de Grenoble & chaire « éthique & IA » MIAI
Université Grenoble Alpes
Bâtiment ARSH, BP 47, Domaine Universitaire, 1281, avenue Centrale
38400 Saint-Martin d'Hères
Thierry.menissier@univ-grenoble-alpes.fr

Le numérique et le retour de la souveraineté

Par Marc Mossé,
Senior Director Government Affairs,
Directeur Juridique, Microsoft Europe
Vice-Président de la l'Association Française des Juristes d'Entreprise

20 ans déjà !

En cette année 2016, la souveraineté à l'ère numérique fête ses 20 ans. C'est en 1996, en effet, que fut proclamée la Déclaration d'indépendance du cyberspace. Son auteur, John Peary Barlow, parolier du groupe *Grateful Dead*, écrivait ainsi : "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us.* ***You have no sovereignty where we gather***"[1].

20 ans après, et cette idée est toujours présente chez certains. Peut-être plus encore aujourd'hui tant elle a quitté le champ des pionniers pour devenir un élément crucial du débat publi. La souveraineté demeure essentielle mais chacun s'interroge sur la meilleure façon de l'adapter aux enjeux numérique.

À l'époque, la contre-culture et l'inspiration des hackers des débuts d'Internet expliquaient en grande partie cette affirmation de principe tendant à l'émancipation de l'individu. En posant la question de la souveraineté en ces termes radicaux, l'ancien musicien hippie signifiait aussi que le numérique allait bouleverser notre rapport au pouvoir, affecter la verticalité de

1. *Gouvernement du monde industrialisé… Je viens du cyberespace, le nouvel ordre de Pensée. Au nom du futur, je vous demande de nous laisser seuls. Vous n'avez pas de souveraineté là où nous nous rassemblons*

nos sociétés et *in fine* modifier notre relation au Politique. C'est, à vrai dire, une affirmation qui pose le concept de souveraineté sous un jour différent de certaines thèses récentes, qui utilisent la souveraineté numérique sur un mode ancien pour ériger des frontières au lieu de penser un monde nouveau qui bouleverse la géopolitique, l'économie, et la démocratie.

Woodstock ou Corée du Nord ? La vérité doit être ailleurs…

20 ans, déjà. À cette époque, 1996, Microsoft, Apple, étaient tout juste adolescents. Google, Facebook… balbutiaient. On ne parlait pas encore de Cloud computing, de Big data, de Machine Learning, d'Internet des objets ou d'Intelligence Artificielle[2]… La donnée n'était pas promise au statut de nouvel or noir, de carburant de l'innovation et de l'économie moderne, et la loi de 1978 d'abord initiatrice d'une prise de conscience juridique bienvenue semblait suivre un long fleuve tranquille. Le transfert transnational des données n'était pas devenu un sujet majeur et les États n'avaient pas encore été confrontés aux interrogations liées à une architecture technologique profondément décentralisée.

Depuis, la souveraineté numérique est devenue un thème clé et nombreux sont ceux qui essayent de la penser en utilisant parfois des outils intellectuels forgés à une époque d'États littéralement bornés. C'est ainsi qu'on a vu apparaitre des projets visant à créer des Cloud Souverain, lesquels se sont terminés par un échec industriel engloutissant des millions d'euros. Il est vrai que le concept du nuage qui s'arrête aux frontières semblait avoir été abandonné depuis Tchernobyl… C'est ainsi qu'a été voté le principe de l'étude de l'opportunité ou non de la création d'un Commissariat à la souveraineté numérique[3]. Allant un pont plus loin,

2. En réalité, l'Intelligence Artificielle est apparue sous un angle conceptuel au XX^e siècle. Citons cette proposition sans doute fondatrice : McCarthy, J. Minsky, M.L. Rochester, N. Shannon, *A proposal for the Dartmouth Summer Project on Artificial Intelligence, Dartmouth University, 1955*, se donnant pour objectif de « *résoudre les types de problèmes aujourd'hui réservés aux humains* ».

3. Voir, à cet égard, l'article 29 de la Loi pour une République Numérique aux termes duquel il est prévu que « *Le Gouvernement remet au Parlement, dans un délai de trois mois à compter de la promulgation de la présente loi, un rapport sur la possibilité de créer un Commissariat à la souveraineté numérique rattaché aux services du Premier ministre, dont les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République*

certains ont même tenté de faire adopter l'idée de la création d'un OS souverain… ; ce que l'on ne commentera pas ici dès lors que l'écosystème s'en est largement chargé sans excès de complaisance s'agissant d'une idée baroque qui aurait pu trouver sa place sans mal dans une nouvelle édition de *Tintin au pays des Soviet*s.

Ces réactions qui participent plutôt du souverainisme, ne doivent pas empêcher d'avoir un vrai débat de fond sur le sujet de la souveraineté. Il s'agit là, en effet, d'un thème majeur car il pose de façon renouvelée, l'interrogation fondamentale de notre rapport à la technologie et du rôle de la machine. J. Ellul considérait déjà que « *c'est le politique qui est de plus en plus induit par la technique et incapable aujourd'hui de diriger la croissance technicienne dans un sens ou dans l'autre*[4] ».

Faut-il, dans le fil de cette vision un brin pessimiste, considérer que le numérique a dessiné une nouvelle carte des rapports de force où les États comme les individus seraient devenus tributaires d'acteurs et de moyens échappant définitivement à leur contrôle ? De grands acteurs du numérique seraient-ils des puissances susceptibles de rivaliser avec les États ?

Qu'il s'agisse de cybersécurité ou de protection des données, la question n'est pas vaine.

Depuis 1996 beaucoup de choses ont changé il est vrai. La cyberguerre est devenue une réalité et la démocratie se trouve parfois à la merci d'attaques qui menace l'expression libre de la souveraineté des peuples. Au lieu d'un retour de la guerre froide, on pourrait même être tenté de voir l'affirmation d'une forme de « guerre chaude » impliquant parfois de nouveaux acteurs non étatiques mais aux capacités de nuisance susceptibles d'affecter gravement les Nations. Par ailleurs, sur le plan de la *privacy*, l'usage des données à des fins parfois étrangères à la finalité de leur collecte a conduit

---

protège. Ce rapport précise les moyens et l'organisation nécessaires au fonctionnement du Commissariat à la souveraineté numérique ». Voir aussi de façon éclairante le projet de rapport d'initiative parlementaire du député européen J.L. Schauffhauser (FN) sur le Cloud souverain dont le contenu initial a conduit la Commission compétente du Parlement européen à le réécrire entièrement sur un mode moins caricatural et conformément au principe du *free flow of data*.

4. *Le système technicien*, 1977, rééd. 2012, p. 136.

les régulateurs à trancher pour que chaque individu ne voit pas sa souveraineté individuelle contrôlée malgré lui ou à l'insu de son plein gré. Quant aux révélations d'E. Snowden, elles ont fini de montrer que la surveillance par des États démocratiques d'autres États – parfois même alliés – et des citoyens pouvait prendre une ampleur inédite.

Comment répondre à ces nouveaux défis ?

Le faire en se référant à des concepts éprouvés par le temps peut rassurer ; mais qu'il soit permis de suggérer, à l'occasion de cette belle journée où le soleil est souverain dans le ciel de Nice, qu'il faille les repenser. Sans doute faut-il dessiner de nouveaux contours quitte, peut-être, à revenir aux racines. La souveraineté demeure une idée puissante, indispensable, à laquelle les peuples se réfèrent toujours en y voyant, à juste titre, l'un des concepts traduisant le besoin de toute société humaine : garantir les libertés dont celle de choisir son gouvernement démocratique, et la protection de la sécurité des gens et des territoires. Il demeure essentiel de redonner tout son – ses – sens à ce mot afin de le rendre pleinement opératoire pour penser le monde qui vient.

Par chance, la souveraineté a montré qu'elle était un concept d'une réelle plasticité. On pourrait ainsi distinguer : souveraineté technologique, souveraineté individuelle et souveraineté étatique, en établissant ce qui les oppose ou les rapproche, pour établir les conditions d'une souveraineté adaptée à la révolution numérique.

1. La tentation de la souveraineté technologique

En affirmant par une formule maintenant classique que "*Code is Law, architecture is politics*"[5], Laurence Lessig a inscrit le numérique dans le champ du politique. Faut-il en déduire que la technologie va s'affranchir du Souverain et, partant, du pouvoir des citoyens ?

Dans la Silicon Valley, le digital est parfois vu comme la solution à tout. Cela soulève des critiques aigües. Ainsi, Evgeny Morozov est l'auteur

5. L. Lessig, *Code and Other Laws of Cyberspace*, Basic Book, 1999, 297 p

d'un ouvrage désormais traduit en français, intitulé : « *Pour tout résoudre cliquez ici : l'aberration du solutionnisme technologique* »[6]. Il y décrit et dénonce cette vision d'une partie de la Côte Ouest des États-Unis, où l'on considère souvent que le numérique peut tout résoudre, répondre à toutes les questions, pourvoir à la décision, se substituer à l'État et, finalement, aux politiques publiques. Selon lui, *« il s'agit d'un mouvement d'explication d'un grand nombre de changements sociaux, politiques et culturels du monde d'aujourd'hui par une force unique : l'Internet. Cette force est censée être autonome, elle est censée agir selon sa propre logique, sans cesse et partout, exactement comme l'économie, le marché ou la nature sont traditionnellement présentés dans certaines théories sociales telles des forces autonomes agissant d'elles-mêmes »…* Cette vision digital-centrée renvoie à cette idée que la technologie serait une source de souveraineté en soi. La critique de Morozov englobe par voie de conséquence la vision irénique du transhumanisme, sorte d'illustration anticipatrice d'un monde où le numérique serait le substrat de l'humanité augmentée. En France, Eric Sadin met en garde tout également contre un monde où la technologie numérique permettrait d'ordonner la société par le biais d'un nouveau déterminisme nécessairement discriminatoire qui ne serait pas plus admissible ni légitime au motif qu'il procéderait d'algorithmes.

D'aucuns poussent l'inquiétude jusqu'à décrire certaines grandes entreprises globalisées en puissances autonomes annonciatrices d'un monde post-étatique, ou, à tout du moins, d'un équilibre nouveau où les États ne seraient plus qu'une forme parmi d'autres de l'organisation de l'espace international dominé par la puissance des technologies numériques. Crainte exagérée, mais il est certain que certaines évolutions seraient évidemment inacceptables.

En revanche, il est loisible de penser tout au contraire au rôle que certaines entreprises peuvent travailler aux côtés des citoyens et des gouvernements à l'émergence de justes régulations[7].

Inévitablement, le développement de l'intelligence artificielle intensifie le questionnement. Il n'est plus un jour sans que fleurissent des craintes

6. FYP Édition, 2014
7. *Cloud for Global Good, Microsoft, Octobre 2016*

sur la fin de l'humain et le triomphe des robots… voire sur l'eugénisme numérique. Sans doute est-il utile de se remémorer les lois d'Asimov[8] et les préventions de Norbert Wiener, l'un des pères de la Cybernétique, sur le risque de voir la « Machine » dotée de capacités logiques toujours plus importantes – notamment en raison du nombre de données traitées – s'imposer à nous. Cela exige une vigilance qui loin de toute forme de techno-pessimisme, appelle à une réflexion sur les conditions de maîtrise de l'innovation technologique sous un angle éthique et juridique.

Heureusement, à rebours de la béatitude des « ravis de la crèche numérique » ou, à l'inverse, d'une approche démiurgique du pouvoir technologique, on voit certains grands acteurs industriels, dont Microsoft, nourrir la réflexion sur le besoin de dessiner les contours d'un numérique de confiance[9] incluant responsabilisation – que le terme d'*accountability* restitue imparfaitement – et transparence des algorithmes. On notera ici que le droit européen comme le droit français permettent d'ores et déjà d'appréhender de nombreux aspects de l'intelligence artificielle ainsi que l'a relevé le groupe de travail contribuant à la stratégie française sur le sujet[10]. Il est aussi intéressant de relever que le droit à l'expérimentation[11] trouve là un terrain fertile pour s'exercer utilement et concilier protection des droits et innovation.

La réflexion est ouverte sur la façon dont les acteurs doivent jouer leur partition pour contribuer, à leur place, à définir les limites nécessaires à l'émergence d'un quelconque pouvoir autonome des technologies c'est-à-dire en réalité de ceux qui les conçoive. La République des développeurs

8. L'auteur de science-fiction a ainsi résumé dès 1942, les 3 lois s'imposant aux robots pour vivre en harmonie avec l'homme : un robot ne peut porter atteinte à un être humain, ni, restant passif, permettre qu'un être humain soit exposé au danger ; un robot doit obéir aux ordres que lui donne un être humain, sauf si de tels ordres entrent en conflit avec la première loi ; un robot doit protéger son existence tant que cette protection n'entre pas en conflit avec la première ou la deuxième loi.
9. http://www.slate.com/articles/technology/future_tense/2016/06/microsoft_ceo_satya_nadella_humans_and_a_i_can_work_together_to_solve_society.html
10. Stratégie nationale en intelligence artificielle, 15 février 2017.
11. Article 37 de la Constitution.

ne saurait être le substitut souhaitable à celle des professeurs. Le futur des technologies ne doit pas substituer une souveraineté aveugle ou a-démocratique à celle qui doit prévaloir dans toute société démocratique, c'est-à-dire celle reposant sur le libre choix des individus.

2. Vers un retour de la souveraineté individuelle ?

D'aucuns ont vu, depuis longtemps, dans la souveraineté individuelle une opportunité d'établir un véritable libéralisme politique hors de tout contrôle social illégitime. Henry David Thoreau dans « *La désobéissance civile* » écrivait en 1849 : « *Je ne veux être considéré membre d'aucune société à laquelle je n'ai pas adhéré* ». Un des pères de l'école autrichienne d'économie, parlant du libéralisme en 1927, considérait que *« la théorie métaphysique de l'État proclame – ce qui peut se comparer, à cet égard, à la vanité et à la présomption des monarques absolus – que chaque État est souverain, c'est-à-dire qu'il constitue l'ultime et la plus haute cour d'appel »* et que « *le libéralisme réclame que l'organisation politique de la société soit étendue jusqu'à ce qu'elle atteigne son point culminant, dans un État mondial qui unirait toutes les nations sur une base d'égalité* »[12]. Dès lors, pour ce courant, le monde ne s'arrête pas aux frontières de l'État, et l'importance que peuvent revêtir les frontières nationales, souvent accidentelles, est subalterne.

On retrouve cette idée chez Pierre Lemieux, auteur canadien, de la possibilité pour les individus de s'affranchir des États, conception proche de celle des libertariens. Il s'agit de s'émanciper de la souveraineté classique chère aux constitutionnalistes, rattachée à la forme étatique. On le voit, il y a là un écho au courant faisant de la technologie le fondement de la souveraineté. Ce courant libertarien, très présent comme déjà dit dans la Silicon Valley, se fonde sur un individualisme poussé qui conteste le rôle de l'État et la souveraineté classique.

À suivre ce libéralisme radical, on devrait logiquement aboutir à ce que l'individu s'affranchisse tout autant de la tutelle étatique que de celle de la technologie.

12. L. Von Mises, *Le Libéralisme*, École Autrichienne de l'Économie, 1927.

C'est vrai d'un double point de vue : à la fois, d'une part, à l'aune des nouveaux pouvoirs que le numérique peut donner à chacun, et d'autre part, au regard de la nécessaire contrepartie qui doit revenir à l'individu afin qu'il puisse contrôler la technologie, surtout si sa promesse est celle de l'émancipation.

D'abord, il est certain que les possibilités pour l'individu de s'affranchir de la tutelle des corps intermédiaires voire de contrôler en permanence ses représentants, élus ou non, vont aller grandissantes. Sans aller jusqu'à une vision absolutiste de la souveraineté individuelle, il est certain que l'on voit s'affirmer les prémices d'un pouvoir plus grand de l'individu grâce aux technologies qui accompagne une contestation des pouvoirs verticaux. La société en réseaux largement décrite, la remise en cause des structures pyramidales, impactent la nature des rapports sociaux, des organisations dont les partis politiques, les syndicats…, et jusqu'aux procédures démocratiques. La possibilité pour l'individu d'exprimer plus facilement sa volonté hors les contraintes des corps sociaux intermédiaires est une réalité dont on ne mesure pas encore tous les conséquences sur nos sociétés. Le décloisonnement des interactions socio-politiques est en devenir. Nul ne pourra les nier ni refuser de les prendre en compte dans le champ démocratique. Clairement cela signifie une participation accrue des citoyens à la fabrique de la loi comme au contrôle des gouvernants. L'accélération du temps par le numérique ou tout du moins le sentiment de sa compression, pourrait même remettre en cause le rythme qui scande la vie de nos régimes politiques. La longue gestation de nos dirigeants, blanchis sous le harnais, pourrait dans le futur être raccourcie de façon spectaculaire De même, la temporalité d'élections suivies de longues plages de silence démocratique ne pourra plus satisfaire la capacité d'expression des individus. La démocratie continue voire permanente trouverait ainsi une voie de réalisation. Certes, le danger existe que se crée une forme d'aristocratie numérique seulement composée des mieux dotés culturellement et en savoirs. Ce risque n'est pas négligeable. Il peut fonder de nouvelles inégalités faisant alors de la souveraineté individuelle une illusion dangereuse. D'où la nécessité de doter chacun d'une compétence propre de maîtrise de son environnement numérique.

À cet égard, ensuite, les anglo-saxons utilisent l'expression difficilement traduisible, sinon par une périphrase, d'« *empowerment* ». L'individu devrait être mis en situation de pouvoir contrôler et décider de la collecte

et de l'usage de ses données. De façon assez étonnante, ce mot fait écho au doit à l'autodétermination informationnelle que la Cour constitutionnelle de Karlsruhe a consacré dans une décision de 1983 faisant du droit à la vie privée une prérogative de chacun constitutionnellement protégée. La jurisprudence du Conseil Constitutionnel n'est jamais allée aussi loin et si le droit à la vie privée a été reconnu par un travail d'interprétation de l'article 2 de la Déclaration de 1789 sur la liberté individuelle, c'est sans grand éclat ni, en vérité, sans jamais véritablement donner aux données personnelles une assise forte, distincte du concept de vie privée alors pourtant que les deux ne sont pas réductibles l'un à l'autre[13]. Cependant, le Conseil d'État dans son rapport de 2014 sur le numérique et les droits fondamentaux[14] a suggéré que le droit français reconnaisse le droit à l'autodétermination informationnelle et la loi sur la République numérique votée en 2016 a suivi cette recommandation puisque son article 54 dispose que « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ».

On le voit, ici, l'enjeu n'est pas seulement de définir le droit à la vie privée comme un droit défensif mais aussi comme un principe actif. D'une certaine façon, le droit à l'oubli, d'abord issu de la jurisprudence de la CJUE avant d'être consacré par le RGDP, ou bien le droit à la portabilité – permettant à un consommateur de rapatrier ses données traitées par un service de communication électronique type messagerie internet pour migrer vers un autre prestataire – sont des traductions législatives ou réglementaire de cette volonté de rendre à chacun le pouvoir de ne pas être totalement soumis à la puissance de la technologie. De façon ambivalente, la *blockchain* constitue une évolution technologique fondée sur le *peer to peer* ouvrant sur une forme d'affranchissement des rapports juridiques et sociaux à l'égard des institutions, mais renvoyant à une autonomisation de la technologie.

13. *On regrettera ici la très décevante décision du Conseil Constitutionnel sur la loi relative au renseignement (Décision n° 2015-713 DC du 23 juillet 2015) alors que l'occasion était donnée, indépendamment des hypothèses de censure ou non, de poser les fondements d'un droit des données personnelles adaptés aux défis à venir.*
14. *Conseil d'État, Rapport annuel 2014, La Documentation Française*

Cela étant, pour éviter la désillusion qui naîtrait du remplacement d'oligarchies épuisées par de nouvelles maîtrisant les codes des élites numériques, il faut s'assurer que chacun peut pleinement bénéficier des potentialités offertes par les technologies. Ainsi, la volonté d'étendre l'apprentissage du code à l'école, dès la primaire, participe du besoin vital pour nos sociétés, non pas de faire de chacun un développeur ou un ingénieur, mais à tout le moins un citoyen maîtrisant la grammaire et les principes d'écriture et de compréhension du monde informationnel. Donner à chacun les moyens de se réaliser, passera par la démocratisation de l'intelligence artificielle

Dans ce monde en mutation, l'individu a donc toujours besoin de la garantie de ses droits. D'où la permanence du principe de souveraineté étatique.

3. La nécessaire permanence de la souveraineté de l'État

La souveraineté étatique existe encore et c'est tant mieux. Trois illustrations permettent de la rencontrer.

D'abord, on rappellera que les États peuvent encore produire des régulations s'appliquant au monde numérique. Celles-ci peuvent être interétatiques, comme le montre l'élaboration du règlement sur la protection des données personnelles[15] qui fixe un cadre européen, et des standards sans doute à portée mondiale. Dans le fil, le débat actuel sur le "*free flow of data*" montre bien cependant que la réglementation ne doit pas contraindre la libre circulation des données nécessaire à l'économie de l'innovation. Microsoft a fait le choix d'investir dans de nombreux data center en Europe, dont plusieurs en France. Cela ne signifie pas pour autant qu'il faille imposer un protectionnisme à la data en limitant les potentialités d'innovation et de croissance, ce dont les entreprises françaises et européennes seraient les premières victimes à termes.

15. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Ensuite, l'adoption du *Privacy Shield* a montré que la question du transfert international des données conserve aux États un rôle important. Suite à l'arrêt *Schrems*[16] aboutissant à l'annulation du "*Safe Harbor*", s'est reposée la question de savoir comment garantir la protection efficace lorsque les données circulent dans le monde. Il importe donc que celles-ci bénéficient, où qu'elles soient, d'un même niveau – ou à tout le moins d'un niveau équivalent – de protection. La décision dite d'adéquation prévue par le droit européen participe de cette logique. Le *Safe Harbor* a ainsi été remplacé par le "*Privacy Shield*", adopté le 8 juillet 2016. Il s'agit là d'une décision prise par la Commission qui a estimé qu'à travers les règles prévues par cet accord entre l'Union Européenne et les États-Unis, un niveau équivalent de protection pour les données existe outre-Atlantique. Ainsi, les entreprises qui s'enregistrent[17] dans le cadre du *Privacy Shield* certifient [c'est un processus d'auto-certification] qu'elles en respectent ses prescriptions. L'Europe et ses États membres ont vraiment pesé dans les négociations et ont réussi à obtenir des avancées fortes de la part de l'Administration du Président Obama. L'une d'elles consiste en la création d'un *Ombudsperson*, c'est-à-dire une personne nommée par le gouvernement américain chargée de recevoir les éventuelles réclamations de citoyens européens qui craindraient de faire l'objet d'une surveillance illégitime de leurs données de la part des États-Unis. Ainsi, le *Privacy Shield* constitue un net progrès par rapport au *Safe Harbor*. Au demeurant, une procédure de revoyure doit intervenir à l'automne 2017 afin de s'assurer que les conditions de sa mise en œuvre demeurent satisfaisantes.

Par ailleurs, les révélations d'Edward Snowden ont placé sous les feux de la rampe la problématique de l'accès aux données par les gouvernements. Là aussi la souveraineté revient sur le devant de la scène. Pour Microsoft, cela passe d'abord par l'affirmation d'une règle simple et ferme : nous ne donnons pas d'accès généralisé aux données que nous stockons ou traitons et c'est pour cela, aussi, que nous considérons le chiffrement comme une garantie nécessaire. Nous répondons, bien sûr, aux réquisitions judiciaires à la condition qu'elles soient pleinement conformes à la loi. C'est en application de ce principe, d'ailleurs, que Microsoft s'est opposé, il y a

16. http://curia.europa.eu/juris/document/document.jsf?docid=169195
17. Microsoft a adhéré au mécanisme très vite après son adoption.

deux ans maintenant, à une demande du FBI d'accès aux données d'un de nos clients stockés en Irlande formulée dans le cadre d'une investigation criminelle, aux motifs que cette demande méconnaissait les principes de "*privacy*" et que, de surcroit, elle était de nature à violer la souveraineté de l'État irlandais. Dès lors que les données circulent, peuvent être localisées sur le territoire de différents États, il est nécessaire de définir le droit applicable dans les relations entre États souverains. Dans le cadre de cette procédure, la Cour d'appel de New York a donné raison à Microsoft par un arrêt du 14 juillet 2016[18]. Microsoft a reçu le soutien de plus de 50 organisations y compris des ligues de défense de droit civil et politiques, des industriels, des parlementaires européens, l'État irlandais etc., certains produisant même des *Amici Curiae* disponibles sur le site créé pour cette cause[19].

Ainsi, la souveraineté perdure dans le monde numérique. Dans ladite affaire, le juge Gerard Lynch, l'un des membres de la Cour d'appel de New-York, dans son opinion concordante, a indiqué que « *nous vivons dans un monde d'États souverains interdépendants où chaque État, chaque pays a ses propres idées, ses propres intérêts légitimes, parfois contradictoires avec les nôtres* ». On trouve là un écho aux propos du juge de la Cour suprême américaine, Stephen Breyer qui, en 2015, dans son livre "*The Court and the World*" et dans un article du Wall Street Journal, mettait lui aussi en avant le besoin d'harmonie entre les Nations.

Cette décision de la Cour d'appel de New York aura montré que s'agissant des règles applicables aux données circulant dans le monde au regard des prérogatives régaliennes des États, il convient de trouver un nouveau cadre juridique permettant de concilier les droits fondamentaux et le cadre de leur protection aux niveaux national, européen et international. Quel est le modèle pertinent qui permet à la fois de protéger les libertés, de respecter la souveraineté des États, de garantir la sécurité ? Est-ce que ce mécanisme passe par un grand traité multilatéral ou par une rénovation des MLAT ("*Mutual Legal Assistance Treaties*" ou traités de coopération judiciaire internationale). Est-ce que cela passe, au préalable, par une harmonisation du droit européen ou par des coopérations

18. https://www.justice.gov/opa/blog-entry/file/937006/download

19. www.Digitalconstitution.com. Le gouvernement américain a finalement décidé de saisir la Cour suprême. On devrait savoir vers octobre 2017 si l'affaire est retenue.

renforcées permises par le Traité de Lisbonne reposant sur une logique de reconnaissance mutuelle ? À l'issue de la présidence néerlandaise de l'Union Européenne, il a été demandé à la Commission européenne de travailler sur ce sujet, notamment sur la « *e-evidence* », c'est-à-dire sur les conditions d'accès à des données susceptibles de constituer des éléments de preuve dans le cadre d'investigations pénales mais stockées dans des serveurs situés sur le territoire d'un État distinct de celui conduisant la procédure. Elle produira, en juin 2017, un rapport d'orientation et de recommandations faisant suite à son rapport intermédiaire prévu pour décembre 2016[20]. S'agissant de la mise en œuvre de compétences régaliennes, et sans anticiper les conclusions à venir, il y aura peut-être de la place pour l'exercice innovant de souverainetés partagées.

Décidément, le numérique est saisi par la géopolitique, à moins que ce soit l'inverse.

En effet, à cet égard, et au-delà de la question du droit des données personnelles, s'ajoute le sujet majeur de la cybersécurité, c'est-à-dire de la mobilisation de l'ensemble des moyens destinés à lutter efficacement contre les cybermenaces qui peuvent provenir de groupes de criminalité organisée ou bien même d'États. Celle-ci est désormais au cœur des préoccupations des pouvoirs publics et des opérateurs économiques, et aussi des citoyens. En Europe, la directive NIS[21] doit être transposée en 2018 au plus tard. Ce texte important permet de développer un certain nombre de règles de protection de systèmes d'informations de l'ensemble des acteurs, y compris des acteurs d'importance vitale pour les États. L'investissement dans la cyber sécurité est un vrai sujet et doit être une priorité pour les gouvernements comme pour les entreprises. Microsoft a beaucoup investi à cet égard en créant la "*Digital Crime Unit"* qui regroupe des ingénieurs, des juristes et des enquêteurs, pour essayer de développer des approches cohérentes pour la protection des données personnelles et la sécurisation des systèmes d'information, en repérant les réseaux de criminels, tels ceux qui mettent en place des réseaux de « *botnet* » [des réseaux d'ordinateurs dormants qui peuvent

20. Le Conseil Justice et Affaires intérieures du 8 juin 2017 a conclu à ce que la Commission propose de légiférer sur le sujet en 2018.
21. http://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

être activés et faire circuler des virus au niveau mondial]. DCU peut interagir avec les gouvernements, en travaillant avec les autorités pour démanteler des réseaux, dans des cas de cyber criminalité sous investigation criminelle.

Néanmoins, il importe d'aller plus loin.

Nul doute que c'est d'un cadre global dont nous avons collectivement besoin et il est certain qu'une réponse internationale devient de plus en plus nécessaire. Sans doute pourrait-elle passer par la mise en œuvre d'une « *Convention de Genève pour la sécurité numérique* ». Ce sera certainement un sujet pour les années à venir afin d'établir de nouvelles règles claires respectueuses des équilibres propres à la souveraineté des États tout en favorisant la libre circulation de l'information et des données dans un cadre sécurisé et garantissant les droits fondamentaux des citoyens.

La souveraineté n'est pas le souverainisme.

La première renvoie à la garantie des droits fondamentaux, le second au repli sur soi. L'une est ouverte sur le numérique, l'autre lui est antinomique. La transformation digitale au cœur de la 4e révolution industrielle nous invite à replacer l'individu au centre de toute réflexion et donc à faire de la souveraineté un moyen et non une fin. La forme étatique demeure fondamentale, et il serait vain tout autant que dangereux de la nier, mais nul ne peut ignorer la force de la décentralisation planétaire désormais en marche. Dès lors, dans un monde de plus en plus en réseaux, œuvrer pour que chacun puisse exercer son pouvoir sur la technologie afin de bénéficier de ses usages, passera certainement par l'émergence d'un patrimoine constitutionnel mondial, où les États auront un rôle majeur à jouer pour définir un nouveau cadre pour des pouvoirs et contre-pouvoirs adaptés au monde qui vient. Il est clair, à cet égard, que l'Europe jouera un rôle majeur dans la définition de la souveraineté à l'ère numérique.

Une approche philosophique du concept émergent de souveraineté numérique

Par Pierre-Yves Quiviger,
Professeur des universités,
Directeur du Centre de Recherches en Histoire des Idées (CRHI, EA 4318),
Département de philosophie, Université de Nice

La principale difficulté par rapport à la notion de souveraineté numérique tient à l'ambivalence d'une formule à laquelle la langue française permet d'accorder deux acceptions.

D'abord la souveraineté *sur* le numérique, le numérique étant alors ce sur quoi porte la souveraineté, ou le champ dans lequel la souveraineté peut rencontrer une limite ou avoir vocation à se manifester plus fermement (ou non).

Mais pour la langue française, au-delà de cette acception qui relève du génitif objectif, ou du complément du nom – la souveraineté portant sur le numérique, dans le champ numérique, etc. – l'adjectif associé au substantif permet aussi de qualifier le substantif : la souveraineté peut être *numérique* comme on parle d'une robe *rouge* ou d'un homme *sympathique*. C'est selon cette même structure grammaticale qu'on a pu distinguer, après Carré de Malberg, une souveraineté populaire et une souveraineté nationale, qui ne sont en rien des souverainetés portant *sur* le peuple ou la nation mais des souverainetés *du* peuple ou *de* la nation, autrement dit exercées par le peuple ou la nation (je ne discute pas ici de la pertinence de cette distinction, ce n'est pas mon propos). On aurait alors un autre sens de l'expression « souveraineté numérique » à savoir, en un sens minimaliste, les manifestations *numériques* de la souveraineté (l'écart est alors mince mais non nul avec la première souveraineté, portant *sur* le numérique),

mais aussi, en un sens disons maximaliste, du *numérique souverain*, c'est-à-dire rien moins qu'un nouveau type de titulaire possible de la souveraineté.

À ce tableau déjà complexe s'ajoute la place de l'État et des États dans l'approche générale de la notion de souveraineté, numérique ou non. Si l'on regarde le *Lexique de droit constitutionnel* de Pierre Avril et Jean Gicquel pour trouver une définition simple de l'État, on trouve ceci :

> « Organisation politique et juridique de la nation qu'elle personnifie. L'État est une personne morale caractérisée par la détention de prérogatives de puissance publique et par sa soumission aux sujétions correspondantes. Sujet du droit international public caractérisé par un territoire, une population et l'existence d'un ordre juridique souverain (*souveraineté* de l'État)[1]. »

Cette définition doit être complétée par celles que donnent les mêmes auteurs de la souveraineté :

> « Signifie, négativement, l'absence de toute dépendance extérieure et de tout empêchement intérieur. Positivement, désigne le caractère suprême de la puissance étatique, et cette puissance elle-même, c'est-à-dire les pouvoirs effectifs compris dans la puissance de l'État. La souveraineté emporte donc à la fois l'indépendance dans l'ordre international (la souveraineté *de* l'État), le pouvoir exclusif et sans limite, sinon celles que *l'État de droit* s'assigne à lui-même, dans l'ordre interne (souveraineté *dans* l'État), et le contenu de ce pouvoir. Elle est l'apanage de l'*État*, à l'opposé d'une organisation internationale (*Union européenne*) qui ne peut bénéficier que de transferts de *compétences* consentis par les États membres[2]. »

On entrevoit bien dans cette définition la possibilité d'une *déconnexion* entre l'État et la souveraineté. Plusieurs positions sont possibles :

1) on peut considérer cette déconnexion comme impossible : dès lors que l'on renonce volontairement à exercer des compétences dans un domaine, on exerce sa souveraineté, on n'y renonce pas, même partiellement ;

1. P. Avril, J. Gicquel, *Lexique de droit constitutionnel*, Paris, PUF, 2003.
2. *Idem.*

2) on peut considérer cette déconnexion comme partielle et non-problématique : mais alors il faut quand même réussir à *légitimer* cette chose étonnante à savoir l'existence d'un morceau de souveraineté non-étatique ;

3) on peut considérer cette déconnexion comme partielle et néanmoins fortement problématique, car elle est en réalité la *fin de la souveraineté* qui, comprend, dans sa définition même, l'impossibilité de toute soumission à une autre souveraineté.

De quelle forme est cette déconnexion entre État et souveraineté, quand on parle de souveraineté numérique ? Parle-t-on d'un État souverain face à une réalité – le numérique – qui semble lui échapper ? Si cette réalité lui échappe, au bénéfice de qui ? Doit-on considérer qu'un État, du fait du numérique, se trouve éventuellement dépossédé d'une partie de sa souveraineté au bénéfice de sujets de droit privé (multinationales, etc.) ou bien qu'il s'en trouve dépossédé au bénéfice de l'État qui héberge les entreprises concernées ? Dans le premier cas, on pourrait plaider, dans un horizon libéral, que ce n'est qu'une manifestation comme d'autres des libertés individuelles et on pourrait, si on est libéral, se réjouir de ce qui serait moins dépossession de la souveraineté étatique qu'un développement d'activités extra-étatiques. Dans le second cas, il est difficile de ne pas s'inquiéter de voir se renforcer la puissance d'un autre État car cela revient à laisser s'accroître un rapport de force défavorable, avec des risques considérables en matière de sécurité nationale et un défaut de maîtrise du destin national.

Mais la relation avec l'État ne prend pas nécessairement la forme d'une dépossession, ou plutôt : même dans le contexte d'une dépossession, plusieurs solutions s'offrent à l'État concerné, qui engagent les différentes acceptions que j'ai dégagées de la souveraineté numérique. La première solution est d'identifier les atteintes portées à la souveraineté *à l'occasion* ou *dans le cadre* du développement du numérique, en définissant de manière explicite ce qu'on pourrait appeler les *données ou réalités sensibles* afin de limiter leur disponibilité. Cette identification accomplie, l'État doit déterminer ce qu'il peut faire : d'un point de vue technique, du point de vue du respect des libertés individuelles, du point de vue des contraintes qu'il a acceptées dans le cadre international. Ces trois leviers sont évidemment distincts : un État peut ne pas pouvoir (du fait d'engagements internationaux) ou ne pas vouloir (par respect pour les libertés individuelles) accomplir ce qui est néanmoins à sa portée techniquement. Il n'y a ainsi

aucune raison de supposer que l'État français soit, *sur le plan de l'informatique,* moins capable que la Chine de limiter l'accès des citoyens français à Internet. On voit bien, avec cet exemple, que la grande difficulté de cette solution tient à son parfum liberticide et éventuellement paternaliste. Il n'est pas sûr qu'une telle solution soit viable politiquement. Elle rencontre aussi sa limite dans la grande liberté de circulation dont jouissent – et tant mieux – les citoyens français. Et, en tout état de cause, cette solution revient à assumer un rôle purement négatif et passif : gendarmer, circonscrire, fermer le robinet.

Une autre solution, plus stimulante, consiste à développer numériquement la souveraineté, c'est-à-dire non pas à « protéger » la souveraineté *contre* un numérique supra-étatique et supra-souverain mais à investir le champ du numérique de telle manière que la maîtrise soit conservée sur les réalités sensibles que j'évoquais. Évidemment, cela est plus facile à dire qu'à faire, pour plusieurs raisons. La première est factuelle : il est difficile de défaire le passé et de porter atteinte à des monopoles ou quasi-monopoles qui ont connu des réussites exceptionnelles. La deuxième est technique : barricader, sécuriser, même si cela marche plus ou moins bien, revient à se situer face à des technologies déjà développées. Ce dont on parle suppose que soient inventées non seulement d'autres technologies, d'autres supports, mais que ceux-ci soient susceptibles néanmoins de s'insérer dans un contexte mondialisé. La troisième est conceptuelle : c'est l'idée même de souveraineté qu'il faut repenser puisque, comme je l'ai dit plus haut, il s'agit bien ici d'autre chose que de la manière dont la souveraineté fait face au numérique, ou lui résiste ou l'accompagne. Le défi est celui de la construction d'un numérique souverain entendu non plus comme un numérique unique (en réalité américain) mais comme un univers numérique dans lequel cohabiteraient plusieurs souverains, de même que cohabitent plusieurs États sur Terre. Je ne veux évidemment pas dire par là que ces souverains numériques devraient être distincts des États, mais simplement qu'un État ne saurait être souverain numériquement comme il est souverain politiquement. Le défi, redoutable, à relever passe par un dialogue entre droit et informatique : les juristes vont devoir inventer une nouvelle modalité de la souveraineté, capable de s'adapter à ce que les informaticiens pourront décrire en termes de possibilité et d'impossibilité technique et, pour parler comme un philosophe, d'*ontologie du réseau*.

Cette révolution conceptuelle n'est pas neuve dans l'histoire de la souveraineté, celle-ci ayant dû plusieurs fois se remodeler, en particulier en fonction des évolutions géopolitiques – songeons à la question européenne, ou à un phénomène comme la justice pénale internationale. La notion de souveraineté a vocation à conserver une certaine ductilité et la révolution numérique est aussi stimulante intellectuellement – et économiquement – qu'elle est inquiétante matériellement. N'oublions pas que la souveraineté ne doit jamais être confondue avec ses *attributs* – son premier grand théoricien, Jean Bodin, en 1566, dans sa *Methodus ad facilem historiarum cognitionem*, donnait une liste de ses attributs qui nous paraît aujourd'hui à la fois incomplète et problématique :

> le premier et le plus important est de nommer les hauts magistrats et de définir à chacun son office ; le second est de promulguer ou d'abroger les lois ; le troisième de déclarer la guerre et conclure la paix ; le quatrième de juger en dernier ressort par-dessus tous les magistrats et le dernier d'avoir droit de vie et de mort aux endroits mêmes où la loi ne prête pas à la clémence[3].

Mais cette liste datée (pas intégralement, cela va sans dire) est indissociable d'une définition plus générale de la souveraineté qui, elle, demeure vivante et peut encore nous aider à penser la souveraineté, y compris numérique :

> La puissance de donner loy à tous en général, et à chacun en particulier : mais ce n'est pas assez, car il faut adjouster, sans le consentement de plus grand, ni de pareil, ni de moindre que soy : car si le prince est obligé de ne faire loy sans le consentement d'un plus grand que soy, il est vray suject : si d'un pareil il aura compagnon : si des sujets, soit du Senat, ou du peuple, il n'est pas souverain[4].

3. Jean Bodin, *La méthode de l'histoire,* Corpus général des philosophes français, PUF, 1951, p. 359.

4. Jean Bodin, *Les 6 livres de la République,* I, 10, Corpus de la philosophie de langue française, Fayard, p. 306. On trouve aussi dans ce livre une célèbre définition de la république : « un droit gouvernement de plusieurs mesnages, et de ce qui leur est commun, avec puissance souveraine » (I, 1, p. 27).

Réflexions introductives sur le concept de souveraineté numérique

Par Dominique Rousseau,
Professeur à l'Université Paris I Panthéon Sorbonne,
Président du Conseil scientifique de l'AFDC

Cet ouvrage est le fruit d'un colloque organisé à la Faculté de Droit et Science politique de Nice le 7 octobre 2016, sous l'égide de l'Association Française de Droit constitutionnel (AFDC) et qui fait d'ailleurs écho à un précédent colloque niçois consacré en 2008 à l'e-démocratie. L'AFDC regroupe les enseignants, chercheurs, doctorants qui travaillent sur le droit constitutionnel, mais aussi tous ceux qui pratiquent le droit constitutionnel, notamment les membres du Conseil constitutionnel, les administrateurs des assemblées, les praticiens et désormais les avocats, depuis l'avènement de la QPC. Notre association a pour politique scientifique de choisir chaque année un thème de réflexion soumis aux centres de recherche en droit constitutionnel. Après l'élection présidentielle, les rapports entre droit constitutionnel et droit international, ou les relations entre le droit constitutionnel et les autres disciplines (mathématiques, économie, psychanalyse..), c'est l'impact du numérique sur le droit constitutionnel qui a été choisi pour 2016. Les Professeurs Pauline Türk et Julien Bonnet ont été sollicités pour définir la problématique soumise aux constitutionnalistes pour l'année 2016, à charge pour les pôles de droit constitutionnel de s'en saisir dans le cadre de manifestations. La Faculté de droit de Nice retrouve ainsi sa place dans la recherche en droit constitutionnel, au travers notamment des travaux organisés lors du colloque dont cet ouvrage est issu.

Les effets d'Internet et des technologies du numérique sur le droit constitutionnel ne sont pas une question classique pour les constitutionnalistes. Si d'autres disciplines se sont saisies du sujet, les constitutionnalistes ont tardé à s'ouvrir à ces objets nouveaux de la science constitutionnelle,

accompagnant un glissement ou un basculement de l'objet du savoir constitutionnel vers des questions de société. Tout ce qui affecte le fonctionnement de la Société interroge le droit constitutionnel, conformément à l'article 16 de la Déclaration de 1789 et au lien ontologique qui existe entre Société et Constitution. La forme étatique n'est qu'un moment historique de l'organisation politique des sociétés. Les sociétés ne se sont pas toujours organisées sous la forme « État ». Elles ne s'organiseront peut être plus sous la forme « État ». En revanche il y aura toujours une constitution, parce qu'il n'y a pas de société sans constitution. Or si l'objet du savoir constitutionnel est la société – les pouvoirs qui y sont à l'œuvre, leur séparation, la garantie des droits des citoyens contre ces pouvoirs – la réflexion doit inclure le phénomène numérique. Comment s'organisent les pouvoirs, économique, technique, politique, financier, qui s'exercent dans le monde numérique ? Comment le phénomène internet bouscule-t-il la science constitutionnelle en bousculant toutes les activités sociales ? L'élaboration des lois et même des constitutions (Islande, Sri Lanka, peut être la Catalogne demain..) font intervenir les internautes sur des plateformes dédiées. Les constitutionnalistes doivent se saisir, même avec retard, même difficilement, de la question numérique, devenue centrale pour le fonctionnement démocratique et pluraliste de nos sociétés.

Le thème précis de la souveraineté numérique, interroge tout particulièrement le constitutionaliste. Le concept de souveraineté est-il pertinent pour penser la révolution numérique ? Il s'agit là d'une vraie question. On peut *a priori* en douter. Le principe classique de souveraineté a été construit par Jean Bodin en 1576, dans son ouvrage classique « Les six livres de la République », comme une arme de combat idéologique. C'est un intellectuel organique qui invente le concept de souveraineté pour permettre au roi de se dégager à la fois des seigneurs féodaux et du pape. Et pour affirmer le pouvoir royal, il faut inventer un concept, un instrument : la souveraineté, qui permet de construire l'État. Faut-il, dès lors, s'appuyer sur le concept de souveraineté, alors que les sociétés tentent de trouver d'autres formes que l'État pour s'organiser politiquement ? Comment penser la souveraineté économique à l'heure où les États concluent des contrats internationaux incluant des transferts de technologies ? Comment penser aujourd'hui la souveraineté politique ? La souveraineté au sens classique renvoie à la capacité de faire la loi, de juger, de battre monnaie

et de décider de la paix et de la guerre. Or les lois ne sont plus tant faites par les parlements nationaux que par des organismes supranationaux. Les jugements sont rendus par des juges européens ou internationaux. La monnaie est européenne. La politique de défense est définie dans le cadre de nos engagements internationaux, notamment l'ONU et l'OTAN.

Peut-être y a-t-il d'autres concept à promouvoir, tels le principe de coopération loyale, issu du droit européen, qui pourrait être un principe structurant du monde numérique ? Dans le prolongement des travaux de Mireille Delmas Marty sur « l'en-commun », Internet pourrait être un bien commun de l'humanité soumis à un droit global qui relèverait du principe de coopération loyale plus que du principe de souveraineté ? Au-delà du concept de souveraineté classique en droit constitutionnel, il est question, ici, d'un concept encore plus énigmatique et controversé : celui de « souveraineté numérique ». Il s'agit, sans parti pris, d'étudier les contours et enjeux de cette notion, afin d'établir si sa consistance juridique est suffisante pour constituer un outil de réflexion sur le sujet. Les contributions de juristes et de spécialistes issus d'univers très différents devraient permettre de nous éclairer.

La « souveraineté numérique » : un concept pertinent en droit constitutionnel ?

Par Pauline Türk,
Professeur de droit public, Faculté de Droit et Science politique de Nice, Université Côte d'Azur, dir. adj. CERDACFF, EA n° 7267

En février 2017, le Danemark a annoncé la nomination d'un ambassadeur auprès des géants mondiaux du numérique, considérant que les GAFA[1], en particulier, ont désormais la puissance d'États souverains et doivent être appréhendés comme des partenaires dans les relations diplomatiques[2]. Ce mélange des genres a suscité autant d'émois que de critiques, à l'heure de la prise de conscience de l'emprise exercée par ces nouveaux acteurs sur le monde économique, politique, diplomatique.

Après la Chine, l'Inde et la Russie, l'Union européenne se préoccupe de développer ses propres moteurs de recherche ou de se doter d'un système d'exploitation (OS) souverain[3], en même temps qu'elle vient d'élaborer

1. Soit Google, Apple, Facebook et Amazon, acronyme classique désormais, devenu GAFAMI avec l'ajout de Microsoft et d'IBM, auxquels s'ajoutent les NATU, c'est-à-dire Netflix, Air BNB, Telsa et Uber.
2. Annonce du ministre danois des Affaires étrangères, Anders Samuelsen, cf. A. Feertchak, « Le Danemark aura un ambassadeur dans la Silicon Valley », Le Figaro, 8 mars 2017.
3. Certains États sont parvenus à développer des moteurs de recherche concurrents aux moteurs américains, qui conservent cependant la prédominance (voir parts de marché respectives de Google, Yahoo, Baidu, Yandex, Bing, Guruji, Qwant..). En revanche, 90 % des ordinateurs personnels et appareils mobiles à travers le monde fonctionnent sur la base d'un système d'exploitation (Operating system ou OS, ensemble de programmes informatiques et de logiciels permettant

un nouveau Règlement général de protection des données personnelles (RGDP, en vigueur en 2018) et de négocier avec les États Unis un nouveau "Privacy shield"[4], afin de mieux protéger les données personnelles des internautes européens. De nombreux autres États tentent de mettre sur pied des politiques industrielles défensives et/ou offensives qui permettraient à leurs citoyens et à leurs gouvernements de reprendre partiellement le contrôle de leur destin numérique[5]. En France, signe d'une préoccupation, l'article 29 de la loi du 7 octobre 2016 pour une République numérique prévoit l'élaboration par le gouvernement d'un rapport sur la création d'un Commissariat à la souveraineté numérique rattaché aux services du Premier ministre, chargé de concourir « à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège ».

Ces initiatives répondent à une problématique nouvelle : le changement de paradigme dans lequel s'exercent les compétences des États et les libertés des individus, à raison d'une dépendance croissante aux technologies du numérique et aux entreprises américaines qui les contrôlent, dans un espace déterritorialisé et dématérialisé. La diversité des domaines concernés (fiscalité, sécurité, défense, culture, commerce, économie, industrie, énergie, transport, protection des libertés), l'ampleur des conséquences engendrées pour les populations, l'incontestable suprématie technologique des géants de la Silicon Valley, conduisent certains observateurs à s'inquiéter d'une forme de « colonisation numérique » des cinq continents par des multinationales américaines érigées au rang de pouvoirs souverains[6].

---

l'utilisation d'un ordinateur) développé par Microsoft. Windows n'est concurrencé que par l'IOS d'Apple, Android ou Linux, et seuls la Chine ou l'Inde tentent réellement de développer leurs propres systèmes d'exploitation. C'est à l'échelle européenne que la France peut contribuer au débat de façon réaliste.

4. Nouvel accord sur le traitement des données personnelles entre l'UE et le département du commerce américain, entré en vigueur le 1er aout 2016 en remplacement de l'ancien mécanisme du « Safe Harbor », invalidé par la CJCE le 6 octobre 2015 pour cause de protection insuffisante des données personnelles des internautes européens.

5. Voir, au Brésil par exemple, la loi civile de l'Internet 12.965 du 23 avril 2014 dite « Marco Civil Da Internet ».

6. E. Sadin, *La siliconisation du monde. L'irrésistible expansion du libéralisme numérique*, éd. L'échappée, 2016, 256 p.

Devant ces nouvelles réalités, le droit tente de s'adapter et certaines de ses branches doivent être profondément reconfigurées. Le droit constitutionnel n'est pas épargné, et certains de ses fondements sont ébranlés[7]. Il réserve classiquement aux États les attributs de la souveraineté et retient l'État comme seul cadre d'exercice de la puissance souveraine unique et indivisible. Celle-ci trouve sa source dans le peuple ou la nation, ce qui légitime l'exercice d'un pouvoir de commandement suprême et indépendant sur la population dans le cadre de frontières physiques délimitées. Cette conception apparaît, aujourd'hui, largement dépassée.

Dans une ère post-moderne où triomphe la logique des réseaux interconnectés, le concept de souveraineté est affecté par la remise en cause de certains attributs de la souveraineté étatique et par l'affirmation d'autres formes de pouvoirs. Le principe de souveraineté des États se heurte aux effets d'une révolution technologique qui modifie ses contours et affaiblit son essence. Sa conception classique est également confrontée à l'émergence d'un concept encore hypothétique et quelque peu énigmatique, qu'il s'agit ici d'appréhender : celui de « souveraineté numérique ». Cette notion est-elle significative et pertinente en droit, et particulièrement en droit constitutionnel ? L'est-elle pour appréhender les phénomènes à l'œuvre dans le « plus vaste espace non gouverné du monde »[8] ? La souveraineté numérique doit-elle être pensée en relation avec l'État, ou la réflexion sur le sujet conduit-elle à découpler la notion de souveraineté de celle d'État ? S'agit-il, encore, dans ce cas, de souveraineté ? Afin d'éclairer la notion de souveraineté numérique, nous allons ici tenter d'en retrouver les origines, d'en déterminer les contours, et d'en cerner les enjeux, afin d'introduire les travaux issus du colloque organisé à Nice le 7 octobre 2016 par le CERDACFF[9], sous l'égide de l'Association Française de Droit Constitutionnel.

---

7. J. Bonnet, P. Türk, « Le numérique : un défi pour le droit constitutionnel », *Nouveaux cahiers du Conseil constitutionnel*, n° 57, 2017 ; P. Türk, « La souveraineté des États à l'épreuve d'Internet », RDP, n° 6, 2013, p. 1489.

8. Voir l'ouvrage du PDG de Google, E. Schmidt et J. Cohen, *À nous d'écrire l'avenir*, Denoël, 2013, p. 12.

9. Centre de Recherche en Droit Administratif, Constitutionnel, Financier et Fiscal EA n° 7267. Remerciement aux doctorants du CERDACFF pour leur contribution à l'organisation du colloque, et particulièrement à Jocelyn Lafaye pour sa contribution à la préparation de cet ouvrage.

1. Les origines de la notion de souveraineté numérique

La notion de souveraineté apparaît en France au XVI^e siècle avec Jean Bodin[10], puis Charles Loyseau, en lien avec l'État car « la souveraineté est du tout inséparable de l'État », elle est « la forme qui donne l'être à l'État »[11]. La souveraineté en droit public est bien celle de l'État, dont c'est la caractéristique essentielle que d'être souverain[12]. La souveraineté de l'État renvoie à son pouvoir légitime de commander et de se faire obéir sur son territoire et par sa population, à sa capacité à se déterminer librement, à traiter à égalité avec les autres États, à n'être pas subordonné et à n'accepter que les limites auxquelles il a consenti. Comme l'écrit Louis Le Fur, « la souveraineté est la qualité de l'État de n'être obligé ou déterminé que par sa propre volonté, dans les limites du droit qu'il s'est fixées[13]. La souveraineté de l'État, c'est enfin l'exercice par un État indépendant de compétences régaliennes rattachées à la puissance publique[14]. Mais la notion de souveraineté, complexe et polysémique, renvoie aussi, en droit constitutionnel, à la source légitime de ce pouvoir suprême. La souveraineté est aussi celle d'une nation ou d'un peuple qui entend s'autodéterminer et s'autogouverner, afin de conserver la maîtrise de son destin. La souveraineté nationale ou populaire est indivisible et s'incarne dans les institutions de gouvernement d'un État, cadre de son exercice. L'unité de la notion est ainsi préservée, dans son rapport avec le cadre étatique.

C'est précisément ce lien entre la souveraineté – pouvoir de commandement suprême – et l'État qui a été affaibli dès le XX^e siècle, sous l'effet de différents facteurs bien connus, liés au développement des organisations internationales, à la construction européenne, à la mondialisation des échanges et à la globalisation du droit. Les États se retrouvent bientôt

10. J. Bodin, *Les Six livres de la République*, 1576.
11. C. Loyseau, *Traité des seigneureries*, ch. 2, n° 4, 1608.
12. O. Beaud, *La puissance de l'État*, PUF, 1994, p. 14 ; P. Nguyen Quoc Dihn, P. Daillier, A. Pellet, *Droit international public*, LGDJ, Paris 2002 ; J. Salmon, *Dictionnaire de droit international public*, Bruylant, 2001, p. 1045.
13. L. Le Fur, *État fédéral et confédération d'États*, 1896.
14. R. Carré de Malberg, *Contribution à la théorie générale de l'État*, 1920.

interdépendants les uns des autres sur les plans économique et politique, concurrencés dans leurs prérogatives par le haut (organisations internationales et institutions européennes) et par le bas (collectivités locales, décentralisation). Si pour certains, la souveraineté des États est redéfinie, transférée, partagée ou mutualisée, et finalement renforcée par l'effet de transferts de compétences consentis et de règles communes choisies, pour beaucoup d'autres, elle est plutôt affaiblie, concurrencée, contournée, démembrée ou menacée.

Et c'est bien le prisme retenu par ceux qui, encore assez rares, s'intéressent aux nouveaux bouleversements subis par le concept de souveraineté du fait de l'irruption de l'informatique dans tous les domaines grâce aux technologies du numérique. Le phénomène, daté de la fin des années 1990, s'amplifie avec la progression d'Internet, qui réunit 3,7 milliards d'utilisateurs en 2017, et devrait prendre des proportions difficilement imaginables avec l'avènement des objets connectés et l'irruption des algorithmes et de l'intelligence artificielle dans un nombre croissant de secteurs[15] (santé, défense, culture, transport, loisirs). Les échanges transnationaux d'idées, de biens et de services se développent ; les modes de pensée et de consommation évoluent grâce aux réseaux sociaux et aux plates formes collaboratives ; les conditions d'exercice des activités politiques, économiques, industrielles, culturelles se transforment. Les États sont affaiblis et concurrencés dans le service rendu aux citoyens, contrepartie de la soumission aux lois et à l'impôt. En effet, rares sont les domaines dans lesquels l'exercice des compétences de l'État n'est pas conditionné, désormais, par sa dépendance aux réseaux numériques et à ceux qui les gouvernent : politiques monétaires et fiscales, défense, systèmes sociaux, politique industrielle, systèmes de santé, énergie, culture, éducation, information et communication, transport, et même conservation des archives… Les États peinent également à assurer leur mission première de protection des droits et libertés des citoyens, d'autant que leurs moyens d'action sont contraints – et heureusement – par la nécessité de respecter les principes libéraux qui structurent les réseaux numériques. Ils rencontrent, on le sait, des difficultés à faire respecter le droit (sécurité et ordre public, droit

15. « Pour une intelligence artificielle maîtrisée, utile et démystifiée », rapport de l'Office parlementaire des choix scientifiques et techniques, n° 464, 15 mars 2017 ; D. Cardon, « À quoi rêvent les algorithmes », éd. du Seuil, 2015.

commercial, droit d'auteur, droit à la vie privée, droit à la protection des données personnelles..) sur des réseaux transnationaux et dématérialisés, face à des contrevenants aux multiples visages, parfois lourdement armés techniquement et/ou juridiquement (État espion, hackers malveillants, services secrets au travail, entreprises commercialement intéressées, utilisateurs diversement inspirés..). Ce sont enfin les modalités de leur action qui sont ébranlées : compte tenu de l'architecture des réseaux et de leurs modes de gouvernance, les États sont en effet confrontés à de nouveaux modes de régulation qui font la part belle aux acteurs privés et remettent en cause le paradigme de l'expression unilatérale, verticale et contraignante du pouvoir normatif des États[16]. Les sociétés politiques doivent dorénavant composer avec l'existence d'un monstre tentaculaire virtuel qui influence très concrètement la vie quotidienne des citoyens, le fonctionnement des administrations, le contenu des politiques publiques. C'est d'autant plus stimulant et préoccupant que les fondements, les modes de gouvernance et de régulation, les codes et les règles du jeu, échappent pour l'essentiel aux États comme aux utilisateurs de ces technologies.

Une série de questionnements agitent ceux qui s'intéressent aux phénomènes précédemment décrits : est-on souverain sur les réseaux ? Qui l'est ? À quelles conditions peut-on le devenir ? Peut-on se déterminer librement et choisit-on les règles auxquelles on se soumet ? Se demander qui décide et qui gouverne dans le monde numérique, et avec quelle légitimité, c'est questionner la souveraineté. Toute communauté humaine, avant même la construction de la société politique, aspire à la maîtrise de ses actes et de son destin. Le principe d'auto-détermination des peuples s'ajoute à la théorie de la souveraineté populaire. Mode d'organisation privilégié des sociétés politiques, l'État devient, dans la théorie du droit constitutionnel, le cadre d'expression du pouvoir politique du peuple sur un territoire. En découle une réflexion sur les principes démocratiques de gouvernement permettant de garantir la légitimité et la représentativité des gouvernants et la protection des droits des citoyens gouvernés. La réflexion sur la

16. B. Barraud, *Repenser la pyramide des normes à l'ère des réseaux*, L'Harmattan, 2002 ; F. Ost et M. Van de Kerchove, *De la pyramide au réseau ? Pour une théorie dialectique du droit,* Publications des Facultés universitaires Saint-Louis, Bruxelles, 2002, 596 p.

souveraineté numérique s'inscrit dans cette perspective : celle du refus de voir les peuples, les communautés d'utilisateurs, les États, les individus perdre le contrôle de leur destin au profit d'entités mal identifiées et non légitimes.

Sur le plan international, la question du contrôle des ressources Internet s'impose comme un enjeu majeur pour la souveraineté des États, soucieux de limiter l'hégémonie américaine sur la gestion du Réseau, notamment concernant les missions stratégiques de l'ICANN[17]. Ces préoccupations sont d'autant plus vives que cette domination historique des États-Unis s'accompagne d'une situation de quasi monopole technique et économique des multinationales américaines, qu'il s'agisse des systèmes d'exploitation informatiques ou du développement des applications numériques. L'expression même de « souveraineté numérique » est utilisée dès 2012, à l'appui des revendications de certains États exprimées lors de la Conférence mondiale des télécommunications internationales (CMTI 12) chargée d'adapter le droit international des télécommunications[18]. Celle-ci fut l'occasion de passes d'armes sur les modalités de gouvernance des réseaux, jugées trop favorables aux États-Unis. La revendication souverainiste s'exprime régulièrement, depuis, dans les différents forums internationaux consacrés au sujet (Netmundial de Sao Paulo en 2014, Conférence annuelle IGF de Bakou en 2012, Bali en 2013, ou Mexico en 2016 par exemple).

En France, parallèlement, l'expression « souveraineté numérique » se diffuse progressivement. Certains observateurs avisés appellent, dès 2006, à repenser le concept de souveraineté dont les « instruments fondamentaux deviendront bientôt indissociables des outils de la puissance

17. Société de droit californien à but non lucratif fondée en 1998 pour superviser la gestion du système des noms de domaine (DNS), ou système d'adressage permettant de rendre lisibles et compréhensibles les adresses informatiques, base des échanges sur internet. Son fonctionnement est progressivement « internationalisé » afin de limiter la dépendance aux États-Unis, notamment à compter du 1er octobre 2016, date d'expiration du contrat liant l'ICANN au département du commerce américain. cf. A. Guiton, « Samedi, l'Internet sera un peu moins américain », *Libération*, 30 septembre 2016.

18. Réunie à Dubaï du 3 au 14 décembre 2012, cette conférence organisée par l'UIT avait pour objet la révision du règlement des télécommunications internationales (RTI) et a associé 193 États membres de l'UIT et 800 entités du secteur privé.

technologique »[19]. Cela implique une refondation du projet démocratique, incluant la question de la gouvernance des réseaux informatiques et celle de l'élaboration d'une « Constitution de l'Internet » fondée sur des principes communs et formulés dans un accord international. L'expression sera ensuite popularisée par Pierre Bellanger, qui multiplie les interventions médiatiques à partir de 2008[20]. En juin 2009, lors d'un colloque organisé à l'Assemblée nationale, le ministre de l'Intérieur en exercice s'interroge publiquement sur le concept. Constatant que « la souveraineté de l'État s'exerce sur un territoire alors qu'Internet ignore les frontières étatiques », il se demande si « la souveraineté des États s'arrête là où commence l'espace numérique ? », avant d'affirmer au contraire la nécessité de « garantir la souveraineté numérique », c'est-à-dire d'« étendre à l'espace numérique le champ de l'état de droit »[21]. L'expression a depuis fait florès, utilisée au sein d'instances spécialisées (Conseil national du numérique, ARCEP, ANSSI[22]) et par des membres du gouvernement[23]. Elle est discutée lors des premières Assises de la souveraineté numérique en 2014, et incarnée depuis par l'Institut de la souveraineté numérique. Association fondée sur la loi de 1901, cet institut a été créé en 2014, après l'affaire Snowden, afin d'organiser la réflexion autour d'« une nouvelle façon d'organiser la vie de la Cité à l'âge du numérique ». Il a pour vocation « de faire connaître les enjeux de la souveraineté numérique au grand public et aux élus, ainsi que de proposer des mesures capables de

19. B. Benhamou et F. Sorbier, « Souveraineté et réseaux numériques », *Politique étrangère*, 2006/3 Géopolitique de l'Internet, p. 519 à 530 ; L. Lessig, *Code and others laws of Cyberespace*, NY, basic Books, 1999.
20. « La réponse à la crise : internet », *La tribune*, 13 octobre 2008 ; « De la souveraineté en général et de la souveraineté numérique en particulier », Les Échos, 30 août 2011 ; « Défendre la république numérique », Le Monde, 14 janvier 2015.
21. M. Alliot-Marie, Colloque du 17 juin 2009 organisé par la Fondation Prométheus à l'Assemblée nationale.
22. Agence nationale de sécurité des systèmes informatiques, dont la mission est notamment de « préserver notre souveraineté et notre autonomie de décision et d'action dans les domaines politique, diplomatique et militaire et de protéger l'ensemble de nos infrastructures critiques », wwwssi.gouv.fr/agence/missions.
23. Interview F. Pellerin, ministre de l'Innovation et de l'Économique numérique, *L'express*, 12 novembre 2012. Par la suite, l'expression a été employée par les ministres successifs en charge du Numérique et de la Défense, puis plus généralement par les autres membres du gouvernement.

promouvoir la souveraineté, tant collective qu'individuelle, sur les structures immatérielles et en premier lieu sur les données », et publie les « Cahiers de la souveraineté numérique ». Enfin, les débats sur la loi du 7 octobre 2016 pour une République numérique, débutés en octobre 2014, ont consacré la notion, notamment dans le cadre des discussions relatives à la création d'un « Commissariat à la souveraineté numérique »[24].

La réflexion s'enrichit et se complique à la fois, du fait de l'évidente dimension européenne de la question : la mission de contrôle et d'information (MCI) sénatoriale intitulée « Nouveau rôle et nouvelle stratégie pour l'UE dans la gouvernance mondiale de l'Internet »[25] l'a bien montré, après plusieurs rapports parlementaires sur la cyberdéfense et l'économie numérique, et un rapport sénatorial très médiatisé intitulé « l'Union européenne, colonie du monde numérique ? »[26]. Les institutions européennes sont invitées à se saisir de ces questions, certains responsables européens appelant à un « réveil européen » sur le sujet[27]. Un colloque organisé à Rennes en 2014, intitulé « Droits et souveraineté à l'âge de l'Internet : quels défis pour l'Europe ? »[28] proposait également de réfléchir à la façon dont l'Europe doit « s'affirmer en raison de sa dimension, de ses compétences et de ses valeurs » face aux différentes formes de domination technique, économique et politique qui s'exercent sur Internet. La souveraineté numérique n'est pas seulement étatique, elle devient européenne…

---

24. Article 29 de la loi. P. Bellanger, « Pourquoi un commissariat à la souveraineté numérique ? », *Le point*, 15 février 2016 ; F. Pellegrini, « Souveraineté numérique : le recours aux logiciels libres constitue la seule alternative viable », *Le Monde,* 26 juin 2016 ; E. Berreta, « La souveraineté numérique : ce dossier qui effraye Hollande et Valls », *Le Point*, 13 janvier 2016 ; B. Benhamou, « Les contresens de la souveraineté numérique », *Les échos*, 29 janvier 2016.

25. Rapport d'information, « L'Europe au secours de l'Internet », Sénat, n° 696, 2 tomes, 8 juillet 2014.

26. Rapport d'information au nom de la commission des affaires européennes, Sénat, n° 443, 20 mars 2013.

27. V. Reding, député européenne et ancienne vice présidente de la Commission européenne, interview, Libération, 10 mai 2016 ; M. Schulz, président du parlement européen, cf. « La NSA espionnait aussi l'Union européenne », *Le Monde*, 1er juillet 2013.

28. Voir Actes du colloque de Rennes du 12 septembre 2014, Annie Blandin (dir.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, 216 p.

Et alors que, classiquement, la souveraineté est indivisible, la souveraineté numérique, pour certains, pourrait être collective et/ou individuelle… On le constate, si la notion est désormais bien établie, ses contours restent flous et ses interprétations diverses.

2. Les contours d'une souveraineté numérique

Il s'agit ici de confronter différentes acceptions de la notion, afin d'en clarifier les contours. La souveraineté numérique implique-t-elle la réinvention du concept de souveraineté ou seulement la transposition, le prolongement d'un concept juridique ancien dans un monde nouveau ? Autrement dit, s'agit-il de repenser la souveraineté au-delà ou sans l'État, ou plus simplement d'adapter les modalités d'expression de la puissance publique des États dans un monde numérique ? La souveraineté numérique est-elle celle des États, celles des communautés d'utilisateurs, celle des individus ou celles des entreprises qui construisent et animent le monde numérique ? Est-elle unique ou démultipliée, indivisible ou fragmentée, collective ou individuelle ? On touche ici aux limites du droit constitutionnel, droit de l'organisation de la Cité et de la garantie des droits fondamentaux, qui conçoit la souveraineté comme celle de l'État, une et indivisible. Pour certains, ces limites sont déjà franchies : le concept est, au mieux, hors du champ de la science constitutionnelle, au pire, inopérant sur le terrain juridique.

Précisément, en France, le concept a été tardivement questionné par les juristes. Ce fut d'abord le président fondateur de Skyrock, P. Bellanger, qui a, avec d'autres, popularisé et tenté de définir le concept émergeant de « souveraineté numérique » dans plusieurs tribunes et interviews[29], et finalement dans un ouvrage paru en 2014[30]. Selon lui, « la souveraineté est, pour une nation démocratique, l'expression sans entrave sur son territoire de la volonté collective de ses citoyens », ce qui a pour conséquence que « le peuple se détermine et fait ses choix par lui-même, sans subordination ni dépendance envers une autorité étrangère ». Partant de là, il dénonce

29. « De la souveraineté en général et de la souveraineté numérique en particulier », *Les échos*, 30 août 2011
30. *La souveraineté numérique*, Stock, 2014, 264 p.

une dérive caractérisée par la « perte de notre souveraineté dans le monde numérique », au profit des États-Unis et des multinationales américaines. Il constate la difficulté pour la République, ses lois et ses valeurs, de se projeter dans le cyberespace, alors qu'il est question de la protection de notre sécurité, de nos libertés et de notre économie. Il s'inquiète d'une « abdication » sans conditions, d'une « vassalisation » de nos sociétés, les citoyens eux-mêmes acceptant « de renoncer à être des sujets auto-gouvernés pour adopter le statut d'animal domestique : objet vivant à la merci de son propriétaire »[31]. De même qu'au XVII[e] siècle, le principe de la liberté des mers ne fut que le paravent de la domination anglo-saxonne sur les océans, les principes directeurs du monde numérique ne feraient que favoriser l'impérialisme américain, dès lors que « nous ne sommes pas collectivement maîtres sur les réseaux, nous sommes subordonnés, soumis, dépendants, à la merci de la volonté d'autrui »[32]. Le constat est sans appel, et la solution claire : il faut retrouver « la maîtrise de notre destin sur les réseaux numériques » afin de protéger nos intérêts et nos libertés, et ainsi reconquérir notre souveraineté numérique. P. Bellanger considère alors possible et indispensable de se doter d'un serveur national performant, un « résogiciel national », proposant aux utilisateurs et aux administrations une offre de service compétitive, grâce à une politique industrielle ambitieuse alliant la puissance publique et les entreprises françaises et européennes disposant de la taille critique et des ressources techniques nécessaires. Il s'agit d'éviter que notre société numérisée « passe sous souveraineté étrangère, emportant vies privées, secrets industriels et bientôt ce qui fonde notre État : la défense et la sécurité »[33]. Ainsi entendue, la souveraineté numérique réside bien dans le prolongement des principes républicains et dans la garantie des droits garantis par notre Constitution sur les réseaux : elle renvoie à « la continuation de la République dans le cyberespace »[34]. Cette conception peut être qualifiée de « fermée » et de « défensive ». Elle est sans doute l'une des plus opérantes en droit constitutionnel puisqu'il s'agit ici de préserver les attributs de la puissance publique souveraine dans le monde numérique.

---

31. *Idem*, p. 13.
32. *Idem* p. 13.
33. P. Bellanger, « Pourquoi un commissariat à la souveraineté numérique », *Le point*, 15 février 2016
34. *Idem*.

Une approche plus ouverte a été proposée par d'autres spécialistes, tels Bernard Benhamou qui rapproche la souveraineté numérique de la « capacité à maîtriser l'ensemble des technologies, tant d'un point de vue économique que social et politique, et de se déterminer pour avoir sa propre trajectoire technologique »[35]. De même, pour François Pelligrini, la souveraineté numérique « impose de doter nos administrations, nos entreprises et nos citoyens d'une infrastructure informationnelle loyale », ce qui passe par le développement de logiciels libres davantage que par le financement d'un système d'exploitation « made in France » voué à l'échec économique[36]. Contre le modèle classique de la souveraineté westphalienne, certains défendent une « souveraineté entendue comme le contrôle des éléments stratégiques (physiques ou immatériels) qui assurent l'existence, l'intégrité et l'identité d'un État et de ses administrés dans le cyberespace »[37]. Pour d'autres encore, la souveraineté numérique est résolument ouverte : si l'on se réfère à un pouvoir de commandement et à une capacité à se faire obéir[38], force est de constater que, dans le monde numérique, ce pouvoir n'est plus l'apanage des États, mais peut être transféré à d'autres acteurs, ou partagé avec eux… Et la notion peut s'élargir encore si cette souveraineté numérique renvoie à l'autonomie, à l'autogouvernement, à la capacité de choisir les règles auxquelles on se soumet : elle peut alors être revendiquée par des communautés ou par des

35. Secrétaire général de l'Institut pour la souveraineté numérique, « Les contresens de la souveraineté numérique », *Les échos*, 29 janvier 2016. La souveraineté numérique peut ici être rapprochée de la « suprématie informationnelle » c'est-à-dire de la maîtrise technique des technologies de l'information, à laquelle se réfère le même auteur dans un article antérieur, voir B Benhamou et F. Sorbier, « Souveraineté et réseaux numériques », *Politique étrangère*, 2006, op. cit.

36. F. Pelligrini, professeur d'informatique à l'Université de Bordeaux, « Souveraineté numérique : le recours aux logiciels libres constitue la seule alternative viable », *Le Monde*, 26 juin 2016.

37. Q. Lenormand, *Les représentations de la souveraineté numérique française*, Mémoire de M2 de géostratégie de l'Institut Français de géopolitique, 2015, p. 15, www.cyberstratégie.org.

38. La souveraineté est l'emprise, le « pouvoir de domination ou de décision sur quelque chose ou quelqu'un », Montaigne, *Essais*, I, XXVIII, éd. P. Villey et V-L. Saulnier, 1978, p. 191. Le dictionnaire Littré renvoie à l'autorité suprême, à la qualité de ce qui s'impose, de ce qui prime, sans appel.

individus. Pour certains, l'enjeu est précisément de « rendre à l'utilisateur la souveraineté sur ses données »[39]. On le comprend, il n'y a donc pas « une souveraineté numérique » mais des « souverainetés numériques », dont on peut identifier les principales acceptions.

La souveraineté numérique, c'est d'abord, naturellement, celle des États qui la revendiquent. Lors de la Conférence mondiale des télécommunications internationales (CMTI) de 2012, la Chine, la Russie ou l'Arabie saoudite, par exemple, ont annoncé vouloir rétablir « leurs droits souverains sur le segment national des réseaux »[40], selon une approche relativement autoritaire. Prolongeant des discussions déjà tenues lors de précédents SMSI[41], où le caractère multipartite de la gouvernance de l'Internet avait été affirmé[42], ces États ont une nouvelle fois tenté d'intégrer aux négociations la reconnaissance du « droit souverain et égal de chaque État à réguler ses télécommunications ». Ils ont tenté aussi, sans succès, de convaincre de l'utilité d'un contrôle international d'Internet confié à l'Union internationale des télécommunications (UIT) ou à une autre organisation internationale placée sous l'égide de l'ONU[43], débats prolongés lors des forums annuels multipartites sur la gouvernance de l'Internet[44]. Dans une approche moins autoritaire, d'autres États, comme

39. L. Chemla, informaticien français et auteur de « *Confessions d'un voleur : Internet, la liberté confisquée* », Denoël, 2002, cité in A. Guiton, « Souveraineté numérique : un modèle à inventer », *Libération*, 20 mai 2016.
40. Voir débats lors du CMTI-12 de Dubaï en décembre 2012, déjà mentionné, cf. www.itu.int/fr/wcit-12.
41. Sommets mondiaux sur la société de l'information, voir notamment les SMSI de Genève en 2003 et de Tunis en 2005.
42. La gouvernance de l'Internet est « l'élaboration par les États, le secteur privé et la société civile dans le cadre de leurs rôles respectifs de principes, de normes, de règles, de procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'usage d'Internet », in rapport final du groupe de travail sur la gouvernance de l'Internet, SMSI, Tunis, 2005.
43. Voir proposition de la Russie, de la Chine et des Emirats arabes unis visant à permettre aux États membres de l'UIT d'obtenir le droit de gérer le nommage, le numérotage, l'adressage et les ressources d'identification nécessaires aux télécommunications internationales sur leur territoire.
44. Forum sur la gouvernance d'Internet (IGF) créé conformément à l'« Agenda de Tunis » (SMSI de 2005).

le Brésil ou l'Allemagne, ont pris des mesures pour reprendre la main et mieux défendre leurs intérêts, notamment face à l'hégémonie américaine[45]. La présidente du Brésil, Dilma Roussef, a d'ailleurs pris l'initiative de convoquer les parties prenantes lors d'un forum Netmundial à Sao Paulo d'avril 2014[46], où il fut question de « désaméricanisation » du monde numérique et de « restauration des droits souverains » sur les réseaux. Cette initiative fait suite aux révélations d'Edward Snowden et au scandale PRISM, qui ont accéléré la prise de conscience dans les États démocratiques, confrontés au risque d'une instrumentalisation du numérique à des fins politiques et de sécurité, mais aussi économiques et commerciales. La France, aussi, s'est saisie de la question, envisageant un *cloud* souverain, un système d'exploitation propre ou, de façon plus concrète, l'adoption de la loi pour une République numérique le 7 octobre 2016. Revendiquée par les États, la souveraineté numérique n'est cependant pas conçue de la même façon par tous : selon une conception autoritaire et offensive, elle fonde le droit pour l'État de reprendre le contrôle des espaces numériques pour y appliquer ses lois et y promouvoir ses intérêts ; selon une conception plus libérale et défensive, elle fonde le droit pour l'État de protéger ses citoyens contre les politiques de surveillance et d'exploitation conduites dans le cyberespace par des entités mues par leurs intérêts propres.

Mais la souveraineté numérique, ce peut être aussi la souveraineté collectivement revendiquée par des groupes d'utilisateurs du numérique, voire par des communautés d'internautes plus ou moins organisées, qui revendiquent d'être associés à la détermination des règles applicables et de

45. Voir loi brésilienne Marco Civil Da Internet, n° 12.965 du 23 avril 2014. En 2014, l'Allemagne a choisi, au sein de la Commission européenne, le portefeuille « Économie et Société numérique ». A également été lancé un plan dit « Agenda numérique » comportant une stratégie de développement technologique, une réflexion sur le stockage des données et une réforme de la législation sur la sécurité informatique, T. Madelin « l'Allemagne veut renforcer sa souveraineté numérique », *Les échos*, 20 juillet 2014.

46. Les 23 et 24 avril 2014, dans le cadre du « Global Multistakeholder Meeting on Internet Governance », 90 États ont été réunis à l'initiative du Brésil et associés aux diverses parties prenantes (secteur privé, académique, technique, société civile) pour discuter de l'avenir de la gouvernance d'Internet après la découverte du système d'espionnage informatique généralisé mis au point par les États-Unis.

participer à l'organisation de la protection de leurs données sur les réseaux. Reconnaître un droit pour les communautés transnationales d'utilisateurs de s'auto-organiser ou de peser dans la décision conduit d'une certaine façon à transposer au monde numérique la réflexion classique sur la formation des sociétés civiles et le passage aux sociétés politiques[47]. Cela amène aussi à penser la souveraineté populaire à l'échelle de communautés d'utilisateurs qui renonceraient à la liberté de l'Internet en échange de règles consenties, dans le cadre d'un nouveau contrat social. Audacieuse, cette approche peut, dans l'avenir, interroger les constitutionnalistes.

La souveraineté numérique, c'est aussi celle de l'individu, sous l'angle de sa capacité à s'autodéterminer, à commander pour lui-même, à maîtriser ses données. L'individu est-il libre de choisir un opérateur, un moteur de recherche, d'accepter ou de refuser des conditions générales d'utilisation (CGU) pré-déterminées par des opérateurs privés[48] ? Est-il en capacité de conserver ses communications secrètes, de contrôler l'utilisation qui est faite de ses données, de maîtriser la façon dont ses activités sont référencées sur les moteurs de recherche, dont son image est exposée ? Peut-il choisir librement ses lectures, les enseignements qu'il souhaite suivre, les hôtels où il souhaite descendre, ce qu'il doit penser, face à la tyrannie des algorithmes ? Cette souveraineté se traduit par la revendication de certains droits : liberté d'accès à Internet, droit à la protection des données personnelles, droit à l'oubli et au déréférencement, droit à l'autodétermination informationnelle, par exemple[49]. Cette conception s'illustre aussi par les réflexions autour du concept de « digital empowerment », qui permet de rendre le pouvoir aux individus grâce au numérique, et se manifeste notamment par les nouvelles modalités de participation politique. Plus individualiste, cette conception

47. P. Lantz, « Société civile et société politique », *L'homme et la société, Revue internationale de recherches et de synthèse en sciences sociales*, L'Harmattan, 1991, vol. 102, n° 4 État et société civile, p. 23.

48. Selon P. Bellanger, « la maîtrise de l'information sur soi est au cœur de la souveraineté individuelle. Nous l'avons abandonnée. Nous avons, sans les lire, accepté d'un clic ces contrats absurdes qui nous obligent à renoncer au bénéfice de certains droits fondamentaux », *La souveraineté numérique*, op. cit.

49. M. Boizard, « vers une souveraineté individuelle ? Le droit à l'oubli numérique », *Droits et souveraineté numérique en Europe*, Bruylant, 2016, p. 31 ; P. Türk, « Le droit à l'autodétermination informationnelle : un droit fondamental émergent ? »Dalloz IP-IT, 2020, n° 11, p. 616.

place l'individu et sa capacité d'autodétermination au centre de la réflexion[50]. Elle est, à notre sens, la moins opérante en droit constitutionnel.

Enfin, la souveraineté numérique, c'est celle des opérateurs privés qui règnent littéralement sur le monde numérique et disposent effectivement du pouvoir de commander aux utilisateurs et de leur imposer des règles. Le professeur Blandin-Obernesser, pour démontrer l'existence « d'entreprises souveraines de l'Internet », constate que les États sont concurrencés dans leur capacité à commander et à se faire obéir par des entreprises multinationales qui bénéficient d'une suprématie grâce à leur position dominante sur le marché[51]. Cette évolution est perceptible dans tous les domaines : réglementation du commerce, numérisation du patrimoine, lutte contre la criminalité et pour la sécurité, production d'une monnaie pour les échanges (cryptomonnaies), élaboration des lois et des règles applicables, défense des libertés individuelles, soutien aux entreprises (*crowdfunding*), information des populations et organisation des télécommunications, politiques de santé, des transports, industrielles, énergétiques[52]. Leur pouvoir s'exerce bien sur un territoire (non physique et transnational) et sur une population (physique, des internautes connectés), et s'approprient certains attributs de la souveraineté : monnaie virtuelle, fiscalité optimisée, police (contrôle, retrait de contenus), règles de gouvernement (CGU), etc.. Dans le même sens, Pierre Trudel propose une reconstruction de la notion de souveraineté : dépassée au sens classique d'un monopole étatique sur le droit et le commandement d'un territoire et d'une population, elle peut être reconstruite et fondée sur la capacité de certains acteurs à se faire obéir, à imposer leur loi, à apparaître comme « devant être respecté », sans référence à un territoire physique[53]. Dans cette approche, plus une entité génère des risques, plus elle inspire l'obéissance et plus elle est dotée des attributs de la souveraineté. Or sous l'angle de la capacité à imposer leurs règles, les multinationales américaines,

50. Sur « le transfert de pouvoir vers l'individu » engendré par la révolution numérique, voir E. Schmidt et J. Cohen, *À nous d'écrire l'avenir*, Denoël, 2013, p. 16.
51. A. Blandin-Obernesser, « Les entreprises souveraines de l'Internet », *Droits et souveraineté numérique en Europe*, Bruylant, 2016, p. 97.
52. Colloque droits et souveraineté à l'âge de l'Internet : quels défis pour l'Europe ? », Rennes, 12 septembre 2014.
53. P. Trudel, professeur à l'Université de Montréal, « La souveraineté en réseaux », *Droits et souveraineté numérique en Europe*, *op. cit.*, p. 10.

qui bénéficient d'une situation de monopole dans l'espace numérique, l'emportent sur les États. Cela pose la question de la légitimité du pouvoir qu'elles exercent et des contrôles qui peuvent s'exercer sur elles, questions non étrangères à l'objet de la science constitutionnelle, on en conviendra.

3. Les enjeux d'une souveraineté numérique

La réflexion sur les origines, fondements et contours du concept de souveraineté numérique, fait apparaître l'existence de « plusieurs cercles de souveraineté »[54] – celui des individus, des entreprises, des États – et des conceptions variables, défensives ou plus positives de la notion. Cette réflexion doit être poursuivie compte tenu de la diversité et de l'importance des enjeux, stratégiques, diplomatiques, économiques, informationnels et culturels, qui y sont liés.

C'est d'abord l'enjeu de la gouvernance des réseaux, de la légitimité et de la représentativité des instances de régulation, et de la place disproportionnée qu'y prennent les États-Unis d'une part, les GAFAMI – toutes américaines – d'autre part[55]. En 2015, le Président Obama a imprudemment parlé de propriété des américains sur l'Internet, affirmant : « Internet était à nous, nos entreprises l'ont créé, étendu et perfectionné de telle façon que la concurrence ne peut pas suivre ». Il dénonce aussi le protectionnisme commercial qui, en réalité, inspirerait les européens sur ces questions[56]. À la vérité, les instances de régulation d'Internet s'ouvrent peu à peu, comme le montre le fonctionnement de l'ICANN, où sont représentés 60 États, et qui s'est libéré le 1er octobre 2016 de son contrat avec le département du commerce américain.

54. F. Gueham, *Vers la souveraineté numérique*, Fondation pour l'innovation politique, janvier 2017, p. 11.
55. A Desforges, « Le cyberespace : un nouveau théâtre de conflits géopolitiques », *Questions internationales*, janv-février 2011, n° 47, p. 46 ; N. Dreyfus, « La gouvernance de l'internet. L'Icann : entre régulation et gouvernance », *Revue Lamy droit de l'immatériel*, n° 81, 2012, pp. 119-122 ; P. Jacob, « La gouvernance de l'internet du point de vue du droit international public », *AFDI,* vol. 56, 2010, pp. 543-563 ; J. Nocetti, « Internet : une gouvernance inachevée », *Politique étrangère*, n° 4, 2014-2015.
56. A. Hervaud, « Obama tacle la politique numérique de l'Europe : Internet était à nous », *Libération*, 18 février 2015.

Et le système de gouvernance repose sur un multipartenariat (*multistakeholderism*) qui associe largement les États, le secteur privé, les communautés techniques, la société civile et les utilisateurs[57]. Après l'élaboration, lors des SMSI de 2003 et 2005, d'une déclaration de principes concernant l'élaboration des règles, pratiques, normes, procédures et programmes relatifs à l'utilisation et au développement d'Internet[58], la transposition aux instances internationales de régulation des principes du constitutionnalisme (légitimité, représentativité, responsabilité, transparence) devrait être envisagée. Ouvrant une nouvelle dimension à la réflexion sur la globalisation du droit constitutionnel, l'idée émerge d'une « constitutionnalisation » des droits et des devoirs attachés à la communication numérique, auxquels la communauté unifiée des utilisateurs accepterait de se soumettre. Les Nations-Unies, le Conseil de l'Europe, diverses organisations non gouvernementales, communautés d'utilisateurs et associations, travaillent à ce projet politique global et à l'élaboration des principes fondamentaux qui pourraient être proposés aux parties prenantes, parmi lesquels l'universalité et la neutralité de l'Internet, l'ouverture et la décentralisation, la diversité linguistique, la sécurité de l'Internet, le respect de l'autonomie et de la vie privée de l'internaute.

La question de la gouvernance suscite des tensions, comme l'a montré la confrontation des États en 2012 sur l'inscription dans le Règlement des télécommunications internationales du principe d'un partage des responsabilités dans la gouvernance de l'Internet, déjà évoquée. 55 États s'étaient alors posés en garants de la liberté de l'Internet, face aux tentatives de reprise de contrôle de l'Internet par certains États aux conceptions souverainistes plus autoritaires[59]. Au risque d'une fragmentation qui conduirait à une

57. Voir par exemple le rôle du W3C (Wordl Wibe Web consortium) ou de l'IETF (Internet Engeneering Task Force).

58. Voir déclaration dite « Agenda de Tunis, adoptée en clôture du SMSI tripartite (gouvernements, multinationales, société civile) de 2005 ; « 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 », doc. WSIS-05/TUNIS/DOC/6(Rév.1)-F.

59. Causant l'échec des négociations sur le Règlement des télécommunications internationales lors du CMTI 12 de Dubaï qui aurait dû permettre aux repré-

balkanisation de l'Internet (voir par exemple « la grande muraille numérique » chinoise), un enjeu crucial tient donc à la conciliation entre les souverainetés étatiques et les principes libéraux du net, affirmés dès 1996 par John Perry Barlow dans une déclaration d'indépendance de l'Internet qui résonne ici particulièrement : « Gouvernements du monde industriels… vous n'avez pas de souveraineté là où nous nous réunissons ».

Car, précisément, un autre enjeu tient aux limites du pouvoir normatif des États, qui ne saurait s'arrêter là où commence la liberté de l'espace numérique sans frontières. C'est la capacité de l'État à faire respecter ses lois et ses valeurs, à garantir les droits et la sécurité de ses citoyens qui est jeu. Certes, l'élaboration du droit et des règles applicables aux activités humaines n'est plus le monopole des gouvernements et des parlements élus, confrontés à l'affirmation de modes de régulation qui associent le secteur privé, la société civile, et bousculent les sources et les formes de normativité[60]. Certes, les cadres juridiques et les conditions d'utilisation sont mis en concurrence par les utilisateurs sur le réseau, ce qui entraîne des phénomènes d'harmonisation forcée et de standardisation des législations et des pratiques. Mais les États doivent pouvoir assurer le respect des lois adoptées au nom du peuple souverain, sous peine de perdre leur légitimité, ciment du pacte social.

D'autant qu'à l'enjeu de la concurrence normative s'ajoute la concurrence exercée, dans toute une série d'autres compétences[61], par des opérateurs privés qui redessinent les politiques publiques en matière commerciale (e-bay, amazone), informationnelle (twitter, facebook),

---

sentants des 193 États parties d'actualiser les principes généraux garantissant la libre circulation des informations dans le monde. La tentative de certains États d'inscrire dans le RTI que « tous les gouvernements devraient avoir égalité de rôle et de responsabilité dans la gouvernance internationale de l'Internet » s'est heurtée au refus de 55 « nonistes » (parmi lesquels la France, le Royaume-Uni, les États-Unis, le Canada ou l'Australie).

60. M. Behars Touchais, « L'effectivité du droit face à la puissance des géants d'Internet », Actes des journées d'études des 14-16 octobre 2014, Paris 1, IRJS éditions, 2015.

61. Selon Bill Gates, « Le niveau des impôts n'est pas la question, la question c'est le service rendu en contrepartie », cité par P. Bellanger, *La souveraineté numérique, op. cit.*, p. 94.

culturelle (amazone, netflix, spotify), de transports (uber, blablacar), de recherche d'emplois (linkedin, monster, indeed), et bientôt de santé (Google, Truven Health Analytics), après avoir contesté aux États leur pouvoir monétaire (Bit coin, Monero et autres monnaies virtuelles ayant ou non des effets dans le monde réel) et fiscal (cadre traditionnel de la fiscalité inadapté au monde numérique[62]). Les ambitions dévoilées laissent croire à une intensification du phénomène, dans tous les domaines[63]. Le Conseil constitutionnel français a déjà été saisi plusieurs fois de questions liées à ces interférences dans les compétences étatiques[64], preuve que le droit constitutionnel est directement touché.

La souveraineté numérique emporte aussi, à l'évidence, de lourds enjeux en termes de défense et de sécurité : lutte contre la cybercriminalité, les trafics, le terrorisme, l'espionnage ou le hacking, cyberdéfense, cryptologie, sécurité économique, renseignement et commandement militaire (objectifs premiers d'Arpanet, l'ancêtre d'Internet). Définie comme « l'ensemble des outils politiques, concepts et mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs »[65], la cybersécurité est un « état recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces

62. Cf. débats sur des amendements aux articles 209 C et D de la seconde partie du projet de loi de finances pour 2017 permettant de taxer les géants du net installés hors des frontières françaises, « Optimisation fiscale : les Gafa montrent patte blanche à Strasbourg », *La tribune*, 17 novembre 2015; « Gafa : le Conseil constitutionnel censure la taxe google », *Libération*, 29 décembre 2016.
63. Voir la traduction de l'ouvrage "The new digital age" écrit par le patron de Google : E. Schmidt, J. Cohen et A. Muchnik, *À nous d'écrire l'avenir : comment les nouvelles technologies bouleversent le monde*, Denoël, 2013.
64. C. Const., n° 2015-468/469/472 QPC du 22 mai 2015, Société UBER France SAS et autres ; C. Const., n° 2016-744 DC du 29 décembre 2016 Loi de finances pour 2017.
65. Recommandation UIT-T X.1205.

systèmes offrent ou qu'ils rendent accessibles »[66]. La cyberattaque massive perpétrée en mai 2017 (via un logiciel de rançon surnommé Wannacry), qui a touché 200 000 victimes dans 150 pays et a paralysé des entreprises publiques et privées (tels Renault ou la Société des chemins de fer allemands Deutsche Bahn), des gouvernements (tel le ministère russe de l'Intérieur) ou encore des dizaines d'hôpitaux britanniques, illustre bien le risque encouru[67], comme la suivante, baptisée « Petya », le mois suivant.

Un autre enjeu, économique, réside dans la perte de compétitivité des entreprises européennes, qui doivent urgemment prendre leur part sur des marchés émergents où, malgré le nombre des consommateurs européens sur le réseau, elles sont pour l'instant largement sous représentées, mis à part quelques « licornes » (zalando, skype, shazam, spotify, et les françaises blablacar, critéo et vente privée.com[68]). Les tentatives de développement de programmes européens, *a fortiori* français, susceptibles de rivaliser avec les outils américains ou même asiatiques ont, pour l'heure, peu convaincu[69]. Le moteur de recherche français Qwant, lancé en 2013, ou la bibliothèque numérique européenne Europeana, suscitent davantage d'espoirs. La masse de données collectées auprès des internautes (big data) constitue pourtant, on le sait, « le pétrole du XXIe siècle », dans la mesure où son exploitation permet de probabiliser – voire d'orienter – le

66. Définition retenue par l'Agence nationale de la Sécurité des systèmes d'informations (ANSSI) chargée de protéger la souveraineté française, ce qui implique de « disposer de compétences scientifiques, techniques et opérationnelles ; mais également de capacité industrielles positionnant la France dans le premier cercle des rares pays capables d'assurer par eux-mêmes leur cybersécurité ». www.ssi.gouv.fr.agence/missions. Voir aussi N. Arpagian, *La cybersécurité*, PUF, 2015, p. 128.

67. Même si le produit de ce « Ransomware » semblait limité, au vu des transactions effectuées via un portefeuille Bitcoin, D. Leloup, « Cyberattaque : tout dans ce scénario fait penser à une attaque criminelle », *Le Monde*, 13 mai 2017 ; « Une attaque informatique de portée mondiale crée la panique », *Le Monde*, 12 mai 2017 ; « Le point sur la cyberattaque qui touche 150 pays », L*e Figaro*, 14 mai 2017 ; « Renault parmi les cibles d'une cyberattaque mondiale », *Libération*, 12 mai 2017

68. Sur la quarantaine de licornes européennes, start up valorisées à plus d'un milliard de dollars, 8 sont britanniques, 6 suédoises, 3 allemandes.

69. Voir l'échec du programme Quaero, créé en 2004, ou des projets de clouds souverains français cloudwatt ou numergy.

comportement des consommateurs et des clients. Cela ouvre des perspectives immenses : adaptation en temps réel de l'offre commerciale, révolution des démarches publicitaires et marketing, comparaison des prix, gestion des stocks[70]. Qu'il s'agisse de préserver ses intérêts économiques et commerciaux ou de protéger les libertés individuelles, l'Europe est désormais sensibilisée au risque d'une exploitation ou d'une marchandisation abusive des données personnelles, elle qui a longtemps naïvement adopté, face au pillage des données de ses citoyens, « le même mécanisme de défense qu'un buffet du club Med ! »[71]. À ce titre, la protection des données personnelles devient un enjeu majeur, et les citoyens européens ont à jouer la carte de leur poids économique dans les marchés pour se faire entendre. La souveraineté sur les données implique la reconnaissance d'un droit à l'oubli ou au déréférencement[72], voire la consécration d'un droit à « l'autodétermination informationnelle »[73]. Mais aussi la redéfinition de la liberté individuelle et du droit à la vie privée, ou encore la clarification des conditions dans lesquelles les données sont transférées et stockées[74]. À l'échelle européenne, la CJUE sanctionne les pratiques abusives de multinationales, reconnaît désormais le droit au déférencement[75], et protège la vie privée des internautes qui utilisent les services de compagnies américaines, en liaison avec la CNIL française et le réseau des CNIL européennes (G29). L'Union européenne cherche à garantir un

70. P. Bellanger, *La souveraineté numérique*, 2014, *op. cit.*, p. 176.
71. P. Bellanger, idem, p. 160.
72. A. Bretonneau, « Le droit au déréférencement », RFDA, n° 3, 2017, p. 535.
73. P. Türk, « Le droit à l'autodétermination informationnelle », n° spécial de la Revue Politeia « Les métamorphoses des droits fondamentaux à l'ère du numérique », n° 31, 2017.
74. Voir, dans un contexte de transfert et de stockage extra-territorialisé des données, les enjeux en termes de souveraineté et d'équivalence des protections du Microsoft Ireland case, cf. United States Court of Appeals for the Second Circuit, 14 juillet 2016, Microsoft Corp. v. United States.
75. CJUE 13 mai 2014, C 131-12 Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González ; M. Boizard, « La tentation de nouveaux droits fondamentaux face à Internet : vers une souveraineté individuelle ? Illustration à travers le droit à l'oubli numérique », in A. Blandin-Obernesser, *Droits et souveraineté numérique*, 2016, *op. cit.*, p. 31.

haut niveau de protection des données personnelles[76], d'où l'adoption du RGDP n° 2016/679 du 27 avril 2016 et la renégociation d'un nouveau « bouclier juridique » concernant les relations transatlantiques en matière de transfert et le stockage de données dit *Privacy shield*[77].

La question du stockage des données renvoie à la problématique du *cloud souverain*, ou des garanties données aux États et aux internautes quant à la sécurité des données stockées par les géants du numérique. C'est ainsi que, par précaution, une note ministérielle est venue interdire en 2016 aux collectivités publiques (les collectivités locales, leurs groupements et leurs établissements publics) de stocker les archives publiques sur des *clouds* non souverains, c'est-à-dire non basés en France et soumis aux lois françaises, afin de garantir en toute hypothèse la traçabilité, la portabilité et la sécurité des données[78].

*
* *

Qu'on en reconnaisse la consistance juridique ou qu'on la conteste, qu'on en fasse le prolongement dans le monde numérique du principe classique de la souveraineté étatique, ou qu'on déconnecte la notion de souveraineté numérique de celle d'État, les fondements de la réflexion sur l'exercice du pouvoir dans nos sociétés sont ébranlés. Deux approches nous semblent, au final, se distinguer. Une première conception, relativement classique, de la souveraineté numérique, correspond au pouvoir

76. CJUE, 8 avril 2014, C.293-12 Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung ; CJUE 21 décembre 2016, tele2 Sverige AB (C-203/15) et Secretary of State for the home department (C-698/15).

77. Le P*rivacy Shield* est un accord international entre l'Union européenne et les États-Unis qui a remplacé le « Safe Harbor » insuffisamment protecteur invalidé par la CJCE le 6 octobre 2015, affaire C 362/14, Maximilian Schrems/Data Protection Commissione. La mise en œuvre du nouvel accord reste problématique, S. Cassini, « Privacy shield : l'Europe demande des garanties aux États-Unis », *Le Monde,* 17 février 2017.

78. Note d'information ministérielle du 5 avril 2016 relative à l'informatique en nuage (cloud computing), 2016/004, NOR DGCC1614354C, DGP. SIAF/2016/006. Voir projets Numergy (SFR), Cloudwatt (orange), et le déploiement de l'entreprise française OVH créée en 1999.

de commander et de fixer les règles du jeu (règles juridiques ou standards techniques du monde numérique), lequel est revendiqué par les États, ceux-ci se trouvant concurrencés par les organismes (tel l'ICANN) et par des entreprises (telles les GAFA ou GAFAMI) qui gouvernent, effectivement, le monde numérique. Une autre approche, rompant avec l'État, renvoie à la capacité (d'une communauté ou d'un individu) à s'autogouverner et à s'autodéterminer, à fixer les règles auxquelles on se soumet, et à commander pour soi-même dans le monde numérique. Cette approche est plus novatrice, bien que non dénuée de lien avec les théories relatives à l'origine de la souveraineté, à la source du pouvoir et à sa légitimité. La souveraineté numérique est ici celle, collective, des communautés d'utilisateurs soucieux de s'autogouverner. Mais elle peut aussi être revendiquée par les individus, désireux de s'autodéterminer, de commander pour eux-mêmes dans le cyberespace, ce qui se rattache à une conception poussée de la liberté individuelle, voire aux idées de certains courants libertariens.

La notion de souveraineté, en droit constitutionnel, déjà partiellement déconstruite, est atteinte par ces nouvelles dimensions, dont toute entreprise de reconstruction doit tenir compte. En particulier, la question des pouvoirs qui s'exercent dans le monde numérique, leurs objectifs, leur représentativité et leur légitimité, et celle, aussi, des garanties assurées pour l'exercice des droits fondamentaux, doivent être clairement posées, y compris par les constitutionnalistes. Si l'on décide d'avoir recours à la notion de souveraineté numérique, par adhésion ou par défaut, il convient, contre toute tentation de repli, d'en privilégier une approche ouverte, libérale, collaborative. Enfin, par souci de réalisme, il faut sans doute la penser, en France, à l'échelle européenne.

Définition et enjeux de la souveraineté numérique

Pauline Türk
Professeur de droit public, faculté de Droit et Science politique de Nice, université Côte d'Azur

Ils règnent sur l'espace numérique, décident de supprimer des contenus, de vendre les données personnelles... Depuis les années 2000, le pouvoir des GAFAM concurrence celui des États et affecte la liberté d'autodétermination des individus, faisant émerger la notion de souveraineté numérique.

Les enjeux de la souveraineté numérique

« Internet est l'une des rares créations de l'homme qu'il ne comprend pas tout à fait (...). C'est la plus grande expérience d'anarchie de l'histoire (...), à la fois source de bienfaits considérables et de maux potentiellement terrifiants, dont nous ne commençons qu'à peine à mesurer les effets sur le théâtre mondial. » (Eric Schmidt et Jared Cohen, *The New Digital Age*, Knopf, 2013, trad. *À nous d'écrire l'avenir*, Paris, éd. Denoël, 2013, p. 11).

Le système post-westphalien : la souveraineté des États contestée

Alors que la plupart des activités humaines sont désormais régies par les technologies digitales, les États sont entrés dans un rapport de force avec les multinationales qui règnent sur les réseaux numériques. Il s'agit de préserver ou de reconquérir une part du pouvoir qui s'exerce dans ces nouveaux espaces, pourtant conçus pour échapper à l'emprise étatique, ce que résume la célèbre Déclaration d'indépendance du cyberespace de l'essayiste libertarien John Perry Barlow en 1996 : « Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit (...) Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté où nous nous rassemblons ».

Nos sociétés deviennent dépendantes de la technologie et des entreprises qui les contrôlent (réseaux et plateformes, télécommunications, information, santé, commerce, justice, sécurité, armée...),

une tendance qui s'accentue avec le développement des algorithmes, des objets connectés, de la robotique, de l'intelligence artificielle. Or ces technologies sont régies par le code informatique : dans l'espace numérique, la régulation des activités et comportements dépend davantage des standards et normes techniques déterminés par les ingénieurs informatiques que des normes juridiques édictées par les États. C'est le sens de la fameuse formule « *code is law* » de Lawrence Lessig, Professeur à Harvard (L. Lessig, *Code and Other Laws of Cyberspace*, Basic Book, 1999).

Code is law ?

Les États se retrouvent à la fois contestés et concurrencés dans l'exercice de leurs prérogatives classiques attachées à la souveraineté. La notion de souveraineté est définie traditionnellement comme le pouvoir suprême exercé sur un territoire, à l'égard d'une population, par un État indépendant, libre de s'autodéterminer (voir l'apport à ce concept juridique de Jean Bodin et Charles Loyseau, au XVI^e^ siècle puis de Louis le Fur et Raymond Carré de Malberg au XX^e^ siècle). Elle est remise en cause, dans une société dite post-westphalienne caractérisée par l'interdépendance des États, la montée en puissance des organisations internationales, la mondialisation économique, le développement des échanges transnationaux, et désormais la globalisation engendrée par des technologies qui échappent largement aux États, et se jouent des frontières physiques.

John Perry Barlow (1947-2018), militant des libertés numériques, auteur de la *Déclaration d'indépendance du cyberespace*

TAAVI BURNS/FLICKR/CC BY-ND 2.0

Une nouvelle forme de colonisation

Le pouvoir exercé à l'échelle mondiale par les multinationales (GAFAM) pourrait les faire reconnaître, à brève échéance, comme des entités rivales ou partenaires pour la gestion des sociétés humaines. Le Danemark n'a-t-il pas décidé, en 2017, de nommer un ambassadeur auprès des géants de la Silicon Valley, comme s'ils étaient des interlocuteurs politiques et diplomatiques légitimes ? Le philosophe Éric Sadin décrit une « colonisation d'un nouveau genre (…) qui ne se vit pas comme une violence subie, mais comme une aspiration ardemment souhaitée par ceux qui entendent s'y soumettre » (*La siliconisation du monde : l'irrésistible expansion du libéralisme numérique*, Paris, éd. L'échappée, 2016, p. 24). Catherine Morin-Desailly utilise la même image (« L'Union européenne, colonie du monde numérique ? », rapport d'information, commission des affaires européennes du Sénat, n° 443, 2013).

L'adjectif « post-westphalien » désigne une organisation mondiale fondée sur la montée en puissance d'organisations supranationales, plutôt que sur les frontières et l'autorité d'États souverains, notamment à l'échelle européenne.

La maîtrise des données numériques générées par les activités de 4,5 milliards d'utilisateurs connectés, ajoutée à une situation de quasi-monopole de certaines entreprises américaines surtout (GAFAM ou NATU – Netflix, Airbnb, Tesla, Uber) mais plus seulement (BATX chinois ou le moteur de recherche russe Yandex), confère à ces opérateurs un pouvoir qui bouleverse les modes de gouvernement. Qui fixe les conditions générales d'utilisation des applications numériques ? Qui décide de censurer le tableau *L'origine du monde* de Gustave Courbet, mais de laisser diffuser en direct, 17 minutes durant, l'attentat de Christchurch en Nouvelle-Zélande en 2019, définissant ainsi les nouvelles règles en matière de liberté d'expression ? Qui détermine les informations ou les suggestions de lectures qui doivent être adressées aux internautes sur les réseaux sociaux ? Qui conserve et exploite les données personnelles, confiées ou laissées à leur insu par les utilisateurs, dont l'agrégation forme le *big data*, considéré comme « le pétrole du XXIe siècle » ?

La réflexion sur la souveraineté numérique naît d'une préoccupation : le refus de voir les peuples, les communautés d'utilisateurs, les États, les individus perdre le contrôle de leur destin au profit d'entités mal identifiées, non légitimes, et dont l'objectif n'est pas la promotion de l'intérêt général.

Émergence de la notion de souveraineté numérique

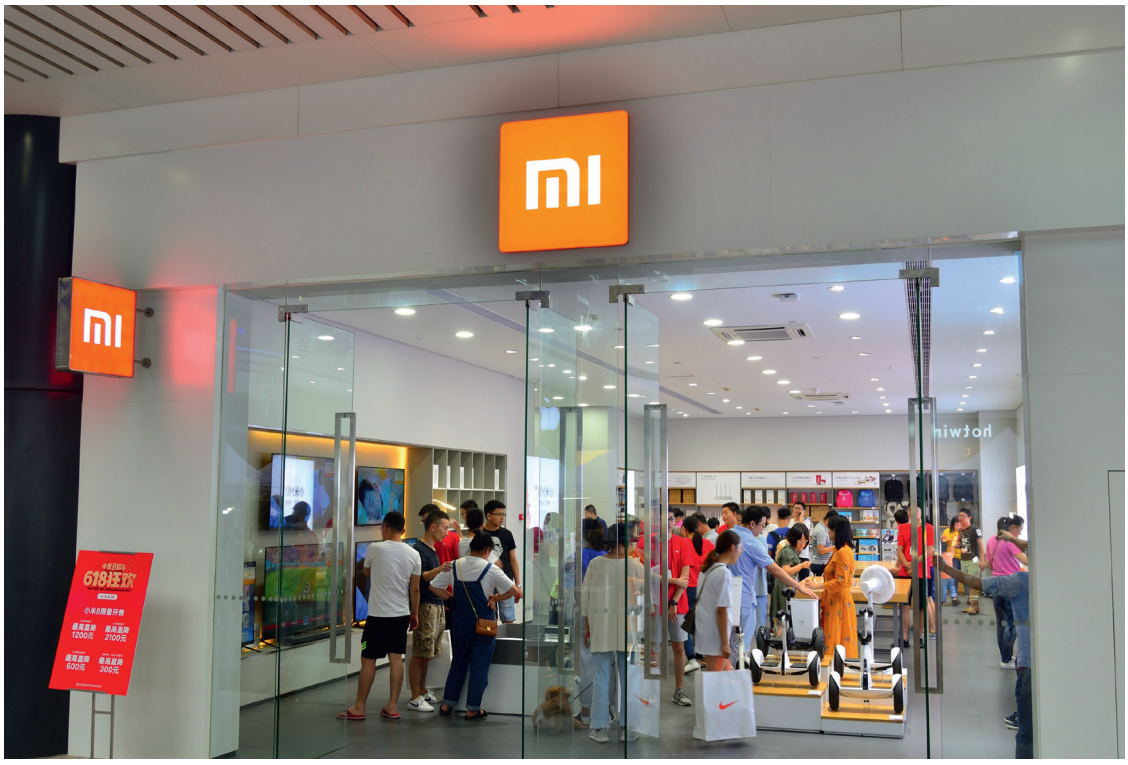
Les années 2000 ont vu apparaître les premières préoccupations sur le sujet, et bientôt la notion même de « souveraineté numérique ».

À l'international

Sur le plan international, c'est d'abord la question du contrôle des ressources internet qui a cristallisé les inquiétudes de certains États, désireux de limiter l'hégémonie américaine sur la gestion du réseau, notamment concernant les missions stratégiques de l'ICANN (Internet Corporation for Assigned Names and Numbers), société californienne créée en 1998 pour superviser la gestion des noms de domaine, racine stratégique de l'internet. Ces préoccupations sont alors d'autant plus vives que la domination historique des États-Unis s'accompagne d'une situation de quasi-monopole technique et économique des multinationales américaines, qu'il s'agisse des systèmes d'exploitation informatiques ou du développement des applications numériques. L'expression de « souveraineté numérique » est utilisée dès 2012 lors de la Conférence mondiale des télécommunications internationales, notamment par la Russie et la Chine qui revendiquent la restauration de leurs « droits souverains » sur la gestion du réseau et l'élaboration d'un traité international permettant de mieux partager les responsabilités. Les États occidentaux sont alors soucieux, avant tout, de protéger la liberté du cyberespace. La donne change à la suite de l'affaire Snowden, en 2013. Les révélations relatives à l'espionnage généralisé au profit des intérêts politiques et économiques américains conduisent à une remise en cause profonde du système de gouvernance des espaces numériques, notamment lors de plusieurs sommets ou forums internationaux consacrés au sujet (NETmundial de Sao Paulo en 2014, Internet Governance Forum annuels de Bali en 2013, Mexico en 2016 ou Paris en 2018…).

Après la Chine, l'Inde et la Russie, de nombreux États, tel le Brésil, lancent des programmes et politiques industrielles dédiés. 2013 marque aussi un « réveil européen » sur le sujet, l'Union européenne (UE) s'intéressant au développement de moteurs de recherche ou de systèmes d'exploitation (OS) « souverains », tout en renégociant avec les États-Unis

BATX : les géants du Web chinois dans les années 2010 : Baidu, Alibaba, Tencent et Xiaomi. Ils sont hégémoniques en Asie, particulièrement en Chine, où les GAFAM sont peu présents en raison des attentes différentes des consommateurs chinois et de l'encadrement de l'économie numérique par les autorités chinoises.



Magasin de la firme technologique Xiaomi, l'un des quatre géants du Web chinois, les BATX (Hangzhou, province du Zhejiang)

RAYSONHO@OPEN GRID SCHEDUILER/GRID ENGINE/CCo

les accords relatifs à la protection des données personnelles des utilisateurs européens.

En France

En France, parallèlement, l'expression « souveraineté numérique » se diffuse progressivement. Certains observateurs avisés appellent, dès 2006, à repenser la souveraineté des États dont l'exercice devient indissociable des outils de la puissance technologique (B. Benhamou et L. Sorbier, « Souveraineté et réseaux numériques », *Politique étrangère*, 2006/3). L'expression est popularisée par l'entrepreneur de radio Pierre Bellanger, qui multiplie les interventions médiatiques à partir de 2008, avant de publier *La souveraineté numérique* en 2014 (éditions Stock). L'expression a depuis fait florès, utilisée au sein d'instances spécialisées (Conseil national du numérique, Autorité de régulation des communications électroniques, des postes et de la distribution de la presse ou ARCEP, Agence nationale de la sécurité des systèmes d'information ou ANSSI) et par les gouvernements successifs. En juin 2009, le ministre de l'Intérieur français annonce vouloir « garantir la souveraineté numérique » et « étendre à l'espace numérique le champ de l'état de droit » (Michèle Alliot-Marie, citée par Martin Untersinger, « L'incertaine mais nécessaire 'souveraineté numérique' », *Le Monde*, 20 novembre 2019).

En 2014, à la suite de l'affaire Snowden, les premières Assises de la souveraineté numérique accompagnent la création d'un Institut de la souveraineté numérique, association chargée de sensibiliser le public et les élus aux enjeux, notamment par la publication des *Cahiers de la souveraineté numérique*. L'article 29 de la

loi du 7 octobre 2016 « pour une République numérique » consacre ensuite la notion en proposant de créer un Commissariat à la souveraineté numérique (finalement abandonné), chargé de concourir « à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège ». La réflexion se poursuit depuis, au Parlement, notamment au Sénat, avec la production de rapports d'information et d'enquête (« Nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'internet », rapport d'information du Sénat, nº 696, 2014 ; « Le devoir de souveraineté numérique », Gérard Longuet, rapport de la commission d'enquête du Sénat, nº 7, 2019) et aussi au sein de l'université (Annie Blandin-Obernesser, Droits et souveraineté numérique en Europe, Bruxelles, Bruylant, 2016 ; Pauline Türk et Christian Vallar (dir.), *La souveraineté numérique, le concept, les enjeux*, Mare & Martin, janvier 2018).

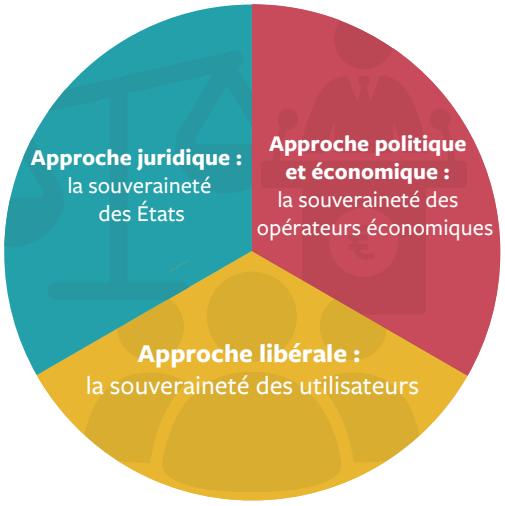
La notion est désormais bien établie, même si ses contours restent flous et ses interprétations variables.

Définition(s) de la souveraineté numérique

Plusieurs définitions ont été avancées

Pour les uns, elle est la capacité à « maîtriser l'ensemble des technologies, tant d'un point de vue économique que social et politique », et de « se déterminer pour avoir sa propre trajectoire technologique » (Bernard Benhamou, cité dans : Amaelle Guiton, « Souveraineté numérique : un modèle à inventer », *Libération*, 20 mai 2016). Pour Pierre Bellanger, elle correspond à « la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques », ce qui implique « l'extension de la République dans cette immatérialité informationnelle qu'est le cyberespace » et « l'expression sans entrave, sur les réseaux numériques, de la volonté collective des citoyens » (La souveraineté numérique, Stock, 2014). Le rapport de la commission d'enquête du Sénat sur la souveraineté numérique, en 2019, la définit comme « la capacité de l'État à agir dans le cyberespace », ce qui est une « condition nécessaire à la préservation de nos valeurs » impliquant, d'une part, « une capacité autonome d'appréciation, de décision et d'action dans le cyberespace » et, d'autre part, la maîtrise de « nos réseaux, nos communications électroniques et nos données ». De façon plus novatrice, d'autres relient la souveraineté numérique à la capacité de certains acteurs à se faire obéir, à imposer leurs lois, à apparaître comme devant être respectés dans l'espace numérique (Pierre

La souveraineté numérique : « S'autodéterminer dans l'espace numérique »



Source : Pauline Türk.

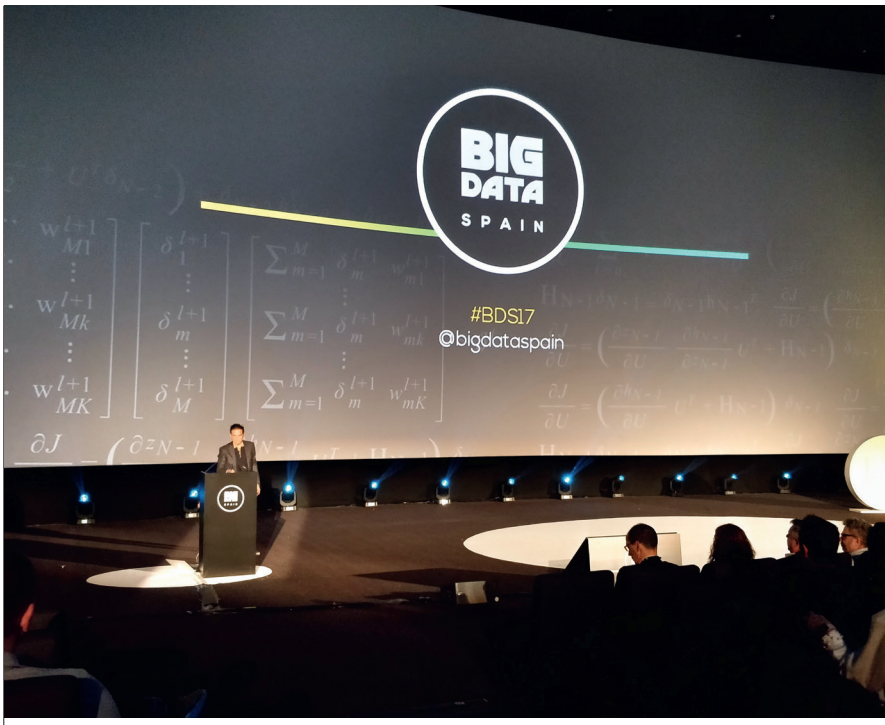
Trudel, professeur à l'université de Montréal). Ou encore se réfèrent, pour l'appréhender, à l'appropriation de certains attributs de la souveraineté par les entreprises, grâce à leur position dominante sur le marché (Annie Blandin-Obernesser, op. cité).

La notion est, on le voit, appréhendée de façons très diverses, qu'il s'agisse de prolonger la souveraineté des États dans l'espace numérique, ou d'imaginer de nouvelles formes de souveraineté, non étatique.Elle reçoit plusieurs acceptions, juridique, économique, technique ou « fonctionnelle », et se conçoit également, selon les cas, à différents niveaux, national (conservation des archives publiques sur un « cloud souverain » par exemple), européen (protection des données personnelles), ou même international (gouvernance des réseaux).Hors du champ juridique, la souveraineté numérique est même parfois conçue comme individuelle, ou collective (communauté d'utilisateurs).

Pour mettre de l'ordre dans ces acceptions, on peut retenir trois approches du concept de souveraineté numérique.

Approche juridique : la souveraineté des États

La première est juridique, naturellement : la souveraineté numérique est celle des États (Pauline Türk, « La souveraineté des États à l'épreuve d'internet », *Revue du droit public*, 2013 n° 6). Alors que les instruments de leur souveraineté deviennent indissociables de la technologie numérique, les États revendiquent le prolongement de leur pouvoir de réglementation sur les réseaux, le respect de leur autorité, et l'égalité dans les instances de gouvernance, face à l'hégémonie des États-Unis et, plus récemment, à la montée en puissance de la Chine. Certains États (Russie, Chine, Iran…), retiennent une conception autoritaire, voire offensive, impliquant le droit de reprendre le contrôle des espaces numériques, d'y appliquer leurs lois, d'y promouvoir leurs intérêts. D'autres, en Europe par exemple (Allemagne, France…), retiennent une approche plus libérale et défensive, consistant dans le droit pour l'État de protéger ses citoyens et leurs libertés contre les entités malveillantes ou mues par des intérêts purement commerciaux.



Big Data Spain (renommé Big Things depuis 2019) est l'une des plus importantes conférences européennes consacrées au big data, à l'intelligence artificielle, aux technologies du cloud et à la transformation numérique

DAVID MARTIN/FLICKR/ CC BY-SA 2.0

Approche politique et économique : la souveraineté des opérateurs économiques

On peut aussi soutenir qu'il existe une deuxième approche, de nature politique et économique : la souveraineté numérique serait alors celle des opérateurs économiques (GAFAM) qui disposent *de facto* du pouvoir d'imposer des règles. Quelques multinationales bénéficient d'une suprématie, grâce à leur domination sur les marchés, et exercent un véritable pouvoir de commandement et

de réglementation dans lecyberespace. Elles fixent ainsi les conditions générales d'utilisation de services en ligne devenus indispensables, développent les algorithmes, décident de supprimer des contenus, de fermer le profil d'un utilisateur, de conserver ou de vendre les données personnelles dont elles assurent le stockage… Certaines créent leurs propres monnaies virtuelles (Bitcoin, projet Libra), et se dotent de leurs propres services de règlement des différends. D'autres bâtissent des projets de sociétés fondées sur le progrès technologique, où elles auraient vocation à rendre des services équivalents, voire supérieurs à ceux des États, ainsi remplacés.

Approche libérale : la souveraineté numérique des utilisateurs

Une troisième approche s'avère possible, plus libérale et individualiste : il s'agirait d'une souveraineté numérique des utilisateurs. Inspirée des fondements de la souveraineté populaire, selon laquelle les citoyens sont la source de tout pouvoir, elle correspond au droit des personnes de s'autodéterminer. Les utilisateurs peuvent effectuer des choix, exprimer des préférences, se détourner de certaines applications, peser dans des forums dédiés à la normalisation technique (par exemple le W3C, organisme de standardisation à but non lucratif, fondé en octobre 1994 chargé de promouvoir la compatibilité des technologies du World Wide Web telles que HTML, XHTML, XML, etc.), ou plus simplement en tant que consommateurs. Le pouvoir envisagé ici peut être exercé collectivement, dans le cadre de communautés d'utilisateurs (transnationales), ou à titre individuel. Il se traduit aussi, concrètement, par des droits et garanties, en cours de consécration, tels le droit à la protection des données personnelles, à la portabilité des données, à l'oubli ou au déréférencement, qui pourraient être inclus dans un droit plus général à « l'autodétermination informationnelle » selon l'approche allemande (P. Türk, « Le droit à l'autodétermination informationnelle », *Revue Politeia*, 2017, n° 31).

> *Les utilisateurs peuvent effectuer des choix et peser dans des forums dédiés à la normalisation technique*

La notion de souveraineté numérique ne se limite donc pas à la stricte perspective juridique classique, attachée au pouvoir des États. Elle renvoie dans son acception la plus large, au pouvoir de commandement et au droit à l'autodétermination dans un monde numérique. Qui fixe les règles ? Sur quel fondement et avec quelle légitimité ? À qui obéit-on, et avec quelles garanties ? Répondre à ces questions, c'est comprendre qui est souverain sur les réseaux et comment s'exprime cette souveraineté.

Implications de la souveraineté numérique

Les défis sont nombreux et divers. Sur le plan juridique et politique, ils apparaissent à plusieurs niveaux.

À l'échelle nationale

À l'échelle nationale, les États sont les grands perdants : dépendants des outils technologiques, ils peinent à faire respecter leur politique fiscale (débats sur la « taxe GAFA ») et leurs lois sur les réseaux (divulgation de données sensibles, adaptation des lois sur la publication des sondages ou sur les jeux en lignes, abus de la liberté d'expression en

En décembre 2012, lors de la Conférence mondiale des télécommunications internationales de Dubaï, Chine et Russie ont exprimé leur volonté de pouvoir administrer eux-mêmes leur internet national

ITU PICTURES/FLICKR/CC BY 2.0

débat, à propos des lois « anti-infox (*fake-news*) » ou de lutte contre la haine sur internet). Ils doivent aussi s'adapter à de nouvelles menaces (cybercriminalité, piratage informatique (*hacking*), espionnage, rançongiciel (ou *ransomware*). Face aux géants de la Silicon Valley, le rapport des forces leur est nettement défavorable (écart important dans la maitrise des technologies (*gap*), situations de monopole, lieu de stockage des données, tribunaux compétents, extraterritorialité, etc...), d'autant que, dans l'espace numérique, le paradigme classique du pouvoir politique hiérarchique, pyramidal et unilatéral (gouvernement et réglementation) cède le pas à une organisation du pouvoir réticulaire, décentralisée, impliquant largement les acteurs privés (gouvernance et régulation).

À l'échelle européenne

À l'échelle européenne, certaines valeurs (inclusion, dignité) et certains droits fondamentaux (vie privée, liberté d'expression) doivent être protégés et promus. Contre la logique de patrimonialisation des données personnelles, la consécration d'un droit à l'autodétermination informationnelle permettrait de garantir le droit des individus à maîtriser l'usage et le devenir des données personnelles fournies, ainsi que les « traces » laissées par l'activité numérique. Certains droits qui en sont dérivés ont déjà été consacrés, notamment au niveau européen, par le Règlement général sur la protection des données personnelles (RGPD) entré en vigueur en 2018, ou par la Cour de justice de l'Union européenne (droit à l'oubli, au déréférencement, à la portabilité des données, au consentement, à l'information et à la rectification...) L'Europe est désormais plus vigilante, elle qui a longtemps adopté, face au pillage et au marchandage des données de ses citoyens, « le même système de défense qu'un buffet du club Med » (P. Bellanger, *La souveraineté numérique*, 2014, Paris, Stock, p. 160). Elle bénéficie d'un atout de poids : les consommateurs

Une rançongiciel rend inaccessible les fichiers de la victime en les chiffrant et lui réclame une rançon en échange de la clef qui pourrait permettre d'en recouvrer l'accès.

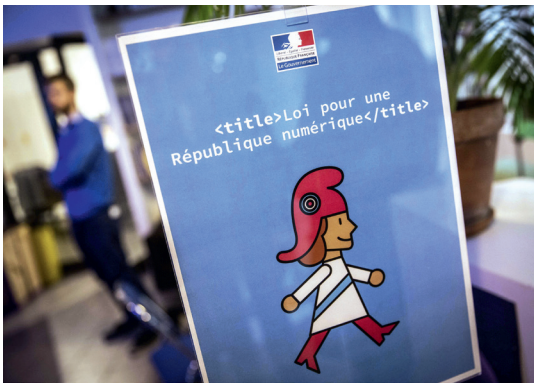
européens constituent le premier marché économique pour les géants du numérique.

À l'échelle internationale

À l'échelle internationale, la gouvernance du monde numérique doit sans doute être réformée, car insuffisamment multilatérale, démocratique et transparente. La fonction de normalisation est confiée à des acteurs privés, des organismes mal connus, ou des groupes informels dont la légitimité et l'indépendance (vis-à-vis des pays occidentaux, des États-Unis en particulier, et des groupes d'intérêts), ne sont pas suffisamment garanties. Faute de partage des responsabilités, les États non occidentaux les plus puissants économiquement ou technologiquement en ont tiré des conséquences en cherchant à faire « internet à part », ce qui est préoccupant pour l'avenir des réseaux. Pour les Européens, prendre notre part dans la gestion des réseaux et y promouvoir nos valeurs est un impératif démocratique : nous avons bataillé deux siècles durant pour avoir des gouvernements élus, responsables, transparents, tenus d'agir dans l'intérêt général et de rendre des comptes. Or ces gouvernements sont concurrencés par de nouvelles instances dirigeantes opaques qui ne sont soumises à aucune de ces contraintes et exigences. C'est pourquoi certains réfléchissent à formaliser, dans une « charte » à vocation universelle, les principes essentiels qui doivent guider le développement des technologies (neutralité, liberté d'expression, diversité linguistique, protection de la vie privée…).

Éduquer les jeunes générations

D'autres enjeux tiennent aux modes d'expression de la citoyenneté, à la responsabilisation des individus, appelés à se réapproprier la fraction de souveraineté qui leur revient (concept anglo-saxon d'« *empowerment* » ou « émancipation »), afin d'expérimenter une citoyenneté plus active. Si elles ne veulent pas subir l'évolution technologique, les jeunes générations doivent apprendre à maîtriser les outils numériques, à connaître et faire valoir leurs droits et libertés, et à se préoccuper de la construction et de la protection de leur « identité numérique », générée par l'ensemble des traces laissées volontairement ou non sur les réseaux.



Le projet d'un Commissariat à la souveraineté numérique chargé de superviser la mise au point d'un système d'exploitation français n'a pas abouti à ce jour
© HAMILTON/REA

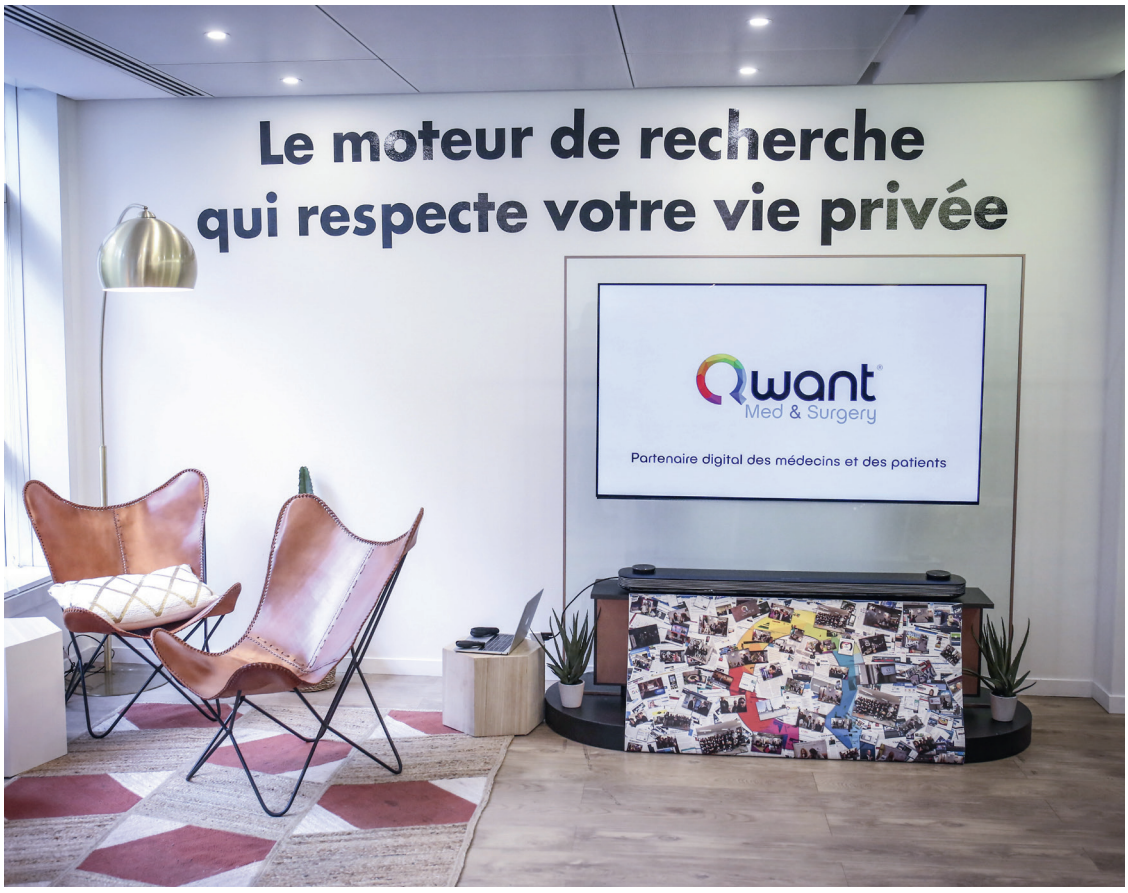
> *Un enjeu majeur réside dans la crédibilité technologique des entreprises européennes*

Les enjeux économiques et industriels

Enfin, de lourds enjeux économiques et industriels résultent de la dépendance de l'économie mondiale au secteur numérique.

L'exploitation de la masse de données collectées (*big data*), agrégées et traitées par des algorithmes, permet de probabiliser – voire d'orienter – le comportement des consommateurs et des clients, ce qui ouvre

Au sujet de «l'internet à part» les Américains parlent de «*splitinternet*» qu'on traduit souvent en France par l'expression «balkanisation du web». Cette expression désigne la fragmentation du web, la scission entre plusieurs réseaux fermés.



Locaux de la société française Qwant. La direction interministérielle du numérique (DINUM) a demandé aux directions du numérique ministérielles que le moteur de recherche Qwant soit proposé par défaut aux agents publics.
© HAMILTON/REA

des perspectives immenses : adaptation en temps réel de l'offre commerciale, révolution des démarches publicitaires et marketing, comparaison des prix, gestion des stocks, etc. Un enjeu majeur réside dans la crédibilité technologique et le niveau de compétitivité des entreprises européennes, qui doivent prendre une meilleure part sur des marchés émergents. Malgré le nombre des consommateurs européens, elles y sont pour l'instant sous-représentées, mis à part quelques « licornes » (startups valorisées à plus d'un milliard de dollars telles que Vinted, Deliveroo, Bolt, Zalando, Skype, spotify, ou les françaises Blablacar, Deezer, Doctolib ou OVHcloud).

Les tentatives de développement de programmes européens, y compris français, susceptibles de rivaliser avec les outils américains ou même asiatiques peinent à convaincre ; les deux projets de *cloud* souverain Numergy et Cloudwatt ont été des échecs. Le moteur de recherche français Qwant lancé en 2013, offrant une alternative aux utilisateurs soucieux de la protection de leurs données personnelles, la bibliothèque numérique européenne Europeana, ou les avancées en matière de « souveraineté des données » (*cloud* souverain, label SecNumcloud), suscitent davantage d'espoirs. #

Complément+

Intelligence artificielle et souveraineté numérique

L'intelligence artificielle (IA) correspond à l'aptitude d'une machine à imiter le cerveau humain, en connectant entre elles les données accumulées afin de produire une action, une décision, un résultat. Une machine capable d'accumuler et de traiter d'immenses masses de données, de réaliser des calculs et d'établir des probabilités, pourrait dépasser l'intelligence humaine, ce qui a déjà été testé aux échecs ou au jeu de go. Les IA les plus prometteuses sont auto-apprenantes (*deep learning*), c'est-à-dire capables de s'auto-entraîner et d'adapter leur comportement, voire leur conversation pour les machines capables d'interagir, en fonction des réactions de l'environnement et de l'expérience acquise. Certaines sont dotées de capteurs sensoriels et d'une coque humanoïde; c'est le cas, par exemple, de Sophia, conçue en 2015 par l'entreprise Hanson Robotics à Hong Kong, capable d'interagir avec les humains. Apprenant de leurs erreurs, ces machines pourraient développer, dans l'avenir, des aptitudes dépassant ou s'écartant de celles qu'ont pu concevoir les ingénieurs chargés de les programmer, manifestant ainsi une intelligence autonome.

La capacité à créer, maîtriser, contrôler, exploiter les potentialités de l'IA conférera à ceux qui l'exerceront une supériorité sur tous les plans. Imaginons le pouvoir de ceux qui seront capables de piloter les robots soldats; de concevoir les robots chirurgiens, de prévoir les épidémies ou de prévenir certaines maladies; de biaiser les algorithmes qui fondent le commerce ou l'exercice de la justice, de programmer ou déconnecter les machines chargées de la conservation de la mémoire d'une famille ou d'une entreprise; de prendre le contrôle à distance de tout appareil connecté, véhicule autonome, drone, assistant personnel, outil domotique, objet connecté de santé... Garder le contrôle de ces machines est un enjeu de souveraineté numérique : il s'agit d'éviter de tomber sous le joug d'opérateurs déjà puissants qui s'approprieraient ces technologies; d'être en capacité d'empêcher certaines entités d'en faire un usage malveillant; voire même d'éviter que les machines elles-mêmes, un jour, ne puissent prendre le contrôle! (Sur les enjeux, voir Claude de Ganay et Dominique Gillot, «Pour une intelligence artificielle maîtrisée, utile et démystifiée», rapport d'information de l'Office parlementaire des choix scientifiques et technologiques Sénat Assemblée nationale, n° 464, 15 mars 2017; Cédric Villani, «Donner du sens à l'intelligence artificielle : pour une stratégie nationale et européenne», rapport au Premier ministre, vie-publique.fr, 2018; Laurent Alexandre, *La guerre des intelligences*, Paris, J.-C. Lattès, 2018.) Une stratégie nationale de recherche en intelligence artificielle a été lancée par le gouvernement en novembre 2018 (www.strategie.gouv.fr/actualites/strategie-nationale-intelligence-artificielle). Elle a pour ambition de favoriser l'écosystème de recherche en IA, d'investir pour soutenir des projets structurants et de faire émerger des champions français ou européens, notamment dans le secteur des véhicules autonomes, d'adapter le cadre réglementaire et financier, ou encore de définir les enjeux éthiques et politiques de l'IA.

Pauline Türk

Des algorithmes toujours plus puissants permettent à l'intelligence artificielle de détrôner les champions humains des jeux de plateau (échecs, go, shogi)
© [SERGEY]/ADOBE STOCK

La souveraineté numérique : rapport de synthèse

par Christian Vallar,
Professeur agrégé de droit public, Doyen de la Faculté de droit et Science politique de Nice, Directeur du CERDACFF, EA 7267, Avocat au Barreau de Nice

À l'issue de ces riches travaux, il nous apparaît que la réflexion sur la souveraineté numérique nous conduit au transhumanisme, à la dimension prométhéenne sinon faustienne d'un certain nombre de problématiques posées par ces grandes firmes, dont les fameux GAFA, auquel s'ajoute Microsoft. Google est emblématique en matière de santé, car sa direction a pour projet déclaré, à l'aide de plusieurs dizaines de milliards de dollars de financement, de bâtir l'homme « amélioré » avec une tension vers l'immortalité physique, faisant de l'homme une espèce de nouvelle divinité. C'est un vieux rêve prométhéen, c'est un vieux rêve faustien que ces entreprises poursuivent à leur niveau, totalement mondialisé. Au-delà des nombreux enjeux, économiques, juridiques, politiques et de sécurité, il s'agit là d'une transformation de la nature de l'homme. Si les États, soit individuellement, soit de manière unie à l'échelle européenne, ne jouent pas leur rôle, c'est-à-dire ne veillent pas au destin de leur nation et de leur peuple, les perspectives d'avenir sont pour le moins troublantes, car l'on sait comment s'est achevée la destinée de Prométhée…

Le professeur Rousseau a rappelé la conception classique de la souveraineté selon Bodin, laquelle, idéologiquement, justifie le pouvoir royal par rapport aux seigneurs féodaux, mais aussi par rapport aussi à l'Église. Il s'est demandé sans détour si elle était pertinente pour appréhender les phénomènes liés à la révolution numérique et si l'approche en termes de souveraineté n'était pas tout simplement dépassée. Il a aussi proposé quelques

échappées européennes voire universelles, au travers des notions de « coopération loyale » ou de « bien commun » qui lui semblent prometteuses.

Le professeur Türk s'est penchée sur la polysémie de la notion de souveraineté. Elle a d'abord rappelé la conception classique, la capacité à se faire obéir pour un État, son auto-détermination, ses compétences régaliennes, la maîtrise sur un peuple, mais aussi la souveraineté affaiblie par le haut et par le bas, que ce soit par la décentralisation ou par la construction européenne ou encore par le rôle des acteurs transnationaux. Elle a souligné, néanmoins, des phénomènes de consolidation, ou de « retour à l'État », justement en réaction aux nouvelles menaces, aux nouveaux enjeux. Elle a ensuite étudié la notion même de souveraineté numérique dans ses différentes acceptions, jugées plus ou moins opérantes ou pertinentes en droit constitutionnel. Elle a évoqué, parmi d'autres, l'ouvrage de Pierre Bellanger qui n'est pas un classique de la doctrine juridique, loin s'en faut, mais un classique du numérique. Pour lui, la maîtrise du destin collectif dans le cadre des réseaux numériques passe par la souveraineté numérique, afin d'éviter la vassalisation des sociétés, appelant à l'alliance des sociétés françaises et européennes, face à ce qui constitue, de son point de vue, une menace, et non pas un acquis. Mais la souveraineté numérique, Pauline Türk l'a rappelé dans son rapport, est parfois présentée comme la souveraineté des individus, des groupes d'individus, sinon d'opérateurs privés, citant le professeur Blandin-Obernesser qui considère que des entreprises s'attribuent des parcelles de souveraineté. Personnellement ces conceptions me laissent perplexe, l'éparpillement de la souveraineté m'apparaissant antinomique de la notion même de souveraineté, qui est une ou n'existe pas ! Parler d'un « individu souverain » me paraît être une contradiction dans les termes. Pour moi, au sens classique, la souveraineté est celle de l'État ou celle d'une institution, mais pas celle d'un individu qui s'auto-détermine librement. La notion même de *souveraineté partagée* entre une pluralité de personnes est un véritable non-sens. Il y a une contradiction dans les termes, la souveraineté ne peut être partagée. D'ailleurs cette conception n'est pas entendue par certains États, qui en retiennent une vision très différente, comme la Russie, la Chine, l'Arabie saoudite, qui ont une appréhension très contrôlante du phénomène numérique favorable à la sécurité, tandis que l'Europe est plus partagée entre sécurité et liberté.

Le professeur Quiviger nous a présenté, du point de vue du philosophe, l'ambivalence de la notion de souveraineté numérique. S'agit-il de

la souveraineté classique de l'État sur le numérique, pour le contrôler ? S'agit-il du *numérique souverain* ce qui, au-delà de l'inversion des mots, est aussi une inversion des concepts ? Il s'est demandé s'il n'y avait pas, de manière positive ou négative selon les points de vue, une déconnexion entre l'État et le numérique, ce qui peut être au bénéfice ou au détriment de l'un ou de l'autre. Le *numérique souverain* revêtirait un caractère positif, c'est-à-dire une dimension que les États peuvent s'approprier, permettant une coexistence des souverainetés gérant le numérique sur le plan international.

Monsieur Nocetti a mis en évidence les fondements de l'affirmation de la souveraineté des États par rapport au numérique, envisagé comme une menace, une source de défiance à l'égard de leur autorité, citant la Chine, la Russie, les Emirats arabes unis, les pays du Golfe dans leur ensemble. Si le numérique défie la souveraineté des États, les parties prenantes développent des conceptions parfois « opposés voire irréconciliables » nous a-t-il rappelé. On pourrait citer le cas extrême de la Corée du nord, qui ne tolère que 26 sites internet, n'autorise qu'un millier de comptes internet et la vente seulement d'une centaine d'ordinateurs par an fabriqués par une société d'État.

Au contraire Marc Mossé, responsable de ces questions chez Microsoft, a fait rimer le numérique développé avec la souveraineté retrouvée. Selon lui, la souveraineté est un concept d'une « réelle plasticité », ce qui permet d'en considérer diverses applications, entre souveraineté technologique, souveraineté individuelle et souveraineté étatique. La thèse d'une souveraineté technologique se distingue fondamentalement de la souveraineté classique de l'État en droit constitutionnel et en droit international. Pour la Silicon Valley, la technologie va se substituer à l'État, ce qui rejoint un courant très fort, celui de la souveraineté individuelle, qui se rattache à Henry David Thoreau et aux libertariens, pour lequels l'État est une gêne. C'est pourquoi Marc Mossé tient à souligner que, chez Microsoft, le respect des droits et des libertés est une valeur fondamentale, prenant exemple de la bataille juridique opposant Microsoft au juge américain dite NY warrant case. La Cour d'appel de New York a finalement donné raison à l'entreprise qui voulait garantir les droits de son client en refusant de communiquer des informations, sous peine de rompre le pacte de confiance. Il est intéressant de préciser que l'État d'Irlande faisait cause commune avec Microsoft, au nom de sa souveraineté. Des informations

peuvent certes être communiquées, mais dans le cadre de traités internationaux, et en l'espèce il y aurait eu atteinte à la souveraineté irlandaise au nom de la soi-disant extraterritorialité d'une loi américaine. Ce cas démontre, il me semble, que les souverainetés ne sont pas mortes, n'en déplaise aux libertariens de la Silicon Valley. Car il y a bien un heurt de souveraineté dans cette affaire, où s'affrontent la souveraineté irlandaise et la souveraineté américaine. Retrouver la souveraineté, finalement, impliquerait une recentralisation, au sens où les États reprendraient le contrôle du numérique ? Faut-il, pour retrouver la souveraineté, créer un commissariat à la souveraineté numérique ou développer des programmes de cloud souverain ?

Bernard Benhamou, quant à lui, travaille depuis 2006 à faire reconnaître la dimension internationale du concept de souveraineté numérique, mettant en avant à juste titre la faiblesse intellectuelle de la classe politique ou des dirigeants des États européens qui ne connaissent pas vraiment les technologies qu'ils veulent réguler. Il faut connaître le code informatique pour comprendre le droit des réseaux, souligne-t-il, en rappelant l'enthousiasme naïf de certains responsables publics quant à certains instruments, tels les monnaies virtuelles, dont le fameux bitcoin, qui soi-disant créerait de nouveaux rapports sociaux idylliques. Tout ceci n'est pas nouveau, puisque resurgit le vieux mythe de la technologie soi-disant neutre, alors que la technologie est tout sauf neutre. Derrière les monnaies virtuelles, il y a la cryptographie de la NSA. L'Europe ne doit pas devenir une colonie numérique, comme l'ont rappelé plusieurs intervenants, citant un rapport sénatorial bien connu, car il s'agit bien d'une forme de colonisation insidieuse. L'Europe est une force de consommation, mais les cathédrales logicielles sont édifiées ailleurs. L'Europe est vulnérable, car elle consomme mais ne fabrique pas. Il est donc indispensable que le politique cesse de méconnaître les GAFAM, et Bernard Benhamou garde l'espoir de voir le numérique, après la bioéthique, après l'écologie, devenir un objet politique. Évoquant les rêves – ou les cauchemars – transhumanistes de certains dirigeants, différents intervenants ont pu souhaiter que l'Europe trouve une voie permettant d'imposer ses conceptions sans pour autant attaquer l'architecture des réseaux. Sans céder à la dérive autoritaire fondée sur le contrôle et la méfiance qui l'endommagerait, Bernard Benhamou souhaite une prise de conscience de l'objet numérique, de ses réalités et ses enjeux, ce qui incombe aussi aux juristes traditionnalistes réactifs, afin

d'avancer vers un grand traité du droit du numérique, qui serait le pendant de la réglementation internationale du droit de la mer.

Le professeur Derosier lui aussi a montré les faiblesses du concept flou de souveraineté numérique, citant Pierre Bellanger, mais se référant également à l'article 29 de la loi sur la République numérique prévoyant un commissariat à la souveraineté numérique, évoquant un concept néo-générationnel, dépassant les modèles établis. La fameuse pyramide de Kelsen est dépassée. Nous vivons l'époque du réticulaire, c'est-à-dire des réseaux. Il faut penser global, au niveau européen et non plus en rester au niveau étatique. La démocratie numérique prolongera-t-elle la démocratie constitutionnelle ? Pour Jean-Philippe Derosier, le concept de souveraineté numérique est bi-dimensionnel en ce sens qu'il peut être juridiquement entendu dans deux dimensions : le numérique est dans la souveraineté et la souveraineté est dans le numérique. La souveraineté dans le numérique peut signifier le contrôle, la domination, la fermeture des frontières numériques, avec les exemples des États déjà cités. Cela peut s'exprimer de façon plus « soft » – pour rester dans la logique du hardware et du software – par la transparence ou la vérification, comme en Europe, que les systèmes fonctionnent correctement. Mais cette souveraineté numérique est d'ordre mondial, donc il risque de ne plus y avoir d'État donc plus de droit, ce qui devient intenable. En tout cas, la souveraineté numérique n'est ici qu'une compétence parmi d'autres, un des éléments de la souveraineté de l'État, ce qui rejoint l'approche classique de la souveraineté numérique, exposée par Pauline Türk précédemment.

La dimension européenne a été développée cet après-midi, d'abord par Madame Falque-Pierrotin, présidente de la CNIL, qui d'emblée a déclaré qu'il y a un déficit de souveraineté, un déficit de l'État, donnant l'exemple des lois extra-territoriales américaines, ce qui fait obstacle à une vraie protection des données en Europe. En effet au niveau collectif comme au niveau individuel, où se situe en principe la capacité de décider librement, le rapport de force est défavorable. Mais la riposte s'organise, à l'échelon pertinent à ses yeux, l'échelon européen. Un arsenal juridique européen se constitue, n'autorisant les exportations de données que de manière dérogatoire, avec l'aide de la Cour de justice de l'Union européenne. Le qualificatif utilisé est celui de « bulle de sécurité ». Un règlement qui entrera en vigueur en mai 2018 autorisera l'application du droit européen quel que soit le lieu où l'entreprise a son siège. L'autodétermination

informationnelle sera favorisée, c'est-à-dire que l'individu pourra consentir à la saisie et au contenu de ses données et pourra changer d'opérateurs sans difficulté. Dans le cadre juridique global ainsi dessiné, la « souveraineté collective et individuelle » reste à reconquérir, mais le processus est en bonne voie.

Madame Roques Bonnet, docteur en droit public et cadre juridique chez Microsoft, a également remis en cause l'approche hiérarchique classique illustrée par la pyramide de Kelsen. Elle a exposé les enjeux de la jurisprudence européenne sur des cas concrets, montrant les lacunes des dispositifs de protection européens, et montrant que Microsoft cherche à garantir la confidentialité des données et à conserver la confiance des utilisateurs, avec l'aide du juge européen et contre le juge américain, parfois, comme l'illustre le fameux contentieux opposant Microsoft et l'Irlande aux États-Unis (NY Warrant case tranché par la Cour d'appel fédérale de New York en juillet 2016).

Sur la question de la protection des données, Rémi Puigventos a ouvert des pistes concernant les conditions de l'exploitation du big data, rappelant le potentiel économique déterminant des grandes banques de données. Il a évoqué l'« incapacité étatique à appréhender l'économie du big data » et notamment la difficulté pour l'État français d'appréhender ce matériau sur le terrain fiscal. La multiplication des « applications », en particulier en matière de santé, remet en cause la légitimité de l'État à définir l'intérêt général et entraine l'obsolescence de certaines politiques publiques. Mais, à l'inverse, l'État peut aussi se servir du big data, par exemple en matière de lutte contre la fraude fiscale ou de gestion des transports, donc l'espoir reste de mise. Quant à Clément Tulloue, il a insisté sur les bouleversements engendrés par la « nouvelle économie de plateformes » et sur la difficulté à transposer au monde numérique l'idée de droit de propriété ou celle de patrimonialisation des données, soulignant une tendance à la contractualisation de la protection des données, et saluant la reconnaissance du « droit à l'oubli » par la Cour de justice européenne.

Mais les enjeux du concept de souveraineté numérique sont aussi et fondamentalement liés à la sécurité. Le professeur Xavier Latour a exploré les arcanes de la cyberdéfense et de la cybercriminalité, mises en perspective par le droit constitutionnel. La cyberdéfense reflète les difficultés issues d'une répartition des rôles complexe au sein de l'exécutif, entre le chef de l'État, le Premier ministre et le gouvernement. En réalité, si l'on suit le

découpage constitutionnel, on frôle le ridicule. Car si ce sont les intérêts vitaux de la Nation qui sont en cause, la compétence revient semble-t-il au Premier ministre, alors que si le risque ou l'opération est purement militaire, c'est au Président de la République d'agir ! Or, évidemment, dans de nombreux cas, nul ne sait *a priori* d'où viennent les menaces et les attaques, qui peuvent provenir du public, du secteur privé, sans suivre ce savant découpage constitutionnel. Les cyber-attaques, particulièrement, peuvent être un instrument au service du terrorisme, sans que l'on sache qui, de la police ou de l'armée, soit appelée en première ligne. Xavier Latour propose judicieusement la notion de *cyber-crise*, précisant qu'il serait opportun que, dans la Constitution, soit mentionné l'usage légitime de la force.

Le Général Watin-Augouard poursuit la réflexion sur le sujet du continuum défense-sécurité dans le cyber-espace, considérant qu'il n'y a pas de cyber-guerre au sens juridique. Car une guerre suppose un ennemi identifié, ce qui est rarement le cas dans le cas de cyber-attaques telles celles vécues à l'échelle mondiale en mai et juin 2017 par exemple. Il faut donc en rester à la notion de cyber-criminalité. Encore faut-il que l'État français réaffirme son autorité, car les acteurs privés prédominent. Avec la révolution numérique, la logique de stock a laissé place à une logique de flux. En matière criminelle également, nous sommes sur des logiques de flux criminels. La loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement s'inscrit dans cette logique, en donnant compétence unique au TGI de Paris. La coopération décisive avec le secteur privé est nécessaire et décisive. Rappelons qu'il manque 900 000 spécialistes à l'échelle de l'Union européenne pour faire face aux cyber-menaces ! Si, pour le général Watin – Augouard, « la transformation numérique entraîne un retour de l'État « gendarme », afin de mieux assurer les missions de défense et de protection, la réponse efficace nécessite une alliance des États, à l'échelle européenne notamment, qui est l'échelon adéquat. Le rôle fondamental des juges, nationaux mais aussi de la Cour de Justice de l'Union européenne, a été abondamment souligné et illustré. L'Europe est un phare en matière de cyber-sécurité, qui porte une troisième voie, entre la démarche sécuritaire et la conception extensive du principe de liberté défendue aux États-Unis, quand cela sert leurs intérêts…

Valentine Martin, traitant des débats relatifs à la loi pour une République numérique, a d'abord rappelé que, du temps du général De Gaulle, un *plan calcul* avait été lancé, sans succès, les américains nous ayant damé

le pion ! En 2009, c'est l'idée d'un centre de données national, d'un cloud souverain, qui est mise en avant, mais hélas sans succès, les deux projets lancés se neutralisant l'un l'autre… Tout espoir n'est pas perdu puisqu'une note de la direction des collectivités locales du 5 avril 2016 demande aux collectivités d'utiliser un cloud souverain. En parallèle, Microsoft nous annonce qu'il va construire un data center en France en 2017. Quant au projet de commissariat à la souveraineté numérique, il en laisse certains dubitatifs, et d'ailleurs, le rapport sur le sujet, qui devait être remis avant janvier 2017, en application de l'article 29 de la loi pour une république numérique, se fait toujours attendre..[1].

Le professeur Meunier a clôturé les travaux en expliquant que la croissance dans l'Union européenne nécessite la création d'un véritable marché unique numérique européen. Une stratégie a été adoptée en 2015 autour de trois axes : fluidifier les activités, développer les réseaux, maximiser la croissance de l'économie numérique. Elle développe largement les compétences partagées entre les États membres et l'Union européenne, allant de la fédération des connexions, jusqu'à la création de centres décisionnels supra nationaux ou le désenclavement des zones rurales pour lesquelles le numérique est bien utile. L'Europe apparaît décidément comme le niveau pertinent de réflexion, et le rôle protecteur et efficace de la Cour de justice de l'Union européenne est ici encore souligné, de même que l'importance de la refonte de la réglementation européenne en matière de police, de justice et de sécurité collective.

Finalement, le numérique est à la fois une chance et une menace : comme toute technologie, elle est ce qu'on en fait. Elle est un outil, ni bon ni mauvais en lui-même. Si l'on en croit les projets de certains dirigeants des GAFAM, son développement est inquiétant[2]. Un ouvrage « L'homme

1. Article 29 Loi du 7 octobre 2016 pour une république numérique : « Le Gouvernement remet au Parlement, dans un délai de trois mois à compter de la promulgation de la présente loi, un rapport sur la possibilité de créer un Commissariat à la souveraineté numérique rattaché aux services du Premier ministre, dont les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège. Ce rapport précise les moyens et l'organisation nécessaires au fonctionnement du Commissariat à la souveraineté numérique ».

2. E. Schmidt et J. Cohen, *The new digital age reshaping the future of People, Nations and Business,* Knopf, 2013.

nu. La dictature invisible du numérique »[3] développe par exemple une vision cauchemaresque du numérique, celle d'une humanité en esclavage et qui se croit libre. La dictature est douce, souple, molle, et d'autant plus efficace qu'elle se présente sous le masque de la liberté. La menace atteint-elle vraiment ce niveau ? Quoi qu'il en soit, en tant que juriste publiciste, je maintiens que la souveraineté des États est déterminante : c'est en quelque sorte un pare-feu qui permettra de protéger les peuples et les Nations. Mais bien sûr il n'est pas possible pour les États de rester isolés, mis à part la Chine, la Russie, ou d'autres très grands États qui peuvent se permettre de jouer en solitaire. L'articulation des compétences nationales et européennes est sans doute la clef. Seul ou allié, un État n'est plus digne de ce qualificatif s'il se départit de sa souveraineté dans le domaine du numérique.

3. M. Dugain et C. Labbé, éd. Plon, 2016.

POUVOIRS

REVUE FRANÇAISE D'ÉTUDES CONSTITUTIONNELLES ET POLITIQUES

LA SOUVERAINETÉ EUROPÉENNE

N° 190

Prix Guy-Carcassonne
« *Le Monde* – *Pouvoirs* – Club des juristes »
du meilleur article constitutionnel

Guy Carcassonne, constitutionnaliste reconnu, eut une vraie passion, celle de l'Université, et un engagement, celui de partager son enseignement avec ses étudiants.

En sa mémoire, le prix Guy-Carcassonne récompense chaque année l'auteur de moins de 40 ans d'un article inédit de cinq mille signes portant sur une question constitutionnelle, *lato sensu*, liée à l'actualité française ou étrangère. Cet article doit aider à faire comprendre au plus grand nombre les enjeux juridiques, politiques et sociaux posés par cette question constitutionnelle.

Le prix Guy-Carcassonne sera décerné pour la dixième fois en début d'année 2025. Les candidats pourront adresser leur article dès le 1er novembre 2024 à l'adresse e-mail dédiée au prix :

prixguycarcassonne@leclubdesjuristes.com

Le jury du prix sera constitué de membres de la revue *Pouvoirs*, du Club des juristes et de la rédaction du journal *Le Monde*, ainsi que de deux professeurs de droit public ou science politique étrangers.

Le lauréat, outre un prix de 1 500 euros, verra son article publié dans le journal *Le Monde* et sur les sites internet de la revue *Pouvoirs* et du Club des juristes.

Pour concourir et obtenir le règlement du prix, consulter :

LeClubdesJuristes.com

Revue-Pouvoirs.fr

« Confrontés à une instabilité et à une concurrence stratégique croissantes et à des menaces grandissantes pour la sécurité, nous avons décidé d'assumer une plus grande responsabilité en ce qui concerne notre sécurité et de prendre de nouvelles mesures décisives en vue de construire notre souveraineté européenne, de réduire notre dépendance et d'élaborer un nouveau modèle de croissance et d'investissement pour 2030. »

Construire notre « souveraineté européenne », le mot est lâché. Le 11 mars 2022, soit quinze jours après le déclenchement de l'invasion de l'Ukraine par la Russie, les chefs d'État et de gouvernement des vingt-sept États membres de l'Union européenne assument pour la première fois, en affirmant leur solidarité avec le peuple ukrainien, l'avènement souhaité d'une souveraineté européenne. Il ne s'agit donc plus seulement d'une prise de position d'un dirigeant d'un État membre, comme avait pu l'être le retentissant discours de la Sorbonne prononcé par le président Emmanuel Macron en 2017, pour « une Europe souveraine, unie, démocratique ». Ce 11 mars 2022, la « souveraineté européenne » est clairement envisagée comme une fin, un objectif ultime à atteindre pour une Union soucieuse d'affermir son indépendance dans un monde toujours plus instable.

Certes, d'aucuns diront que la force symbolique de la notion sert une finalité exclusivement politique, sans souci de la rigueur juridique qui doit conduire à dénier à l'Union européenne toute forme de « souveraineté ». D'autres insisteront au contraire sur la capacité performative d'un tel discours, sur ses potentialités et les effets d'ores et déjà avérés de ce dernier sur la manière dont l'Union réagit, construit ses politiques, se positionne au sein de son environnement, dans des domaines aussi variés que la politique économique, industrielle, de défense, sanitaire ou numérique. C'est l'objet du présent numéro que de mesurer la portée de cette « souveraineté » controversée et d'ouvrir la réflexion sur les multiples questionnements qu'elle suscite.

Myriam Benlolo-Carabot

SOMMAIRE

Miguel Poiares Maduro
Souveraineté européenne : un bilan démocratique 9

Céline Spector
La souveraineté à l'épreuve de l'Europe 23

Stéphanie Novak
L'Union, *policies without politics* ?
Vers un rééquilibrage de ces notions 33

Zaki Laïdi
Europe : une souveraineté à pas lent 45

Enrico Letta
Le marché intérieur,
au carrefour des souverainetés nationales et européenne 59

Jorge E. Viñuales
La politique industrielle verte de l'Union européenne
et l'indépendance énergétique 69

Pauline Türk
La souveraineté numérique européenne,
vers une troisième voie ? 79

Stéphane de La Rosa
Souveraineté et santé : les enjeux juridiques pour l'Europe 91

Francesco Martucci
La souveraineté budgétaire dans l'Union européenne 103

Jean-Louis Bourlanges
Europe souveraine
Entre provocation juridique et refondation politique 113

Anne Levade
Le rejet de la constitution européenne,
ou la fin d'un rêve politique 123

Mathilde Unger
Être européen, est-ce être deux fois citoyen ? 133

CHRONIQUES

REPÈRES ÉTRANGERS
(1er janvier – 31 mars 2024)
Pierre Astié, Dominique Breillat et Céline Lageot 147

CHRONIQUE CONSTITUTIONNELLE FRANÇAISE
(1er janvier – 31 mars 2024)
Jean Gicquel et Jean-Éric Gicquel 153

Summaries 185

LA SOUVERAINETÉ EUROPÉENNE EST ÉTUDIÉE PAR

Jean-Louis Bourlanges, ancien président de la commission des affaires étrangères à l'Assemblée nationale (2021-2024), ancien membre du Parlement européen (1989-2007). Il participe régulièrement à l'émission « Le nouvel esprit public » de Philippe Meyer, diffusée en podcast sur LeNouvelEspritPublic.fr.

Stéphane de La Rosa, professeur de droit public à l'université Paris-Est Créteil, directeur de l'équipe de recherche MIL, titulaire de la chaire Jean-Monnet sur les instruments de la souveraineté économique européenne (stephane.delarosa@u-pec.fr).

Zaki Laïdi, directeur de recherche à l'IEP de Paris, ancien conseiller spécial du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (2020-2024). Il est notamment l'auteur de *La Norme sans la force. L'énigme de la puissance européenne* (Presses de Sciences Po, 2013).

Enrico Letta, président de l'institut Jacques-Delors, ancien président du Conseil des ministres italien (2013-2014). Il a remis aux institutions européennes, en avril 2024, un rapport sur l'avenir du marché unique.

Anne Levade, professeure de droit public à l'université Paris 1 Panthéon-Sorbonne, présidente émérite de l'Association française de droit constitutionnel.

Francesco Martucci, professeur de droit public à l'université Paris-Panthéon-Assas, membre du Haut comité juridique de la place financière de Paris. Auteur de manuels de droit européen, il consacre une partie de ses écrits à l'Union économique et monétaire.

Stéphanie Novak, agrégée de philosophie, professeure de science politique et relations internationales à l'université Ca' Foscari de Venise (Italie).

Miguel Poiares Maduro, doyen de la faculté de droit de l'Université catholique de Lisbonne (Portugal), professeur adjoint à l'école de gouvernance transnationale de l'Institut universitaire européen.

Céline Spector, professeure de philosophie à Sorbonne Université. Dans le sillage de sa réflexion sur l'héritage des Lumières, elle a engagé une analyse de la démocratie et de la souveraineté européennes.

Pauline Türk, professeure à l'université Côte d'Azur, directrice du CERDACFF. Spécialiste de droit constitutionnel et des institutions politiques, elle s'intéresse aux questions de souveraineté et de citoyenneté numériques, ainsi qu'à la plateformisation de l'État et des services publics.

Mathilde Unger, maître de conférences en droit public à l'université de Strasbourg. Elle a notamment publié *La Justice sociale dans l'Union européenne* (Classiques Garnier, 2022) (m.unger@unistra.fr).

Jorge E. Viñuales, professeur à l'université de Cambridge (Royaume-Uni) et à l'Université internationale libre d'études sociales (Italie), fondateur du Cambridge Centre for Environment, Energy and Natural Resources Governance.

Pauline Türk

LA SOUVERAINETÉ NUMÉRIQUE EUROPÉENNE, VERS UNE TROISIÈME VOIE ?

La souveraineté numérique européenne renvoie à la capacité, pour les États membres de l'Union européenne, de maîtriser leur destin commun dans l'espace numérique. Cela implique l'exercice d'un pouvoir légitime et efficace permettant de protéger les droits et intérêts des citoyens européens face à des États hégémoniques (États-Unis, Chine) et face à des entreprises multinationales (GAFAM, BATX et autres NATU) qui prétendent exercer, grâce à leur situation de quasi-monopole, un pouvoir non seulement économique mais aussi normatif et politique.

Cette souveraineté numérique constitue « une ambition politique forte, celle d'une autonomie stratégique à conquérir de la France et de l'Europe en matière d'équipements et de technologies numériques[1] ». Elle renvoie à la capacité de l'Union à défendre ses intérêts et ses valeurs dans des domaines divers : contrôle du traitement des données, stockage et *cloud*, intelligence artificielle, déploiement de la 5G, approvisionnement en matériaux semi-conducteurs, investissements industriels, positionnement sur le marché des cybermonnaies, enjeux environnementaux, mobilité, e-santé, etc. L'ambition européenne est aussi d'ouvrir de nouveaux marchés et de proposer des services compétitifs et innovants en évitant que les « grands groupes américains deviennent le point d'entrée du web » ; de protéger les espaces d'expression libre et les utilisateurs européens « contre le côté obscur de la technologie » ; de limiter les « abus de pouvoir » des géants du numérique et de créer

1. Assemblée nationale, *Bâtir et promouvoir une souveraineté numérique nationale et européenne*, rapport d'information n° 4299, juin 2021, p. 21.

les conditions d'émergence de leaders mondiaux dans les moteurs de recherche, l'e-commerce, les réseaux sociaux[2].

Après un temps de latence, qui contribue à expliquer le retard européen, les stratégies se renforcent et se diversifient pour faire de l'Union européenne un acteur politique et économique crédible, capable d'exercer une influence sur le développement des infrastructures et sur la régulation des réseaux numériques. Il s'agissait aussi, les premiers temps, de développer un moteur de recherche européen (face à Google, Yahoo ou Bing, la Chine a, de son côté, su créer Baidu et la Russie Yandex) et un système d'exploitation informatique « souverains ». Il s'agit aujourd'hui, plus généralement, de récupérer des parts de marché pour nos entreprises. Les premiers résultats tangibles tiennent sans doute à la « stratégie européenne pour les données » : la création d'un marché unique des données vise à garantir à la fois la compétitivité mondiale, la souveraineté de l'Europe en matière de données, et la protection des personnes dans le développement des technologies. RGPD, directive « police-justice » européenne, *Data Act* : depuis 2016, les réglementations européennes permettent de porter, mais aussi d'exporter mondialement (grâce à l'« effet Bruxelles »[3]), une conception protectrice des données numériques, au cœur des valeurs européennes.

La souveraineté numérique d'abord saisie par les États membres

La réflexion sur la souveraineté numérique naît au milieu des années 2000[4], d'une préoccupation : le refus de voir les peuples, les communautés d'utilisateurs, les États, les individus, perdre le contrôle de leur destin au profit d'entités mal identifiées, non légitimes, et dont l'objectif n'est pas la promotion de l'intérêt général (sommets mondiaux sur la société de l'information de Genève en 2003 et de Tunis en 2005). L'hégémonie américaine, en particulier, cristallise les inquiétudes. Surtout, certains États demandant un meilleur partage des responsabilités dans la gouvernance du réseau, davantage de multilatéralisme, notamment dans la gestion des ressources critiques d'internet (mission stratégique de

2. Margrethe Vestager, vice-présidente de la Commission européenne en charge de l'Europe numérique et de la concurrence, entretien au *Figaro*, 2 juin 2021.

3. Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, New York (N. Y.), Oxford University Press, 2020.

4. Cf. Pauline Türk, « Définitions et enjeux de la souveraineté numérique », *Cahiers français*, n° 415, 2020, p. 18-28.

l'Internet Corporation for Assigned Names and Numbers). La Russie, l'Iran ou la Chine furent les premiers à revendiquer la restauration de leurs « droits souverains » sur la gestion du réseau et l'élaboration d'un traité international (conférence mondiale des télécommunications internationales à Dubaï en 2012). Après le tournant de l'affaire Snowden, en 2013, la succession des scandales résultant de fuite de données, de piratages et de stratégies d'espionnage de certains États, ou d'entreprises et entités qui en dépendent, engendre une prise de conscience plus générale (sommet international sur la gouvernance d'internet à São Paulo en 2014). Dès lors, les démocraties européennes aussi se préoccupent de la dépendance de nos sociétés civiles et politiques aux technologies et à ceux qui les contrôlent (forums annuels sur la gouvernance d'internet), surtout depuis la multiplication des cyberattaques qui frappent presque quotidiennement aussi bien le secteur privé que public (« rançongiciels » WannaCry ou NotPetya en 2017, cyberattaques mortelles à l'hôpital de Düsseldorf en 2020 ou sur les hôpitaux français en 2022). En février 2024, encore, c'est l'OTAN ainsi que les gouvernements britannique, américain et néo-zélandais qui auraient été piratés par un prestataire informatique chinois.

En 2014, la France crée un institut de la souveraineté numérique et envisage, deux ans plus tard, l'institution d'un commissariat sur le sujet (art. 29 de la loi pour une République numérique). Le 8 décembre 2020, la présidence allemande du Conseil de l'Union européenne initiait la signature de la déclaration de Berlin pour une société numérique et une transformation numérique des administrations respectueuses des valeurs démocratiques, des droits humains et de l'environnement. Les États membres ont pris tour à tour des initiatives en ce domaine (stratégie d'indépendance numérique suédoise en 2020 ; charte espagnole des droits numériques en 2021 ; déclaration d'intention commune franco-allemande le 6 février 2024). Les Européens ont ainsi, sur une décennie, pris la pleine mesure des enjeux, du caractère irréversible des transformations à l'œuvre, de la nécessité de résorber le retard pris sur le plan technologique et industriel, et des implications politiques et juridiques majeures en termes de souveraineté des États, fragilisés dans l'exercice de leurs missions. Car la dépendance aux technologies concerne aussi bien les populations que les administrations et les institutions politiques. Rappelons qu'en 2024 5,3 milliards d'êtres humains sont connectés à internet, soit 66 % de la population mondiale. L'utilisateur moyen passe six heures par jour en ligne. Google Chrome occupe 66 % du marché mondial des navigateurs web. Google est le moteur de recherche le plus

utilisé au monde. Les technologies numériques ont investi la plupart des domaines d'activité quotidienne, et les modes de pensée et de consommation sont transformés par les réseaux sociaux et les plateformes collaboratives.

Les États en ressortent affaiblis et concurrencés dans le service rendu aux citoyens, contrepartie de la soumission aux lois et à l'impôt. En effet, rares sont les domaines dans lesquels l'exercice des compétences de l'État n'est pas conditionné, désormais, par sa dépendance aux réseaux numériques : politiques monétaires et fiscales, défense, systèmes sociaux, politique industrielle, systèmes de santé, énergie, culture, éducation, information et communication, transport, et même conservation des archives… En outre, au regard de leur chiffre d'affaires, certaines plateformes peuvent rivaliser avec le PIB de nombreux États. Leurs cryptomonnaies concurrencent les monnaies fiduciaires. Leurs bénéfices échappent largement à la fiscalité des États. Leurs organes de règlement des différends font figure de nouvelles cours suprêmes (*Oversight Board* de Meta pour le contentieux relatif à la liberté d'expression). Leur pouvoir normatif (normalisation technique, régulation, conditions générales d'utilisation) concurrence celui des États[5]. Les sociétés politiques doivent dorénavant composer avec l'existence d'un monstre tentaculaire virtuel qui influence très concrètement la vie quotidienne des citoyens, le fonctionnement des administrations, le contenu des politiques publiques. Or les modes de gouvernance et de régulation, les codes et les règles du jeu, ont longtemps échappé aux États comme aux utilisateurs de ces technologies.

Sur le plan juridique, ce contexte heurte de plein fouet la notion de souveraineté, définie classiquement comme le pouvoir suprême exercé sur un territoire, à l'égard d'une population, par un État indépendant, libre de s'autodéterminer, dans la ligne des écrits fondateurs de Jean Bodin et Charles Loyseau au XVI^e siècle, puis de Georg Jellinek, Louis Le Fur et Raymond Carré de Malberg au XX^e siècle. Cette conception était déjà remise en cause du fait de l'interdépendance des États entraînée par la mondialisation économique, le développement des échanges transnationaux, la montée en puissance des organisations internationales, la globalisation des problématiques politiques et du droit (ère post-westphalienne), l'intégration dans l'Union européenne (réflexion sur la souveraineté partagée, fractionnée, déléguée, etc.). L'avènement du

5. Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York (N. Y.), Basic Books, 1999.

« tout-numérique » s'accompagne d'une dilution des frontières physiques qui achève de fragiliser les États, dépendants des technologies et de ceux qui les contrôlent, en perte de maîtrise, incapables d'imposer leur autorité ou de protéger leurs citoyens face à des menaces nouvelles.

La souveraineté numérique au-delà de l'État

Reconquérir la souveraineté numérique est d'abord l'affaire des États, qui revendiquent le prolongement de leur autorité et de leur pouvoir de réglementation sur les réseaux. Mais face aux États-Unis et à la Chine, et tandis que la Russie, le Brésil ou l'Inde parviennent à tirer leur épingle du jeu, force est de constater que l'échelle étatique n'est plus la bonne échelle pour la France et ses voisins européens, lorsqu'il s'agit de peser sur les marchés et sur la gouvernance mondiale des réseaux, de développer des entreprises et services compétitifs, d'obtenir des garanties des multinationales américaines dont les Européens restent dépendants. « Les espaces nationaux semblent, à tout le moins, inadaptés et constituent même de véritables obstacles à l'émergence et au développement d'une économie numérique ; de même, les territoires étatiques ne sont plus guère adaptés pour prémunir les citoyens et les consommateurs face à la cybercriminalité[6]. »

C'est alors que, dans le discours politique, la souveraineté numérique devient européenne. En septembre 2020, après le pic de la crise de la Covid-19, la présidente de la Commission, Ursula von der Leyen, annonce, dans son discours sur l'état de l'Union, un vaste plan de reconquête européenne de la souveraineté numérique à l'horizon 2030[7]. Le Conseil européen, le 2 octobre 2020, fixe le cap : « Pour être souveraine sur le plan numérique, l'UE doit mettre en place un marché unique véritablement numérique, renforcer son aptitude à définir ses propres règles, à opérer des choix technologiques autonomes et à développer et déployer des capacités et des infrastructures numériques stratégiques. Au niveau international, l'UE tirera parti de ses instruments et de ses pouvoirs de réglementation pour contribuer à la définition de règles et de normes mondiales. » La « boussole numérique » présentée en mars 2021 poursuit des objectifs concrets (formation au numérique, consolidation des

6. Patrick Meunier, « Les compétences de l'Union européenne et la souveraineté numérique », *in* Pauline Türk et Christian Vallar, *La Souveraineté numérique. Le concept, les enjeux*, Paris, Mare & Martin, 2018, p. 197.

7. Cf. aussi Commission européenne, « Façonner l'avenir numérique de l'Europe », communication du 19 février 2020, p. 2.

infrastructures, transformation numérique des entreprises, numérisation des services publics), complétée en janvier 2022 d'une déclaration sur les droits et principes numériques. Le concept de souveraineté numérique européenne a pris une dimension politique, économique, philosophique, et il interpelle désormais les juristes[8].

Certes, l'Union européenne, dotée d'une personnalité juridique depuis le traité de Lisbonne (art. 47 du traité sur l'Union européenne), ne saurait avoir de souveraineté au sens juridique, puisqu'elle n'est pas un État, n'est pas dotée de la compétence de sa compétence, et ne dispose pas des attributs de la souveraineté. En son sein, « les compétences souveraines doivent être valorisées, à l'aune du principe de coopération loyale, par un exercice concomitant de celles attribuées par les États à l'Union européenne ». Le droit de l'Union, au travers des exigences de cohérence et de solidarité, « a la capacité d'inciter les États membres à coopérer afin d'optimiser leurs actions dans un cadre harmonisé », et de mettre en commun leurs ressources : il en ressort que « l'exercice par l'Union européenne de ses compétences afin de réglementer des activités entrant dans le champ numérique requiert l'accord des États membres », dans une mesure variable selon que sont sollicitées les compétences exclusives, partagées ou d'appui[9]. Diverses politiques et divers programmes contribuent au déploiement d'une politique numérique de l'Union, à défaut de dispositions spécifiques des traités[10]. C'est ainsi l'article 114 du traité sur le fonctionnement de l'Union européenne qui constitue le fondement d'une partie de la législation relative au numérique, au titre de l'établissement et du fonctionnement du marché intérieur. La politique de cohésion et ses programmes de subvention sont également mobilisés, ainsi que les articles 101 à 109 du même traité et autres dispositions fondant la politique de la concurrence, les instruments de la politique industrielle (art. 173 du TFUE), voire, à certains égards, ceux de la politique étrangère et de sécurité commune en matière de cybersécurité. La jurisprudence de la Cour de justice de l'Union contribue à

8. Luciano Floridi, « The Fight for Digital Sovereignty: What Is It, and Why It Matters, Especially for the EU », *Philosophy & Technology*, vol. 33, n° 3, 2020, p. 369 ; Brunessen Bertrand, « La souveraineté numérique européenne : une "pensée en actes" ? », *Revue trimestrielle de droit européen*, n° 2, 2021, p. 249.

9. Patrick Meunier, « Les compétences de l'Union européenne et la souveraineté numérique », chap. cité, p. 197. Sur les principes de coopération loyale, de cohérence et de solidarité, cf. les articles 4, § 3, et 3, § 3, du traité sur l'Union européenne (TUE), ainsi que l'article 7 du traité sur le fonctionnement de l'Union européenne (TFUE).

10. Brunessen Bertrand (dir.), *La Politique européenne du numérique*, Bruxelles, Bruylant, 2022.

l'expression d'une souveraineté numérique européenne par la garantie des droits et libertés numériques.

Si la souveraineté numérique européenne fait figure d'aporie sur le plan juridique, sur les terrains politique, technologique, économique, l'Union européenne porte effectivement une ambition : celle de la reconquête d'un poids significatif dans les rapports de force avec les États et multinationales qui contrôlent les technologies. La souveraineté numérique européenne apparaît ici « compensatoire », pour reprendre l'expression d'Anne Peters à propos de la façon dont le constitutionnalisme se développe à l'échelle globale en corrélation avec sa fragilisation à l'échelle nationale[11]. La souveraineté érodée des États trouverait une compensation dans la prise en charge par l'Union du destin commun des utilisateurs européens. Les responsables politiques nationaux le perçoivent clairement : ils sont convaincus que « l'enjeu est désormais moins de s'interroger sur l'évolution des prérogatives classiques de l'État que sur la façon dont la France peut, dans un contexte où l'autonomie absolue est impossible, maximiser ses atouts et réduire ses dépendances, en s'appuyant sur le levier de puissance que constitue aussi l'Union européenne[12] ».

Les trois volets de la souveraineté numérique européenne

La souveraineté numérique européenne fait référence à la capacité de l'Union et de ses États membres à exercer un contrôle sur les technologies et infrastructures numériques au service de leurs propres intérêts politiques, économiques et sécuritaires. Cela implique de réduire la dépendance à l'égard des entreprises étrangères, en particulier celles basées aux États-Unis ou en Chine, et de promouvoir une autonomie numérique au sein de l'Europe. À défaut, en 2024, de bases juridiques spécifiques, cette stratégie de l'Union s'appuie sur les politiques sectorielles existantes pour en développer les volets numériques. La puissance de l'Union européenne apparaît liée, dans le domaine numérique, à sa triple capacité à peser sur les réglementations, à protéger sa population et ses valeurs, et à renforcer son positionnement sur le plan économique et industriel.

11. « Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures », *Leiden Journal of International Law*, vol. 19, n° 3, 2006, p. 579-610.

12. *Bâtir et promouvoir une souveraineté numérique nationale et européenne*, rapport d'information cité, p. 20.

Imposer sa réglementation

Là où les États-Unis innovent et exploitent, l'Union européenne réglemente et régule, selon la boutade d'une entrepreneuse italienne. Le fait est que l'Union européenne est parvenue à exercer une influence significative sur la réglementation des activités numériques, grâce au poids de son marché de consommateurs, mais aussi à la crédibilité de ses institutions, et à l'attrait de son système de valeurs, d'essence libérale. L'Union serait une « superpuissance réglementaire mondiale » qui « n'a pas besoin d'imposer ses normes de manière coercitive à qui que ce soit – les seules forces du marché suffisent », et ce *Brussels effect de facto* serait en outre « complété par un effet Bruxelles *de jure*, c'est-à-dire l'adoption de réglementations de type UE par des gouvernements étrangers »[13]. Les réglementations européennes font figure de modèle de référence pour de nombreuses juridictions, et dans différents forums de négociation, en raison à la fois du poids politique et commercial de l'Union et de sa crédibilité en matière d'ingénierie juridique. De nombreux textes illustrent cette capacité de l'Union à « commander et se faire obéir », attributs de la souveraineté, dans l'espace numérique. À l'automne 2022 ont été adoptés le *Digital Markets Act*, visant à limiter le poids des plateformes jouant le rôle de *gatekeepers* (contrôleurs d'accès) et à restaurer la concurrence sur les marchés numériques, ainsi que le *Digital Services Act*, visant à lutter plus efficacement contre les contenus et produits illicites en ligne. Ils s'ajoutent au RGPD, entré en vigueur le 25 mai 2018, au *Data Governance Act*, en vigueur depuis septembre 2023, visant à favoriser et sécuriser le partage des données, et au *Data Act*, en vigueur depuis janvier 2024, visant plus spécifiquement les données industrielles et l'internet des objets. Au cœur de la stratégie numérique européenne, l'Union a aussi adopté, en février 2024, une réglementation pionnière, l'*Artificial Intelligence Act*, proposant au monde une approche « par les risques » qui doit assurer un développement de l'intelligence artificielle encadré, fiable et sécurisé. L'Union promeut à l'échelle mondiale, grâce à l'ensemble de ces réglementations, une conception spécifique et exigeante en matière de protection de la liberté individuelle et de la vie privée.

La façon dont les pays européens parviennent à contribuer aux instances de gouvernance d'internet et des réseaux numériques est un autre aspect de la question, moins documenté. Par exemple, l'ICANN, organisme international de supervision de la sécurité et de l'interopérabilité d'internet

13. Anu Bradford, « Penser l'Union européenne dans la mondialisation : l'"effet Bruxelles" » (entretien), *Revue européenne du droit*, n° 2, 2021, p. 76.

déjà évoqué, chargé de la gestion des adresses et noms de domaine, assure depuis 2014 une représentation relativement équilibrée des zones géographiques du monde et a créé un bureau régional à Bruxelles. Les Européens sont également parvenus à intégrer, dans une proportion difficile à mesurer cependant, les instances internationales chargées de la régulation, de la normalisation des activités numériques, par adoption de standards (Internet Engineering Task Force ou World Wide Web Consortium). Ils participent chaque année au Forum sur la gouvernance d'internet.

Protéger sa population et ses valeurs

Dès le début des années 2000, la Cour de justice de l'Union a entrepris de développer une jurisprudence protectrice des utilisateurs européens et de leur liberté individuelle, mettant en place un véritable système de protection des données, uniformisé et efficace, sous l'empire de la directive 95/46/CE puis du RGPD[14] : conservation des données par les États membres ; consécration et interprétation des droits numériques (notamment droits au déréférencement, à l'oubli, à l'effacement) ; défense d'une conception non patrimoniale et marchande de la donnée personnelle ; protection contre les effets de l'extraterritorialité des lois américaines (invalidation successive des dispositifs de protection des données États-Unis-Union européenne *Safe Harbor* et *Privacy Shield*, remplacés en 2024 par un *Privacy Shield 2.0*). La déclaration interinstitutionnelle « sur les droits et principes numériques pour la décennie numérique », adoptée en 2022, témoigne de la volonté politique, au sein de l'Union, de prendre les devants sur le terrain de la formalisation des droits et libertés numériques.

Mais les menaces ne concernent pas seulement la liberté individuelle et la vie privée des utilisateurs. L'espionnage, le piratage, la désinformation, les cyberattaques, menacent plus largement les sociétés, leurs institutions de gouvernement et le fonctionnement des services publics, l'exercice des libertés civiles et politiques, ainsi que le fonctionnement même de nos démocraties. Après plusieurs appels à renforcer le niveau de protection sur le territoire de l'Union (à Nevers par exemple, le 9 mars 2022, lors

14. CJUE, 6 novembre 2003, *Lindqvist*, C-101/01 ; 9 mars 2010, *Commission c. Allemagne*, C-518/07 ; 13 mai 2014, *Google Spain c. AEPD*, C-131/12 ; 8 avril 2014, *Digital Rights Ireland et Seitlinger*, C-293/12 et C-594/12 ; 6 octobre 2015, *Schrems c. DPC*, C-362/14 ; 21 décembre 2016, *Tele2 Sverige*, C-203/15 et C-698/15 ; 24 septembre 2019, *Google c. CNIL*, C-507/17 ; 16 juillet 2020, *DPC c. Facebook Irlande et Schrems* (« *Schrems II* »), C-311/18 ; 6 octobre 2020, *La Quadrature du Net*, C-511/18, C-512/18 et C-520/18.

du conseil des ministres des Télécommunications), les États membres ont entrepris des démarches communes de lutte contre les cyberattaques, avec le soutien de la Commission et de l'Agence européenne pour la cybersécurité. Le « plan d'action pour la démocratie » lancé par la Commission en 2020, visant à protéger la liberté d'information et la liberté d'expression en ligne, qui a déjà abouti au *Digital Services Act*, devrait se prolonger dans plusieurs directions : sincérité des consultations électorales et des campagnes qui les précèdent, transparence sur les activités des représentants d'intérêts, fiabilisation de la participation du public aux processus décisionnels face aux dérives de la désinformation, aux ingérences d'États étrangers et aux nouvelles formes de manipulation de l'opinion publique.

88 ***Promouvoir ses entreprises et sa puissance industrielle***

L'Union européenne a pris du retard sur le plan technologique et industriel dans le domaine numérique. Les disparités entre États membres sur le plan économique, social et des infrastructures ont constitué un frein au développement d'une stratégie industrielle efficace, d'autant que certains États européens jouent de leur fiscalité pour attirer sur leur territoire les multinationales, là où d'autres projettent de leur imposer une « taxe GAFA » pour soutenir le développement d'entreprises européennes soumises, elles, à l'imposition. Un impôt mondial sur les multinationales, négocié au sein de l'OCDE, est finalement entré en vigueur en janvier 2024 sur le territoire de l'Union, pour mettre fin à une concurrence fiscale inéquitable.

Depuis la crise sanitaire, l'Union s'est engagée dans un vaste programme d'accompagnement des entreprises européennes vers la transition numérique. Il s'agit aussi bien de soutenir les « licornes » européennes (European Sovereign Tech Fund) que d'améliorer la compétitivité des PME (accès aux services internet à haut débit, formation de la main-d'œuvre aux compétences numériques, environnements innovants) ou d'accompagner les start-up innovantes (initiative *Scale-Up Europe*, lancée en mars 2021). L'objectif est aussi d'anticiper sur la révolution de l'intelligence artificielle et des technologies quantiques, de prendre des parts de marché dans la production de ressources numériques (logiciels, technologies blockchain, microprocesseurs à basse consommation, plateformes *cloud*) et de renforcer les infrastructures numériques (câbles sous-marins, réseau de téléphonie mobile en 5G, fournisseurs d'accès à internet, systèmes d'exploitation, systèmes de sécurité, centres de données). La démarche est ambitieuse, comme l'ont été le lancement du moteur de

recherche Qwant, le développement de solutions européennes pour un *cloud* de confiance (OVHcloud) ou en matière d'intelligence artificielle générative (Mistral AI), la sécurisation de l'approvisionnement en puces électroniques (règlement européen sur les semi-conducteurs de juillet 2023). Parallèlement, depuis 2020, grâce à une initiative franco-allemande, un projet d'infrastructure de données voulue compétitive, sécurisée et fiable pour l'Union européenne, dit Gaia-X, est porté par un large consortium d'entreprises. Les résultats sont encore fragiles, sur le terrain du réarmement industriel et technologique, au cœur des enjeux de la « boussole numérique pour 2030 ».

La promotion d'une troisième voie

Si elle soutient la compétitivité des entreprises européennes sur les marchés, l'Union promeut aussi une troisième voie, orientée vers le développement de « communs numériques », impliquant la création d'infrastructures logicielles et matérielles non rivales et non exclusives, dans une approche alternative au modèle concurrentiel et monopolistique. Il s'agit de développer des ressources partagées et accessibles en ligne, coproduites et maintenues collectivement par des communautés qui en définissent elles-mêmes les droits d'usage. En effet, pendant la pandémie de Covid-19, l'efficacité des logiciels libres développés par des ingénieurs bénévoles, comme le site d'information CovidTracker ou l'application de localisation des vaccins Vite ma dose !, a été démontrée. Enfin, au-delà d'une approche axée sur la concurrence et la compétition entre les plateformes, l'Union européenne s'oriente dernièrement vers une logique de partenariat, permettant de collaborer avec elles et de les responsabiliser, ce qu'illustre par exemple la mise en œuvre du *Digital Services Act*.

Ainsi, entre les États-Unis d'une part, qui portent un modèle capitaliste fondé sur le libre jeu du marché, la marchandisation de la donnée et la liberté d'expression contre tout excès de régulation, et la Chine d'autre part, qui s'inscrit efficacement dans la compétition mondiale mais applique de strictes restrictions sur le plan des libertés (censures et *Great FireWall*), d'autre part, une « troisième voie » européenne se dessine.

Elle peut être identifiée sur le terrain du rapport à l'exploitation des données, à la protection des droits des utilisateurs, de leur dignité et de leur vie privée, ainsi que sur le plan des options alternatives à la compétition mondiale comme mode de gestion des ressources numériques, sous l'angle d'un développement de « communs numériques mondiaux » qui

reposent sur des infrastructures ouvertes et partagées, fondées sur des standards libres et ouverts. La reconquête d'une souveraineté numérique européenne doit permettre de promouvoir cette troisième voie, au service des valeurs et intérêts de l'Union.

De façon générale, à l'heure où les progrès fulgurants de l'intelligence artificielle annoncent une nouvelle révolution des outils et pratiques, l'Union porte une certaine conception des rapports entre l'homme et la machine : « La technologie devrait tenir compte de cela et le marché aussi, à savoir que nous ne sommes pas uniquement une matière première ou des produits. Les humains doivent être au centre, à la fois, du marché et de la technologie[15]. »

15. Margrethe Vestager, « Les Européens doivent faire mieux avec les données » (entretien), Euronews.com, 7 mai 2021.

RÉSUMÉ

La notion de souveraineté numérique déborde la perspective juridique classique, attachée au pouvoir des États et au cadre national. Elle reçoit d'autres acceptions, économique, technique ou fonctionnelle, et peut se concevoir plus utilement à l'échelle de l'Europe. La souveraineté numérique européenne renvoie à la capacité des États membres de l'Union à s'autodéterminer dans l'espace numérique, face aux puissances – américaines et chinoises notamment – qui s'y déploient. Reconquérir son autonomie et sortir de la dépendance technologique implique de renforcer la capacité de l'Union à peser sur l'élaboration des normes applicables, à protéger ses ressortissants de menaces protéiformes, et à développer son poids industriel et ses capacités d'innovation.