Souveraineté numérique :

Essai pour une reconquête

SOUVERAINETÉ NUMÉRIQUE : ESSAI POUR UNE RECONQUÊTE

Avertissement de l'Éditeur

Toute utilisation ou traitement automatisé, par des tiers, de données personnelles pouvant figurer dans cette étude sont formellement interdits.

ISBN: 978-2-9581579-0-6
Dépôt légal : janvier 2022
Directeur de publication : Matthieu Bourgeois

Liste des auteurs et contributeurs

Clotilde Bômont, Doctorante.

Philippe Boulanger, Professeur des Universités.

Matthieu Bourgeois, Avocat spécialisé en droit du numérique et des communications.

Carole Chartier-Djelaïbia, Juriste IP & IT, spécialiste en droit des données personnelles.

Erwan Cotard, Directeur de Marché.

Bernard de Courrèges d'Ustou, Inspecteur Général des Finances.

Thibaut de Saint Maurice, Philosophe.

François-Xavier Deniau, Diplomate.

Mathieu Gras, Consultant Data et Conformité.

Marie-Charlotte Grasset-Illouz, Responsable juridique digital & gouvernance.

Stéphane Larrière, Data Protection Officer.

Isabelle Manevy, Juriste, spécialiste du droit de la consommation.

Jean Martinot, Responsable des Systèmes d'Information.

Thierry Menissier, Philosophe.

Denis Pélanchon, Consultant en Sécurité des Systèmes d'Information.

Myriam Quéméner, Avocat Général près la Cour d'Appel de Paris.

Franck Régnier-Pécastaing, VP Data Governance Advisor.

Nicolas Salles, Chief Data Officer.

Anne Souvira, Chef de la mission « Cyber » de la Préfecture de Police.

Arnaud Tanguy, Directeur de la Sécurité.

Remerciements chaleureux à :
- Philippe Lavault, pour avoir cru dans ce projet dès sa genèse,
- Alix Durand, pour son soutien durant les réunions de travail,
- Fiorella Moray, pour son aide précieuse dans ce projet.

Liste des abréviations

AFNIC	Association française pour le nommage Internet en coopération
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARCEP	Autorité de régulation des communications électroniques, des postes et de la distribution de la presse
BHATX	Baidu, Huawei, Alibaba, Tencent et Xiaomi
Cass. crim.	Cour de cassation, chambre criminelle
C. défense	Code de la défense
CIR	Crédit d'impôt recherche
CMI	Complexe militaro-industriel
CNIL	Commission nationale de l'informatique et des libertés
Conv. EDH	Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales
Dir.	Directive
DMA	*Digital Market Act*
DNS	*Domain Name System*
Doc. fr.	La Documentation française
DPO	Délégué à la protection des données
DSA	*Digital Services Act*
EPN	Espace public numérique
ESG	Critères environnementaux, sociaux et de gouvernance
ESN	Entreprise de services numériques
FAI	Fournisseur d'accès à Internet
FCA	Fournisseur de contenu et d'applications
FinTech	*Financial Technology*
GAFAM	Google, Apple, Facebook, Amazon et Microsoft
IA	Intelligence artificielle
ibid.	*ibidem* (au même endroit)
ICANN	*Internet Corporation for Assigned Names and Numbers*
IGF	*Internet Governance Forum*
infra	ci-dessous
Insee	Institut national de la statistique et des études économiques
IP	*Internet Protocol*
ISOC	*Internet Society*
JCP E	*JurisClasseur périodique*, édition Entreprise et affaires
L.	Loi
LIR	*Local Internet Registries*

NATU	Netflix, Airbnb, Tesla et Uber
NSA	*National Security Agency*
OIV	Opérateur d'importance vitale
ONG	Organisation non gouvernementale
ONU	Organisation des Nations unies
OSE	Opérateur de services essentiels
OTAN	Organisation du traité de l'Atlantique nord
PME	Petites et moyennes entreprises
préc.	précité
R&D	Recherche & Développement
Règl.	Règlement
RF sociologie	*Revue française de sociologie*
RGPD	Règlement général sur la protection des données
RIR	*Regional Internet Registries*
RSE	Responsabilité sociétale des entreprises
RTD com.	*Revue trimestrielle de droit commercial et de droit économique*
SaaS	*Software as a Service*
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SI	Système d'information
ss dir.	Sous la direction de
supra	ci-dessus
TFUE	Traité sur le fonctionnement de l'Union européenne
UE	Union européenne
V.	Voir
W3C	*World Wide Web Consortium*

Préface

La souveraineté numérique suscite actuellement nombre de débats houleux sur des objets technologiques divers : le Cloud, l'intelligence artificielle, la 5G, … Des solutions très variées sont offertes face à cette problématique, allant de la standardisation technique aux investissements industriels en passant par la réglementation. Les missions d'information et de contrôle, les travaux de *think tanks* ou encore les prises de position politiques interrogent fréquemment cette notion de souveraineté numérique dont on peine à définir les contours. Bien que les liens entre souveraineté numérique et sécurité numérique soient étroits, l'ANSSI assiste le plus souvent en observateur intéressé à ces débats qui dépassent largement ses missions. Cependant, au cours de ses observations, un constat apparaît clairement pour l'ANSSI : la notion de souveraineté numérique emporte des acceptions divergentes, dont certains jouent pour mettre à mal l'affirmation d'une telle souveraineté. L'absence de définition de la souveraineté numérique et les difficultés qui existent à circonscrire précisément cette notion contribuent largement à complexifier la mise en œuvre de politiques dédiées à la préservation de notre souveraineté numérique. L'étude conduite conjointement par le Cercle de la Donnée et l'Agora41, espace de réflexion libre sur la sécurité numérique animé par l'ANSSI, fournit en réponse un cadre de réflexion solide qui s'appuie sur une analyse historique, politique et juridique complète de la notion de souveraineté et de ses possibles traductions dans l'espace numérique. Elle donne ainsi des clés de lecture indispensables à l'appréhension des tensions qui façonnent notre espace numérique et du « combat » pour son contrôle auquel s'adonnent les acteurs principaux du cyberespace, qu'il s'agisse d'États, de sociétés privées ou d'organisations internationales. Enfin, sur la base d'un diagnostic étayé, des propositions d'actions concrètes sont soumises aux lecteurs, avec comme fil conducteur l'idée selon laquelle la puissance publique n'est pas entièrement démunie face aux enjeux de la souveraineté numérique.

Deux axes de réflexion développés dans l'étude, qui sont un pas de côté par rapport aux activités plus traditionnelles de l'ANSSI, me semblent particulièrement intéressants.

En premier lieu, la question de la compréhension réelle des enjeux numériques et de leurs traductions politiques par les citoyens. Tant les outils technologiques sont conçus pour disparaitre du regard des utilisateurs, effaçant toute complexité et ne délivrant que le service numérique dans une forme la plus fluide et intuitive pour chacun de ses utilisateurs, tant les enjeux politiques qu'ils véhiculent disparaissent aussi. Sans compréhension des technologies, des choix qui précédent à leur conception et à leur déploiement, des luttes structurelles entre acteurs économiques pour l'accès au marché, comment un utilisateur peut s'imaginer qu'en choisissant de recourir à une solution de visioconférence plutôt qu'à une autre, il choisit un modèle numérique, souverain ou non, basé sur l'exploitation des données personnelles ou non, contrôlé par un État ou non… Le développement massif du recours à une application de messagerie sécurisée comme Signal suite aux annonces de Facebook de la modification des conditions d'utilisation de Whatsapp

dénote un intérêt réel, quoique ponctuel, pour ces questions. Pour lutter contre « l'indifférence citoyenne », seule la diffusion d'une culture numérique à tous les âges peut permettre à chacun de prendre conscience des problématiques numériques, qu'elles soient de cybersécurité ou de souveraineté. L'introduction dans les programmes scolaires, au primaire comme au secondaire, de modules d'enseignement sur le numérique doit à ce titre être salué et encouragé, en développant des outils pédagogiques au profit des enseignants souvent déstabilisés face à cette discipline nouvelle et particulière qu'est le numérique. Cette sensibilisation des élèves et étudiants doit s'accompagner d'une sensibilisation des adultes, à la fois dans leur vie personnelle et professionnelle, pour que la souveraineté numérique ou en tout cas la gestion des dépendances numériques soit désormais pleinement intégrée comme un critère dans le choix d'une solution numérique plutôt qu'une simple considération annexe. Comme la cybersécurité, le recours à une solution numérique pourrait désormais être analysé à l'aune de la souveraineté numérique. Les choix stratégiques de nos administrations et de nos entreprises en matière de numérique ne peuvent plus aujourd'hui faire l'économie d'une analyse selon des critères de souveraineté. Pour conduire à cette prise de conscience, les travaux menés par les associations professionnelles, les autorités sectorielles et les dispositifs de formation continue sont essentiels et doivent être encouragés pour diffuser largement dans l'entreprise, dans l'administration, une culture numérique robuste, capable de conduire à des choix éclairés dans le domaine.

Deuxièmement, l'élaboration au niveau européen de cadres réglementaires tenant compte de la nécessité de promouvoir une conception européenne du cyberespace et affirmant la prise en compte des valeurs et du droit européen. La discussion à l'échelle européenne est souvent complexe et chronophage, avec des États-membres très divisés sur leurs besoins dans le cyberespace et des divergences de cultures politiques assez marquées quant à l'opportunité de permettre le renforcement du contrôle de l'Union et de ses États-membres sur une activité économique par défaut transnationale, comme le numérique. Toutefois, il n'en demeure pas moins que l'Union européenne est l'échelle de pertinence pour construire un cyberespace stable et respectueux des valeurs démocratiques, tout en étant performant. Pour aboutir à ce résultat, il ne faut surtout pas que l'Union cède à des solutions de facilité, en acceptant une simple localisation des données sur son territoire par exemple. Cette solution, souvent mise en avant comme une mesure de souveraineté, en particulier dans le débat sur le Cloud, est cependant inopérante dans un espace numérique, où des données peuvent être stockées de partout au travers le monde sans aucune garantie de sécurité juridique pour l'utilisateur. Aussi, un cloud basé sur un logiciel d'un GAFAM sur un serveur opéré par un GAFAM dans un datacenter d'un GAFAM sur le sol européen, avec des liens quotidiens vers l'architecture centrale du GAFAM pour accéder à des services plus sophistiqués, n'emporte aucune garantie de souveraineté, pourtant les données sont bien localisées dans l'Union européenne. Pour apporter des réponses concrètes et adaptées, une analyse fine doit être menée et des critères plus précis pour apporter des garanties robustes. Aussi, des critères visant à limiter au strict minimum le contrôle sur l'entreprise fournissant la solution de Cloud d'entités non-européennes, restreignant

strictement les accès aux données pour les intervenants non-européens et imposant des modèles de supervision de sécurité au plus proche des données stockées doivent être conçus. Les travaux qui ont été menés par l'Union européenne en matière de 5G ou de Cloud illustrent de fait la possibilité désormais de combiner la souveraineté nationale avec la souveraineté européenne pour dessiner un cadre réglementaire applicable au cyberespace conforme à nos intérêts et au maintien de notre souveraineté.

Sans dévoyer plus avant le contenu de cette étude, je terminerai par rappeler que l'ambition doit rester celle de maintenir la France parmi les Nations qui comptent dans le cyberespace. Cette ambition passe par une capacité d'affirmation et de promotion de modèles de numérique, avec évidemment pour la France et pour l'Union européenne, un refus catégorique de se vassaliser auprès d'acteurs non-européens. Être en capacité de réfléchir aux concepts et s'en faire une idée propre est un prérequis crucial au développement d'une vision française et européenne du cyberespace auquel l'étude du Cercle de la Donnée et de l'Agora41 contribue ainsi.

Bonne lecture !

Guillaume Poupard
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information (ANSSI)

Sommaire

Introduction

1. – **La souveraineté : une notion ébranlée au XXe siècle.** Être souverain c'est énoncer sa propre loi de manière inconditionnelle, chez soi. Cette définition s'entend facilement dans un environnement fermé comme ont pu l'être les États dans le passé. Mais cet état immuable a été perturbé par l'intensification de la circulation des hommes et des échanges de marchandises d'abord (dont l'aboutissement a été la mondialisation), puis d'informations (dont la traduction a été la révolution médiatique avec la démocratisation des grands médias – radiophonie, télévision… – dans les années 1950-1960, pour donner ensuite, au tournant du XXIe siècle, la révolution numérique avec l'adoption massive d'équipements informatiques par les administrations, les entreprises et les individus). Ces changements ont ébranlé la souveraineté, notamment en donnant un rôle clé aux détenteurs des moyens de production et de diffusion de l'information (des médias jusqu'aux plateformes numériques), ainsi qu'en décuplant l'influence d'acteurs non étatiques (groupes de pression, collectifs…) capables de défier et parfois même concurrencer la puissance des États.

2. – **La naissance du multilatéralisme européen n'a malheureusement pas favorisé les acteurs numériques locaux.** Limité autrefois à des espaces territoriaux bien circonscrits entraînant des conflits entre États, l'exercice de la souveraineté s'est étendu sous l'effet des progrès techniques et de l'intensification des échanges, à l'espace international, et a abouti, au XXe siècle, à deux guerres mondiales faisant prendre conscience aux peuples du risque d'anéantissement que courait l'humanité. S'en est suivie une tentative de construction d'un ordre international destiné à tempérer, autant que possible, les ardeurs des différents souverains nationaux. Certains ont été plus loin en tentant de bâtir des organisations régionales comme l'Union européenne. Cette dernière construction, si elle a permis aux États européens de se doter d'outils de puissance commune comme la monnaie (l'euro), ne s'est en revanche pas traduite par une vision et une politique industrielle favorables à l'émergence d'un écosystème d'acteurs locaux dans le domaine numérique, puisque le marché unique a davantage favorisé les intérêts des consommateurs que ceux des producteurs européens en la matière.

3. – **Les technologies numériques : un instrument de puissance dont se sont emparées certaines nations étrangères.** Les autres puissances (à savoir les États-Unis d'Amérique, la Chine et, dans une moindre mesure, la Russie) se sont emparées des technologies, en particulier l'informatique, pour se parer d'un nouvel attribut de puissance, au-dedans, mais aussi au-dehors, dans un cyberespace qui – contrairement à l'espace traditionnel délimité par des frontières claires – apparaissait moins aisé à cerner, et a donc échappé à l'ordre mondial (Organisation des Nations unies…). Ces puissances ont, en outre, appréhendé efficacement le numérique qui, à la différence des industries traditionnelles, requérait une grande réactivité.

4. – **Pour les acteurs européens : un inéluctable retard.** Le retard pris par l'Europe sur les technologies numériques, du fait de son manque d'anticipation et d'ambition politique en la matière, a défavorisé l'émergence d'acteurs locaux européens, conduisant à un déséquilibre des forces dans le cyberespace, désormais fortement dominé par des plateformes et des États étrangers.

5. – **La dépendance préoccupante de l'Europe à l'égard des puissances étrangères.** En Europe, alors que les voies de communication physique avaient toujours été sous le contrôle « souverain », les routes de l'information ont été ouvertes (et sont aujourd'hui exploitées) massivement par des puissances étrangères (essentiellement la Russie, la Chine et, dans une plus large mesure, les États-Unis, soit directement par l'usage massif de ces technologies aux fins de renseignements, soit indirectement, par l'influence qu'elles exercent au sein d'organismes de gouvernance/normalisation – ICANN[1], IAB[2]… –, soit enfin par des plateformes aux mains d'actionnaires nationaux et en hyperdomination sur leur marché). Cette suprématie menace gravement la souveraineté des États européens, désormais à la merci de puissances étrangères pour s'approvisionner et faire circuler de l'information.

6. – **Une situation mettant en péril la prospérité et la sécurité européennes.** Les symptômes de ce mal, en Europe, sont multiples : captation de valeurs sur des secteurs autrefois prospères et qui sont désormais confisqués par des acteurs étrangers (américains notamment) ; insécurité sur les réseaux (recrudescence des cyberattaques) ; ravages de l'économie de l'attention auprès des citoyens, chaque jour plus démunis et dépendants des plateformes auxquelles ils confient des pans entiers de leur vie, s'exposant également à une fragilité émotive et à une plus grande crédulité ; péril écologique engendré par la sollicitation exponentielle des réseaux numériques en l'absence de capacité européenne à en réguler l'usage…

7. – **L'inaction politique et l'indifférence citoyenne.** Les causes de ces déficiences sont mal connues, mais il est possible de considérer qu'elles remontent, pour l'informatique, aux années 1970, lorsque les élites d'alors n'ont pas su reprendre le flambeau légué par leurs aînés, pères de l'Europe qui avaient mis le vieux continent sur les rails d'une coopération industrielle forte dans certains secteurs stratégiques comme le charbon et l'acier, puis ensuite l'aéronautique et l'aérospatiale. Peu ont fait l'effort d'identifier et d'expliciter ces causes, ni encore moins d'y réagir. Ceci explique probablement l'ignorance et l'indifférence citoyennes, ainsi que l'expatriation du savoir-faire et de l'entrepreneuriat.

8. – **L'effet loupe de la crise sanitaire.** La crise sanitaire (puis économique et peut-être demain sociale) causée par le SARS-Covid-19, le montre : la donnée et le numérique maintiennent le lien et sont donc essentiels à la vie de la nation. En d'autres temps, cette crise sanitaire aurait conduit à l'arrêt pur et simple de toute vie économique et sociale. Grâce au numérique, une partie des travailleurs peuvent poursuivre leur activité en télétravail, le lien social et familial peut être entretenu,

(1) *Internet Corporation for Assigned Names and Numbers* (Société pour l'attribution des noms de domaine et des numéros sur Internet).
(2) *Internet Architecture Board*.

l'école peut continuer, même à distance. Toutefois, cet usage intense et permanent des réseaux numériques montre cruellement à quel point les États européens et leurs peuples sont sous la dépendance des acteurs non européens dominant l'économie numérique.

9. – **L'indispensable défense des valeurs humanistes françaises et européennes sur les réseaux.** À l'image de la voix forte qu'elle a portée en réaffirmant sa fidélité à des valeurs essentielles de protection des plus faibles et de solidarité, la France – et, avec elle, l'Europe – doit prendre en main son destin sur les réseaux numériques. En particulier, en proposant une troisième voie, entre le modèle *freemium* américain (basé sur l'économie de l'attention et l'exploitation débridée des données personnelles) et le modèle chinois de l'hypersurveillance étatique. Le monde a besoin de cette alternative.

10. – **La nécessité de définir une doctrine européenne pour l'exercice de la souveraineté numérique.** L'Europe doit investir massivement dans ce qui lui permettra d'exercer sa souveraineté sur les réseaux : intelligence artificielle, informatique quantique, protection des données essentielles à la nation et à ses citoyens (données de santé, identité numérique, biométrie…). Mais cet investissement serait perdu si la France, et avec elle l'Europe, ne conçoivent, formulent et appliquent une doctrine ambitieuse de souveraineté numérique. Celle-ci doit préserver le « vivre libre et en paix » dans un pays économiquement sain, et l'on sait maintenant que le « laissez-faire, laissez-passer » n'a pas permis d'atteindre cet objectif dans l'espace numérique (notamment en raison de certaines singularités de cet espace, comme l'effet réseau et la gratuité). Une méthode d'inspiration « colbertiste », en tout cas en partie interventionniste, semble indispensable à condition d'être menée par un gouvernement éclairé en la matière et cultivant une vision à long terme.

11. – **Le rôle clé de la donnée.** Au sein de cette doctrine, la donnée doit avoir une place importante car c'est une conviction forte des auteurs de cette étude : la maîtrise de cette ressource est un enjeu essentiel de souveraineté, au même titre que la maîtrise des ressources naturelles d'un État sur son territoire.

12. – **Notre démarche : définir, débattre et proposer. Notre but : interpeller et réveiller. Notre public : vous !** Fidèles à leurs convictions plaçant la meilleure compréhension des concepts liés à l'univers numérique comme élément central d'un renouveau civilisationnel, le Cercle de la Donnée et l'Agora 41 ont souhaité débuter la présente étude par une définition des termes de son sujet. Ainsi, après avoir rappelé la signification de la notion de souveraineté, puis avoir décrit l'espace numérique (Première partie), nous verrons que son application à cet espace révèle de graves carences faisant naître d'importantes menaces pour la prospérité et la sécurité française et européenne (Deuxième partie). Le temps viendra alors de formuler des propositions fortes, en interpellant le politique, mais aussi les acteurs économiques et les citoyens (Troisième partie). Cette étude s'adresse à tous ceux qui partagent l'urgence de défendre la liberté, l'indépendance et la primauté de valeurs humanistes sur les réseaux numériques.

PREMIÈRE PARTIE

DÉFINITIONS

13. – **La souveraineté à l'épreuve de l'espace numérique.** Il est nécessaire de rappeler les éléments constitutifs de la souveraineté politique, au commencement d'une réflexion sur la souveraineté numérique. Ainsi, après avoir rappelé les éléments principaux de la constitution et de la remise en cause de la souveraineté, il s'agira de décrire les éléments principaux de ce nouvel espace sur lequel elle est désormais amenée à s'appliquer : l'espace numérique.

CHAPITRE 1

LA SOUVERAINETÉ

14. – Issu d'une longue histoire, le concept de souveraineté traditionnelle connaît depuis la seconde moitié du XX^e^ siècle une certaine remise en cause aussi bien quant à son objet qu'à son but.

SECTION 1

LA SOUVERAINETÉ TRADITIONNELLE

15. – La souveraineté désigne le pouvoir politique suprême. Après avoir été conçue comme étant d'origine divine, puis comme puisant à l'autorité du pouvoir paternel, les philosophes du droit naturel ont établi que la souveraineté a sa source dans le consentement d'un peuple(1). On commencera par en rappeler les éléments constitutifs pour ensuite décrire les buts qu'elle peut servir.

I. – L'objet de la souveraineté

16. – En son objet, la souveraineté est à l'État ce que l'autonomie est à l'individu. Elle désigne donc à la fois l'autorité d'un pouvoir légitime et la puissance dont ce même pouvoir est doté pour *agir* efficacement. Un État souverain est un État dont la légitimité et la capacité effective à agir sont établies, à l'égard du peuple sur lequel il a autorité comme à l'égard des autres États souverains. Considérant ici l'action de l'État, il s'agit donc de décrire la souveraineté nationale.

17. – D'un fondement de la puissance nationale à la construction d'un ordre international. Alors que la souveraineté des nations s'est construite à travers le temps par le renforcement de la puissance de l'État, aussi bien vis-à-vis du peuple que des autres nations, le XX^e^ siècle constitue un tournant au cours duquel des

(1) À partir de là, on peut distinguer la souveraineté populaire et la souveraineté nationale. La souveraineté populaire appartient au peuple, comme le pense Rousseau (*Du contrat social*, Livre I, ch. 7). Elle est l'expression du droit acquis par chaque citoyen qui accepte le pacte social. La souveraineté nationale quant à elle désigne le pouvoir légitime de la nation et s'incarne en l'État. La souveraineté nationale n'appartient pas à chaque citoyen mais exprime l'unité de la nation et repose sur un processus de délégation.

nations souveraines ont décidé de bâtir, entre elles, un ordre mondial basé sur la coopération et s'appuyant sur des organisations internationales. Imposant d'un côté des « transferts de souveraineté » ou des « délégations de souveraineté », ces organisations offrent en retour à leurs membres la possibilité de bénéficier d'une puissance supplémentaire, émanant précisément du renforcement de la coopération. C'est dans ce cadre que peut s'analyser aujourd'hui l'Union européenne (UE), car s'il est peut-être difficile de parler d'une véritable « souveraineté » européenne, il est en revanche possible d'observer par exemple la monnaie unique (l'euro) comme un instrument de puissance que l'Union européenne confère à chacun des États qui l'adoptent, face aux autres superpuissances mondiales. Cet exemple peut d'ailleurs être une source d'inspiration pour le numérique.

II. – Les éléments constitutifs de la souveraineté nationale

18. – Quatre piliers de la souveraineté nationale. La souveraineté nationale procède de la volonté commune d'un peuple pour faire nation sur un territoire commun. De cette volonté commune, elle retire puissance et légitimité. L'État souverain est ainsi une collectivité humaine stabilisée sur un territoire, au sein de laquelle la contrainte est légitimement monopolisée[2].

A. – La population

19. – La population est à la fois la source et le terme de cette souveraineté de l'État. Ce qui fait qu'elle ne peut s'y réduire puisqu'elle est aussi ce qui constitue le peuple en tant que tel. Le modèle du contrat social ou du pacte d'association, pensé dès la Renaissance et tout au long du siècle des Lumières, permet de rendre compte des deux faces de cette population : un ensemble d'individus qui consentent à se reconnaître comme membres d'un même corps politique dont ils deviennent les citoyens. Le périmètre de cette population est donc strictement dépendant d'une « volonté commune » de faire nation : volonté qui trouve à s'exprimer dans l'adhésion à des institutions. C'est cette adhésion qui fait régulièrement l'objet de renégociations ou de transformations dans la vie politique d'une nation.

B. – Le territoire

20. – Le territoire permet d'identifier le lieu ou les lieux de cette souveraineté. Il contribue à en constituer la réalité en définissant le champ d'application du pouvoir de l'État. La souveraineté territoriale s'exerce donc sur l'ensemble des territoires compris à l'intérieur de frontières reconnues, mais aussi, par extension, sur un espace maritime (par ex., la zone d'exclusion économique de 200 miles des côtes), sur un espace aérien (plus difficilement définissable puisqu'il est compris comme l'espace sub-atmosphérique avec plusieurs « couches » différenciées) et sur le sous-sol de ce même territoire. Le territoire d'une nation peut être continu ou discontinu. Mais si le territoire et ses extensions sont les lieux propres de l'exercice de

(2) J. Gicquel et J.-E. Gicquel, *Droit constitutionnel et institutions politiques*, LGDJ, coll. « Précis Domat Droit public », 33e éd., 2019-2020, § 87.

la souveraineté, cet exercice ne s'y réduit pourtant pas. C'est toute la question des compétences extraterritoriales de la souveraineté, particulièrement sensible, dans un double contexte militaire et économique. C'est à la « frontière » du territorial et de l'extraterritorial que la question de la souveraineté de l'État sur le numérique se pose.

C. – La puissance

21. – La puissance est l'attribut premier de la souveraineté d'un État. Sans puissance, la souveraineté n'est qu'un principe formel incapable de se traduire dans la réalité. La puissance est à comprendre ici comme la capacité à *agir* d'un État souverain, c'est-à-dire à produire des effets dans le champ dans lequel il agit, qu'il soit militaire, économique ou culturel. Cette puissance implique une maîtrise des technologies stratégiques. Ainsi par exemple, dans le champ militaire, la France dont la puissance militaire avait décru à l'issue de la Seconde Guerre mondiale avait néanmoins recouvré un certain rayonnement par sa maîtrise de technologies stratégiques, comme la puissance nucléaire (lui permettant d'avoir une voix au Conseil de sécurité de l'Organisation des Nations unies [ONU]). Dans le champ économique, et en collaboration avec ses voisins européens, la puissance française trouve à s'exprimer à travers des réalisations comme Airbus ou Ariane, reposant sur la maîtrise des technologies de l'aéronautique et de l'aérospatial. Ceci a eu lieu avant l'avènement des réseaux numériques, dont elle n'a pas réussi, dans les décennies 1980-2010, à dominer les technologies stratégiques (micro-informatique, logiciels, plateformes, *etc.*).

D. – La légitimité politique

22. – La légitimité politique est le dernier élément constitutif de la souveraineté. Elle peut se comprendre selon deux dimensions : une dimension rationnelle de légitimité juridique et une dimension émotionnelle d'assentiment et d'adhésion du peuple. D'abord du point de vue de la raison, l'État souverain est celui qui s'inscrit dans le cadre d'un État de droit. La puissance de l'État est absolue précisément parce qu'elle est juridiquement définie et encadrée. Ensuite du point de vue du sentiment vécu, la souveraineté de l'État est respectée parce qu'elle est consentie et qu'elle suscite une adhésion vécue par ceux auxquels elle s'applique. Cette double légitimité confirme la puissance de l'État souverain en ce qu'elle en garantit l'unité et l'autorité.

III. – L'exercice international de la souveraineté

23. – Penser la souveraineté d'un État, c'est aussi penser ses relations avec les autres États souverains. Cette articulation des souverainetés ouvre le champ des relations internationales et pose la question de l'affrontement ou de la coopération des différentes souverainetés des États. Par la guerre ou la coopération (traités), les États n'ont eu de cesse de s'affronter, ou de s'accorder, sur les sujets essentiels (partage des territoires, accès aux ressources, coopération militaire, règles commerciales, *etc.*)

dont la maîtrise des technologies a fait partie intégrante (force nucléaire, survol des espaces aériens, *etc.*), dans un mouvement conduisant à une consécration du multilatéralisme dont les institutions internationales peuvent témoigner[3]. Ce mouvement conduit cependant à deux questions. D'abord, la souveraineté comme puissance d'agir est-elle soluble dans l'action multilatérale ? C'est tout l'enjeu de l'action de ces organisations multilatérales dont la légitimité est assurée mais dont la puissance réelle se trouve parfois mise en cause. Ensuite, comment comprendre que ce mouvement d'organisation ne soit pas parvenu à coordonner l'apparition et le développement des réseaux numériques, voire même que la question du numérique soit marquée par le retour d'actions unilatérales, comme c'est le cas par exemple de certaines dispositions du *Patriot Act* ou du *Cloud Act* des États-Unis qui s'appliquent de façon extraterritoriale à des entreprises françaises ou européennes ?

A. – Le recours à la guerre

24. – Exprimer la souveraineté d'un État par les armes. Pendant longtemps et encore aujourd'hui, la lutte armée fut le premier instrument de l'expression de la souveraineté d'un État à l'égard des autres. Qu'il s'agisse de se protéger d'une agression extérieure ou d'étendre au contraire son territoire ou d'augmenter ses intérêts, la guerre est la prérogative du pouvoir souverain. Ce recours à la guerre n'échappe pourtant pas au paradoxe de la démonstration de force. La force ne faisant pas droit, elle légitime la résistance à son expression et finit par affaiblir celui qui y a eu recours. Par ailleurs, le risque majeur d'anéantissement, du fait des progrès de la puissance nucléaire, a conduit à envisager le registre de la coopération multilatérale – à travers l'ONU – et le principe de non-prolifération nucléaire, en tant que nouvelles perspectives de régulation de l'affrontement des souverainetés des États.

B. – Le recours à la coopération

25. – Un nouveau cadre d'expression de la souveraineté. Au XX^e^ siècle, depuis la Société des Nations (SDN) jusqu'à la naissance de l'ONU, les institutions internationales, d'une part, et les organisations régionales, d'autre part, installent le recours à la coopération comme le nouveau cadre de l'exercice international de la souveraineté des États.

1° De la diplomatie classique au recours à des institutions internationales

26. – Les organisations internationales renforcent-elles ou affaiblissent-elles les États souverains ? La création de l'ONU, le 24 octobre 1945, ajoute à la pratique des traités circonstanciels entre États souverains un cadre permanent de coopération, de négociation et de régulation des relations internationales. À travers ses différentes agences, l'ONU accompagne les États dans la négociation

(3) Sur ce dernier point, les États ont créé des institutions internationales au sortir de la Seconde Guerre mondiale en leur confiant certains sujets d'intérêt supérieur dont le bon fonctionnement d'Internet ne fait pas partie à ce jour (sécurité, accès équitable, absence de surveillance, *etc.*), si l'on fait fi du forum sur la gouvernance de l'Internet créée certes par l'ONU mais dénuée de tout pouvoir contraignant (V. *infra*).

multilatérale de leurs prérogatives régaliennes. D'autres organisations comme le Fonds monétaire international (FMI), ou plus récemment l'Organisation mondiale du commerce (OMC) viennent renforcer les outils de négociation et de coopération. Mais, pour chacune de ces organisations, se pose la question de savoir si elle permet de renforcer la souveraineté de chacun de ses membres ou, si au contraire, elle n'est que le nouveau théâtre de leur affrontement. Par ailleurs, chacune de ces organisations se heurte à la réalité de sa puissance effective. Ainsi l'Union internationale des télécommunications (UIT) – au passage l'une des plus anciennes organisations internationales[4] – ne s'impose pas aujourd'hui comme l'instance capable d'une régulation efficace du numérique, garantissant à chaque État souverain la maîtrise de ses technologies et de ses usages.

2° L'avènement d'organisations régionales : l'exemple de l'Union européenne

27. – Une Europe en paix et prospère, mais dont la puissance pose question. À sa naissance, le projet européen est clair : il s'agit d'assurer durablement la paix en Europe à travers la production d'une prospérité résultant d'une coopération industrielle et économique renforcée entre les États qui la composent. Il n'est pas étonnant alors que le projet commence par la production d'une organisation susceptible d'assurer la maîtrise des ressources essentielles à la puissance industrielle de l'Europe : le charbon et l'acier. À l'épreuve du temps, le centre de gravité de la construction européenne se déplace et passe désormais par la construction d'un « marché unique » favorisant la consommation au détriment de la capacité de production. La mise en place d'une monnaie unique, l'euro, vient consacrer cette option d'une construction commerciale et financière de l'Union européenne mais reste finalement un cas assez isolé. Sur le plan diplomatique ou militaire, l'Europe peine à faire entendre une voix puissante et unifiée.

28. – À quelles conditions une puissance numérique européenne est-elle possible ? Le cadre actuel du fonctionnement des institutions européennes exige un accord assez large sur des intérêts partagés pour la mise en place d'initiatives de coopération renforcée. Cela demande beaucoup de temps et génère souvent une complexité qui rend finalement l'initiative périmée ou peu efficace. Par ailleurs – et peut-être que cela est la conséquence de la remarque précédente –, le contexte actuel d'une défiance à l'égard de la pertinence du projet européen pour les peuples qui en font partie, depuis l'échec du projet de Constitution européenne jusqu'au Brexit, interroge sur la capacité de l'Union européenne à faire face aux défis lancés par les puissances numériques américaines, chinoises ou russes. Le problème est que face à ces mêmes puissances, les États européens, pris individuellement, semblent aussi incapables de faire face. Ainsi, la puissance numérique de l'Europe doit-elle passer par un renforcement de la coopération industrielle et technologique entre pays membres ? Ou bien doit-elle plutôt découler d'un renforcement de l'intégration politique de l'Union ? Dans les deux cas, il s'agirait de situer l'objectif

(4) Puisqu'elle est l'émanation de l'Union internationale du Télégraphe créée en 1865.

de souveraineté numérique de l'Europe comme le nouveau moteur de la construction européenne, comme le furent en leur temps la construction du « marché unique » et la mise en place de l'euro.

IV. – Le but de la souveraineté

29. – **De l'objet de la souveraineté au but de la souveraineté.** Après avoir explicité les éléments constitutifs de la souveraineté de l'État et ses enjeux, il est nécessaire de préciser le but de cette souveraineté. Si la souveraineté est l'instrument de la puissance d'un État, à quoi cette puissance doit-elle servir ?

A. – Protéger

30. – **L'État souverain doit protéger le peuple.** C'est le socle fondamental du régalien. Le but premier de la souveraineté est de protéger les citoyens et le pays en préservant le socle de l'État de droit, en protégeant les ressources propres et en assurant un égal accès et une égale répartition des « biens communs » qui permettent de garantir à chacun un juste exercice de ses droits. Dans le détail, cela implique que l'État ait des prérogatives régaliennes dans les domaines de la sécurité (extérieure et intérieure), la monnaie, la justice, l'éducation, la santé ou encore l'accès à l'information. Qu'il soit l'opérateur ou le régulateur de ces domaines, la souveraineté de l'État se mesure à travers sa capacité à *agir* de son propre chef dans ces sphères. Si la nature de ces domaines est inscrite dans l'objet même de la souveraineté, leur extension peut faire l'objet d'un débat public en fonction de situations ou de circonstances particulières. La crise sanitaire du printemps 2020 a démontré qu'afin d'assurer la protection des populations des effets d'une pandémie, il est nécessaire de pouvoir s'appuyer sur un État puissant et souverain.

B. – Rayonner

31. – **La puissance d'un État souverain doit lui servir à rayonner.** Par rayonnement, il faut entendre ici la capacité d'influence d'un État. Dans le registre de l'action d'une nation, sa puissance peut s'exprimer par des moyens directs de contrainte au sein d'un rapport de force ou bien par des moyens indirects de persuasion au sein d'échanges ouverts. C'est la distinction introduite par le politiste Joseph Nye entre *hard power* et *soft power*(5). L'industrie culturelle (cinéma, séries, musique, *etc.*), la gastronomie, le tourisme ou les arts peuvent devenir des instruments d'influence et donc de puissance, à travers le rayonnement qu'ils permettent à l'expression du « génie d'une nation ». Encore faut-il que le pouvoir en ait conscience et y apporte son soutien par des actions dédiées. La mise en place d'une exception culturelle en France et en Europe témoigne ainsi du souci de préserver la possibilité pour les États européens de créer les conditions d'un dynamisme culturel permettant de diffuser des valeurs et des modèles bien au-delà des frontières géographiques(6).

(5) J. Nye, *Bound to lead : The Changing Nature of American Power*, Basic Books, 1990.
(6) La conceptualisation de ce rayonnement international est récente, mais la pratique, elle, est plus ancienne. Le choix de Francois Ier de faire venir Léonard de Vinci en France, ou pour Louis XIV de s'associer les services du Bernin ou de Lully a participé de cette pratique rayonnante de la souveraineté.

C. – Dominer

32. – Les États souverains ont souvent été amenés à interpréter leur puissance comme un facteur de domination, finalement à leurs dépens. Puisqu'elle est l'expression du pouvoir politique suprême, la souveraineté conduit logiquement les États à la domination. Cette domination s'est notamment exprimée historiquement à travers la colonisation et aujourd'hui, sous des formes indirectes, elle continue de s'attester à travers des formes indirectes de domination paradoxalement compatibles avec le jeu des organisations internationales.

1° Quelques exemples historiques

33. – **Jusqu'au milieu du XX^e^ siècle, la colonisation a été une expression de la puissance des États souverains.** Dans ses formes passées, la colonisation est une forme d'extension de la souveraineté d'un État sur un autre territoire pour en revendiquer la maîtrise, au mépris du droit des peuples colonisés. Cette souveraineté acquise s'est traduite par l'appropriation forcée des ressources des territoires colonisés et par la soumission des populations à un pouvoir auquel elles n'ont pu consentir. Plusieurs pays européens sont ainsi devenus de grandes puissances coloniales avant de devoir en payer les frais. Aujourd'hui encore la tentation coloniale reste vive pour certains États souverains, comme en témoignent les prétentions de la Chine sur le Tibet ou celles de la Russie sur certains États frontaliers (Tchétchénie, Ukraine, Géorgie…). Mais cette propension à la domination signale aujourd'hui davantage une souveraineté abusive que l'expression légitime d'une puissance.

2° Les séquelles

34. – La volonté de domination des États souverains a conduit et conduit encore à une instabilité internationale et à un affaiblissement des États. Le monde aujourd'hui reste durablement marqué par les stigmates de la colonisation. Entre les anciennes puissances coloniales et les anciennes colonies, les relations restent tendues et sources d'inimitiés durables. Plus encore à terme, la domination coloniale comme mode d'expression de la puissance souveraine des États présente un bilan très largement négatif. La domination coloniale reposait et repose encore sur une interprétation abusive de la souveraineté comme pouvoir politique suprême et reste donc empreinte d'un caractère illégitime. Les crimes que la domination coloniale n'a pas manqué de rendre possibles laissent des traces durables dans la structure des pays colonisés et dans la mémoire collective des populations anciennement colonisées. Si la domination coloniale a pu participer d'un fantasme de puissance des nations occidentales, elle a conduit en fait à un affaiblissement moral de ces mêmes États qui continue de produire aujourd'hui ses effets en frappant, à raison, toute volonté de domination du sceau de l'illégitimité. Du fait de cette histoire troublée, la puissance des États souverains est vouée à trouver de nouveaux modes d'expression et d'affirmation, plus collaboratifs, plus multilatéraux et donc plus respectueux du droit de chaque État souverain. Tel est le nouveau cadre dans lequel doit se penser la souveraineté numérique des États.

SECTION 2

LA SOUVERAINETÉ REMISE EN QUESTION

35. – La souveraineté traditionnelle a connu des évolutions au cours de ces dernières décennies. Si les formes de la souveraineté traditionnelle ont pu être observées jusqu'à la fin de la Seconde Guerre mondiale, des évolutions notables sont ensuite apparues, notamment avec la construction de nombreuses instances internationales et régionales puissantes faisant du multilatéralisme la norme de la majorité des relations internationales et reléguant ainsi au second plan certains pans de la souveraineté traditionnelle des États-nations. Ces instances ont parfois pu être utilisées par certains États comme des outils de puissance, en particulier par l'unilatéralisme affiché des États-Unis, ou encore par la « Volonté de puissance » renouvelée par les néo/rétro-puissances du XXIe siècle (Chine, Russie, *etc.*). Par ailleurs, nous avons pu assister à l'essor d'acteurs non étatiques, de groupes d'intérêts et d'organisations non gouvernementales (ONG), ainsi qu'à la dilution de la notion d'appartenance citoyenne à l'État-nation au profit d'appartenances multiples de diverses natures. Tout cela a profondément redéfini la notion de la souveraineté, au point que l'on puisse se demander ce qu'il en reste et quelles en sont les nouvelles modalités d'exercice.

I. – Les poussées historiques et leurs conséquences

36. – L'histoire du multilatéralisme commence par son opposé. Dans le courant du XIXe siècle, les souverainetés traditionnelles des États-nations se sont teintées de nationalisme(7), par suite du « Printemps des peuples », entraînant ainsi plusieurs guerres à partir de la fin du XIXe siècle. Après chacune des guerres mondiales, sous l'impulsion des vainqueurs et de quelques belligérants, de nombreux États engagent d'imposantes réformes des relations internationales au travers d'instances qui, pour certaines, portent une aspiration commune avec la Société des Nations puis l'Organisation des Nations unies. Ces instances, qu'elles soient pensées comme un équilibre des forces entre États-nations, comme un accélérateur à la coopération économique ou encore comme une alliance militaire, se révéleront être de formidables outils de puissance, voire de domination pour les États majeurs qui les financent et les animent.

37. – Initialement créée afin de favoriser la coopération internationale, l'ONU est le théâtre des jeux de puissance entre les États. L'Organisation vise, originellement, trois objectifs : garantir la paix internationale, assurer le développement humain, favoriser les échanges commerciaux et la stabilité économique(8). Le développement durable est venu compléter ces objectifs ultérieurement (en 2015, avec l'adoption du Programme 2030)(9). L'ONU est dès l'origine un instrument de pouvoir

(7) S. Berstein et P. Milza, *Nationalismes et concert européen, 1815-1919*, t. 4, Paris, Hatier, 1996.
(8) Cinquante et un pays participants à la Conférence des Nations unies pour l'Organisation internationale, Charte des Nations Unies, 51 Pays, San Francisco, 26 juin 1945 (www.un.org/fr/about-us/un-charter).
(9) ONU, *Les 17 objectifs pour l'humanité et la planète*, Programme 2030, New York, 2015 (www.un.org/sustainabledevelopment/fr/development-agenda).

entre les mains du bloc de l'Ouest et du bloc de l'Est. La crise du canal de Suez en 1956 et l'implication de la France et du Royaume-Uni seront l'occasion pour le Conseil de sécurité de mettre en avant le rôle secondaire des anciennes puissances et l'affirmation des nouvelles superpuissances[10]. Ainsi, dans les faits, l'ONU sera plutôt la caisse de résonance de la puissance américaine et un outil de régulation de la guerre froide entre les blocs[11]. Après les États-Unis, la Russie[12] puis la Chine[13] ont fait usage de leur droit de veto[14] dès que leurs intérêts ou ceux de leurs alliés étaient mis en péril, surtout depuis le désengagement progressif des États-Unis sous les administrations républicaines à partir du début des années 1980. Ces néo/rétro-puissances font ainsi preuve d'une volonté de réaffirmer leur pouvoir et de légitimer à nouveau leur rôle sur la scène internationale. La conjugaison de ces velléités ainsi que les pressions, au nom de la souveraineté d'État, des populo-nationalistes lors de la dernière décennie obligent l'ONU à se réinventer[15] ; ce chantier devenant un enjeu de première importance pour lui éviter le même destin que celui de la Société des Nations.

38. – Les premières instances créées au sortir de la guerre ont une vocation égalitaire ou intégratrice, mais nombre d'entre elles se révéleront être vecteur de puissance. Les accords de Bretton Woods signés dès juillet 1944 ont dessiné les grandes lignes du système financier international de l'après-guerre avec la création de la Banque mondiale et du Fonds monétaire international (FMI). Ces instances rejoindront par la suite l'ONU après sa création. De nombreuses autres agences, unions, pactes, accords, chartes ou instances verront ensuite le jour et, parmi eux, beaucoup existent encore[16]. Sur le Vieux Continent, la Communauté européenne du charbon et de l'acier (CECA), la Communauté économique européenne (CEE) puis l'Union européenne (UE) sont devenues un axe de pouvoir au fur et à mesure que la dimension fédérale de l'Europe, qui était l'idée des Pères fondateurs européens[17], s'effaçait au profit de la dimension économique. Mais le

(10) Délibérations du Conseil de sécurité de l'ONU sur la situation créée par l'abrogation unilatérale de la gestion internationale du canal de Suez par le Gouvernement égyptien, New York, 1956-1958 (www.un.org/en/sc/repertoire/56-58/Chapter%208/56-58_08-3-Situation%20created%20by%20the%20unilateral%20action%20of%20the%20Egyptian%20Government%20in%20bringing%20to%20an%20end%20the%20system%20of%20international%20operation%20of%20the%20Suez%20Canal%20.pdf).

(11) C. Maurel, *Histoire des idées des Nations unies. L'ONU en 20 notions*, Paris, L'Harmattan, 2015.

(12) S. Huvé, *L'Organisation des Nations unies, cadre et instrument de la politique extérieure russe, 1999-2015*, L'Harmattan, 2015.

(13) H. Thibault, B. Pedroletti et M. Bourreau, *La Chine à l'assaut des Nations unies : Le Monde* 31 mai 2019.

(14) Conseil de sécurité de l'ONU, bibliothèque Dag Hammarskjöld, New York, 2020 (https://research.un.org/fr/docs/sc/quick).

(15) Représentation permanente de la France auprès des Nations unies, *Alliance pour le multilatéralisme : pour une coopération internationale rénovée*, New York, 2 avr. 2019.

(16) C'est le cas du [*modern*] Commonwealth, créé en avril 1949, de l'Organisation du traité de l'Atlantique nord (OTAN) mise en place en septembre 1949, de la Communauté européenne du charbon et de l'acier (CECA) fondée en avril 1951, du Pacte de Varsovie, conclu en mai 1955, de la Communauté économique européenne (CEE), fondée en mars 1957, de l'Organisation des pays exportateurs de pétrole (OPEP), fondée en septembre 1960, de l'Association des nations de l'Asie du Sud-Est (ASEAN), fondée en août 1967, du Traité sur la non-prolifération des armes nucléaires (TNP) signé en mars 1970, de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) créée en mai 1975, du Groupe de Visegrád, créé en février 1991, du Marché commun du Sud (Mercosur), créé en mars 1991, de l'Union européenne (févr. 1992), de l'Accord de libre-échange nord-américain (ALENA) signé en janvier 1994, de l'Organisation de coopération de Shanghai (OCS) fondée en juin 2001 et succédant au Groupe de Shanghai ayant vu le jour en avril 1996, parmi beaucoup d'autres.

(17) Aristide Briand, *Mémorandum sur l'organisation d'un régime d'union fédérale européenne* ou « Mémorandum Briand », Genève, sept. 1929. – Union des fédéralistes européens (Altiero Spinelli et groupe « Francs-tireurs » de

désengagement des États-Unis de la scène européenne ainsi que les risques nouveaux générés par les néo/rétro-puissances et l'agitation des populo-nationalistes requièrent une transformation de l'Union européenne. Les évolutions de cette dernière portent alors sur les multiples leviers régaliens : la défense[18], la souveraineté industrielle[19] (sujet amplement relancé avec la pandémie de Covid-19)[20], le numérique[21], *etc.* L'Organisation du traité de l'Atlantique nord (OTAN) et, en miroir, le Pacte de Varsovie, sont évidemment des leviers de puissance, respectivement pour les États-Unis et l'URSS. Ce qui n'empêcha pas la France de vouloir sauvegarder sa souveraineté (d'abord navale puis nucléaire) en se retirant progressivement de l'OTAN, jusqu'à sa sortie en 1966[22] (avant sa réintégration en 2009). Au sein du Pacte de Varsovie, l'Armée rouge sera utilisée pour faire rentrer les États vassaux dans le rang (révolution hongroise de 1956, Printemps de Prague de 1968)[23]. La chute du mur de Berlin, sans réaction militaire de l'URSS, entraîna la fin du Pacte en 1991. Depuis, certains des pays du Pacte ont rejoint l'OTAN. La réaction russe dans son ancienne sphère d'influence est encore sensible de nos jours (Ukraine, Crimée, Biélorussie, *etc.*).

39. – Ces développements historiques constituent les prémices de profondes modifications de la notion de souveraineté. S'il semble éloigné des questions posées aujourd'hui par la souveraineté numérique, l'abandon, même partiel, de dimensions régaliennes telles que la défense, l'éducation, la santé, l'énergie, les télécommunications, les infrastructures, *etc.*, s'est en premier lieu opéré au sein d'instances mondiales (en particulier l'ONU et ses agences spécialisées) ou régionales. La complexité du « jeu des puissances » s'est amplifiée, passant d'un monde bipolaire à l'avènement de la domination des États-Unis, avant de revenir à un monde multipolaire complexe, ouvrant la porte à deux tendances majeures qui se renforcent jusqu'à nos jours, à savoir :

– l'interventionnisme des États au sein de leurs sphères d'influence, sous couvert de multilatéralisme (ou de refus du multilatéralisme). Ce jeu utilise de multiples leviers, allant du *soft power* à la coercition économique ou militaire, en passant par la diplomatie ou des opérations « noires » ;

– la complexification, en particulier par la multiplication des leviers utilisés, qui ouvre la porte à des acteurs non étatiques, pour figurer et influer sur les différents plateaux du « jeu des puissances ».

Lyon), Montreux, 1947. – Winston Churchill, Discours de Zurich, sept. 1946, mais finalement W. Churchill se montrera plus unioniste que fédéraliste.

(18) Collectif, *Revue stratégique de défense et de sécurité nationale* 2017, DGRIS, Paris, oct. 2017 (www.defense.gouv.fr/dgris/politique-de-defense/revue-strategique/revue-strategique). – Synthèse sur le site du ministère de l'Europe et des Affaires étrangères : www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/l-europe-de-la-defense.

(19) E. Delbecque et A. Lafont, *Vers une souveraineté industrielle ?*, Paris, Vuibert, 2012.

(20) Plan d'action pour la relocalisation des industries de santé en France (www.economie.gouv.fr/plan-daction-pour-relocalisation-industries-sante-en-france).

(21) B. Thieulin. *Pour une politique de souveraineté européenne du numérique*, Paris, Conseil économique social et environnemental, 2019.

(22) A. Giglioli, *Le Retrait de la France du Commandement Intégré de l'OTAN* (p. 12), OTAN, 1998.

(23) A. Dubček, *C'est l'espoir qui meurt en dernier*, Autobiographie, Paris, Fayard, 1993. Seule l'Albanie se retira du Pacte en 1968 sans invasion militaire car elle ne partage pas de frontière avec les autres membres du Pacte. Le désengagement albanais datait de fait de 1961.

II. – Les conséquences du passage du libéralisme au néolibéralisme

40. – Le néolibéralisme résultant d'une volonté de refonte du libéralisme au milieu du xx^e siècle promeut un désengagement de l'État. La première tentative a lieu à Paris du 26 au 30 août 1938. Elle rassemble, lors du colloque Walter Lippmann, vingt-six intellectuels, philosophes, ingénieurs et surtout économistes de multiples nationalités, représentant l'ensemble des tendances du libéralisme économique – alors dominé par la Théorie générale de Keynes – et politique de l'époque[24]. Dès l'après-guerre, la Société du Mont-Pèlerin reprend ces travaux, mais en abandonne les dimensions les plus sociales. Elle est créée en avril 1947 et compte parmi ses membres huit détenteurs du Prix de la Banque de Suède (dit « Prix Nobel d'économie »), dont Friedrich Hayek et Milton Friedman[25], et nombre de ses membres ont essaimé dans de nombreux pays des *think-tanks* néolibéraux et conservateurs. Ces néolibéraux promeuvent le désengagement de l'État dans la plupart des domaines, hormis ceux qui garantissent l'épanouissement des entreprises et qui assurent l'ordre et la défense, la liberté individuelle la plus totale possible et la liberté d'expression dans son sens le plus strict, au détriment des notions d'équilibre, de protection ou de développement humain.

41. – La financiarisation de l'économie, induite par ces théories, réduit les marges de manœuvre des États. Avec le monétarisme[26], promu par Milton Friedman, la masse monétaire et les taux d'intérêt deviennent les leviers principaux utilisés par les États, ou plutôt les banques centrales. La réduction de la masse monétaire permet de juguler l'inflation, et les taux, définis par les banques centrales, permettent d'assouplir ou de contraindre l'économie au travers de l'emprunt. L'emprunt étant aux mains des institutions financières, l'économie est de plus en plus centrée autour de la finance. *De facto*, les marges de manœuvre des États en sont diminuées, notamment concernant la redistribution pour laquelle seule la fiscalité reste un levier.

42. – L'expansion du néolibéralisme a entraîné l'affaiblissement de la souveraineté économique des États. L'expansion du néolibéralisme commence au Chili, à travers un groupe d'économistes chiliens, influencés par Milton Friedman et Arnold Harberger, qui furent à l'origine des principales réformes économiques de la dictature militaire chilienne dirigée par le général Augusto Pinochet dans les années 1970[27]. Milton Friedman considéra leur politique comme le « miracle chilien ». Cet apparent succès chilien encouragea les dirigeants conservateurs de grands pays à adopter à leur tour des politiques néolibérales. Ainsi, au début des

(24) F. Urbain Clave, *Walter Lippmann et le néolibéralisme de La Cité Libre : Cahiers d'économie politique* 2005/1, n° 48, p. 79 à 11, L'Harmattan, Paris (www.cairn.info/revue-cahiers-d-economie-politique-2005-1-page-79.htm). – Collectif, *Le colloque Lippmann*, Paris, Librairie de Médicis, 1939. – S. Audier, *Le Colloque Walter Lippman – Aux origines du « néolibéralisme »*, Le Bord de l'Eau, 2012. – F. Copeau, *Recension de l'ouvrage de Serge Audier sur le Colloque Lippmann*, Contrepoints, 2010 (www.contrepoints.org/2010/10/29/5647-le-colloque-lippmann).
(25) www.montpelerin.org.
(26) Faciléco, Fiche Milton Friedman, Paris (www.economie.gouv.fr/facileco/milton-friedman).
(27) M. Délano et H. Traslaviña, *La herencia de los Chicago boys*, Ediciones del Ornitorrinco, 1989.

années 1980, plusieurs chefs d'État ou de gouvernement devinrent les promoteurs de cette doctrine politico-économique : ce fut le cas par exemple de Ronald Reagan aux États-Unis, Margaret Thatcher au Royaume-Uni ou encore Davíð Oddsson en Islande. Progressivement, la doctrine néolibérale devint la doctrine dominante de l'économie mondiale. En Europe, l'Allemagne – bien qu'étant moins néolibérale – était déjà adepte de l'orthodoxie monétaire et appliqua la plupart des principes néolibéraux dès la première moitié des années 1980. Cela renforça sa place au sein de l'Europe et en particulier au sein du couple franco-allemand (comme en témoignent les nombreuses dévaluations[28] du franc vis-à-vis du mark[29] ou encore le sauvetage conjoint du franc de 1992[30]) et favorisa la croissance de l'économie allemande. L'impact du néolibéralisme a offert des leviers aux institutions financières telles que les banques, les assurances, les fonds d'investissement, les grandes entreprises, *etc.*, en les plaçant au centre de pratiques monétaires de plus en plus avantageuses pour les entreprises, que les banques centrales ont souvent bien du mal à maîtriser. L'affaiblissement des leviers souverains économiques a ainsi contribué à renforcer le poids des acteurs non étatiques.

III. – L'entrée des acteurs non étatiques dans le « jeu des puissances »

A. – Les entreprises

43. – Par le passé, les entreprises nécessaires au Royaume de France dépendaient déjà de la politique de l'État. Par exemple, sous l'impulsion de Colbert, Louis XIV engagea un large plan de développement de la Marine royale menant à la création d'arsenaux, de cordonneries, d'écoles de marine, *etc.* Pour ce faire, il mit en place une intégration verticale allant de la plantation de forêts de chênes à la construction des navires, chaque maillon appartenant à l'État. Cela permit la professionnalisation et l'indépendance de la Marine royale[31], qui était jusqu'alors soumise à l'achat de bois ou de navires auprès de puissances étrangères et qui avait recours à la « presse », un système de recrutement qui consistait à enrôler de force des marins, brutalement et sans préavis.

44. – La révolution industrielle et les guerres qui ont suivi ont permis une accélération de l'innovation, avec comme corollaire le recours des États à des entreprises privées. La révolution industrielle a induit l'avènement d'armes modernes, produites en grande quantité. Dès lors, l'État s'est appuyé sur les capacités des entreprises privées à fournir « l'effort de guerre », depuis les matières premières, à savoir les minerais et le pétrole, en passant par les produits intermédiaires (chimie), jusqu'aux produits finis tels que les canons, les chars, les uniformes et les infrastructures.

(28) AP, *Les grandes dates de l'histoire du franc : L'Obs* févr. 2002.
(29) F. Allemand, *Le couple Mitterrand-Kohl*, Luxembourg, CVCE, 2007 (www.cvce.eu/education/unit-content/-/unit/7124614a-42f3-4ced-add8-a5fb3428f21c/bcadd9d0-df8a-4798-980f-2f2aa2631fb1).
(30) C. Lhaik et P. Coste, *Comment le franc fut sauvé : L'Express* 1993 (www.lexpress.fr/informations/comment-le-franc-fut-sauve_594678.html).
(31) D. Morano, *Colbert, ou la révolution de la Marine royale*, Paris, Ministère des Armées, 2015 (www.defense.gouv.fr/portail/dossiers/10-personnalites-qui-ont-marque-la-defense/portraits-de-l-ete-colbert-ou-la-revolution-de-la-marine-royale).

La Seconde Guerre mondiale a démontré que la puissance productive des États-Unis, en support des Alliés, fut essentielle au renversement de l'Axe. Dès le milieu du XIXe siècle, les guerres ont été d'extraordinaires accélérateurs de l'innovation : aviation, chars, sous-marins, motorisation diesel et électrique, balistique, propulsion, cryptographie, calculateurs, électronique, nucléaire, *etc.*, sont autant de secteurs ayant bénéficié de ces progrès dans le domaine militaire.

Ainsi, la genèse du complexe militaro-industriel (CMI) remonte, *a minima*, au début du XXe siècle. Il se généralise à partir des prémices de la Seconde Guerre mondiale, suivant des schémas différents en fonction des États et s'amplifie dans le contexte du « jeu des puissances » et de l'affrontement des blocs, en se matérialisant notamment au travers de la conquête spatiale, l'indépendance énergétique, l'indépendance alimentaire, la puissance de calcul. Sous un contrôle plutôt fort au travers d'entreprises d'État en Europe, le CMI prend une proportion importante aux États-Unis. Ainsi, le Président Dwight D. Eisenhower, lors de son discours de fin de mandat en janvier 1961, met en garde contre les dangers d'une trop grosse influence des industriels liés au département de la Défense, dans le contexte de la course aux armements liée à la guerre froide(32). L'URSS n'est pas en reste puisque son CMI est la structure vertébrale de son industrie.

Suivant les États, le CMI ne se limite pas aux entreprises de l'armement. Ainsi, industrie automobile, industrie aérospatiale, chantiers navals, industrie nucléaire, industrie de défense (vecteur d'arme ou charge), industrie électronique, entreprise d'infrastructures et du bâtiment, industrie textile (textiles techniques), entreprises énergétiques et pétrolières, industrie des télécommunications ou encore industrie informatique ou logicielle sont autant de domaines connectés au CMI, et cette liste n'est bien entendu pas exhaustive.

La présence de sociétés militaires privées (SMP) – ou, en France, d'entreprises de services de sécurité et de défense (ESSD) – ne se limite plus au matériel mais à la présence de personnels sous contrat dans un éventail d'activités allant de la prévention de la criminalité (protection des entreprises en zones à risques, gestion de prises d'otages) à la sécurité civile et au maintien de l'ordre, en passant par le soutien logistique (approvisionnement, gestion de camps), la formation et le conseil militaire ou encore le soutien militaire (participation aux opérations)(33).

45. – Une coopération « public/privé » qui, dans certains cas, peut ressembler à un transfert de pans entiers de souveraineté. La dépendance accrue des armées aux entreprises privées n'a eu de cesse de se renforcer depuis la chute du mur de Berlin, et encore plus depuis l'état de guerre permanent qui a fait suite aux attentats du 11 septembre 2001(34). Se pose alors une question essentielle : quelle autorité garantit que cette coopération n'engendre pas, dans les faits, un véritable

(32) D. Dwight Eisenhower, *Farewell Address*, Washington DC, janv. 1961 (www.francetvinfo.fr/replay-radio/histoires-d-info/histoire-d-infos-dans-son-discours-d-adieu-eisenhower-denonce-le-complexe-militaro-industriel-et-semble-nous-parler_1999673.html).

(33) P. Darantière, *Les sociétés militaires privées : succès et contraintes : Inflexions* 2007/1, n° 5, p. 107 à 125, Paris, Armée de terre, Doc. fr. (www.cairn.info/revue-inflexions-2007-1-page-107.htm). – E. Even, *La France et les sociétés militaires privées : enjeux et état du débat : Inflexions* 2014/1, n° 25, p. 149 à 157, Paris, Armée de Terre, Doc. fr. (www.cairn.info/revue-inflexions-2014-1-page-149.htm).

(34) P. Sartre, *Soldats privés : Études* 2008/4, t. 408, p. 452 à 462 (www.cairn.info/revue-etudes-2008-4-page-452.htm).

transfert des prérogatives de souveraineté ? En principe, c'est l'autorité donneur d'ordres qui y veillera, mais encore faut-il qu'elle en ait la capacité réelle. Certains cadres juridiques comme le « Document de Montreux », d'initiative suisse[35], ou le *Contractor accountability bill* américain[36] existent déjà à ce sujet. Toutefois, la question reste entière de savoir si l'État seul est bien en capacité d'assurer un tel contrôle, et certains incidents graves permettent d'en douter (comme les dérives de la société privée Blackwater[37], dont certains membres ont été impliqués dans des attaques de civils en Irak en 2007, puis ont été mis en cause et condamnés grâce notamment à la vigilance d'associations citoyennes telles que « Xe Watch »). Certains États ont fait le choix de l'autorégulation, comme le Royaume-Uni avec le *Approved contractor scheme* »[38]. Cette question dépasse de loin les domaines de la défense et de la sécurité. Ainsi, l'ensemble des autres domaines régaliens, tels que l'autonomie énergétique, l'autonomie alimentaire, la santé ou encore l'éducation sont maintenant, et pour certains pays, depuis longtemps ouverts à la sphère privée. Chacun de ces domaines ouverts offre des opportunités de plus en plus importantes et génère une osmose plus forte entre État et domaine privé[39].

46. – L'ingérence des entreprises dans le domaine social, et l'apparition d'un sentiment de « citoyenneté d'entreprise ». L'ouverture de ces domaines ou leur délégation sont aujourd'hui de deux ordres, à savoir la privatisation ou la délégation étatique de leviers régaliens, ou bien la montée de la prise en charge par les entreprises de plusieurs de ces dimensions à destination de leurs employés et parfois de leurs familles (mutuelles, retraites complémentaires, congés complémentaires, compte épargne temps, crèches, bourse d'études…). Dans ce dernier cas, nous pouvons parler de citoyenneté d'entreprise. Encore une fois, les géants du web et des technologies sont aujourd'hui en pointe sur ces deux dimensions[40]. À d'autres époques ce furent les industriels, rétrospectivement qualifiés de « paternalistes »[41],

(35) Le Document de Montreux a été conçu pour promouvoir le respect du droit international humanitaire et des droits humains lorsque des entreprises militaires et de sécurité privées (EMSP) opèrent dans le cadre d'un conflit armé. Ce document, adopté en 2008 par dix-sept États à la suite d'une initiative conjointe lancée par la Suisse et le Comité international de la Croix-Rouge (CICR), était soutenu, en juillet 2017, par cinquante-quatre États et trois organisations internationales. Il constitue le premier document d'envergure internationale qui réitère les obligations incombant aux États en vertu du droit international eu égard aux activités des EMSP. Il ne constitue pas un traité juridiquement contraignant et ne crée pas de nouvelles obligations juridiques (Confédération suisse, Département fédéral des affaires étrangères, Document de Montreux, sept. 2006 : www.eda.admin.ch/eda/fr/dfae/politique-exterieure/droit-international-public/droit-international-humanitaire/entreprises-militaires-securite-prives/document-montreux.html).

(36) M. Meehan, H.R. 4387 (108th) : *Contractor Accountability Act*, US Congress, 2004. Depuis 2004, en vertu de ce texte, les sociétés militaires privées (SMP) basées aux États-Unis doivent obtenir une licence auprès du *Defense Trade Control Office* (www.congress.gov/bill/108th-congress/house-bill/4387?s=1&r=55).

(37) Blackwater fut renommée Xe puis Academi.

(38) G.-H. Martin-Bricet, *Le marché des ESSD : Quelle évolution à terme ?*, Goron SA, 2019 (https://rendre-notre-monde-plus-sur.goron.fr/le-marche-francais-des-essd-quelle-evolution-a-terme).

(39) T. Porcher, *Traité d'économie hérétique*, Paris, Fayard, 2019.

(40) « Le néo-paternalisme peut sembler efficace, Google est souvent cité comme référence d'entreprise où il fait bon travailler et de nombreux jeunes actifs se pressent pour devenir les prochains "Googleurs" Les GAFAM diffusent des cultures d'entreprise qui poussent l'employé à donner toujours plus de son temps libre et de ses idées, bien au-delà du contrat de travail. Tous ces avantages font émerger un sentiment de redevabilité envers l'entreprise qui va inconsciemment faire accepter des heures de travail plus longues et des tâches moins intéressantes que les aspirations de l'employé » (https://medium.com/@j.harari/neo-paternalisme-ou-la-promesse-du-bonheur-au-travail-462efb1b6520).

(41) Le Familistère de Guise (www.familistere.com/fr/decouvrir/cent-ans-d-experimentation-sociale). – D. Fortin, *Et le paternalisme céda la place au management : Les Échos* oct. 2010 (www.lesechos.fr/2010/10/et-le-paternalisme-ceda-la-place-au-management-1087891).

puis les énergéticiens[42], les banquiers et quelques administrations qui furent à l'initiative de ce type de pratiques. Demain, celles-ci pourraient peut-être s'étendre aux clients de certaines entreprises, notamment de certains acteurs numériques. En extrapolant, on pourrait alors imaginer parler, un jour, de « citoyen franco-Facebook » ou de « citoyen anglo-TikTok »… Plus utopique encore, sauf pour les entreprises libertariennes, une citoyenneté purement d'entreprise et non plus d'État n'est-elle pas imaginable ? Le sujet est traité depuis longtemps par la littérature[43], et plus récemment par le cinéma[44]. Mais il fait aussi l'objet de projets, dont l'un est défendu par le petit-fils de Milton Friedman, Patri Friedman[45]. Ainsi, l'on assiste à un lent phénomène d'émiettement de la souveraineté, fruit du désinvestissement de l'État, sur le cœur du régalien (santé, éducation…), mais aussi fruit – comme vu précédemment – de partenariats « public/privé » dans lesquels l'État a perdu une partie de son autonomie concernant certaines de ses prérogatives essentielles et historiques (défense et sécurité).

B. – Groupements d'intérêt et *lobbies*

47. – La disparition des corporations et l'avènement du libre-échange. La fin des corporations et l'avènement des *lobbies* commencent à la suite de l'apparition des idéaux libéraux au long du XVIII^e^ siècle. Dans le Royaume de France, cela signifie la lente désagrégation du colbertisme, jusqu'à la Révolution française et la loi Le Chapelier de 1791 qui mit un point final à ce système datant de l'Antiquité. Cette transformation systémique a accompagné le passage de l'artisanat, de son système de caste et de sa production très localisée à l'industrialisation, l'échange des savoir-faire entre provinces et pays, et une production de masse. C'est aussi une transformation systémique où l'ouvrier se spécialise et est moins bien rémunéré que dans le système corporatiste.

48. – L'apparition des *lobbies*. Dès le début du XIX^e^ siècle, les industriels se regroupent et influencent les politiques dans les couloirs du Parlement anglais (d'où le terme *lobby*)[46]. Les *lobbies* conservateurs sont rapidement rejoints par les premières organisations ouvrières qui se structurent à un niveau national dès les années 1830 puis se renforcent des années 1850 aux années 1870[47], marginalisant les acteurs les plus violents en entrant dans le jeu démocratique. En France, par suite des révolutions de 1789 puis de 1830, la société est plus libérale, libre-échangiste et (légèrement) moins conservatrice, en contrepoint des organisations ouvrières qui se structurent plus tard et donnent naissance au droit de grève

(42) J.-C. Bourbon, *Les coûteux avantages des agents d'EDF pointés par la Cour des comptes : La Croix* 6 févr. 2019 (www.la-croix.com/Economie/France/couteux-avantages-agents-dEDF-pointes-Cour-comptes-2019-02-06-1201000597).
(43) Par ex. : J. Lovegrove, *Days*, Phoenix, nov. 1997.
(44) J. Ponsoldt, *The Circle*, 1978 Films / EuropaCorp / Imagenation Abu Dhabi FZ / Likely Story / Parkes/MacDonald Image Nation / Playtone / Route One Entertainment, USA, avr. 2017.
(45) Patri Friedman (http://patrifriedman.com).
(46) Le terme *Lobby of the House* est utilisé dès les années 1830 en Angleterre, en référence aux « couloirs de la Chambre des communes », la « salle des pas perdus » où les membres de groupes de pression pouvaient venir « faire les couloirs », c'est-à-dire discuter avec les *members of Parliament* (parlementaires) (https://fr.wikipedia.org/wiki/Lobby).
(47) *Trade unionism*, The National Archives, Londres (www.nationalarchives.gov.uk/pathways/citizenship/struggle_democracy/trade_unionism.htm).

en 1864 et aux syndicats en 1884, avec la loi Waldeck-Rousseau. Ainsi, la puissance économique des uns leur permet d'intervenir au plus tôt pour faire valoir leurs avantages mais se retrouve à moyen terme concurrencée par la structuration de mouvements contestant les iniquités. À l'origine, ce mécanisme se trouve accéléré par la diffusion des opinions et de l'information au travers de l'imprimerie[48], puis surtout de la presse[49]. Au tournant du XX^e^ siècle, les acteurs industriels et politiques comprennent que leur structuration et leurs capacités d'intervention au sein des instances de pouvoir ne sont plus suffisantes pour conserver leurs avantages. Ils trouvent d'abord chez Gustave Le Bon[50] une délivrance à leurs craintes :

– la justification de la violence d'État pour maîtriser la « foule » comme une entité « histérisante », anesthésiant les pensées individuelles de ceux qui la composent ;

– une approche du contrôle des masses au travers de propagandes ciblées, en parallèle de leurs actions de *lobbying*[51].

Gustave Le Bon est précurseur concernant la jugulation de l'ochlocratie[52], mais son approche reste balbutiante et empreinte de biais. D'autres penseurs, comme Edward Bernays et Walter Lippmann adoptent rapidement et concomitamment une approche plus rationnelle de l'opinion publique : tous deux s'intéressent à ce que l'on nomme alors « propagande », Edward Bernays avec une approche démagogique et mercantile et Walter Lippmann avec une approche politique et bienveillante du sujet.

49. – Edward Bernays invente la notion de « relation publique ». Il crée la première agence du genre mi-1919 à New York. Il décrit « les masses » comme irrationnelles et moutonnières[53]. Ces masses, incapables de penser, peuvent être manipulées par une élite dirigeante[54]. Parmi ses faits d'armes, on pourra citer les suivants :

– pour le compte de la *Beech-Nut Packing Company* et s'appuyant sur des études commandées à des scientifiques de complaisance et largement diffusées auprès des médecins, il fait des « œufs au bacon » le petit-déjeuner type des Américains. L'industrie porcine voit exploser son chiffre d'affaires ;

– il était mal vu que les femmes fument des cigarettes, en particulier en public. En 1929, pour le compte de *The American Tobacco Company*, lors du défilé de Pâques sur la Cinquième Avenue, il fait défiler et fumer des femmes et renomme les cigarettes, pour cette occasion, « Torches de la liberté ». Il manipule le féminisme,

(48) Il fallut dépasser de longtemps les incunables, pour arriver à l'impression des idées porteuses du XVIII^e^ siècle, celles des lumières.

(49) À titre d'exemple : J.-P. Marat, *L'ami du peuple ou le Publiciste parisien, journal politique, libre et impartial*, Paris, 1789 à 1792. Pour la petite histoire, Marat écrivait ses feuillets au Procope et sonnait une cloche installée pour lui afin que ses collaborateurs accourent, les impriment et en fassent la distribution.

(50) G. Le Bon, *Psychologie des foules*, Paris, Ancienne librairie Germer Baillière & C^ie^, Félix Alcan Éditeur, 1895 (https://fr.wikisource.org/wiki/Psychologie_des_foules).

(51) Y.-J. Thiec et G. Le Bon, *Prophète de l'irrationalisme de masse : RF sociologie* 1981, 22-3, p. 409-428, Paris, édition du CNRS (www.persee.fr/doc/rfsoc_0035-2969_1981_num_22_3_3438).

(52) Gouvernement où le pouvoir est aux mains de la foule (www.cnrtl.fr/definition/ochlocratie).

(53) E. Bernays, *Crystallizing public opinion*, New York, Horace Liveright, 1923 (https://archive.org/details/in.ernet.dli.2015.1607/page/n1/mode/2up).

(54) E. Bernays, *Propaganda*, New York, Horace Liveright, 1928 (https://archive.org/details/BernaysPropaganda).

et transforme ces produits du tabac en symbole d'émancipation et en événement national, repris par les médias. Les cigarettiers vont ensuite accroître considérablement leur marché.

50. – Walter Lippmann forge, quant à lui, le concept de « fabrique du consentement ». Cet intellectuel américain, qui peut être qualifié de social-libéral, est l'initiateur du colloque Walter Lippmann de 1938 à Paris[55]. Il considère que l'opinion publique peut être manipulée en s'appuyant sur les recherches en psychologie et sur les moyens de communication[56]. Selon lui, le « public » est inapte à créer et diriger sa propre politique, mais ce « public » peut apporter son soutien aux idées raisonnables ou raisonnées de ceux qui les défendent, quitte à ce que ces figures défient le régime en place[57]. L'autogestion est pour lui une utopie, l'intermédiaire d'une figure d'autorité et de ses appuis est nécessaire pour gérer la complexité du monde et la traduire au public, de la même manière que nous remettons nos vies à des chirurgiens dans un acte conscient. Walter Lippmann invite à la prise en main des affaires par les plus compétents et les plus représentatifs. Il favorise une forme d'élitisme mais souhaite, en miroir, un public éclairé, éduqué et informé[58]. D'autres intellectuels continuent de travailler sur ces sujets, tels Noam Chomsky et Edward S. Herman, qui ajoutent au débat deux notions[59]. La première est l'intérêt commun des acteurs de pouvoir dans l'information (politiques et industriels), signifiant la mise sous tutelle des grands médias par les acteurs économiques majeurs ; elle est combinée à la distorsion des faits au travers de biais, essentiellement inconscients, en fonction du contexte, des croyances collectives ou des intérêts. Chacun de ces théoriciens comprend que l'information, ou la communication, est une question de *momentum*, de *timing*. Créer l'événement, révéler une information pour faire un *scoop*, ou interférer avec une autre histoire, délivrer les informations ou des éléments de langage, suivant un certain rythme, participent des ressorts utiles.

51. – Avec l'avènement des médias de masse, le dérèglement de l'information. La formidable accélération du rythme de production et de diffusion des contenus par les médias s'est d'abord traduite auprès de la presse audiovisuelle qui s'est jetée dans la quasi-instantanéité, avec les chaînes d'information en continu, et s'est accompagnée de la disparition de limites légales (*fairness doctrine*)[60], ce qui a eu un effet dévastateur sur la qualité de l'information ou la précision de la communication. L'avènement d'Internet a ensuite bouleversé le modèle économique de la presse écrite, en donnant accès, gratuitement, à des informations jusqu'alors payantes. Cette gratuité a radicalement changé les équilibres d'avant,

(55) Dans les faits, le colloque a été organisé par Louis Rougier (www.wikiberal.org/wiki/Louis_Rougier).
(56) W. Lippmann, *Public Opinion*, New York, Harcourt, Brace & Co., 1922 (https://archive.org/details/publicopinion00lippgoog).
(57) W. Lippmann, *The Phantom Public*, États-Unis, Transaction Publishers, 1925. – G. Bastin, « *Le Public fantôme », de Walter Lippmann : la déroute des citoyens : Le Monde* 9 oct. 2008.
(58) W. Lippmann, *Liberty and the News, Harcourt, Brace & Co*, New York, 1920 (https://archive.org/details/libertyandnews01lippgoog).
(59) E. Herman et N. Chomsky, *Manufacturing Consent : The Political Economy of the Mass Media*, New York, Pantheon Books, 1988.
(60) *Syracuse Peace Council* vs *F.C.C*, United States Court of Appeals of Columbia Circuit, févr. 1989. – Brooks Boliek, *FCC finally kills off fairness doctrine : Politico* 22 août 2011, États-Unis (www.politico.com/story/2011/08/fcc-finally-kills-off-fairness-doctrine-061851).

où l'information était payante par le lecteur et par l'annonceur, pour ne laisser place qu'au seul financement par la publicité. Sur le web, s'est engagée une course folle au clic et au référencement, avec les dérives que l'on connaît sur la qualité de l'information : l'amplification démesurée de certains micro-événements ou faits divers (les médias étant incités à écrire toujours plus d'articles sur le même sujet qui fait plus d'audience), oubli des priorités éditoriales, prime à la vitesse (quitte à ne pas prendre le temps de la vérification), *etc.* Ce *maelstrom* a permis l'émergence de médias clivants (Fox News), de médias alternatifs (sites de l'*alt-rigth* ou sites de réinformation en France), de sites populistes tel « Le Média » en France, ou encore de médias de manipulation (RT, Sputnik, CGTN, *etc.*). Cette florescence multiplie les possibilités de manipulation de groupes d'intérêt de plus en plus segmentés, de plus en plus centrés sur des opinions sans contrepoints, tendant parfois au délire complotiste (par ex. : QAnon)[61]. Dans ce contexte, la manipulation de masse, théorisée en particulier par Edward Bernays, n'a quasiment plus de limite et est ouverte aux gouvernements, aux entreprises, comme aux groupes d'intérêt ou de pression, mais aussi à des tribus d'individus, jusqu'aux plus délirantes comme par exemple les « platistes ».

52. – **L'aboutissement récent de ce dérèglement : le phénomène *fake news* (fausses nouvelles), et la riposte récente qui s'organise en France et en Europe.** L'avènement d'Internet et surtout ensuite l'ouverture de vecteurs alternatifs aux médias traditionnels, à travers les réseaux sociaux, propices à la prise de parole irréfléchie ou volontairement polémique, ont vu se décupler le phénomène (ancien) de diffusion de fausses nouvelles (*fake news*). Lorsque celles-ci sont conçues et/ou diffusées pour servir les intérêts d'entreprises ou d'États, on peut y voir un héritage des précédents historiques de Bernay et Lippmann. Ces fausses nouvelles (aussi appelées « infox ») sont des informations dont on peut prouver qu'elles sont fausses ou trompeuses, présentées et diffusées dans l'intention délibérée de tromper le public. Les effets de la désinformation sur nos sociétés sont importants, en ce qu'elle altère la confiance des citoyens dans les institutions et les médias et porte atteinte à la démocratie en empêchant une prise de décision éclairée et réfléchie. Les réseaux sociaux sont acteurs incontournables de la propagation et la lutte contre des *fake news*. Pour de nombreuses personnes, les réseaux sociaux sont devenus la principale source d'information. Par leur intermédiaire, des campagnes de diffusion de fausses informations destinées à influencer les comportements des électeurs ont été dénoncées lors des élections présidentielles de 2016 et 2020 aux États-Unis ou du référendum sur le Brexit au Royaume-Uni. En France, selon le baromètre des médias 2017, 83 % des utilisateurs des réseaux sociaux seraient soumis à une forte exposition aux rumeurs et un tiers des personnes interrogées pensent que certaines *fake news* sont vraies. D'après l'Observatoire du journalisme européen (EJO), entre 2018 et 2019, le nombre de *tweets* ayant relayé ou commenté une *fake new* a augmenté de près de 30 %. Ce phénomène s'est fortement accentué avec la pandémie de Covid-19 de sorte que l'Organisation mondiale de la santé (OMS) a pu

(61) A. LaFrance, *The Prophecies of Q, American conspiracy theories are entering a dangerous new phase : The Atlantic* juin 2020, États-Unis (www.theatlantic.com/magazine/archive/2020/06/qanon-nothing-can-stop-what-is-coming/610567).

évoquer une « infodémie ». Enfin, selon une étude récente menée par la société Zignal Labs et relayée par le journal *The Washington Post*, la désinformation liée aux élections présidentielles américaines de novembre dernier aurait chuté de 73 % après que les comptes de Donald Trump ont été bloqués par Twitter, Facebook, Instagram, YouTube et d'autres réseaux sociaux. Face à la diffusion rapide et massive des fausses nouvelles *via* les réseaux sociaux, des mesures ont été adoptées au niveau européen. Les institutions de l'Union européenne ont ainsi mis en place un outil de *fact-checking*, les Décodeurs de l'Europe (qui apporte des réponses claires, simples et accessibles à de nombreux mythes et idées reçues sur l'Union européenne, son fonctionnement, et les politiques qu'elle mène), ainsi que des sites de lutte contre la désinformation en général (site du *Disinformation Hub*) et plus particulièrement celle liée au coronavirus. La Commission européenne a en outre publié, le 15 décembre 2020, le projet de règlement *Digital Services Act* (DSA) qui a vocation à instaurer un nouveau cadre de régulation pour mettre fin à l'irresponsabilité des opérateurs de plateformes. En France, la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information impose notamment en période de campagne électorale une obligation de transparence pour les plateformes (signalement des contenus sponsorisés en publiant le nom de leur auteur et le montant de la rémunération ; publication de leurs algorithmes, *etc.*).

C. – Associations, fondations et organisations non gouvernementales

53. – Les œuvres de charité. Au long du XIXe siècle, les œuvres de charité, pour une large majorité d'obédience religieuse, se voient concurrencées par des œuvres de bienfaisance financées par la nouvelle bourgeoisie. Ces œuvres nouvelles ne sont pas toutes progressistes et/ou laïques, mais cette inflexion deviendra majoritaire sur le long terme, du moins en Europe occidentale.

54. – D'emblée, ces associations s'installent sur des terrains régaliens. Louis XIV a créé les Invalides pour soigner les blessés de ses campagnes, et même si, plus tard sous le règne de Napoléon, le baron Dominique Larrey créa les premiers secours sur les champs de bataille, il a fallu attendre la création de la Croix Rouge (devenue l'*International Red Cross and Red Crescent Movement* [IRCRCM]) par Henry Dunant[(62)] pour qu'une organisation non gouvernementale (ONG) indépendante intervienne sur les terrains d'opération, sans parti pris concernant les belligérants.

Les ONG se distinguent par :

– l'intérêt public, humanitaire, social, sanitaire, écologique ou économique de leurs actions ;

– le but non lucratif de leurs actions ;

– l'indépendance politique ;

– l'indépendance financière.

D'abord de nature humanitaire intervenant principalement dans les domaines de la santé et du social, ces associations ont par la suite investi d'autres champs et

(62) Collectif, *Fondation et premières années du CICR (1863-1914)*, Suisse, mai 2010.

se sont étendues à l'international. Elles remplissent aujourd'hui deux rôles essentiels en se substituant à un retrait, une incapacité ou une abstention étatique (ou multiétatique) et en assurant le contrôle de défaillances étatiques (régulations) face à d'« autres pouvoirs » dans le « jeu des puissances ».

55. – **Aujourd'hui les grandes ONG sont intimement intégrées au « jeu des puissances ».** Leurs représentants sont des cibles au même titre que les militaires. Elles sont utilisées dans le débat politique. Elles interviennent parfois en lieu et place des États et sont même instrumentalisées par les entreprises[63].

D. – Sujet, citoyen, salarié, consommateur, individu…

56. – **Sujet du souverain et de ses vassaux, puis citoyen de l'État-nation, la personne a vu ses rattachements se multiplier.** D'abord soumis à la pression sociale à travers la religion et au lien de proximité au sein de la communauté du lieu de vie, les liens de la personne sont devenus de plus en plus hétérogènes. Ce mouvement s'est accéléré avec les transformations sociales et les déplacements de populations liés à la révolution industrielle et s'est encore amplifié par la suite avec l'accroissement du niveau d'éducation, puis la généralisation des médias. La notion d'individu, ses intérêts et ses passions remplacent peu à peu la notion de communauté. Et cet individualisme trouve dans l'Internet des réseaux le média parfaitement adapté à l'expression de sa singularité, jusqu'à menacer l'idée de communauté nationale au profit de la multiplication de communautés particulières.

IV. – Conclusion : la désagrégation de la souveraineté, une aubaine pour le « numérique »

57. – **La notion de souveraineté subit une rapide dilution, puis une désagrégation entre la fin de la Seconde Guerre mondiale et aujourd'hui.** Cette désagrégation n'est pas formelle : les États existent, les gouvernements existent, les frontières existent, les nations existent, mais seulement jusqu'à un certain point. *A priori*, ce point est celui de l'intersection de la dimension économique, de la puissance militaire et du poids démographique. Mais ce point est aussi contrebalancé par les puissances attenantes ou parties prenantes de chaque pays. Ce point peut devenir si infime (ce qui correspond à sa définition mathématique) que considérer la quasi-disparition de la souveraineté n'est plus un tabou. Les divers leviers régaliens, fondements de l'autorité, piliers de la nation, constituants du « vivre-ensemble » se dissolvent entre de multiples acteurs, aux agendas divers. La monnaie, la défense, l'énergie, l'éducation, la santé, l'espace, *etc.*, sont autant de domaines qui sont convoités par de nouvelles puissances.

Depuis plusieurs décennies, certains États, certaines entreprises, certains groupes d'intérêt et enfin des communautés de citoyens mobilisés autour d'une cause se permettent des actions qui parfois s'affranchissent du droit pour fracturer le « faire-nation » au

(63) A. Piquard, *Facebook réussit à réunir vingt membres pour sa « cour suprême » : Le Monde* 6 mai 2020 (www.lemonde.fr/economie/article/2020/05/06/facebook-reussit-a-reunir-vingt-membres-pour-sa-cour-supreme_6038898_3234.html).

profit d'intérêts particuliers. Seuls quelques ONG et États luttent encore pour un pluralisme et un multilatéralisme équilibré, notamment les grands pays européens.

58. – La question de la souveraineté numérique n'est pas une question de numérique, mais une question de souveraineté. Plus qu'un nouveau terrain diplomatique, le numérique est devenu un champ de bataille, à fleurets plus ou moins mouchetés. Parmi ces acteurs, les plus rapides, les plus puissants, les plus riches, ne pourraient-ils pas devenir des intervenants, si ce n'est des maîtres du « jeu des puissances » ?

L'avènement de l'ère numérique à partir des années 1980 (concomitante avec la désagrégation du régalien), d'abord porté par la généralisation des ordinateurs individuels puis par l'avènement des réseaux, offre à ces acteurs privés un univers déréglementé et ouvert à d'importants potentiels. Les industries du numérique que sont les fondeurs, les constructeurs informatiques et réseau, les éditeurs de logiciels, en passant par les prestataires de services digitaux, ont bénéficié d'une extraordinaire liberté d'action sur les champs régaliens. Ainsi l'« aspiration à la puissance » (*Verlangen nach Macht*)[64] fut vite remplacée par la « volonté de puissance » (*Wille zur Macht*)[65] des acteurs du numérique (GAFAM, BHATX…) ou des pays qui en font une arme (Chine, Russie, Israël, Iran, États-Unis, *etc.*), les uns utilisant parfois les autres dans leurs conquêtes. Cette « volonté de puissance » est d'autant plus remarquable qu'elle émane d'acteurs non étatiques aux moyens et aux ambitions sans mesure.

59. – Ce qui change avec le numérique, c'est la taille des acteurs et l'extrême agilité et rapidité de leur déploiement[66]**.** Les acteurs du numérique sont encore, pour certains, des industriels, mais ils sont avant tout devenus des aspirateurs à données. Ils aspirent au sens que Stephen Hawking donne aux singularités supermassives. Données personnelles, données d'usage, données d'entreprise et de collectivités dans le *cloud*, données de santé, e-mails, livres, presse, images et vidéo partagées et toutes autres données sont autant d'exemples des données traitées par ces géants. En plus de l'incroyable collecte d'informations qu'ils intègrent, ces opérateurs ont aussi la capacité de traiter ces informations pour les rendre actionnables et monétisables.

Ayant bien compris leurs avantages stratégiques, les géants du numérique ont initié des manœuvres de conquête agressives, visant la prise de pouvoir sur certains secteurs, sur certaines zones géographiques. Il suffit de parler avec la direction d'une banque systémique pour comprendre que Google[67], Apple[68] ou Tencent[69], seuls ou au travers de la prise de possession de *FinTech*, sont déjà les principaux

(64) F. Nietzsche, *Le Gai Savoir*, chez Ernst Schmeitzner, Chemnitz, 1882.
(65) F. Nietzsche, *Fragments posthumes*.
(66) J. Zanna, *Nasdaq 100 : Apple franchit le seuil des 2 000 milliards de dollars de capitalisation*, dailyfx.com, 2020 (www.dailyfx.com/francais/actualite_forex_trading/fondamentaux/alertes_de_marches/2020/08/20/Nasdaq-100-Apple-franchit-le-seuil-des-2-000-milliards-de-dollars-de-capitalisation.html).
(67) R. Shevlin, *Who Wants A Google Checking Account?*, New York, Forbes, 2020, https://www.forbes.com/sites/ronshevlin/2020/08/10/who-wants-google-to-be-their-bank.
(68) R. Bloch et S. Dumoulin, *Apple Pay achève de tisser sa toile en France : Les Échos* 28 janv. 2020 (www.lesechos.fr/finance-marches/banque-assurances/apple-pay-acheve-de-tisser-sa-toile-en-france-1166846).
(69) R. Gueugneau, E. Lederer et F. Schaeffer, *Le chinois Tencent poursuit son incursion dans la FinTech française : Les Échos* 21 janv. 2020 (www.lesechos.fr/finance-marches/banque-assurances/le-chinois-tencent-poursuit-son-incursion-dans-la-fintech-francaise-1164625).

concurrents du *Retail Banking*[70]. Plus insidieusement encore, ces sociétés se diversifient en ne proposant qu'une interface client et en s'appuyant sur les banques existantes pour fonctionner. Ainsi, en taxant chaque transaction, chaque opération, et en offrant des services que les banques ne peuvent ou n'ont pas le droit d'offrir, les géants du numérique se comportent en « parasites » sur les industries qu'ils investissent ; en détournant une part massive des bénéfices, sans payer l'ensemble des coûts et sans subir l'ensemble des risques et des réglementations afférents au secteur.

60. – **Les croisements différenciés des intérêts politiques et économiques.** Rares sont les États qui peuvent concurrencer ou garder sous contrôle les géants du numérique. Il s'opère donc une alliance de fait entre les pays les plus importants et leurs champions numériques. Pour les États de second rang la position devient défensive, au travers de la réglementation. Pour les autres, il n'y a guère d'autre solution que de subir, en dehors de la résurgence d'une forme de multilatéralisme.

Plus surprenant encore, alors que la confiance dans les États et la représentation politique s'effondre, celle envers les acteurs du numérique s'est longtemps maintenue. Cela est moins vrai aujourd'hui, notamment suite à l'affaire *Cambridge Analytica*. Il y a cependant une grande disparité de perception de cette confiance entre les continents et entre les pays vis-à-vis de chacune de ces entreprises (GAFAM, BHATX, *etc.*).

Reste à voir, plus en détail, les périls ou opportunités numériques, en France et en Europe, et comment les protéger ou les garantir alors que notre histoire a plutôt démontré nos défaillances en ce domaine. En attendant, poursuivons en arpentant l'espace numérique et ses singularités.

(70) R. Bloch, R. Gueugneau et E. Lederer, *Comment les banques européennes préparent la riposte face aux Gafa : Les Échos* 18 nov. 2019 (www.lesechos.fr/finance-marches/banque-assurances/face-aux-gafa-les-banques-europeennes-preparent-la-riposte-1148689).

CHAPITRE 2

L'ESPACE NUMÉRIQUE

61. – Le mythe de la virtualité. Le numérique n'est pas un espace « virtuel », c'est-à-dire, selon le dictionnaire, « qui n'existe pas ». Il n'est pas non plus un « autre » monde, qui serait différent et distinct du monde réel : les réseaux numériques sont le prolongement du monde réel ; ils « sont » ce monde. À la différence du monde physique, le tout un chacun ne possède pas le bon sens, le « sens commun » qu'il possède dans le monde naturel. Et pour cause : si nous héritons de repères culturels, historiques ancestraux qui s'ancrent dans le monde naturel, il en va différemment pour l'univers numérique, peuplé d'objets techniques dont le fonctionnement et les concepts sous-jacents n'ont pas été enseignés et restent l'apanage des experts et vendeurs de technologie ; ces derniers ne sont pas toujours exempts de velléités de domination, au moins économique, pouvant se prolonger par une suprématie politique au service d'une stratégie étatique. Avant d'examiner les singularités de cet espace numérique, commençons par l'arpenter en en découvrant sa géographie, tant d'un point de vue technique que fonctionnel.

SECTION 1

GÉOGRAPHIE : DESCRIPTION DE L'ESPACE NUMÉRIQUE

62. – L'« espace » numérique est le résultat de la mise en réseau des machines. Si le « numérique » est né avec l'apparition des premières machines informatiques, c'est le raccordement progressif entre elles qui a créé les premiers réseaux, dont l'ampleur et l'étendue croissantes ont fini par faire naître, dès les années 1980[1] et au début des années 1990[2], le sentiment qu'il existait un « cyberespace », prélude à « l'espace numérique ». Avec l'apparition puis le succès planétaire d'Internet, aux ramifications complexes, l'usage de ce concept s'est répandu pour désigner, *de facto*, ce « réseau de réseaux » dont, pourtant, il se distingue.

(1) W. Gibson, *Burning home : Omni* juill. 1982.
(2) P. Lévy, *L'intelligence collective : pour une anthropologie du cyberespace*, La Découverte, coll. « Poche », 1994.

63. – L'espace numérique est un concept plus large qu'Internet. Pouvant être défini succinctement comme le « réseau télématique international (...) résultant de l'interconnexion d'ordinateurs du monde entier utilisant un protocole commun d'échanges de données (IP pour Internet Protocol) »[3], Internet n'est pas un réseau ordinaire : c'est un réseau de réseaux, puisqu'il relie entre eux une multitude de réseaux privés (c'est-à-dire propres à chaque organisation). Néanmoins, Internet n'équivaut pas à la somme de tous les réseaux, car quantité d'entre eux ne sont pas reliés à Internet. Pour autant, à l'instar de l'Agence nationale de sécurité des systèmes d'information (ANSSI)[4], nous assimilerons, pour les besoins des développements ci-après, l'espace numérique (synonyme, pour nous, de « cyberespace ») au réseau Internet. Et, lorsque nous évoquerons « les réseaux », nous nous référerons indistinctement à Internet ainsi qu'à l'ensemble des réseaux qui y sont reliés.

64. – L'espace numérique est constitué de trois couches : matérielle, logicielle et informationnelle. Il est en effet devenu classique[5] de présenter l'espace numérique comme étant constitué :

– « d'une couche matérielle qui correspond à l'ensemble des appareils, serveurs, routeurs, ordinateurs qui permettent l'interconnexion des machines ;

– d'une couche logique ou logicielle qui couvre les éléments de communication entre les machines elles-mêmes, autrement dit les protocoles, ou bien entre les humains et les machines, c'est-à-dire les logiciels »[6] ; et,

– d'une « troisième couche, dite sémantique ou informationnelle » qui « correspond à l'ensemble des informations qui transitent au travers des deux premières ».

L'intérêt de cette présentation conceptuelle est de permettre d'appréhender facilement, de manière schématique, les différentes dimensions de l'espace numérique : son contenant (couches matérielle et logicielle) et son contenu (couche informationnelle).

65. – Construction humaine ne répondant à aucune organisation centralisée, l'espace numérique est difficile à comprendre et à décrire. Les voies de communication sont des constructions humaines ayant, dans les temps anciens, emprunté les voies naturelles (cours d'eau, vallées, *etc.*) puis édifiées sous la forme d'ouvrages artificiels (routes, ponts, péages, *etc.*) facilement perceptibles car visibles à l'œil nu. L'apparition des télécommunications modernes, avec notamment le téléphone, a apporté de la complexité, mais celle-ci a été atténuée par la construction, en France en tout cas, d'un réseau fortement encadré par l'État (ayant pris en gestion, notamment, le plan de numérotation nationale téléphonique à partir de 1879)[7] répondant, de ce fait, à une logique d'organisation centralisée lui

(3) Le Petit Larousse Illustré (2012), p. 583.
(4) L'ANSSI définit le « cyberespace » comme l'« espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques » (www.ssi.gouv.fr/entreprise/glossaire/c).
(5) F. Montauge et G. Longuet, Rapport fait au nom de la commission d'enquête sur la souveraineté numérique remis à M. le Président du Sénat le 1er octobre 2019, p. 17.
(6) Le rapport au Sénat du 1er octobre 2019 précise que les « deux premières couches forment l'organisation technique du cyberespace et définissent la manière dont les réseaux fonctionnent ».
(7) https://fr.wikipedia.org/wiki/Plan_de_num%C3%A9rotation_en_France.

conférant une intelligibilité. De ce fait, la perception de ces réseaux était aisée puisqu'il existait une ou des autorité(s) publique(s) associée(s) à leur conception et à leur édification : il s'agissait de réseaux organisés. L'arrivée d'Internet a marqué une rupture : ne répondant à aucune logique d'organisation centralisée (mais seulement à l'adoption de protocoles techniques)[8], ce « réseau de réseaux » s'est développé de manière tentaculaire, en répondant aux logiques – par essence multiples et hétérogènes – de tous ceux qui l'utilisent et l'exploitent. Ceci explique, d'une part, pourquoi il est probablement si difficile de décrire ce réseau et, d'autre part, pourquoi le chemin suivi par la donnée, sur ce réseau, est susceptible de varier. De ce fait, la vue schématique de l'espace numérique – que nous présenterons ci-après – ne prétend à aucune exhaustivité.

I. – Vue technique

66. – Débutons par un aperçu statique, décrivant les composants essentiels auxquels il faut faire appel pour communiquer dans le cyberespace, avant de tenter de retracer le chemin qu'y suit la donnée, dans une démarche dynamique.

A. – Aperçu statique

67. – **Les équipements terminaux des utilisateurs sont les frontières du numérique.** L'espace numérique est, tout d'abord, peuplé de la multitude des points de terminaison qui sont sous le contrôle des organisations ou des individus consommant des services sur les réseaux (« utilisateur[s] »). Aux premiers temps, il s'agissait essentiellement des ordinateurs individuels (fixes ou portables) reliés à Internet. L'informatisation du monde a été poussée à un tel degré qu'a ensuite été brouillée « la frontière entre l'ordinateur et les produits du quotidien »[9], aboutissant à un accroissement sans précédent du nombre et de la diversité de ces points de terminaison : serveurs, ordinateurs individuels, mais aussi tablettes numériques, smartphones (« ordiphones » en français) ou encore toute la variété d'objets du quotidien (montres, compteurs d'énergie, équipements électroménagers, *etc.*) qui acquièrent, par leur connexion à Internet, le statut « d'objets connectés ». Ce sont désormais tous ces équipements qui constituent les points de terminaison de l'espace numérique, c'est-à-dire ses frontières avec l'espace non numérique.

68. – **Les réseaux privés locaux des organisations (entreprises, administrations...) : du filaire au non-filaire.** Un réseau est dit « privé » lorsqu'il est utilisé par une organisation pour référencer et permettre la communication entre ses différents équipements, des adresses « privées » (c'est-à-dire qui sont définies uniquement localement et sont corrélées de l'indexation générale Internet).

(8) Si les réseaux numériques présentent de fortes disparités, l'histoire de l'Internet est cependant marquée par des protocoles d'échanges majeurs qui permettront une telle rapidité d'interconnexion et la mondialisation que l'on connaît. Pour ne citer que le protocole TCP-IP inventé en 1974 (V. Cerf et R. Kahn, *A Protocol for Packet Network Intercommunication*, IEEE, 1974, cs.princeton.edu) qui fut utilisé dès 1982 par le département de la Défense américain sur ses réseaux militaires puis par le réseau Arpanet à partir de 1983.

(9) I. Saleh, *Les enjeux et les défis de l'Internet des Objets* (IdO), 2017 (www.openscience.fr/IMG/pdf/iste_idov1n1_1.pdf).

Le développement des technologies de connexion sans fil (notamment le Wifi[10] et le Bluetooth[11]) a permis aux organisations (entreprises, administrations, *etc.*) de s'affranchir des contraintes d'un réseau filaire, pour relier des équipements de manière non filaire.

69. – Internet est un réseau de réseaux, improprement[12] nommé « réseau public », fonctionnant grâce à l'interconnexion. Constitué de la multitude de réseaux privés locaux répartis dans le monde entier, Internet permet à la donnée de circuler grâce aux infrastructures effectuant l'interconnexion de ces réseaux entre eux[13]. Ces infrastructures d'interconnexion sont privées, c'est-à-dire détenues et exploitées par des opérateurs qui sont aujourd'hui privés – même si certains (comme Orange par exemple) sont issus des vestiges d'anciens services publics.

70. – Le rôle essentiel des intermédiaires techniques. Parmi les intermédiaires techniques impliqués dans l'interconnexion, les FAI[14] et les hébergeurs, dont très peu sont situés en Europe, jouent un rôle essentiel. Dans les six catégories d'acteurs économiques appelés à intervenir dans l'interconnexion que recense l'ARCEP[15], nous nous arrêterons un instant sur les deux qui constituent les extrémités de la chaîne et qui, de ce fait, sont essentiels à l'exercice de la souveraineté sur l'espace numérique, ne serait-ce que par leur rôle incontournable lorsqu'il s'agit de faire cesser la diffusion d'un contenu illicite en ligne[16] : les FAI (au plus près des utilisateurs) et les hébergeurs (au plus près des fournisseurs de

(10) Terme suggérant *Wireless Fidelity*, par analogie aux termes *Hi-fi* pour *High Fidelity* (https://fr.wikipedia.org/wiki/Wi-Fi).

(11) Terme faisant référence à l'entreprise d'unification nationale du roi viking « Harald Blatand », se prononçant « Harald Bluetooth » (https://fr.wikipedia.org/wiki/Bluetooth).

(12) En réalité, l'adjectif « public » n'a jamais été aussi mal attribué qu'au réseau Internet : Internet est tout sauf « public », puisque ses infrastructures sont toutes « privées », c'est-à-dire appartenant à des opérateurs privés (et non à des États/personnes publiques).

(13) ARCEP, Baromètre de l'interconnexion de données en France, 2019. Ainsi que l'explique l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) : « l'interconnexion s'effectue entre différents AS (*Autonomous Systems*). Pour que l'information puisse être échangée d'un point à un autre de l'Internet, elle doit être acheminée d'AS en AS, et au sein de chaque AS, de routeur en routeur, le routeur étant l'équipement de base assurant l'aiguillage des paquets de données au sein de l'Internet. Pour ce faire, chaque AS annonce aux autres AS avec lesquels il est interconnecté physiquement les routes vers les équipements de réseau et utilisateurs finals qu'il dessert » (www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/interconnexion-de-donnees/barometre-de-linterconnexion-de-donnees-en-france.html).

(14) Fournisseur d'accès à Internet.

(15) Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. L'ARCEP recense ainsi les catégories suivantes d'acteurs (Baromètre de l'interconnexion de données en France, 27 juin 2019, p. 3) : « – les fournisseurs de contenu et d'applications (FCA) : les propriétaires du contenu, qui font appel à plusieurs intermédiaires pour acheminer leur contenu aux utilisateurs finals ;
– les hébergeurs : les propriétaires des serveurs hébergeant un contenu géré par des tiers (FCA ou individus) ;
– les transitaires : les gestionnaires des réseaux internationaux qui font office d'intermédiaires entre les FCA et les FAI pour acheminer le trafic ;
– les points d'échange Internet (IXP – *Internet Exchange Point*) : les infrastructures qui permettent aux différents acteurs de s'interconnecter directement, *via* un point d'échange, plutôt que par le biais d'un ou de plusieurs transitaires ;
– les réseaux de diffusion de contenu (CDN – *Content Delivery Network*) : les réseaux qui se spécialisent dans la livraison de volumes de trafic importants vers plusieurs FAI, dans des zones géographiques variées et grâce à des serveurs cache au plus proche des clients finals afin d'optimiser l'acheminement améliorant les performances et réduisant les coûts ;
– les fournisseurs d'accès Internet (FAI) : les opérateurs de réseaux qui sont chargés de livrer le trafic à l'utilisateur final ».

(16) Ainsi qu'en témoigne le pouvoir conféré à l'autorité judiciaire, par la loi n° 2004-575 du 21 juin 2004 (art. 6, I, 8), à l'encontre des hébergeurs et des FAI (V. M. Bourgeois, *Droit de la donnée – principes théoriques et approche pratique*, LexisNexis, 2017, n^{os} 1768 et s.).

services ou de contenus). L'ARCEP donne les exemples suivants d'entreprises et les catégories d'acteurs auxquelles elles appartiennent :

EXEMPLES D'ACTEURS D'INTERNET

FOURNISSEURS D'ACCÈS INTERNET (FAI)	RÉSEAUX DE DIFFUSION DE CONTENU (CDN)	POINTS D'ÉCHANGE INTERNET (IXP)	TRANSITAIRES	HÉBERGEURS	FOURNISSEURS DE CONTENU ET D'APPLICATIONS (FCA)
orange, SFR, free	CLOUDFLARE, maxcon, Limelight, Akamai	NL-IX, DE-CIX, Convergence hub	Level(3), cogent, Telia Carrier, NTT Communications	OVH.com, online, 1&1, koula	NETFLIX, skype, a, YouTube

Parmi ce panel, si les entreprises françaises semblent être bien représentées parmi les FAI, tel est moins le cas parmi les hébergeurs, OVH faisant face à des poids lourds étrangers, en grande partie américains.

71. – **Le nommage Internet est le sous-jacent indispensable à l'accessibilité des contenus pour le grand public.** Les machines sur lesquelles sont stockés les contenus (sites web, boîtes de messageries électroniques, *etc.*) sont accessibles grâce à l'adoption de protocoles, c'est-à-dire de règles définissant un langage, permettant à ces différentes machines d'acheminer les données au destinataire voulu par l'expéditeur. Parmi ces protocoles, le plus connu est dénommé « IP » (*Internet Protocol*) et correspond à un numéro d'identification attribué à chaque ressource matérielle (ordinateur, smartphone, objets connectés, *etc.*). Afin de faciliter l'accès aux ressources présentes sur le réseau, un mécanisme a été mis en place pour associer un nom à une adresse IP (jugée trop difficile à retenir). Ce nom, le « nom de domaine », est composé de deux niveaux :

– les domaines de « premier niveau », qui suivent immédiatement l'arobase, et peuvent faire référence soit à une zone géographique (« .fr » pour la France, « .bzh » pour la Bretagne, *etc.*), soit à une nature d'organisation ou d'activité (« .com » pour les organisations commerciales, « .org » pour les organismes à but non lucratif, ou plus récemment le « .radio » ou encore le « .bike » pour des activités de radio ou de cycle), soit enfin au nom d'une marque (comme le « .axa » ou le « .apple ») ;

– les domaines de « second niveau », qui correspondent à la suite de mots que réserve une personne ou une organisation ; concrètement, il s'agit de l'adresse d'un site web.

L'attribution et la gestion des noms de domaine de premier niveau sont assurées exclusivement par un organisme de droit privé à but non lucratif situé en Californie, l'*Internet Corporation for Assigned Names and Numbers* (ICANN), en français « la société pour l'attribution des noms de domaine et des numéros sur Internet »), en vertu d'un contrat conclu avec le département du commerce des États-Unis, qui a pris fin le 1er octobre 2016[17]. En application de ce contrat, l'ICANN avait également – et a conservé – pour mission **d'accréditer les offices d'enregistrement**

(17) www.nextinpact.com/news/101613-gouvernance-icann-semancipe-officiellement-controle-americain.htm.

(*registries*) en charge des noms de domaine « de second niveau », ainsi que de **désigner les organismes compétents en matière de litige** relatif aux noms de domaine. Les *registries* (offices d'enregistrement, par exemple l'AFNIC[18] pour le « .fr ») matérialisent leur accréditation par l'adhésion à une convention passée avec l'ICANN. Cette dernière reste, pour le moment, seule compétente pour décider de la création de nouvelles extensions, ce qui est sujet à controverse. Les *registrars* (bureaux d'enregistrement comme, par exemple, la société Gandi, ou encore la société Domainoo) sont quant à eux des prestataires qui ont seule compétence pour enregistrer un nom de domaine auprès d'un *registry* avec lequel ils passent, eux aussi, une convention d'accréditation (dénommée « contrat d'enregistrement »). Schématiquement, le système des noms de domaine obéit à une hiérarchie dont le sommet est appelé la « racine », que l'on représente par un point. Par exemple, dans le nom wikipedia.org, le « .org » correspond au domaine du premier niveau, et le « wikipedia » au domaine de deuxième niveau.

À ce jour, la racine est administrée depuis treize séries[19] de serveurs (dénommés « serveurs racine du DNS » [*Domain Name System*]) gérés sous l'autorité de l'ICANN[20]. Ces serveurs racine sont exploités par douze organisations, dont deux seulement sont établies en Europe[21], étant précisé qu'un grand nombre de ces serveurs correspond à plusieurs installations réparties dans des lieux géographiques divers[22].

B. – Aperçu dynamique

72. – Le cheminement à travers la « boucle locale »[23]. La donnée circule grâce à la connexion entre les terminaux et réseaux privés, d'une part, et le réseau public d'Internet, d'autre part. Cette connexion est réalisée par des intermédiaires techniques. Parmi ces intermédiaires, celui qui est en contact direct avec l'utilisateur est le « fournisseur d'accès à Internet » (FAI). Dans le détail, voici les principaux nœuds du réseau qui, localement, permettent cette circulation :

– la *box* (ou « passerelle domestique »), servant d'interface entre un FAI et un abonné haut débit à Internet (par ADSL, fibre ou câble) ; la donnée sort ainsi de l'équipement terminal de l'utilisateur (ordinateur, tablette numérique, *etc.*), vers la *box* précitée, sauf pour les utilisateurs disposant d'un abonnement leur permettant de se connecter en liaison directe par ondes (3G, 4G, *etc.*) ;

– les points de concentration (accueillant les liaisons individuelles qui viennent de chaque abonné) ;

(18) Association française pour le nommage Internet en coopération.

(19) Par « série », il faut entendre par là qu'il ne s'agit pas de treize serveurs racine du DNS, mais « plutôt de treize "identités de serveur" (…) ayant chacune une seule adresse IP assignée, elles sont communément référées comme étant les "serveurs racines" » (https://fr.wikipedia.org/wiki/Serveur_racine_du_DNS).

(20) https://fr.wikipedia.org/wiki/Serveur_racine_du_DNS.

(21) RIPE NCC, établie aux Pays-Bas, et NETLOD/AUTONIMICA, établie en Suède.

(22) Au 19 juillet 2019, il y aurait ainsi « plus de 997 sites dans 53 pays qui hébergent un serveur racine du DNS. En 2007, on comptait 130 sites » (https://fr.wikipedia.org/wiki/Serveur_racine_du_DNS).

(23) En France, où l'accès à Internet a historiquement emprunté les lignes téléphoniques, les premiers FAI ont été des opérateurs de téléphonie (Orange – ex-France Télécom –, SFR, Bouygues Télécom…), avant d'accueillir de nouveaux entrants (OVH, Nordnet…). Pour cette raison, en référence à l'expression utilisée au sujet des lignes téléphoniques, nous emploierons le terme de « boucle locale » pour désigner la partie du réseau Internet la plus proche de l'utilisateur.

– les sous-répartiteurs ;

– les nœuds de raccordement d'abonnés (NRA).

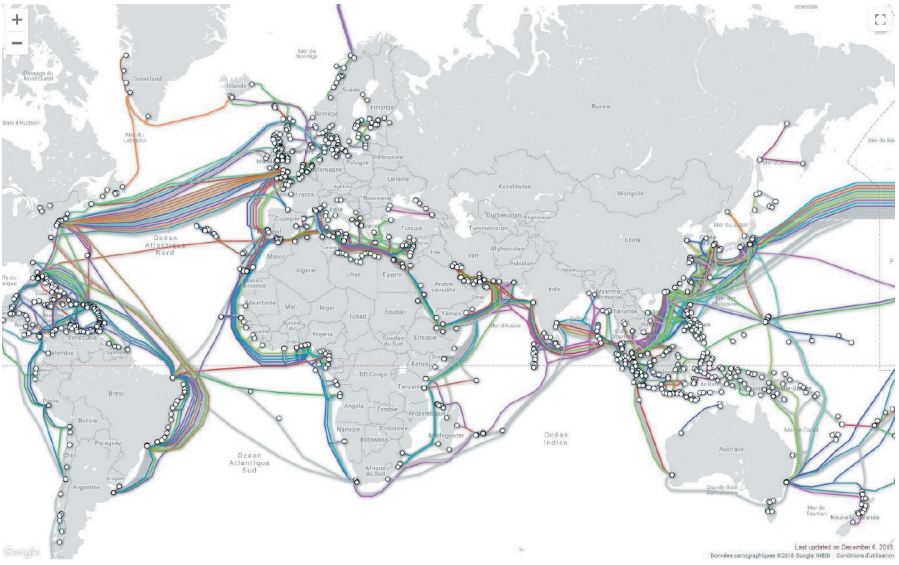
73. – **Le cheminement se poursuit à travers les liaisons nationales et internationales.** Sur ce réseau longue distance filaire (câbles terrestres et maritimes) et non filaire (satellites), interviennent :

– des entreprises propriétaires et exploitant des câbles, qui louent ces câbles auprès de ceux qui les utilisent ;

– le cas échéant, des opérateurs de transit « IP », qui fournissent le service de transport de données.

En France, Orange investit régulièrement dans les câbles sous-marins, notamment grâce aux navires câbliers de sa division, Orange Marine, qui déploient et assurent la maintenance de ses infrastructures à travers le globe. L'opérateur français a ainsi notamment participé à l'installation du *Sea-Me-We* 5 (*South East Asia-Middle East-Western Europe* 5), un câble de 20 000 km reliant le sud de la France à Singapour, en passant par la Turquie, l'Égypte ou encore l'Arabie saoudite(24).

Vue schématique des câbles sous-marins installés à travers le monde(25) :



74. – **La règle du meilleur nœud, et la variabilité incessante du chemin de la donnée dans l'espace numérique.** Sur Internet, les données sont propagées *via* les différents réseaux et nœuds précités, grâce au système d'adressage universel mis en place par l'ICANN ainsi qu'aux adresses IP. Les différents équipements constituant les nœuds du réseau orienteront la donnée sur le chemin le plus rapide possible, qui ne sera pas nécessairement le plus court géographiquement ; ainsi, si la circulation

(24) https://cartonumerique.blogspot.com/2018/04/les-cables-sous-marins-enjeu-majeur-de.html.

(25) www.01net.com/actualites/plongee-au-coeur-d-internet-cinq-chiffres-pour-tout-savoir-des-cables-sous-marins-1588422.html.

de la donnée se heurte à des ralentissements dus, par exemple, à un encombrement ou à un dysfonctionnement des équipements réseau sur le chemin géographiquement le plus court, alors il lui sera préféré un autre chemin qui peut être bien plus long en distance, mais pas en temps. Cet aiguillage s'opère en quelques fractions de seconde, de manière automatisée. Il est par conséquent très difficile à connaître et à anticiper. Cette caractéristique explique en partie la difficulté à percevoir le franchissement des frontières par la donnée, faisant naître le sentiment que le numérique efface la notion de territoires, alors que rien n'est plus faux.

II. – Vue fonctionnelle

75. – Après avoir arpenté la géographie « physique »[26] de l'espace numérique, nous allons désormais nous pencher sur sa géographie « humaine »[27], c'est-à-dire l'étude de l'activité humaine à travers cet espace numérique. Intéressons-nous aux objets puis aux acteurs de cet espace.

A. – Les objets

76. – **Les données sont le reflet, dans le numérique, des choses et des personnes.** Souvent définie comme « une description élémentaire d'une réalité »[28], la donnée correspond à la représentation du réel dans une forme perceptible par des agents, en l'occurrence les parties prenantes d'un réseau numérique, que sont les machines et leurs utilisateurs (d'un bout à l'autre du réseau : de l'expéditeur au destinataire de la donnée). Malgré l'existence de divergences sur la nature et l'étendue de son contenu, nous retiendrons que la donnée est toujours porteuse d'une signification à des degrés divers[29] et qu'en outre, sur les réseaux numériques, le terme « données » désigne aussi bien des données brutes (au « signifiant » très élémentaire) que des données plus riches (notamment contextualisées) et même des œuvres de l'esprit (textes, images, vidéos). C'est à ce vaste ensemble de signes que nous nous référerons pour désigner la « donnée », constituant la substance de la couche « informationnelle » (dite aussi « sémantique » ou « cognitive ») de l'espace numérique. Or, ces données ne sauraient exister sans l'objet auquel elles se rattachent : une personne (auquel cas on parlera de données « à caractère personnel », comme par exemple les données de géolocalisation d'un smartphone d'une personne) ou d'une chose (comme, par exemple, les données constituées de références techniques de produits, ou encore de mesures météorologiques dans une région). Il existe ainsi un lien indissoluble entre la donnée et son objet car, sans lui, elle n'existerait pas : elle en constitue, en quelque sorte, sa représentation dans l'univers numérique. Sur le plan juridique, cette approche permet d'envisager un lien d'accessoire à principal, entre la donnée et la chose ou la personne à laquelle elle se rapporte,

(26) Selon un parallèle que nous prenons avec la science géographique, la vue technique de l'espace numérique consiste, selon notre démarche, à étudier les composants et phénomènes techniques qui constituent les réseaux numériques et y surviennent (V. *supra*, n[os] 66 et s., « Vue technique »).
(27) Branche de la géographie qui consiste en l'étude spatiale des activités humaines.
(28) S. Abiteboul et V. Peugeot, *Terra Data : qu'allons-nous faire des données numériques ?*, éd. Le Pommier, 2017.
(29) Mais il s'agit là d'une différence de degré, et non de nature.

autorisant, lorsque nécessaire[30], le recours à la règle de l'accessoire (« l'accessoire suit le principal »), et faisant ainsi suivre à la donnée le même régime juridique que celui applicable à son objet[31]. Ainsi perçues, les données constituent donc le reflet, dans l'espace numérique, des choses et des personnes présentes sur un territoire. Cette approche permet de percevoir sans difficulté le lien qui existe entre les données et l'exercice de la souveraineté : cette dernière, qui s'exerce sur une population et un territoire, n'a aucune raison de se limiter à l'espace non numérique.

77. – **Les moyens de traitement permettent l'extraction et l'analyse des données.** Les moyens de traitement désignent l'ensemble des outils permettant aux acteurs de l'espace numérique de collecter puis, dans certains cas, d'étudier de grandes quantités de données afin d'en tirer toute la valeur informationnelle possible, pour ensuite l'exploiter, ou bien la revendre, sous diverses formes, à des tiers. L'univers numérique est ainsi devenu un espace d'échange, donnant naissance à une véritable économie de la donnée, autrement dit un commerce de l'information. À l'image du monde industriel qui a permis aux propriétaires de moyens de production physiques (machines-outils, usines, *etc.*) d'asservir économiquement les ressources matérielles et humaines pour la production de biens et de services, l'économie dans l'espace numérique appartient à ceux qui détiennent les infrastructures – matérielles et logicielles – permettant d'extraire et de traiter les données.

B. – Les acteurs

78. – **Tentative de classification des acteurs en plusieurs catégories.** Dans l'espace numérique, au vu de la confusion qui règne et dont les symptômes se font sentir jusque dans le vocabulaire employé (peuplé d'anglicismes et d'hyperonymes[32]), l'utilité de l'exercice apparaît évidente. D'emblée, il paraît possible de distinguer ceux qui fournissent des produits ou services numériques de ceux qui utilisent ces produits/services et, enfin, de ceux qui régulent ces derniers. **La première catégorie** comprendra tous ceux (concepteurs, fabricants/développeurs, distributeurs, *etc.*) qui jouent un rôle dans la création et la mise en circulation de produits de la couche matérielle ou logicielle de l'espace numérique ; il faudra y inclure également les fournisseurs de services liés à ces produits (comme par exemple les experts en recherche et analyse de vulnérabilités informatiques), mais en exclure les prestataires de services qui, bien qu'exécutant tout ou partie de leur mission sur l'espace numérique, existaient avant et indépendamment du numérique (tels les experts en intelligence économique). Appartiennent à **la deuxième catégorie** les organisations et individus qui, à titre professionnel ou privé, utilisent tout ou partie des produits/services numériques. Enfin, appartiennent à **la troisième catégorie** les États mais aussi les organisations non étatiques qui émettent des normes juridiques et/ou techniques, applicables à l'espace numérique.

(30) C'est-à-dire en cas de vide juridique apparent, autrement dit en l'absence de texte spécial.
(31) M. Bourgeois et L. Thibierge, *Droit de la donnée : plaidoyer pour un régime général : JCP* E 21 mai 2020, n° 21-22, p. 22.
(32) Terme dont le sens est plus large que celui pour lequel il est employé. Par exemple, l'emploi du terme « bâtiment » au lieu de « maison ». Dans l'univers numérique, il est fréquent d'employer des hyperonymes – parfois en choisissant un terme qui, en plus d'être imprécis, se révèle faux –, le plus souvent par ignorance du terme adéquat.

79. – Classer les acteurs par catégorie permet de mieux comprendre l'écosystème et d'améliorer sa régulation. L'ébauche de classification précédente ne présente pas d'intérêt tant qu'elle reste aussi sommaire. L'exercice pourrait en revanche se montrer très utile à poursuivre, s'il servait des objectifs d'intérêt général : ainsi, si, parmi la première catégorie, il était possible de regrouper certains acteurs présentant des caractéristiques communes et sur qui reposerait l'équilibre du cyberespace (en termes de confiance et de fiabilité technique, notamment), alors on pourrait songer à créer de nouvelles professions réglementées (comme des commissaires à la donnée, des auditeurs d'IA, *etc.*), mieux connues et enseignées au grand public – ce qui passe notamment par des titres compréhensibles et francisés –, à l'image des professions du droit et du chiffre qui ont accompagné la naissance de la France moderne tout au long du XIX^e^ siècle. La deuxième catégorie nécessiterait certainement d'opérer des distinctions sectorielles afin d'identifier des catégories d'utilisateurs devant répondre à des obligations plus fortes que les autres, en raison de l'exposition accrue de leurs activités aux risques numériques (cyberattaques) : c'est la démarche suivie en France avec le statut des « opérateurs d'importance vitale » (OIV)[33] et des « opérateurs de services essentiels » (OSE)[34]. La troisième catégorie permettrait de constater que les États sont désormais directement concurrencés, dans l'espace numérique, sur certaines de leurs prérogatives régaliennes, et pourrait ainsi s'organiser pour réagir. Selon nous, un travail de recensement et de classement des acteurs serait aussi très utile au législateur qui a souvent du mal à appréhender l'espace numérique, et dont la qualité inégale des textes est le reflet.

80. – La plateforme est un acteur insolite et incontournable de l'espace numérique. En partant de l'étymologie, il est possible de voir des références dans le terme « plateforme » : tout d'abord, un lieu stable (car plat) propice à accueillir des matériaux (construction), des marchandises (transports), des idées (« plateforme syndicale »), ou encore des agents économiques désireux de procéder à des échanges (bourse) ; enfin, une structure utilisée pour extraire des ressources (plateformes pétrolières, minières, *etc.*). Ces références conviennent tout à fait à ce que la pratique appelle communément « plateforme numérique », sans que le terme ne fasse l'objet d'une réelle définition précise. Ainsi, les géants du web[35] :

– ont, pour la plupart, organisé un lieu d'échanges qui confère à leur modèle économique un caractère multiface[36] ; et,

(33) C. défense, art. R. 1332-1 et s.

(34) L. n° 2018-133, 26 févr. 2018, qui a transposé la directive (UE) 2016/1148 du 6 juillet 2016 destinée à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite « NIS » (*National Information Security*).

(35) Que sont notamment Google, Amazon, Facebook, Apple, Microsoft (les « GAFAM »), mais aussi Netflix, Airbnb, Tesla et Uber (les « NATU »), ainsi que leurs homologues asiatiques Baidu, Huawei, Alibaba, Tencent et Xiaomi (les « BHATX »).

(36) La face visible (celle de la vente – ou de la fourniture gratuite – du service numérique) et la face non visible (par les utilisateurs) de la réutilisation de ces données. De la sorte, la rémunération de ce type d'acteurs aura deux sources :
– la vente rémunérée directement par l'utilisateur (qui peut ne donner lieu à aucun paiement dans certains cas – comme, par exemple, les services gratuits proposés par Google ou encore Facebook) ;
– et l'exploitation des données collectées gratuitement auprès d'utilisateurs, ensuite (re)monétisées sur le vaste marché de la donnée.

– en toute hypothèse, ont tous intégré à leur activité un processus d'extraction systématique des données de leurs utilisateurs.

L'importance jouée par ces plateformes, au vu de leur poids économique et de leur situation quasi monopolistique, milite en faveur d'un régime spécial, à l'image de celui qui a été imposé, au sortir de la Seconde Guerre mondiale, aux banques dont le trop faible encadrement les avait rendues inaptes à jouer un rôle énergique qui aurait pu endiguer la grande crise économique des années 1930. Pour ce faire, il faut tâcher de mieux comprendre les caractéristiques de ces plateformes. Il apparaît alors pertinent de citer les cinq catégories de plateformes que distingue le spécialiste reconnu de l'économie numérique Nick Srnicek[37] :

– la « plateforme publicitaire » : comme Google et Facebook, elle fournit des services apparemment gratuits en extrayant de l'information sur ses utilisateurs afin de la revendre notamment à des annonceurs publicitaires ;

– la « plateforme nuagique » : comme Amazon, elle met « en place l'infrastructure fondamentale, (…) de façon à la louer à d'autres pour en tirer des profits tout en collectant des données pour son propre usage »[38] ;

– la « plateforme industrielle » : comme la plateforme « Mind-Sphere » développée par Siemens, elle permet de superposer au procédé de production industrielle un processus de production de données ;

– la « plateforme de produits » : comme celle mise en place par Rolls-Royce, fabricant de moteurs aéronautiques, intégrant des capteurs dans ses produits qui seront ensuite commercialisés sous la forme d'abonnements, à l'image du modèle *as a service* de certains éditeurs de logiciels ;

– la « plateforme allégée » : comme Uber ou Airbnb, elle fonctionne « selon un modèle d'hyper-externalisation, dans lequel les travailleurs, le capital fixe, les coûts d'entretien et la formation sont tous confiés à des sous-traitants », et ne conserve « que le minimum nécessaire à l'extraction » de données qui leur « permettent de percevoir une rente de monopole »[39].

L'auteur met en garde contre la nature hégémonique des plateformes[40], et souligne leur mainmise sur les données : « loin d'être de simples propriétaires de l'information, ces firmes deviennent peu à peu propriétaires de l'infrastructure même de la société ».

Ainsi, il apparaît clairement que la soumission effective des plateformes aux prérogatives régaliennes est un enjeu essentiel de souveraineté. Celle-ci n'aura pas lieu spontanément et impliquera vraisemblablement l'usage d'une contrainte réglementaire (coercitive ou incitative), qui devra être soigneusement préparée par un travail de formalisation d'une vision claire et puissante sur la donnée et le numérique, guidée par l'intérêt général : les bénéfices que l'on considère essentiels à

Ce modèle offre la possibilité de baisser le prix du service – voire de l'offrir –, puisqu'une autre source prend le relais (la donnée) et permet en outre de rendre « captif » le consommateur dans certains cas, notamment pour des services qui finissent par devenir essentiels ou addictifs, comme ceux fournis par les moteurs de recherche ou les réseaux sociaux.

(37) N. Srnicek, *Capitalisme de plateforme – l'hégémonie de l'économie numérique*, Lux, Cambridge, 2017.

(38) N. Srnicek, *Capitalisme de plateforme – l'hégémonie de l'économie numérique*, préc., p. 69.

(39) N. Srnicek, *Capitalisme de plateforme – l'hégémonie de l'économie numérique*, préc., p. 81.

(40) N. Srnicek, *Capitalisme de plateforme – l'hégémonie de l'économie numérique*, préc., p. 97 : « Loin d'être de simples propriétaires de l'information, ces firmes deviennent peu à peu propriétaires de l'infrastructure même de la société ».

obtenir sur l'espace numérique, et les risques que l'on refuse de faire courir à l'humanité sur cet espace. Le tout débouchant sur des droits et des devoirs pour tous les acteurs, avec un statut « à part » pour les plateformes au vu de leur singularité et de leur puissance, dont il faut contenir les méfaits possibles et stimuler les bienfaits indiscutables.

SECTION 2

LES SINGULARITÉS DU NUMÉRIQUE

81. – Si le monde numérique présente des liens de parenté avec le monde réel, il n'en garde pas moins certaines singularités. La description de l'espace numérique nous aura montré que celui-ci recueille les réalités du monde qui, sous la forme de données exprimées en langage binaire, se sont transportées dans les réseaux. Contrairement à une croyance répandue, les données circulant sur le cyberespace entretiennent avec la réalité un lien et des ressemblances indéniables. Néanmoins, l'espace numérique présente certaines singularités qui le distinguent du monde non numérique : s'y intéresser est essentiel si l'on veut ensuite transposer, comme nous le ferons, les concepts de souveraineté traditionnelle au cyberespace. Nous examinerons trois singularités (ne prétendant, à ce sujet, à aucune exhaustivité) : la puissance exponentielle des machines, le caractère non rival des données et l'effet réseau.

I. – La puissance exponentielle des machines et le rythme effréné de l'innovation qui s'ensuit

82. – À la différence des autres réseaux, les réseaux numériques ne semblent pas en proie à la saturation. Les réseaux ferroviaires, routiers et électriques sont depuis de nombreuses années stables, et pour certains d'entre eux nettement saturés au vu de l'accroissement constant de la consommation de ces services. Ces révolutions successives ont toutes mis quelques décennies pour parvenir à maturité. Même s'il est peut-être encore trop tôt pour conclure sur le numérique, il est un fait qu'Internet voit son volume de données croître indéfiniment depuis sa création et les machines voient aussi leur capacité de traitement croître constamment.

83. – Les nanotechnologies font naître de nouvelles perspectives. Selon la loi de Moore : « La puissance des machines doublera tous les deux ans »[(41)]. Si cette loi empirique prononcée en 1965 par Gordon E. Moore s'est vue incroyablement vérifiée durant presque cinquante ans, elle se heurte aujourd'hui aux limites de la physique, certaines parties des composants de base ne possédant désormais plus que quelques atomes. En effet, la prochaine voie dans l'augmentation de la capacité

(41) E. Gordon Moore, *Cramming More Components Onto Integrated Circuits*, Electronics, 1965, vol. 38 : la durée fut corrigée rapidement à tous les dix-huit mois et se vérifie moins depuis 2014 même si la croissance se maintient.

de calcul réside désormais dans la nano-informatique en général et le calcul quantique en particulier. Le binaire laisserait ainsi la place au qbit (superposition d'états 0 et/ou 1) qui permet de traiter davantage d'opérations élémentaires en un temps record. Étant donné la complexité du processus inhérent aux machines quantiques, il paraît raisonnable d'imaginer des premières solutions de type QAAS (*Quantique as a service*). L'impact du calcul quantique sur les capacités de traitement, dans le domaine du décryptage typiquement, ne laisse guère de doute sur l'intérêt évident que les États auront à maîtriser cette technologie pour préserver leur souveraineté.

84. – L'expansion infinie de la puissance de calcul représente un véritable défi écologique. L'humanité, avec la multiplication des capteurs de données (du smartphone à l'objet connecté), produit toujours davantage de données. Dans ce contexte, le réseau Internet semble s'inscrire dans une expansion infinie qui pousse les machines à se perfectionner et les serveurs à stocker toujours davantage de données. Cela étant, les problématiques de consommation énergétique qui vont avec cet accroissement de puissance participent significativement au réchauffement climatique et font émerger un fort besoin de recherche de technologies plus vertes.

II. – Le caractère non rival de la donnée

85. – Selon le concept économique de la non-rivalité, le régime général de la propriété ne peut s'appliquer aux informations. Notion issue des réflexions économiques, la « rivalité » correspond à la propriété physique d'un bien ne pouvant pas être utilisé simultanément par plusieurs personnes, à l'inverse d'un bien « non rival » pouvant être utilisé par plusieurs personnes en même temps[(42)]. La plupart des biens corporels sont dits « rivaux » (produits alimentaires, vêtements…), car leur matérialité vient s'opposer à une consommation simultanée par plusieurs agents économiques[(43)]. Au contraire, les biens incorporels sont traditionnellement présentés comme « non rivaux » car ils peuvent être consommés en même temps par plusieurs agents. Cette distinction a, de toute évidence, influencé le législateur lorsqu'il a édicté les fondements de la propriété intellectuelle en s'attachant à prévoir des monopoles limités par des critères stricts et en dehors desquels le régime de liberté du commerce et d'industrie retrouvait son empire. Ainsi, les informations (synonymes – pour nous – de « données ») sont exclues du champ de la propriété privée (« les idées sont de libre parcours »)[(44)], sauf si elles remplissent les conditions strictes de l'un des monopoles institués par la loi (brevet, marque, dessins et modèles, droits d'auteur…). Prenant néanmoins conscience de l'importance croissante des dépenses réalisées par certains acteurs pour rassembler de vastes quantités de données, le législateur a instauré, à la fin des années 1990[(45)], un monopole limité pour les producteurs de bases de données. Toutefois, cette protection,

(42) *Dictionnaire des biens communs*, ss dir. M. Cornu, F. Orsi et J. Roshfeld, PUF, 2017, p. 89.
(43) Excepté pour certaines infrastructures, telles que les routes ou les transports en commun qui admettent plusieurs usagers en même temps dans certaines limites (jusqu'à saturation).
(44) H. Desbois, *Le droit d'auteur en France*. Dalloz, 3e éd., 1978, p. 22.
(45) L. n° 98-536, 1er juill. 1998 transposant la directive (CE) 96-9 du 11 mars 1996 « concernant la protection juridique des bases de données ».

soumise au critère de « l'investissement substantiel »[46], n'infléchit pas le principe qui reste celui de la réutilisation de l'information qui n'est entravée par aucun droit – de propriété, ou autre – à portée générale. D'ailleurs, jusqu'à un passé récent[47], la jurisprudence refusait d'appliquer la qualification de « vol » pour des actes non autorisés d'extraction des données, considérant implicitement qu'à la différence d'un bien corporel (dont la soustraction le fait disparaître des mains de son propriétaire), l'accès et la captation illégitimes d'un contenu informationnel ne déposèdent pas son détenteur initial[48]. Cette position, critiquable[49], a été récemment abandonnée[50], ce qui montre que la non-rivalité « en fait » des données n'aboutit pas nécessairement à un laisser-faire « en droit » sur celles-ci ; car le droit n'a pas pour fonction d'épouser systématiquement la réalité, mais plutôt de traduire des choix de société[51].

86. – Tirant parti de cette situation, les détenteurs de moyens de traitement (en particulier les plateformes) ont pu collecter librement d'immenses quantités de données, dont le caractère non rival leur a ensuite offert un champ des possibles à peu près illimité. La nature non rivale des données a conféré aux plateformes numériques un potentiel immense en raison de la multiplicité d'usages auxquels se prêtent les données numériques. Ainsi, il est facile d'imaginer, par exemple, un fournisseur d'une solution SaaS[52] de gestion de ressources humaines, *leader* sur son marché, se lancer aisément dans de nouveaux services, comme la production d'études sur les tendances en matière d'emploi, à partir des vastes quantités de données RH qu'il héberge[53], tout en poursuivant son activité première : ceci grâce à la non-rivalité – autrement dit à l'ubiquité – des données, leur permettant d'être utilisées à plusieurs fins en même temps. Cette singularité, source d'une grande puissance pour les opérateurs extrayant et exploitant massivement des données, peut mettre ces derniers en position de concurrencer la puissance d'État sur certaines prérogatives régaliennes (comme la santé ou l'éducation).

(46) Preuve que doit rapporter le producteur souhaitant bénéficier de cette protection.
(47) Jusqu'au célèbre arrêt *Bluetouff* (Cass. crim., 20 mai 2015, n° 14-81.336).
(48) Sauf si le voleur détruit les données lors de la soustraction, ce qui n'est pas toujours le cas.
(49) On peut en effet considérer que « si le détenteur de données numériques ne se trouve pas toujours dépossédé de ses données par un acte d'extraction frauduleux, il n'en demeure pas moins que la valeur de ses données (qui résulte souvent du caractère exclusif dont jouit son détenteur légitime, qui les conserve secrètes) se trouve obérée par l'acte frauduleux du tiers, qui fait perdre au détenteur l'exclusivité qu'il avait auparavant : s'il n'y a pas "soustraction" des données, il y a bien soustraction de leur valeur, et c'est précisément ce que doit protéger le droit pénal » (M. Bourgeois, *Droit de la donnée – principes théoriques et approche pratique*. LexisNexis, 2017, n° 1801, p. 424).
(50) Arrêt *Bluetouff* (Cass. crim., 20 mai 2015, n° 14-81.336) ; V. égal. Cass. crim., 28 juin 2017, n° 17-81.113.
(51) Ainsi, à titre d'exemple, s'il est possible à un intrus de s'introduire dans un domicile mal sécurisé, une telle action (à l'aide de manœuvres, menaces, voies de fait ou contrainte) n'en constitue pas moins une violation de domicile punie par l'article 226-4 du Code pénal.
(52) Pour *Software as a Service*, l'acronyme SaaS désigne un type de service consistant en la mise à disposition d'un (ou d'un catalogue de) logiciel(s) applicatif(s) destiné(s) à une population de clients utilisateurs. Appartiennent à cette catégorie des suites bureautiques comme « Google Apps » ou « Office 365 », les applications CRM de SalesForce, les services de vente en ligne d'Amazon (Rapport CIGREF 2012-2013 – « Fondamentaux du *Cloud Computing* – le point de vue des grandes entreprises », p. 14, https://images.cigref.fr/Publication/2012-2013-Fondamentaux-Cloud-Computing-Point-de-vue-grandes-entreprises.pdf).
(53) À condition que le fournisseur ait pris soin de s'y faire autoriser dans les contrats signés avec ses clients (à défaut de quoi, il y aurait infraction à la réglementation protégeant les données à caractère personnel – notamment pour détournement de finalité, incriminé par l'article 226-21 du Code pénal).

III. – L'effet réseau

87. – L'effet réseau est une menace pour la libre concurrence, et pour la souveraineté économique. L'effet réseau désigne le phénomène par lequel l'utilité d'un produit ou service est fonction de la quantité de ses utilisateurs. Cet effet peut être négatif, comme pour des infrastructures routières rendues inefficaces en raison de leur saturation, ou bien positif, comme pour un réseau téléphonique dont le nombre d'utilisateurs accroît l'utilité de ce réseau pour chacun d'eux. Nous pouvons citer deux exemples emblématiques dans les technologies numériques de cet effet réseau : la suite bureautique Microsoft, et le réseau social Facebook. En imposant dans les années 1980, puis 1990, une suite bureautique adoptée par une écrasante majorité d'organisations (entreprises, administrations…), le groupe américain Microsoft a pu, ensuite, acquérir une véritable suprématie sur le marché grâce au vaste réseau d'utilisateurs ayant adopté ses logiciels. Cette situation poussait mécaniquement les débutants à privilégier leur apprentissage d'outils bureautiques sur les produits Microsoft, plutôt que sur leurs concurrents, par souci d'efficacité au vu de la taille du parc installé. De la même manière, le succès du réseau social Facebook, au milieu des années 2000, a été conforté – se trouve encore aujourd'hui sans cesse conforté – par le nombre sans cesse croissant de ses utilisateurs et les vastes quantités de contenus en tous genres que ces derniers y mettent en ligne. Un nouvel entrant aura ainsi clairement intérêt à s'inscrire sur ce réseau social plutôt que sur un autre à moindre audience sur lequel il aura moins de probabilités de pouvoir retrouver des proches. Ce n'est pas un hasard si les géants du numérique les plus emblématiques (Facebook, Google, Amazon…) ont pu conquérir, en quelques décennies seulement – parfois même quelques années – des parts de marché qui confinent au monopole : tous ont pour point commun d'avoir bénéficié (de continuer à le faire) d'un effet réseau évident. Le rôle de la donnée y est central, ne serait-ce que parce que celle-ci enrichit sans cesse l'offre de services de l'opérateur qui les détient : le réseau social Facebook est sans cesse plus séduisant à mesure que de nouveaux utilisateurs s'inscrivent et y déposent des textes/images ; le moteur de recherche Google est sans cesse plus performant à mesure que son nombre d'utilisateurs et d'annonceurs croît ; la plateforme de vente en ligne Amazon est sans cesse plus attractive pour les acheteurs à mesure qu'elle compte de nouveaux vendeurs… Or, les entorses commises au droit de la concurrence par ces acteurs sont multiples et de plus en plus fréquentes (comme, par exemple, l'influence anticoncurrentielle des résultats de Google constatée par la Commission européenne en 2017)[(54)]. Le rapport fait au Sénat le 1er octobre 2019 « sur la souveraineté numérique » identifie clairement « les effets de réseau et les rendements d'échelle » comme les deux facteurs qui poussent à la concentration les plateformes numériques, en relevant la formule – bien connue dans l'univers numérique – « le gagnant prend tout »[(55)].

(54) Le placement et l'affichage plus favorables réservés par Google, dans ses pages de résultats de recherche générale, à son propre service de comparaison de prix par rapport aux services de comparaison de prix concurrents constituent un abus de position dominante (Commission européenne, 27 juin 2017, aff. *Google Search [Shopping]* AT.39740).

(55) Rapport remis au président du Sénat le 1er octobre 2019, au nom de la Commission d'enquête sur la souveraineté numérique, t. I, p. 30 à 32.

Ce même rapport préconise de renforcer substantiellement le droit de la concurrence, notamment en y ajoutant un cadre général préventif de régulation pour les acteurs dits « systémiques » (c'est-à-dire disposant d'effets de réseaux massifs, maîtrisant un volume considérable de données non réplicables, étant en situation incontournable sur un marché multiface, disposant d'informations asymétriques, pouvant influer sur des pans sensibles du lien social…)[56].

(56) Rapport remis au président du Sénat le 1er octobre 2019, au nom de la Commission d'enquête sur la souveraineté numérique, t. I, p. 47.

DEUXIÈME PARTIE

RÉFLEXION

CHAPITRE 1

LA SOUVERAINETÉ APPLIQUÉE À L'ESPACE NUMÉRIQUE

SECTION 1

L'OBJET DE LA SOUVERAINETÉ NUMÉRIQUE

88. – Éléments constitutifs et modalités d'exercice. S'agit-il d'une ligne Maginot virtuelle qui relèverait d'une certaine utopie défensive ? Est-ce la simple transposition numérique de processus, d'objets existant dans le monde « physique » ? Ou encore, un ensemble de notions nouvelles ? Afin de répondre à ces questions, il faut tout d'abord identifier les éléments constitutifs de la notion de souveraineté numérique pour en comprendre les modalités d'exercice tant sur les plans civil que militaire.

I. – Les éléments constitutifs

89. – La souveraineté numérique : la transposition des attributs de la souveraineté traditionnelle dans l'espace numérique et la technologie, mais pas seulement. Depuis l'émergence de l'informatique et d'Internet en particulier, la plupart des activités humaines se « numérisent », c'est-à-dire sont transposées dans le monde numérique, y compris les missions régaliennes. Dans ce monde, « l'homme est moins un citoyen et un sujet de droit, mais de plus en plus une somme de données à exploiter » d'après le rapport du Sénat[1], et les attributs de la souveraineté d'un État – à savoir la capacité de celui-ci à assurer son autonomie et la protection des citoyens qui le composent – nécessitent d'être redéfinis. Aussi, nous proposons-nous, dans ce chapitre, de définir, par analogie avec la vie « réelle », les attributs de cette souveraineté numérique.

90. – La population. Dans le monde numérique, la notion de population peut être caractérisée par l'ensemble de données, des « traces numériques » que chaque

(1) « L'homme est moins un citoyen et un sujet de droit, mais de plus en plus une somme de données à exploiter », Rapport du Sénat sur la souveraineté numérique (www.senat.fr/rap/r19-007-1/r19-007-11.pdf).

citoyen génère et qui permet de les identifier ou de les caractériser. Aujourd'hui, tout être humain produit près de deux mégaoctets de données par seconde[2]. Le stockage et l'exploitation de ces données autorisent une connaissance fine, voire une plongée dans l'intimité des citoyens. Alors qu'une part infime de ces données est connue et stockée par les États, les acteurs privés qui les gèrent en masse disposent dorénavant d'une meilleure connaissance de la population que les États eux-mêmes. Le recensement et la gestion de l'état civil des citoyens demeurent une prérogative étatique ; toutefois, on peut considérer aujourd'hui qu'ils ne sont plus l'apanage unique des États. Ainsi l'administration des identités (édition des pièces d'identité de l'état civil, capacité à identifier formellement un individu), responsabilité historique des États, est aussi de nos jours gérée dans l'univers numérique par un grand nombre d'acteurs privés, notamment les GAFAM qui fournissent l'accès aux services sur Internet. Ils disposent même d'un droit de contrôle, d'usage et de supervision sur une grande part de l'activité numérique des citoyens.

91. – **Territoires et frontières numériques : l'accès aux données.** Dans un monde où la vitesse des communications réduit les distances, la territorialité physique n'existe pas. Le citoyen dispose d'un accès immédiat à des services, à des données et à d'autres personnes à l'échelle mondiale pendant que les données qu'il génère sont stockées dans des infrastructures informatiques sur l'ensemble de la planète. Dans ce contexte, la « frontière » numérique peut être définie comme la capacité de contrôle et de gestion des accès aux données : le chiffrement[3] des données garantissant que celles-ci ne sont accessibles qu'aux personnes disposant de clés[4] ; l'accès à ces clés étant déterminé par la gestion des identités et l'authentification des utilisateurs. Ainsi, établir une frontière consiste à chiffrer les données et à en limiter l'accès. Néanmoins, une donnée chiffrée ne peut pas être exploitée. En effet, pour bénéficier de services en ligne (messagerie, traitement de texte, vidéoconférence…) les données doivent être, à un moment, déchiffrées. Aussi l'utilisateur fait-il face à un dilemme quant à la protection de ces données : soit il stocke des données chiffrées, garantissant ainsi leur protection mais sans pouvoir bénéficier des services proposés, soit il utilise les services mais pour ce faire, la donnée est déchiffrée à un moment ou un autre, et donc accessible au fournisseur de service. Toutefois, une nouvelle technologie prometteuse devrait à terme permettre la manipulation de données sensibles protégées : le chiffrement homomorphe[5]. Concrètement, la donnée sensible chiffrée, par exemple votre position géographique, pourra être analysée par une société tierce, qui déterminera par exemple votre proximité géographique avec un médecin, sans jamais être révélée. Dans une autre logique de protection, certains États font le choix de s'isoler du reste d'Internet en filtrant les communications entrantes et sortantes vers les réseaux et centres de données hébergés physiquement sur leur territoire, à l'image de la Chine avec sa grande muraille numérique[6]

(2) www.lebigdata.fr/chiffres-big-data.
(3) Souvent appelé improprement cryptage selon l'anglicisme d'encryption.
(4) www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement.
(5) https://hellofuture.orange.com/fr/chiffrement-homomorphe-la-cle-de-la-securite.
(6) *Great Firewall* : www.franceculture.fr/emissions/le-numerique-et-nous/la-chine-durcit-son-controle-dinternet.

ou de la Russie[7]. Certains travailleraient à l'élaboration d'Internets alternatifs[8]. Ces choix technologiques ne représentent pas une frontière inviolable. Ils ne prémunissent pas, par exemple, les États contre les cyberattaques ou les intrusions extérieures. Ils servent souvent (i) des objectifs de politique interne, comme le contrôle de l'accès à des données ou des services étrangers par les populations locales notamment, ou (ii) une dimension géopolitique, brandissant notamment la menace ultime de couper les services ou l'accès informatique de pays non-amis.

92. – Infrastructure et réseaux informatiques, maîtriser les routes et les autoroutes de l'information. La couche « virtuelle » de l'accès aux données numériques transite par un maillage complexe d'infrastructures physiques. Réseaux filaires (téléphonie, fibre optique, câbles sous-marins…), réseaux mobiles (antennes 4G, 5G…), centres de données sont autant d'équipements et d'infrastructures situés sur un territoire donné et dont, *de facto*, la gestion relève de la souveraineté. Leur installation, leur protection, la maîtrise de ceux-ci sont cruciales pour garantir l'accès de la population au monde numérique. L'expertise et la connaissance de ces technologies sont également fondamentales, car la souveraineté dans ce domaine passe également par la capacité à produire, commercialiser et maintenir ces infrastructures.

93. – La puissance numérique et technologique. La course à la puissance, garantie d'indépendance et de souveraineté, se traduit dans le monde numérique par une course à la capacité de calcul informatique. Enjeu historique de souveraineté militaire, elle a été accélérée par la rivalité entre les États-Unis et l'URSS lors de la guerre froide, au profit notamment de la simulation nucléaire. Les États se sont lancés dans la construction de « supercalculateurs » qui servent aujourd'hui dans les domaines militaire et civil à une multitude de simulations numériques (climatologie, physique atomique, astrophysique, essais nucléaires, intelligence artificielle, cryptographie)[9]. Cette puissance de calcul est devenue un enjeu fort de souveraineté, comme le dit Thierry Breton, commissaire européen pour le marché intérieur : « Les supercalculateurs seront au cœur de l'Europe numérique de la prochaine décennie »[10]. La prochaine révolution attendue en la matière est l'informatique quantique[11]. La course mondiale est d'ailleurs lancée entre États, géants du numérique et *startups* innovantes. Cette technologie devrait ainsi effacer des tablettes les performances actuelles des plus puissants supercalculateurs.

Pour être mise à profit, cette puissance nécessite la maîtrise des algorithmes les plus performants et des talents du numérique.

94. – Des forces de l'ordre pour assurer le respect de l'ordre public et la cyberpaix sur Internet. L'environnement numérique est un terrain de jeu de choix pour une cybercriminalité toujours plus forte, structurée sous la forme de groupes organisés

(7) www.france24.com/fr/20190502-internet-souverain-russie-censure-chine-poutine-runet.
(8) www.zdnet.fr/actualites/la-russie-totalement-deconnectee-d-internet-39896419.htm.
(9) www.leparisien.fr/high-tech/5g-cinq-minutes-pour-comprendre-la-mise-a-l-ecart-de-huawei-en-france-08-07-2020-8349573.php ; https://www.cea.fr/comprendre/Pages/nouvelles-technologies/essentiel-sur-supercalculateurs.aspx.
(10) https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/how-supercomputers-will-be-core-our-european-digital-decade.
(11) https://lejournal.cnrs.fr/articles/ordinateur-les-promesses-de-laube-quantique.

qui se coalisent au gré des opportunités et qui côtoient organisations mafieuses, cartels traditionnels et grand banditisme. Les revenus issus de cette cybercriminalité se sont envolés, rapportant désormais plus de 2,8 fois l'argent du trafic de drogue au niveau mondial[12]. S'ajoute à cette menace celle qui est pilotée par les États eux-mêmes (V. *infra*, n^{os} 102 et s., « La cyberguerre »), qui pour certains s'appuient plus ou moins ouvertement sur ces mêmes groupes de *hackers*[13].

Pour y faire face, les États se dotent de capacité de cyberdéfense, d'enquête, d'intervention et de maintien de l'ordre numérique.

Il est à noter ici une différence majeure avec le monde de la sécurité traditionnelle. C'est la proportion du nombre d'individus intervenant dans le domaine de la cybersécurité entre secteur privé et public. Là où la majorité des forces de sécurité traditionnelles relèvent de l'État (forces de police ou armées), la proportion est inversée dans le monde cyber. Ainsi la part des capacités étatiques de maintien de l'ordre et de cyberdéfense est minoritaire dans un écosystème qui s'appuie significativement sur les champions privés nationaux et internationaux pour la défense des intérêts souverains face aux cyberattaques.

95. – **La légitimité juridique et politique remise en cause.** Selon le rapport du Sénat de 2019, un des objets de la souveraineté est de « garantir l'intégrité démocratique des élections »[14]. Par extension, il s'agit ici de garantir dans un espace numérique ouvert, des règles, des lois qui régissent les valeurs et principes de la République. L'espace numérique fait d'ailleurs l'objet d'un renforcement des réglementations, permettant aux États d'assurer la souveraineté et le respect de leurs valeurs (RGPD, lois extraterritoriales…). C'est aussi un endroit où les acteurs privés, et notamment les géants du numérique américains, se posent en quasi-législateurs, obligeant notamment leurs utilisateurs à consentir à des conditions générales d'utilisation, à la portée rarement comprise, en échange de leurs services. Ces conditions sont parfois même en opposition avec la réglementation locale, et déportent souvent la gestion de litiges sous des juridictions lointaines et moins favorables aux utilisateurs, notamment européens.

96. – **La monnaie et les transactions financières.** La monnaie est un attribut régalien de la souveraineté d'un État ou d'un groupement d'États. Les flux monétaires internationaux sont depuis longtemps numériques. Dans ce contexte, les régulateurs internationaux ont défini de nombreuses réglementations locales et internationales visant à s'assurer de la maîtrise, de la traçabilité et d'une certaine transparence des échanges. Aujourd'hui, les monnaies traditionnelles et les échanges financiers sont concurrencés par les cryptomonnaies. Décentralisées, s'appuyant sur des protocoles libres de droit (principalement la *blockchain*)[15], elles s'affranchissent notamment des institutions financières et des banques centrales. Les échanges échappent donc le plus souvent aux États et sont *de facto* largement utilisés par la criminalité et à des fins d'échapper aux autorités de contrôle. C'est un domaine auquel s'intéressent les

(12) www.lesechos.fr/tech-medias/hightech/les-cybercriminels-a-lheure-des-bandes-organisees-1257195.
(13) www.franceculture.fr/oeuvre/les-nouvelles-guerres-sur-la-piste-des-hackers-russes.
(14) Rapport du Sénat sur la souveraineté numérique.
(15) https://journalducoin.com/blockchain.

GAFAM qui se lancent dans la course, notamment avec la cryptomonnaie Libra, issue d'un consortium de partenaires du monde de la technologie piloté par Facebook. Ce choix illustre une nouvelle fois de la volonté des grandes sociétés du numérique de se doter des attributs de souveraineté des États.

II. – Les modalités d'exercice

A. – La voie concertée : la gouvernance d'Internet et du numérique, actuellement nettement aux mains des États-Unis

97. – Deux modalités d'exercice de la souveraineté numérique peuvent être étudiées : d'une part, la voie concertée, avec la mise en œuvre d'une gouvernance pour l'Internet dans une logique apparente de collaboration et, d'autre part, la cyberguerre ou cyberconflictualité qui consiste à transposer dans l'espace numérique des rivalités armées étatiques, et qui vise à asseoir la domination et la souveraineté par des forces armées numériques.

1° L'aspect technique : une gouvernance distribuée, mais dominée dans les faits par les Américains[16]

98. – L'attribution des adresses : un contrôle américain historique, qui s'est relâché depuis 2016, en apparence. Comme nous l'avons vu *supra* (V. n° 71), c'est un organisme de droit privé américain, situé en Californie (l'ICANN) reste, pour le moment (malgré la fin du contrat conclu avec le département du commerce des États-Unis en octobre 2016), compétente pour gérer la racine de l'internet et décider de la création de nouvelles extensions de noms de domaine, ce qui est sujet à controverses. En dehors des noms de premier niveau, l'ICANN attribue également des blocs d'adresse IP à des *Regional Internet Registries* (RIR) qui, à leur tour, les attribuent à des *Local Internet Registries* (LIR), lesquels – en pratique – correspondent souvent à des fournisseurs d'accès à Internet. Ces RIR, au nombre de cinq actuellement[17], gèrent des ressources rares (une même adresse IP ne pouvant pas être utilisée par deux acteurs différents en même temps), et qui peuvent avoir un impact significatif sur l'accès au marché dans l'espace numérique. Il est par ailleurs intéressant de relever que ces RIR agissent ici en dehors de toutes prérogatives régaliennes puisque les États ne se sont pas, dans leur très grande majorité, emparés

(16) Nous avons repris, ici, en partie la formule de M^me^ la Sénatrice C. Morin-Desailly, dans son rapport d'information fait au nom de la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », 2014) (www.senat.fr/rap/r13-696-1/r13-696-11.pdf).

(17) Ainsi, les RIR actuels sont :
– RIP-NC (basé aux Pays-Bas), compétent pour recevoir et attribuer les noms de domaine aux entités situées en Europe et au Moyen-Orient ;
– APNIC (basé en Australie), compétent pour recevoir et attribuer les noms de domaine aux entités situées Asie et Pacifique ;
– ARIN (basé aux États-Unis d'Amérique), compétent pour recevoir et attribuer les noms de domaine en Amérique du Nord ;
– LACNIC (basé en Uruguay), compétent pour recevoir et attribuer les noms de domaine aux entités situées en Amérique latine et aux Caraïbes ;
– AFRINIC (basé à Maurice), compétent pour recevoir et attribuer les noms de domaine aux entités situées en Afrique (https://fr.wikipedia.org/wiki/Registre_Internet_r%C3%A9gional).

de ce sujet[18]. Ainsi, l'attribution des adresses (IP et noms de domaine) reste sous l'égide de l'ICANN qui, bien que n'étant plus liée formellement par un contrat avec l'administration américaine, n'est pas pour autant devenue une organisation internationale, qui aurait pu être intégrée à l'ONU, et demeure une entité de droit américain, soumise à la justice américaine.

99. – La production de normes techniques faisant autorité sur le marché : la suprématie de l'ISOC, établie aux États-Unis, et du W3C, créé avec le soutien de l'administration américaine. Tout d'abord, la célèbre et prestigieuse *Internet Society* (ISOC) a été créée aux prémices de l'Internet actuel, en 1992, par deux pionniers (Vint Cerf, embauché par Google en 2005, et Robert E. Kahn), pour promouvoir et coordonner l'extension d'Internet à travers le monde, en intégrant, dès sa création, l'*Internet Architecture Board* (IAB)[19]. Sur le plan opérationnel, l'ISOC, aujourd'hui dirigée par Andrew Sullivan, précédemment employé par l'éditeur américain Oracle, et établie aux États-Unis en Virginie, s'appuie sur deux principaux groupes de travail :

– d'une part, l'IETF[20], actuellement dirigée par Alissa Cooper (occupant en parallèle la fonction de *VIP Technology Standard* au sein de la société américaine Cisco), qui sert d'instance d'appel et de validation dans le processus de production des normes ;

– d'autre part, l'IRTF[21], actuellement dirigée par Colin Perkins (professeur associé à l'Université de Glasgow, au Royaume-Uni), qui travaille sur des questions de recherche à plus long terme (protocoles, architecture, *etc.*).

Ensuite, le non moins célèbre W3C[22] a été créé par Tim Berners-Lee en 1994, au laboratoire de science informatique du MIT[23], avec les soutiens de la DARPA[24], organisme de défense américain, et de la Commission européenne, avant d'essaimer dans près d'une centaine de bureaux actuellement répartis dans le monde. Berners-Lee est considéré comme l'un des pères d'Internet pour avoir notamment conçu, avec son équipe du CERN[25], les quelques briques fondatrices comme le protocole HTTP, les liens hypertextes et le langage HTML. Actuellement toujours présidé par son fondateur, le W3C est géré aux États-Unis par le MIT, en Europe par l'ERCIM[26], au Japon par l'Université Keio et en Chine par l'Université Beihang.

Parmi ses missions, le W3C supervise le développement des normes techniques, et veille à préserver l'interopérabilité et l'universalité d'Internet. En pratique, les normes du W3C, qui s'est imposé comme l'un des producteurs de standards les plus

(18) C'est le cas notamment de la Chine et du Japon qui se voient attribuer directement par les RIR un ensemble d'adresses IP, puis le redistribuent ensuite souverainement aux LIR de leur juridiction.
(19) Toujours actif et que l'agence de défense américaine « DARPA » (*Defense Advanced Projects Agency*) avait créé en 1979 sous le nom initial d'ICCB (*Internet Configuration Control Board*), devenu *Advisory Board* en 1984, puis *Activities Board* en 1986.
(20) *Internet Research Engineering Task Force.*
(21) *Internet Research Task Force.*
(22) Acronyme de *World Wide Web Consortium.*
(23) *Massachusetts Institute of Technology* (États-Unis d'Amérique).
(24) *Defense Advanced Research Projects Agency.*
(25) Conseil européen pour la recherche nucléaire.
(26) *European Research Consortium for Informatics and Mathematics*, organisation ayant pour objectifs de stimuler la collaboration à l'intérieur de l'Union européenne, fondée par l'INRIA pour la France (Institut national de recherche en informatique et en automatique), le GMD pour l'Allemagne (centre allemand de recherche sur les technologies informatiques) et le CWI pour les Pays-Bas (centre néerlandais de recherche en informatique).

influents aux côtés de l'ISOC et de ses satellites, ont un poids considérable. Adoptées par un très grand nombre d'opérateurs, qui y voient l'avantage non seulement d'une référence connue et rassurante, mais également la garantie d'une compatibilité technique avec un grand nombre d'acteurs du marché, ces normes finissent par faire autorité et orienter la technologie sous-jacente à Internet bien plus efficacement que n'importe quelle réglementation locale puisque, à la différence de celles-ci, les normes du W3C ont une portée mondiale. En attestent, par exemple, les normes HTML[27] utilisées par les navigateurs pour présenter de manière homogène les pages web. Bien que n'étant sous la tutelle d'aucun État, l'ISOC et le W3C n'en demeurent pas moins, par leur histoire, leur localisation géographique et les personnalités qui les dirigent et les ont dirigés, fortement influencés par l'écosystème technologique et idéologique américain et, dans une moindre mesure, britannique. Il est en tout cas un fait que les ressortissants européens (français, allemands, espagnols, italiens, *etc.*) sont nettement moins représentés dans ces instances que leurs homologues américains ou chinois.

2° L'aspect diplomatique : l'initiative onusienne en 2006 et ses limites

100. – Le lancement du Forum sur la gouvernance de l'Internet (en anglais : *Internet Governance Forum* [IGF), sous l'égide de l'ONU. Né en 2006 à l'initiative du Secrétaire général des Nations unies, fruit d'une proposition du WGIG[28], le Forum sur la gouvernance de l'Internet, plus connu sous le nom d'IGF, visait à combler le vide laissé par l'absence d'instance mondiale et multipartite compétente pour traiter les questions de politique publique liées à Internet. L'intransigeance des États-Unis, acceptant une implication et une participation multipartites, sans pourtant abandonner le contrôle d'Internet à une instance onusienne en invoquant être seuls capables de garantir la sécurité et la stabilité de la toile, n'a pas permis de faire émerger une véritable gouvernance internationale et multilatérale de l'Internet, partagée par les États. Aussi, l'IGF ne s'est vu doté que de missions visant à faciliter le dialogue, identifier les difficultés et à émettre des recommandations, mais n'a reçu aucun pouvoir ni rôle décisionnel.

101. – Une efficacité contestée. Dans son rapport remis au Sénat en 2014, la sénatrice Catherine Morin-Desailly[29] dressait un bilan mitigé de l'IGF, en mettant en exergue son rôle purement consultatif et, par là, son absence de pouvoir décisionnel. Bien que le champ d'analyse de ce forum soit vaste en couvrant des sujets tels que la protection de l'enfance, la protection des données personnelles et la lutte contre la cybercriminalité ainsi que la réduction de la fracture numérique mondiale, la sénatrice relève, dans ce rapport, que l'IGF « permet en effet l'expression des nombreux points de vue mais, à son terme, les questions soulevées restent entières », et qu'il est « concurrencé par une multitude d'événements traitant de la gouvernance de l'Internet ». Les révélations du quotidien britannique *The Guardian*, en 2013, relatives à l'affaire *Snowden*, dévoilant les opérations de

(27) *Hypertext Markup Language.*

(28) *Working Group on Internet Governance*, lequel avait été créé trois ans plus tôt, lors du premier Sommet mondial sur la société de l'information (SMSI) de 2003.

(29) Rapport d'information fait au nom de la mission commune d'information, « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », 2014 (www.senat.fr/rap/r13-696-1/r13-696-11.pdf).

surveillance généralisée mises en œuvre notamment par les services de renseignement américains sur Internet, ont provoqué un véritable séisme, brisant la confiance dans la capacité et la volonté des États-Unis de gérer un Internet libre et respectueux des droits fondamentaux. Cet événement a marqué un tournant, créant un « hiver » diplomatique et une crispation des autres pays qui ont cherché à se protéger soit par une politique nationale énergique et unilatérale, comme la Chine et la Russie, soit par le renforcement d'une réglementation protectrice, comme l'Europe avec le règlement général sur la protection des données (RGPD) adopté en 2016. Quoi qu'il en soit, la voie diplomatique étant dans une impasse depuis cette affaire, l'espace numérique n'a eu de cesse, depuis, de connaître des tensions croissantes que d'aucuns assimilent à la guerre en parlant de « cyberguerre ».

B. – La cyberguerre

1° La cyberguerre comme prolongement naturel de la conflictualité classique

102. – « D'anciens conflits, de nouvelles batailles »(30)**.** C'est ainsi que l'on pourrait décrire la conflictualité entre États qui se joue dans l'espace numérique. Historiquement, « (…) cette cyberguerre nous permet d'avoir une supériorité opérationnelle sur nos théâtres d'opérations extérieures (…) », comme l'indique le général Didier Tisseyre(31). Elle fut longtemps une force au service des combattants, utilisée notamment pour collecter du renseignement, rendre indisponibles des systèmes d'arme, désorganiser les moyens de communication. Ces capacités cyber sont dorénavant regroupées sous la forme d'une armée(32) dans beaucoup de pays. Une partie de la conflictualité s'exprime dorénavant par le numérique au sein des réseaux publics comme Internet et des réseaux militaires, au travers de ce que l'on appelle généralement des « cyberattaques ». Ces cyberopérations se développent comme des alternatives à des actions armées traditionnelles. Plus furtives, moins visibles du grand public, elles présentent des avantages pour nos forces armées. Elles sont politiquement plus acceptables car en apparence sans armes et sans victimes et n'attirent pas le même niveau d'attention, et financièrement attractives car le niveau d'investissement, principalement humain, s'avère moins coûteux que pour un armement traditionnel.

103. – Cette course à l'armement numérique est donc une guerre, mondiale et multilatérale. Comme le proclamait M^me^ Florence Parly, ministre des Armées, dans son discours du 18 janvier 2019 : « La guerre cyber a commencé et la France doit être prête à y combattre »(33). Les attaques cyber perpétrées par un État contre un autre État sont dorénavant considérées comme des actes de guerre. À titre d'exemple, l'OTAN a ajouté en 2016 ce type d'attaques à la liste des menaces

(30) www.iss.europa.eu/content/cyber-conflict-uncoded#_old_conflicts__new_battles_.
(31) www.challenges.fr/entreprise/defense/en-cyberdefense-nous-sommes-parmi-les-toutes-meilleures-nations-selon-le-patron-du-comcyber_685959.
(32) Au même titre que l'Armée de terre, la Marine, l'Armée de l'air.
(33) Déclaration de M^me^ Florence Parly, ministre des Armées, sur la stratégie cyber des armées, Paris, 18 janv. 2019 (www.defense.gouv.fr/salle-de-presse/discours/discours-de-florence-parly/discour-de-florence-parly-ministre-des-armees-strategie-cyber-des-armees).

qui déclenchent une réponse collective des membres de l'Organisation (Traité de l'Atlantique nord, art. 5). Cette extension qui a été interprétée comme un signe de fermeté à l'égard de la Russie, soupçonnée d'avoir attaqué l'Estonie en 2007 et la Géorgie en 2008[34], est aussi devenue un signe fort de l'émergence de ce que les Anglo-Saxons appellent le *cyber warfare*. Issue de la période de la guerre froide principalement active entre les deux blocs rivaux de l'est et de l'ouest, la guerre cyber est dorénavant **mondiale et multilatérale**. L'interconnexion des pays, des entreprises et des individus par les réseaux de communication fait de cette menace une préoccupation sérieuse. Le coût limité pour conduire des cyberattaques entraîne une multiplication des belligérants.

104. – Les belligérants. Les États traditionnellement militarisés (États-Unis, Russie, Chine, France, Royaume-Uni…) côtoient des États moins armés qui ont cependant fait de leurs capacités *cyber* offensives et défensives une priorité pour obtenir une reconnaissance militaire et diplomatique (Israël, Corée du Nord, Pays-Bas)[35]. Certes, les États-Unis ont pris une grande avance dans ce domaine. L'attaque en 2010 contre les centrifugeuses iraniennes d'enrichissement d'uranium au moyen du ver informatique américano-israélien *Stuxnet*[36] en est probablement l'illustration la plus médiatisée. Toutefois, il ne faut pas oublier les révélations d'Edward Snowden sur la *National Security Agence* (NSA) en 2013, qui montrent comment les États-Unis s'appuient sur leur domination numérique pour asseoir leur puissance en matière de cyberguerre. Israël est également réputé être à la pointe dans le domaine, ayant depuis de nombreuses années développé une force armée offensive reconnue, et ayant, politiquement et économiquement, fait le choix de développer un écosystème de cybersécurité s'exportant dans le monde entier. En France, le Livre blanc de 2008 marque l'entrée du cyber comme dimension importante de notre stratégie militaire, confirmée par les versions suivantes et le renforcement significatif dans les années passées de nos capacités défensives (ANSSI) et offensives (ComCyber). Les exemples sont également multiples pour la Russie et la Chine régulièrement soupçonnées dans des cas de cyberattaques, tout comme la Corée du Nord. Une particularité de cette cyberguerre est la dimension asymétrique de la menace. Les armes cyber sont, pour la plupart d'entre elles, accessibles à tous. Un attaquant ou un groupe d'attaquants disposant de ces outils et de temps bénéficiera d'une forte capacité de nuisance dans le cyberespace. La cyberguerre s'ouvre donc à des acteurs disposant de moyens financiers plus limités ou à des organisations pseudo-étatiques ou autorevendiquées[37].

105. – Un prolongement de la lutte armée offensive et défensive. Comme dans le domaine militaire classique, la cyberguerre peut être décrite selon ses composantes offensives et défensives. Offensivement, elle regroupe aussi bien les attaques numériques visant à rendre indisponibles les réseaux des États et de leurs armées, à porter atteinte au fonctionnement des systèmes d'armes, que le vol

(34) www.silicon.fr/cyber-attaques-actes-guerre-otan-96436.html.
(35) www.belfercenter.org/publication/national-cyber-power-index-2020.
(36) www.courrierinternational.com/article/2013/02/28/la-cyberguerre-les-guerres-secretes.
(37) www.lorientlejour.com/article/933589/cyberattaque-de-larmee-electronique-du-califat-contre-le-site-de-losdh.html.

d'informations tactiques et stratégiques. L'ex-chef d'état-major des armées (CEMA), le général de Villiers, l'exprimait en 2015 : « [Le cyberespace] permet (…) de s'attaquer à la disponibilité et à l'intégrité de tous les systèmes et réseaux de fonctionnement des États et de leurs armées »[38]. Cette dimension offensive est généralement une prérogative étatique comme c'est le cas en France, sous l'égide du ministère des Armées. Mais cette activité est parfois sous-traitée au secteur privé, officiellement ou officieusement, dans de nombreux pays[39]. Défensivement, elle contient (i) les mesures de protection mises en œuvre pour contrer les cyberattaques, qui peuvent être techniques (sécurisation des serveurs, systèmes antivirus,…), organisationnelles (mises à jour des systèmes, responsabilités) ou humaines, notamment *via* la sensibilisation ; (ii) les mesures de détection qui comprennent l'ensemble des mesures de détection et de réaction en cas d'incident (centre de sécurité opérationnelle, systèmes de détection d'incidents) ; (iii) les mesures de résilience permettant la continuité de fonctionnement des systèmes, des réseaux, des opérations durant l'attaque et leur reconstruction en cas de succès de l'attaque. La défense, bien qu'organisée par les États pour assurer la résilience des forces armées, des administrations et des organismes d'importance vitale[40], n'est pas l'apanage de ces mêmes États. Le secteur privé et les citoyens eux-mêmes doivent mettre en œuvre ces mêmes moyens de protection.

2° La cyberguerre : assurer la domination de l'espace numérique en dehors

106. – Le renseignement et l'espionnage économiques sont également au cœur de cette guerre. Le cyberespace est une formidable source d'information pour les services de renseignement en complément de leurs activités traditionnelles. L'intrusion dans les systèmes ennemis permet l'obtention d'informations stratégiques ou tactiques. L'accès aux informations et services publics depuis Internet est précieux pour les services, comme par exemple les cartographies en ligne, les webcams non protégées, les informations partagées sur les réseaux sociaux Autant d'informations utiles dans le cadre de conflits et de lutte contre le terrorisme, mais qui peuvent se retourner contre les forces armées elles-mêmes. En 2018, les armées françaises et américaines ont mis en garde leurs soldats face à l'usage de l'application Strava. Cette application, prisée des coureurs, permet d'enregistrer ses trajets et ses performances sportives. Quand elle était utilisée par des militaires, les données stockées permettaient de fournir des informations sensibles sur l'emplacement des troupes sur des terrains d'opérations extérieures[41].

107. – Les frontières entre renseignement militaire et économique sont parfois minces. Snowden, l'ancien agent de la NSA, a dévoilé un vaste plan d'interception des

(38) www.opex360.com/2016/01/18/pour-le-general-de-villiers-le-domaine-de-linfluence-constitue-nouveau-champ-daction.
(39) www.franceculture.fr/emissions/le-monde-des-espions-saison-2-les-nouveaux-corsaires/les-auxiliaires-prives-du-renseignement-francais-avec-bernard-barbier.
(40) www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france.
(41) www.lemonde.fr/pixels/article/2018/01/30/l-armee-francaise-met-ses-troupes-en-garde-contre-l-application-de-jogging-strava_5249157_4408996.html.

communications numériques par les autorités américaines, le programme PRISM[42]. La NSA, collaborant avec de nombreux acteurs du numérique américains, notamment les GAFAM, a mis en place un vaste système de collecte des informations détenues par ceux-ci. L'objectif officiel de lutte contre le terrorisme et de prévention des cyberactivités hostiles ou la prolifération nucléaire[43] couvre également une activité d'espionnage militaire et économique de leurs adversaires mais aussi de leurs alliés, notamment européens. Plus généralement, le cyber est un espace où convergent de multiples (i) intérêts, entre acteurs étatiques et groupes de *hackers* (les corsaires des temps modernes ?), et (ii) bénéfices, entre cyberdiplomatie, cyberguerre et économie.

108. – La cyberguerre est également une guerre de l'information. Citons à nouveau le général de Villiers : « [le cyberespace] permet de porter la guerre pour, par et contre l'information. Ce champ de bataille, qui n'est pas lié à une géographie physique, offre de nouvelles possibilités pour la connaissance et l'anticipation, ainsi qu'un champ d'action pour modifier la perception et la volonté de l'adversaire »[44]. Le cyberespace a la caractéristique, *via* l'émergence des réseaux sociaux et l'immédiateté de l'accès à l'information, vérifiée ou non, de pouvoir toucher une vaste audience sans contrainte temporelle ni géographique. Nous sommes à l'âge de « l'infox » et de rumeurs bénéficiant de caisses de résonance mondiales et immédiates. Les États s'adonnent donc maintenant à cette guerre d'influence et de perception. À titre d'exemple : la Russie, derrière les élections des pays occidentaux – France, États-Unis, Royaume-Uni – ou encore l'État islamique passé maître dans la propagande sur les réseaux sociaux, poussent les États à adapter leurs mesures de défense sur le terrain de l'opinion publique et à la vérification de l'information.

109. – La difficulté de l'attribution des cyberattaques. L'apparente simplicité d'une cyberattaque, l'accessibilité des outils et le relatif anonymat que permet Internet rendent délicat le travail d'identification de l'attaquant. Les cybercombattants et les cybercriminels mettent tout en œuvre pour éviter d'être identifiés et de subir des représailles directes. La *Central Intelligence Agency* (CIA) intégrait par exemple du farsi, du russe ou du coréen à ses lignes de code, selon les documents dévoilés par *WikiLeaks*[45]. Certains groupes travaillent également sur des créneaux horaires différents de leur localisation.

110. – La cyberguerre est-elle une guerre ? Certains spécialistes réfutent le terme de guerre en raison de l'absence de létalité de cette guerre numérique[46]. Néanmoins, en dépit de l'absence de victime humaine, les impacts de ces conflits entre États peuvent toucher des pans entiers de l'économie. Les victimes sont en

(42) www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html.
(43) www.lemonde.fr/technologies/article/2013/06/10/bataille-d-informations-autour-de-l-outil-de-surveillance-prism_3427534_651865.html.
(44) www.opex360.com/2016/01/18/pour-le-general-de-villiers-le-domaine-de-linfluence-constitue-nouveau-champ-daction.
(45) www.lefigaro.fr/secteur/high-tech/2017/04/10/32001-20170410ARTFIG00136-cyberguerre-une-course-a-l-armement-preoccupante.php.
(46) www.cairn.info/revue-les-cahiers-du-numerique-2002-1-page-77.htm.

effet des entreprises qui font faillite. Elles peuvent être des systèmes essentiels au fonctionnement des pays tels que l'énergie, l'eau, la santé, la finance où les dysfonctionnements pourraient ultimement porter atteinte à l'humain.

111. – **Une maîtrise incertaine de « l'arme » cyber.** L'interconnexion des systèmes et des réseaux rend également hasardeuse la maîtrise du périmètre d'une cyberattaque. Certaines attaques emblématiques récentes ont perdu le contrôle de leur auteur. C'est le cas du ver informatique *Stuxnet* destiné à déstabiliser les installations nucléaires iraniennes, qui a fait d'autres victimes dans le monde industriel dont Air Liquide[47], et qui s'est disséminé dans près de six millions d'ordinateurs et 10 000 sociétés en Chine[48]. Le cas le plus emblématique est certainement le virus informatique *NotPetya*[49], attribué à la Russie, qui avait pour objectif de déstabiliser l'Ukraine, en 2017, en plein conflit armé entre les deux pays. Ce virus initialement implanté sur des logiciels ukrainiens, pour déstabiliser le pays, s'est ensuite propagé dans le monde entier, générant la cyberattaque à l'impact financier le plus important à ce jour, estimé à plus de dix milliards de dollars américains[50] et ayant entraîné la faillite de nombreuses sociétés à travers le monde.

SECTION 2

LE BUT DE LA SOUVERAINETÉ NUMÉRIQUE

112. – **La souveraineté numérique de l'État démocratique doit servir la souveraineté nationale** (V. *supra*, n^os^ 16 et s.). Celle-ci, pour agir efficacement, doit détenir des prérogatives régaliennes reconnues tant par le peuple que les États. Elle a le devoir d'agir pour et au nom du Peuple, afin d'assurer la protection de ses citoyens pour qu'ils puissent vivre libres et en paix. La souveraineté numérique poursuit ce même but dans une **déclinaison de souveraineté appliquée au cyberespace**, pour assurer, **la cyberdéfense de la nation**, sur tous les plans : cybersécurité, économie numérique et développement industriel numérique, maîtrise des réseaux sociaux pour assurer la démocratie et déjouer d'éventuelles influences extérieures telles que celles qui vicieraient des élections démocratiques ; prévention, autonomie stratégique et régulation doivent permettre d'asseoir des positions nationale et européenne dans ce cyberespace ouvert, au service de la souveraineté nationale dans les valeurs démocratiques européennes. Parce qu'il n'y a pas de liberté sans sécurité, l'enjeu de cette souveraineté est d'exercer son propre arbitraire dans ce premier but de protection. Le but de la souveraineté numérique est donc bien d'être en mesure d'exercer sa (ses) propre(s) norme(s) pour assurer la sécurité de son potentiel économique, scientifique et technique, informationnel, nécessaire au développement des activités du pays et spécialement au regard du marché numérique dans le

(47) https://o.nouvelobs.com/high-tech/hacker-ouvert/20121120.OBS0013/la-societe-air-liquide-piratee-par-stuxnet.html.
(48) www.journaldunet.com/solutions/dsi/1075692-stuxnet-infecte-6-millions-de-pc-en-chine.
(49) www.lemonde.fr/pixels/article/2017/11/07/le-virus-petya-a-coute-plus-d-un-milliard-d-euros-aux-entreprises_5211421_4408996.html.
(50) www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

cyberespace et aujourd'hui d'un marché unique numérique[51] européen, politique de la Commission européenne menée depuis 2015[52].

113. – La construction d'une cybersécurité collective doit préserver le vivre libre et en paix dans un pays économiquement sain. L'État doit être respecté et se faire respecter à l'intérieur comme à l'extérieur. Il faut donc d'abord construire à l'état de l'art une cybersécurité collective interne efficace, de la veille technique sur les réseaux et infrastructures des systèmes d'informations surtout critiques, moyens de télécommunications de l'armée en OPEX[53] ou de ceux des fonctionnaires expatriés, voire des entreprises privées au savoir-faire crucial pour l'État ; fabriquer, contrôler, réparer les câbles sous-marins qui transportent des données d'intérêt général ou privées et/ou qui doivent rester confidentielles.

114. – Les États membres de l'UE se conçoivent dans un contexte continental européen de valeurs démocratiques à défendre. C'est pourquoi ils sont soumis par des instruments législatifs européens à une standardisation des obligations de sécurité, mais pas nécessairement des moyens de les remplir. C'est un système de valeur qui peut être attaqué, il faut prévenir également les menaces d'États que l'on qualifiera d'inamicaux, car parfois alliés, qui se livrent une cyberguerre[54] plus sournoise mais tout autant destructrice en portant atteinte à la souveraineté numérique lorsque les attaques s'effectuent *via* nos réseaux, infrastructures ou les visent ainsi que l'appropriation de nos données. L'impact de l'attaque peut avoir lieu dans le réel par une conséquence indirecte sur la vie humaine[55], voire sur la démocratie elle-même lorsqu'elle influence une élection. Ce dernier cas, qui a nécessité de légiférer, mais trop tard, montre bien que la souveraineté nationale est menacée par un défaut de souveraineté numérique.

115. – La contribution des textes européens à la cybersécurité collective. La directive NIS (*Network and Information System Security*)[56] et le *Cybersecurity Act*[57] de l'Union européenne contribuent, par la mise en place d'obligations techniques renforcées, à favoriser l'autoprotection, donc la souveraineté numérique, tant au bénéfice des États membres qu'à celui de l'Union européenne. On assiste donc à l'installation d'une doctrine de souveraineté numérique européenne vis-à-vis d'autres continents et qui ne se confond ni dans la souveraineté de chaque État qui y contribue, ni dans une souveraineté européenne fédérale qui ne l'est pas politiquement. On se protège mieux ensemble ou l'union fait la force. Cela, les États victimes d'attaques de leurs réseaux, comme l'UE, en ont compris la nécessité en dépit de politiques internes très différentes mais reposant sur des valeurs communes[58] relatives à l'intimité de la vie privée, au droit de propriété par exemple. Cela permet la

(51) https://ec.europa.eu/commission/publications/factsheets-digital-single-market_fr.
(52) https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-a_digital_single_market.pdf.
(53) OPEX : Opérations extérieures, déploiement de forces à l'étranger utilisant des systèmes d'information et de communication.
(54) USA, Chine, Corée du Nord, Iran pour les pays identifiés et divulgués par l'attribution politique.
(55) www.usine-digitale.fr/article/un-ransomware-provoque-le-deces-d-une-femme-en-urgence-vitale-dans-un-hopital-allemand.N1006284.
(56) www.ssi.gouv.fr/entreprise/reglementation/directive-nis.
(57) www.ssi.gouv.fr/administration/reglementation/cybersecurity-act.
(58) Conv. EDH, art. 8 ; Règl. (UE) n° 2016/679 [RGPD]) et Dir. (UE) 2016/680.

confiance pour développer l'économie européenne devenue numérique pour assurer l'avenir numérique de l'Europe qui passe par l'exploitation de ses propres données. La France comme les États membres est adossée dans ce domaine à la doctrine européenne de l'équilibre promue par Talleyrand au Congrès de Vienne en 1814, en tant qu'instrument de limitation des ambitions hégémoniques des États pour garantir la paix par l'équilibre des forces.

116. – **Pour maintenir la paix publique dans le cyberespace, il faut assurer la cyberdéfense de la nation.** La revue stratégique de cyberdéfense du 12 février 2018 a synthétisé les travaux[59] pour la maîtrise des risques du numérique, l'organisation des chaînes pour assurer la souveraineté tout en permettant parallèlement un développement économique et un rayonnement à l'étranger positif. Ce document qui a réuni tous les ministères est un Livre blanc dont beaucoup des recommandations restent encore à appliquer, tellement la tâche est vaste. Éduquer en masse selon les niveaux, surveiller, prévenir, réagir aux cybermenaces et à leurs effets directs ou indirects, être en capacité de maîtriser l'exploitation autonome de composants électroniques essentiels, ce sont des actes de souveraineté. Pas sûr qu'un composant d'origine étrangère sans alternative ne soit pas une arme possible, et si peu cher qu'il soit il n'en reste peut-être pas moins essentiel. Peut-on être à la merci d'un pays qui est fabricant monopolistique ? L'affaire des masques de la crise du Covid-19 a montré que non ; comme d'autres médicaments régulièrement en pénurie. Tout comme elle a montré que le numérique a permis une certaine continuité d'activité permettant d'éviter le pire mais démontrant aussi le retard d'agilité et « l'incybersécurité » de réseaux privés virtuels (VPN) mis en place rapidement ou d'autres ressources sans sécurité… du tout. Très certainement la souveraineté numérique a été mise à mal en cette période, et ce indépendamment des *ransomwares* qui étaient légion et continuent de l'être…

117. – **La cybersécurité, gage de la souveraineté numérique économique et de la souveraineté nationale.** L'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui dépend du Secrétariat général de la défense et de la sécurité nationale (SGDSN), a des prérogatives défensives et d'analyse mises en commun avec les services de renseignement. C'est **l'acteur premier de la souveraineté numérique intérieure** par son rôle de cybersécurisateur, contrôlant les importations de matériels d'investigation numérique spécifiques tout comme le matériel de guerre est contrôlé par le SGDSN. On l'a vu pour le numérique, pour les systèmes d'information des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE), des administrations, l'ANSSI est aussi le chef de file pour élever le standard de la cybersécurité collective de l'Union européenne. Elle assure, par sa discipline de mise en œuvre, la cybersécurité intérieure et en conséquence la cybersécurité des autres pays liés donc leur propre souveraineté. La qualité de la cybersécurité collective de l'État constitue une action préventive pour ses partenaires et *vice versa*… D'où l'intérêt de la solidarité. Chaque acteur de cybersécurité assure la sécurité des autres. On peut le résumer par la formule des

(59) www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense.

mousquetaires : « Un pour tous et tous pour un ». C'est le sens de l'appel de Paris[60] du 12 novembre 2018 par le président de la République.

118. – Assurer la souveraineté numérique par la cybersécurité pour être toujours plus compétitif et emporter les parts de marchés. Cette protection juridique de l'État, il est vrai coûteuse aussi pour les entreprises qui l'assument, n'a pas de prix pour éviter le pillage ou l'espionnage. C'est la rançon de la souveraineté numérique, composante de la souveraineté nationale, puisque le cyberespace devient de plus en plus vaste. Il convient de rester souverain dans les secteurs d'activité d'importance vitale[61] – ceux qui, en cas d'attaque, seraient critiques pour la vie de la nation –, de rester souverain par le développement de produits de confiance de cybersécurité toujours plus novateurs, d'assurer leur compétitivité technique voire leur normalisation pour un développement économique à l'international qui assure une reconnaissance qualitative de la souveraineté nationale. De la même façon qu'il n'y a pas de liberté sans sécurité, il n'y a pas de confiance sans cybersécurité et donc pas d'affaires. La confiance réside dans la cybersécurité de chacun et donc de tous pour assurer la cyberdéfense des intérêts fondamentaux de la nation : à savoir son potentiel économique, scientifique et technique qu'il s'agit de protéger dans le domaine numérique tant sous les aspects matériels (infrastructures de systèmes d'information) qu'immatériels (logiciels, données, concept d'algorithmes…) pour préserver son développement technologique à l'ère du tout numérique et de la compétition qui fait rage entre les nations. Il faut profiter de l'émergence du marché unique numérique entre autres pour les industries de sécurité. Les efforts d'Hexatrust[62], l'association d'entreprises de pointe en cybersécurité et sous divers angles, tels que l'identité numérique, la sécurité des transactions, s'inscrivent dans cette approche en partenariat avec l'État *via* les comités de filières[63], pour assurer la souveraineté numérique par les produits, les passages à l'échelle des entreprises et les exportations. Cet engouement économique permet de rayonner à l'international et pareillement en créant et diffusant plus de contenus culturels français et européens sur les réseaux numériques, et de qualité.

119. – La préservation de ces savoir-faire doit assurer une souveraineté numérique à l'état de l'art. Être toujours le plus performant techniquement, technologiquement et en mouvement dans cette intention de motiver une démarche dynamique telle que celle d'assurer la compétitivité économique. Il faudra alors préserver ses savoir-faire et développer la recherche et le développement (R&D), pour pouvoir innover. Cette compétitivité sera un atout par rapport aux pays concurrents de valeur. Elle entraînera également l'adhésion à la souveraineté par un phénomène de boule de neige. Il ne s'agit pas de satisfaire uniquement un besoin ; il faut penser les usages du numérique à venir et leurs incidences. C'est pourquoi

(60) www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/les-domaines-d-action-de-la-diplomatie-numerique-francaise/garantir-la-securite-internationale-du-cyberespace-a-travers-le-renforcement-de/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la.

(61) SAIV : Secteurs d'activité d'importance vitale (douze) (www.sgdsn.gouv.fr/communication/la-securite-des-activites-dimportance-vitale/).

(62) www.hexatrust.com/solutions/securisation-des-transactions.

(63) www.gouvernement.fr/comite-de-la-filiere-industrielle-de-securite-cofis.

il faut être formés à ces problématiques d'anticipation de l'avenir pour éviter d'être dépendant et avoir le choix dans le domaine du numérique qui se répand dans tous les autres domaines. La 5G est une illustration de la difficulté du retard pris, faute d'avoir conçu l'avenir. La captation de la valeur est principalement réalisée pour l'heure par les plateformes d'intermédiation donc des services. Ce secteur tertiaire ne construit pas ; il forme les besoins et les usages.

120. – **L'autonomie stratégique par des savoir-faire de haut niveau nécessite de recommencer à penser l'inventivité en France et en Europe.** Selon Louis Pouzin[64] : « Si on a perdu la main sur Internet, c'est parce qu'on n'a pas formé les gens correctement ». Pour n'avoir besoin de personne pour l'essentiel de la vie, pas seulement numérique, de la nation, la souveraineté numérique s'appuie sur une autonomie stratégique pour vivre libre et en paix. En détenant des savoir-faire de haut niveau mais également de simples savoir-faire qui, détenus par d'autres, pourraient asservir le pays (cf. la crise du Covid ou le médicament manquant contre le cancer[65] dans un autre domaine). Il y a lieu de redynamiser ces savoir-faire dans un plan stratégique avec le partenaire allemand, pour ne pas être à la merci d'un retournement d'alliance internationale, en se plaçant dans la construction de l'avenir numérique de l'Europe. Ainsi être *leader* en produits certifiés, labellisés, permet de disposer d'un avantage concurrentiel pour exploiter la demande interne du marché européen, par la concurrence entre les entreprises produisant de la cybersécurité, logicielle ou matérielle ou tout simplement des produits technologiques tels que les *blockchains*[66]. Ce marché devra continuer de cimenter la confiance dans le numérique, en respectant les exigences des valeurs communes du respect de la vie privée et des conventions internationales. À cet égard, il est intéressant de lire les discours de la Chine contre les USA relatifs à l'affaire *TikTok*[67].

L'Union européenne souligne l'importance que représente le développement des supercalculateurs et l'informatique en nuage en tant que facteurs de souveraineté technologique, de compétitivité au niveau mondial et de réussite de la transformation numérique, en soutenant des domaines prioritaires tels que l'intelligence artificielle, les données volumineuses, les chaînes de blocs et l'Internet des objets.

121. – **La question de la normalisation est un des attributs de la souveraineté numérique.** Il faut reprendre du terrain sur la normalisation. Elle est traitée par le ministère de l'Intérieur, le ministère des crises. Les nombreux groupes de normalisation doivent être réinvestis par la France car ils sont trop à la main des pays anglo-saxons qui ainsi décident des normes, donc des standards à utiliser, faussant ainsi la compétitivité en les faisant appliquer par tous leurs fabricants qui y travaillent. Les pays anglo-saxons n'ont pas le même droit que nos pays du sud de l'Europe.

(64) www.rtl.be/info/monde/europe/le-cyberpionnier-louis-pouzin-en-croisade-pour-un-autre-internet--1167569.aspx.
(65) www.francetvinfo.fr/sante/medicament/penurie-de-medicaments-il-faut-rapatrier-la-fabrication-des-medicaments-d-importance-majeure-plaide-le-president-de-la-ligue-contre-le-cancer_4105339.html.
(66) Rapport d'information sur les *blockchains* déposé par les députés Laure de la Raudière et Jean-Michel Mis, 2018 (www.assemblee-nationale.fr/dyn/15/rapports/micblocs/l15b1501_rapport-information).
(67) www.parismatch.com/Actu/International/La-Chine-critique-l-interdiction-de-TikTok-et-WeChat-aux-États-Unis-1703234 ; https://finance.orange.fr/actualite-eco/article/la-chine-riposte-apres-l-interdiction-americaine-de-telecharger-les-applis-tiktok-et-wechat-CNT000001to4Yv/photos/les-etats-unis-ont-annonce-l-interdiction-a-partir-de-dimanche-du-telechargement-des-applications-tiktok-et-wechat-ef213a365b757d200b3bdaca209395fd.html.

Même si la norme n'a pas de valeur juridique contraignante, elle l'est économiquement parlant, surtout à l'ère de l'interopérabilité. On a vu les difficultés avec la norme de la 5G, la cinquième génération des standards en matière de téléphonie mobile, et les spécificités techniques de la 5G NR (*New Radio*) non autonome, standard pas nécessairement compatible avec les investigations numériques par exemple et à répercussion sur la radio du futur pour les services de police. Ensuite, les produits sur le marché ont tous la même norme, mais l'avantage concurrentiel a été détenu par le décideur de la norme. La normalisation est aussi un sujet d'autonomie stratégique en tant que but d'influence économique pour asseoir la souveraineté numérique.

122. – L'exploitation des données, charbon de l'intelligence artificielle, est au cœur de la souveraineté numérique et de la stratégie européenne(68)**.** Les données que le monde entier veut s'approprier servent la souveraineté numérique en premier lieu si elles sont exploitées en France et/ou en Europe au service du développement technologique de l'IA par exemple. Cela permettra d'entraîner les IA avec des jeux de données massives, de faire de la R&D sur les algorithmes ; là encore, on constate que **l'intérêt de la souveraineté numérique est de préserver les données**, **le savoir** au profit de l'État ou de l'Europe pour leur permettre la captation de la valeur. Mais tout en respectant les principes de transparence, de traçabilité et le contrôle humain dans les choix relatifs aux intelligences artificielles. Toutefois, ces principes ne se heurteront-ils pas aux usages bien ancrés des plateformes et autres réseaux sociaux auxquels les usagers livrent volontiers toutes leurs données, tels que les GAFAM et autres BHATX ? En effet, pour l'heure, le droit de la concurrence ne permet pas de lutter contre la concentration des GAFAM ni de créer des plateformes similaires faute de résultats rapides en R&D et surtout d'anticipation à long terme. On peut comprendre que les occasions manquées mènent finalement à un partage des données sur le projet GAIA-X(69) ou à la mise à disposition de nos données au *Health data hub* détenu par Microsoft, un système de base de données et de services liés pour les produits de santé. Sans alternative il serait vain de chercher à reproduire des entreprises de la taille des GAFAM et leurs investissements. Mieux vaut traiter et maîtriser les données et les garanties afférentes, notamment leur réversibilité, retrouver un esprit créatif et repenser l'innovation à long terme en croyant aux projets qui sortent des sentiers battus(70). Un exemple : selon le projet RINA (*Recursive InterNetwork Architecture*), une bulle récursive pourrait être implémentée sur une partie de la France, assurant la souveraineté numérique nationale, le reste des contenus numériques pouvant continuer à être accessible sur l'Internet.

123. – La valeur des données doit être sous une souveraineté numérique qualifiée. Elle ne peut être laissée à d'autres ; le pays doit s'enrichir avec *l'open data*, créateur de valeur par des utilisateurs innovants, par des gains de temps. Le rapport de

(68) https://siecledigital.fr/2020/02/24/leurope-et-le-numerique-la-commission-devoile-sa-strategie-pour-lintelligence-artificielle ; https://ec.europa.eu/france/news/20200219/strategie_avenir_numerique_europe_fr.
(69) www.economie.gouv.fr/concretisation-projet-gaia-x-infrastructure-europeenne-donnees.
(70) https://la-rem.eu/2019/09/rina-un-projet-pour-linternet-de-nouvelle-generation.

décembre 2020 de la mission du député Éric Bothorel[71] sur la politique publique de la donnée (*open data*) développe cette problématique tout en montrant la nécessité de la souveraineté numérique. La valeur de ces données, or noir de ce siècle et du futur sans doute, sera captée grâce à la formation massive aux nouveaux métiers du numérique, dans leur développement et leur promotion spécialement auprès des femmes. En pénurie de main-d'œuvre qualifiée et sachant les besoins de l'avenir, l'Europe estime que 90 % des métiers seront numériques à terme. On ne peut continuer de recourir à la main-d'œuvre de pays spécialisés dans le développement logiciel pour nos entreprises, masquant la pénurie, entravant l'avenir et peut-être en risquant pillage, espionnage ou sabotage, individuel ou d'État. Or, l'économie d'une entreprise réside pour une bonne part dans sa main-d'œuvre. Sans la formation et le développement de cette main-d'œuvre aux métiers de demain, les entreprises ne pourront se développer, et les *startups* seront rachetées sans jamais atteindre la taille critique pour se développer normalement. La souveraineté numérique nécessite de créer et développer la formation qualifiante de masse de nos étudiants dans les meilleures écoles ; de l'informatique à la cryptographie en passant par les *data scientists* et les statisticiens et combien d'autres métiers, peut-être même encore inconnus.

124. – **La souveraineté numérique doit permettre le contrôle des stratégies d'influence extérieure des pays inamicaux.** La souveraineté numérique doit également viser et permettre de surveiller les *fake news* et les risques d'influence sur les élections que l'on a pu voir. C'est un acte de souveraineté que de réguler les comportements illégaux en ligne comme dans la vie réelle grâce à ses instruments juridiques souverains[72] à la mesure de la répartition des compétences européennes et subsidiaires et à l'application des textes internationaux. Le fonctionnement des réseaux sociaux, la création en nombre de faux comptes en ligne permettent de diffuser des fausses informations et de garder dans un enfermement algorithmique les diffuseurs et *retweeteurs* par exemple. Les contenus présentés tournent toujours autour de ce que l'on consulte et écrit. L'influence des réseaux sociaux est particulièrement pernicieuse dans ce cas et la diffusion de *fake news*, non vérifiées et prises pour argent comptant par les asservis du net, a posé et pose la question du contrôle des contenus au regard de la liberté de communication. La presse d'influence, telle que par exemple *Sputnik* ou *RT*, diffuse des informations hostiles dans ses articles[73], et les relations entre les États se détériorent par presse interposée ou sollicitée. Toute donnée n'est pas bonne à *retweeter*, à diffuser et ne doit pas polluer cet espace numérique, prometteur de beaucoup d'opportunités mais terni au même titre que le monde réel. La diffusion de l'attaque de Christchurch en *live* sur Facebook durant dix-sept minutes a montré que la souveraineté numérique pèche dans son application concrète, qu'elle est surtout interdépendante avec celle des autres pays et qu'elle se heurte à des principes qui ne sont pas partagés par tous dans le monde. L'hyperliberté d'expression se confronte à la morale. C'est pourquoi

(71) É. Bothorel, député LREM, chargé de mission associé à R. Vedel, coordonnateur national pour l'intelligence artificielle.
(72) L. n° 2018-1202, 22 déc. 2018, relative à la lutte contre la manipulation de l'information.
(73) https://fr.sputniknews.com/trend/affaire_skripal_032018.

la coopération avec les plateformes, pour leur faire comprendre notre façon de voir et notre droit dans un esprit de régulation et d'exigence de leur responsabilisation, ne milite pas pour la souveraineté numérique en transférant la responsabilité de retrait ou de suppression d'accès à des contenus par exemple. Il faut bien la construction de textes européens importants pour les services de l'État qui doivent maîtriser la veille des réseaux pour intervenir en partenariat avec ces opérateurs de l'Internet afin d'éviter la diffusion virale de fausses nouvelles. Mais beaucoup d'exemples permettent de douter de la souveraineté numérique qui est transverse à plusieurs domaines, et ne s'exerce finalement souvent qu'en partenariat.

125. – **La souveraineté numérique effective reste à construire.** En effet, à la lecture au 16 décembre 2020 du rapport de la mission d'information parlementaire de la Conférence des présidents, présidée par le député Jean-Luc Warsmann sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne » dont sont membres les députés Jean-Michel Mis, Laure de La Raudière et Éric Bothorel, cette souveraineté n'existe pas encore et reste à construire. C'est également ce qui transparaît de cette étude sur le but de la souveraineté numérique. On constate qu'elle touche tous les sujets de la souveraineté régalienne appliquée au numérique dans le cyberespace. Il faut dès maintenant faire les efforts pour ne pas dépendre du savoir des autres et développer une réelle autonomie stratégique.

CHAPITRE 2

LES DÉFIS À RELEVER

SECTION 1

LA CONCURRENCE DES ÉTATS ENTRE EUX

I. – Le cyberespace est un espace peu régulé dans lequel la confrontation des États est naturelle

126. – Produit de la technique et de la mondialisation, c'est le premier espace de confrontation internationale créé par l'homme. Il a des points communs avec l'espace maritime, où la liberté est la règle. Un espace vaste et sans propriétaire où ce qui n'est pas interdit est autorisé et où ce qui est interdit est souvent difficile à contrôler.

127. – Comme la mer, l'espace cyber a ses flibustiers et ses corsaires. Les premiers sont, par exemple, les criminels qui diffusent des rançongiciels. Les seconds sont les groupes qui agissent pour le compte d'un État mais sans produire la lettre de course qui permettait à leurs ancêtres d'être traités en prisonniers de guerre.

128. – Quatre catégories d'agresseurs ont été recensées par une étude menée en 2019 par Thalès sur 490 campagnes d'attaque : cyberattaquants parrainés par des États (49 %) ; cyberactivistes aux visées idéologiques tel le groupe anarchiste *Anonymous Italia*, apparu en 2012 (26 %) ; cybercriminels (20 %) et cyberterroristes (5 %). Nous nous attacherons ici à l'activité des États et de leurs corsaires.

129. – L'affrontement des États dans le cyberespace est dans la nature des choses, dès lors que les États sont naturellement en compétition. Historiquement, cette compétition n'a été contenue que dans des cas relativement limités :

– système d'alliance entraînant une solidarité effective ;
– parité stratégique ;
– coût excessif de la compétition ;
– règle internationale forte.

II. – Dans le domaine du contrôle et de l'usage de l'espace numérique, certains pays ont développé une stratégie et des méthodes conformes à leurs objectifs et à leurs capacités et ces stratégies ne sont que partiellement défensives

130. – Pour les trois principales puissances concernées, elles ont été précisément décrites dans le rapport du Sénat sur la souveraineté numérique du 1er octobre 2019, dont nous retiendrons les axes suivants.

131. – Les États-Unis se sont assuré la suprématie économique par le modèle des plateformes monopolistes. Comme pour l'espace, l'État sous-traite désormais à l'entreprise privée une fonction de projection de la puissance américaine, laissant aux grands groupes du web la maîtrise des contenus. Mais, comme le souligne le rapport du Sénat, l'État contrôle des éléments clés : « C'est une vision libérale, avec des segments fixes détenus par le *Department of Defense* sur les serveurs racines, comme le serveur qui appartient au laboratoire de recherche de l'armée américaine, ou le serveur propriété de la NASA. L'État américain exerce ainsi un contrôle matériel très fort, l'action privée s'exerçant surtout sur les couches logicielle et sémantique »(1).

132. – La Chine développe comme la Russie des politiques visant à « garantir sa souveraineté numérique et à s'émanciper de l'hégémonie américaine, segmentant l'espace numérique pour en avoir un parfait contrôle sur son sol, interdisant aux entreprises étrangères de transférer leurs données électroniques vers leurs sièges nationaux, utilisant les données personnelles de ses citoyens pour asseoir la domination du parti communiste chinois »(2). Le volet externe de cette politique, ce sont les « nouvelles routes de la soie » électroniques. Le processus est long, mais la Chine sait gérer le temps long. Et le quasi-monopole chinois sur certains composants lui donne une arme extrêmement puissante.

133. – La Russie, qui ne dispose pas de multinationales de l'Internet ou de l'informatique, pratique la guérilla ou la menace et investit dans les couches du cyberespace à sa portée, notamment la couche sémantique. En matière défensive, ses récentes avancées en informatique devraient lui permettre « de ne plus dépendre ni de Microsoft ni d'Intel pour ses systèmes sensibles. Si ses acteurs industriels ne sont pas de premier rang international, ils parviennent apparemment à développer des outils autonomes »(3). Mais il y a d'autres joueurs, peut-être pas tous identifiés.

134. – Israël a une doctrine et agit. L'ancien directeur du renseignement militaire israélien a expliqué lors d'une conférence publique en 2009 que « le développement du cyber est aussi important pour la conduite de la guerre que le fut le soutien aérien au début du XXe siècle. Il combine tous les éléments d'une dimension militaire : récolte de renseignements, offensifs et défensifs… Le cyberespace peut

(1) Sénat, Rapport cité.
(2) Sénat, Rapport cité.
(3) Sénat, Rapport cité.

garantir au petit et au faible ce qui fut le monopole des superpuissances… Comme les drones, les forces cyber peuvent frapper sans risquer la vie de soldats. Toutes les technologies sont produites localement, sans intervention extérieure, dans un domaine où les jeunes israéliens excellent ».

135. – **La Corée du Nord a un bureau chargé des cyberopérations**, le bureau 121, qui serait notamment représenté par le groupe cybercriminel Lazarus. La Corée du Nord a entre autres été accusée par le *Federal Bureau of Investigation* (FBI) d'avoir piraté en 2014 la société Sony et empêché la sortie d'un film mettant en scène le président nord-coréen.

136. – **L'Inde a des capacités humaines et informatiques immenses.** Il est presque étonnant qu'elle ne se soit pas encore manifestée sur ce terrain, mais ce n'est sans doute qu'une question de temps.

III. – Selon leurs objectifs et leurs moyens, des États utilisent le cyberespace pour agresser, espionner, dominer économiquement ou influencer

137. – **La furtivité de l'arme cyber la désigne particulièrement pour un usage agressif**, éventuellement militaire, qui restera souvent difficile à documenter, sauf à vouloir laisser une trace. On n'en connaît donc que peu d'applications, l'une des plus illustres étant l'introduction du ver *Stutnext* qui a détruit près des trois quarts des centrifugeuses iraniennes de Natanz. Les autorités militaires israéliennes, qui ont sans doute participé à cette opération, ne se cachent pas d'investir dans la cyberguerre. Le 16 avril 2018, « des experts américains et britanniques ont fait état d'une cyberactivité malveillante d'acteurs soutenus par l'État russe », dont les « cibles (…) sont principalement les gouvernements et les organisations du secteur privé, les fournisseurs d'infrastructures cruciales et les fournisseurs d'accès à Internet ». Une opération plus récente relevant de la menace a été attribuée au renseignement militaire russe (GRU) par la Géorgie dont 15 000 sites, notamment officiels, ont été attaqués en octobre 2019. Londres et Washington ont également accusé la Russie d'être derrière cette attaque informatique.

On rappellera pour mémoire qu'il existe de nombreux groupes de *hackers* qui conduisent des attaques informatiques pour des raisons non étatiques (la moitié selon l'étude précitée de Thalès), raisons qui peuvent être idéologiques, ludiques ou le plus souvent crapuleuses. Des entreprises françaises en ont sévèrement pâti, comme Saint-Gobain en 2017 (NotPetya). Mais il existe aussi, semble-t-il, un banditisme d'État pratiqué par la Corée du Nord pour se procurer des devises.

138. – **La cyberintrusion, technique duale, peut servir pour le renseignement militaire comme pour l'espionnage commercial.** Et cela fait des décennies qu'elle est utilisée, même s'il y a par nature peu de publicité faite autour des succès remportés. Qu'on se rappelle seulement que les États-Unis ont à coup sûr écouté les communications téléphoniques de dirigeants étrangers alliés.

Le rapport du Sénat relève pour sa part que « depuis de nombreuses années (…) les pouvoirs russes sont accusés d'espionner les infrastructures critiques des pays

occidentaux en vue d'élargir l'arsenal des outils utilisés en cas d'attaque hybride ». L'entreprise de téléphonie canadienne Nortel a été victime dans les années 2000 d'un piratage massif d'origine chinoise visant à exploiter les secrets du colosse industriel pour créer des avantages au service de l'étoile montante des télécommunications chinoises : Huawei[4]. Une opération d'intrusion attribuée à la Chine, *Aurora*, a concerné en janvier 2010 Google et d'autres entreprises américaines. L'opération a utilisé une faille du navigateur Internet Explorer et conduit à un incident diplomatique entre la Chine et les États-Unis. Cette action, probablement destinée à imposer à Google une censure de ses activités en Chine, a amené la secrétaire d'État américaine à déclarer qu'« un nouveau rideau (de fer) est en train de s'abattre sur l'information dans une grande partie du monde ». Citons aussi, dans le domaine de l'espionnage politique, l'affaire de l'Union Africaine, à laquelle la Chine a offert un nouvel immeuble avec son système informatique clé en main. Celui-ci comportait une faille par des portes numériques dérobées donnant un accès discret à l'intégralité des échanges et des productions internes de l'organisation[5]. Dans le domaine civil, on n'a pas de preuve que *Facebook*, *Waze* ou *Zoom* servent à espionner leurs utilisateurs, mais qu'est-ce qui s'oppose à l'utilisation aux États-Unis, en Israël ou en Chine, d'informations librement données à ces plateformes ? Serait-ce même illégal ? Dans le cas américain, c'est même parfois une obligation depuis la promulgation du *Cloud Act*.

139. – Enjeu de domination économique, le cyberspace est *un far-west* très faiblement défendu par les uns, colonisé par les autres. La revue stratégique de défense et de sécurité nationale de 2017 (§ 135) le décrit ainsi :

> « Les États-Unis, la Chine et la Russie ont favorisé l'émergence de géants nationaux de l'Internet dans le cadre de stratégies globales de puissance et de souveraineté. La suprématie des États-Unis dans toutes les dimensions de l'espace numérique (matérielle, technologique, économique, juridique, politique et militaire) offre un contraste saisissant avec la situation des Européens, qui demeurent fortement dépendants de l'extérieur et dont les investissements comme les acteurs peinent à atteindre une taille critique. La Chine investit massivement dans l'Internet du futur, l'innovation et l'e-commerce et le développement d'une route de la soie numérique. Ce faisant, elle vise à assurer un contrôle souverain sur la partie de l'espace numérique qu'elle assimile à son territoire national et à étendre son influence au-delà. Imposant la localisation des données relatives à ses citoyens sur son territoire, la Russie investit massivement dans la construction de *data centers* dans une stratégie de maîtrise des données et de sécurité informationnelle ».

La domination économique mise en place est bien connue. Une formule la résume : « Si le service est gratuit, c'est que le produit, c'est vous ».

140. – Le cyberespace est un milieu favorable à l'influence politique, économique et culturelle. Il a d'ailleurs donné lieu à la création du métier d'influenceur. Permettant de s'adresser directement aux individus sans passer par le filtre d'institutions civiles, médiatiques, politiques ou religieuses, il permet de plus de les atteindre en grand nombre. Le *soft power* n'est pas une invention récente : les États-Unis en étaient conscients lorsqu'ils ont exigé après la guerre de contrôler l'industrie cinématographique allemande, mais il trouve dans le cyberespace des conditions

(4) J. Frémicourt, Y. Parent et H. Sall, *Les particularités du cyberespionnage chinois (2016-2018)*, EGE, 2018.
(5) J. Frémicourt, Y. Parent et H. Sall, *Les particularités du cyberespionnage chinois*, 2016-2018.

d'épanouissement exceptionnelles. Le *soft power* qui, utilisé par des régimes non démocratiques, devient un *sharp power*, peut ainsi tout aussi bien servir de propagateur des modes « politiquement correctes » américaines, de la propagande russe vers les milieux conservateurs ou pour la radicalisation en vue du *djihad* ou l'extension en Eurasie (voire *via* la 5G à l'ensemble du monde) de l'influence chinoise à travers des routes électroniques de la soie véhiculant sa vision du monde. Côté russe, on relèvera la création de l'« usine à trolls » destinée à diffuser la pensée officielle russe sur l'Internet. L'appétit que suscite le contrôle du cyberespace entraîne le risque de sa balkanisation. Ce serait effectivement dommage, mais pour rester dans les analogies géopolitiques, combien plus dangereuse sera sa finlandisation par des grandes puissances.

IV. – En France, la prise de conscience de l'enjeu et de la menace que représente le cyberespace ne date pas d'hier

141. – Une prise de conscience précoce. Déjà le rapport Nora-Minc sur l'informatisation de la société relevait les nombreux défis que l'informatisation poserait en termes de souveraineté, notamment du fait des banques de données nord-américaines, domaine où notre pays courait selon les auteurs « un risque d'aliénation »[(6)]. Nous étions en 1977 ! Un peu plus de quarante ans après, le risque s'est concrétisé. Le 1er octobre 2019, la commission d'enquête du Sénat sur la souveraineté numérique a rendu un rapport qui témoigne d'une prise de conscience salutaire. Il affirme un « devoir de souveraineté numérique » sans résignation ni naïveté. Inspiré par les travaux de Pierre Bellanger qui avait publié *La souveraineté numérique* en 2014[(7)], le rapport dresse un constat sans appel : la souveraineté de l'État est remise en cause par les géants du numérique, établis à l'étranger, fragilisant les monopoles régaliens (notamment en matière de défense, de fiscalité et de monnaie).

142. – Mais cette prise de conscience a ses limites. Il existe en effet un fort courant libéral (ou libertaire ?) en ce qui concerne l'usage de l'Internet, et de fortes réticences à le réglementer. Dans un article de 2017, Joseph Nye, professeur à Harvard, soutenait que la solution n'est pas la souveraineté numérique nationale[(8)] mais la gouvernance mondiale pour protéger les fonctions vitales d'Internet. Le bannissement du protectionnisme en matière de numérique permettrait selon lui d'éviter des cyberconflits et de conserver Internet comme un espace ouvert. Il serait effectivement beau d'avoir une gouvernance mondiale non partisane de l'Internet, mais on peut gager que lorsque cet objectif sera atteint, s'il l'est jamais, les pays européens auront définitivement perdu toute capacité à exister dans le cyberespace.

143. – D'autres, pour des raisons pratiques, jugent irréaliste une politique colbertiste en la matière. En mars dernier, l'économiste Bruno Alomar dénonçait

(6) Rapport sur l'informatisation de la société, 1977, p. 71.
(7) Stock, coll. « Essais-Documents ».
(8) Joseph Nye, *Maîtriser les cyberconflits*, Project Syndicate, 8 août 2017.

dans *Les Échos* une approche européenne de la souveraineté jugée « défensive et agressive »[9]. « L'Europe se condamne à ne pas comprendre les raisons des succès américains : esprit d'initiative, fiscalité avantageuse, liaison intelligente entre l'université et l'entreprise, financement du capital-risque, *etc.* ». Pour lui, l'approche *top-down* avec un État qui contrôle tout ne créerait pas un environnement optimal pour que des géants européens se développent. La création d'un environnement fiscal, universitaire et financier susceptible de favoriser le développement de grandes sociétés européennes est en effet éminemment souhaitable. Mais, même en cas de succès, que pèseraient ces entreprises face à leurs homologues américaines protégées par le *big stick* que le Gouvernement américain vient par exemple de ressortir pour défendre les privilèges fiscaux des très indépendantes GAFAM ?

144. – **La Chine n'a pas fait une bonne publicité à la notion de cyber-souveraineté.** Amnesty International affirmait sur son site en 2015 que « depuis 2014, le Gouvernement chinois essaie de plus en plus souvent d'imposer la notion de "cyber-souveraineté" dans le cadre de la gouvernance mondiale d'Internet ». Pour faire bonne mesure, Amnesty International ajoutait dans le texte précité : « Les gouvernements américain et britannique compromettent les libertés des internautes avec des programmes de surveillance de masse systématique menés par la NSA, l'Agence de sécurité nationale des États-Unis, et le GCHQ[10], le Quartier général des communications du Gouvernement britannique, qui portent atteinte au respect de la vie privée dans le monde entier. Les programmes de surveillance omniprésents de ces deux gouvernements, et le refus obstiné des autorités de les remanier en profondeur ont créé un précédent dangereux pour d'autres pays ».

145. – **Arme de grande efficacité face à laquelle l'angélisme n'est pas ou plus de mise, l'arme cyber crée une menace qui doit nous mobiliser.** En 1962, Raymond Aron écrivait dans *Paix et guerre entre les nations* : « À l'ombre de l'apocalypse thermonucléaire comme hier à l'ombre des divisions blindées ou avant-hier à l'ombre des légions ou des phalanges, hommes d'État et simples citoyens doivent agir selon la prudence, sans illusion ni espoir de sécurité absolue ». En matière de cyber, nous n'aurons pas non plus de sécurité absolue, mais retenons qu'il faut agir pour préserver au moins un peu de notre souveraineté.

V. – Au niveau international, nous pouvons agir politiquement, juridiquement, économiquement et, si nécessaire, militairement

A. – L'action politique et diplomatique est nécessaire, car il n'y a pas de souveraineté sans sécurité

146. – **La naissance d'une diplomatie numérique.** À cet égard, notre pays a mené une réflexion cohérente et rationnelle sur la cybersécurité et tient un discours extrêmement construit sur le sujet. On renverra en particulier au rapport transmis

(9) B. Alomar, *Ne sombrons pas, en Europe, dans le « nationalisme numérique » : Les Échos* 4 mars 2020.
(10) *Government Communications Headquarters* (quartier général des communications du gouvernement).

aux Nations unies au printemps 2020[11]. Outre son action au sein de l'ONU ou de l'UE, la France a mobilisé avec énergie les différents forums internationaux auxquels elle appartient, y compris le G7, l'OTAN et l'OSCE[12] et promeut activement la coopération internationale en matière de cybersécurité. Elle s'est dotée d'une « diplomatie numérique ». Dans la lignée de la stratégie internationale de la France pour le numérique, rendue publique le 15 décembre 2017, cette diplomatie numérique s'articule autour de quatre enjeux :

– garantir la sécurité internationale du cyberespace, à travers le renforcement de l'autonomie stratégique européenne et la promotion de la stabilité du cyberespace dans les instances internationales (*a*) et la régulation des contenus diffusés sur l'Internet ainsi que la régulation des plateformes (*b*) ;

– contribuer à la gouvernance de l'Internet en renforçant son caractère ouvert et diversifié, tout en renforçant la confiance dans son utilisation ;

– promouvoir les droits humains, les valeurs démocratiques et la langue française dans le monde numérique ;

– renforcer l'influence et l'attractivité des acteurs français du numérique.

Elle entend également promouvoir le *leadership* de la France et de l'Union européenne dans le développement et la maîtrise des technologies de rupture, notamment avec l'intelligence artificielle. Le problème est bien posé, mais cela suffit-il ? On a d'ailleurs vu qu'il l'était dès 1977. Notre pays est connu comme le « pays de la Déclaration des droits de l'homme », mais n'est-il pas aussi parfois le « pays de la déclaration » ? Quels sont nos moyens pour transformer des déclarations de principe en actions au-delà de l'effort nécessaire que nous faisons pour convaincre les autres pays ? On peut en citer trois : le droit, l'investissement, l'action militaire.

B. – Le droit international existant suffit-il ?

147. – L'initiative du Conseil de l'Europe. Il existe un droit international, notamment la convention du Conseil de l'Europe sur la cybercriminalité conclue le 23 novembre 2001. Celle-ci a principalement pour objet d'obliger les États parties à créer des incriminations pour certains actes de cybercriminalité. Il est intéressant de noter qu'elle a été ratifiée par tous les États membres de l'UE, avec souvent des réserves, mais pas par l'Irlande ni la Suède. La Russie, qui est membre du Conseil de l'Europe, ne l'a pas ratifiée. Les États-Unis, qui ne sont pas membres du Conseil de l'Europe, y ont en revanche adhéré, avec de nombreuses réserves qui portent notamment sur les questions de territorialité. Le Conseil de l'Europe a publié en juillet 2020 un bilan de mise en œuvre de la convention dont il ressort qu'elle a stimulé l'incrimination des actions cyber malveillantes et la coopération judiciaire entre États ainsi que la capacité des systèmes judiciaires à aborder ce sujet.

148. – La réticence française. Faut-il aller au-delà ? Dans le rapport fait à l'ONU au printemps 2020, la France a répondu par la négative, estimant que les

(11) Réponse de la France à la résolution 74/28 de l'Assemblée générale des Nations unies : « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale ».
(12) Organisation pour la sécurité et la coopération en Europe.

instruments existants suffisaient à ce stade[13]. Cette frugalité juridique a de bonnes raisons. Tant qu'il existe des dispositions de droit international permettant d'appréhender une situation nouvelle née de l'évolution technologique, il est tentant de s'y rattacher. C'est par exemple ce qu'a fait la France pour justifier la mise en place d'une capacité de riposte à une agression dont serait victime un de ses satellites, que nos juristes considèrent comme une agression armée au sens de l'article 51 de la charte des Nations unies.

149. – La pertinence du parallèle avec le droit de la mer. Mais notre analyse n'est pas partagée par tous et s'il fallait un jour un droit du cyberespace, il s'inspirerait sans doute du droit de la mer, dont on a relevé en introduction les ressemblances avec le cyberespace. Le droit de la mer a d'ailleurs déjà inspiré celui d'espaces nouveaux : le Traité sur l'Antarctique de 1959, puis celui sur l'espace extra-atmosphérique, dont les analogies avec l'espace cybernétique sont également nombreuses. Les dispositions de ces traités portent principalement sur la non-appropriation, la liberté de circulation ou d'utilisation et le non-placement d'armes. Le Traité sur l'espace, négocié en 1966, est entré en vigueur dès 1967. On ne saurait sans doute pas aller aussi vite aujourd'hui, ni surtout parvenir à négocier un traité, c'est-à-dire du droit dur, sur un sujet aussi vaste. C'est en quelque sorte la guerre froide qui a rendu la chose possible en obligeant les États-Unis et l'URSS à négocier pour prévenir une escalade militaire dans l'espace. Mais est-on arrivé à un point ou la concurrence internationale imposerait un accord sur le cyber, surtout dans un jeu à trois ? Ou faudra-t-il attendre que les « nouvelles routes de la soie » aient créé un Yalta numérique ?

150. – Le problème des institutions privées de gouvernance. Dans le domaine de la négociation multilatérale, la France occupe une position supérieure à celle que lui donnerait son seul poids économique. Les résolutions adoptées par le Conseil de sécurité sont par exemple aux trois quarts d'origine française ou franco-britannique. Notre pays est en revanche moins à l'aise dans les instances privées qui régissent l'Internet.

C. – En matière d'action économique, la pandémie de Covid-19 a donné un nouvel élan au volontarisme industriel des autorités françaises

151. – Les prémices. Déjà le 3 octobre 2019, le ministre de l'Économie et des Finances, Bruno Le Maire, avait annoncé une collaboration entre l'État et les sociétés

(13) La France considère que l'émergence d'un cadre de cybersécurité collective ne pourra reposer que sur le respect des règles existantes du droit international. La France estime ainsi que la création d'un nouvel instrument international juridiquement contraignant spécifique aux enjeux de cybersécurité n'est pas nécessaire à ce stade. Dans le cyberespace comme dans les autres domaines, le droit international existant s'applique et doit être respecté.
Ainsi que le groupe des experts gouvernementaux de l'ONU (GGE) a pu le conclure dans son rapport publié en 2013, les principes et règles de droit international s'appliquent aux comportements des États dans le cyberespace. Si le cyberespace présente des spécificités propres (anonymat, rôle des acteurs privés), le droit international offre bien les moyens nécessaires pour encadrer de manière responsable le comportement des États dans cet environnement.
Le principe de souveraineté s'applique au cyberespace. À ce titre, la France réaffirme qu'elle exerce sa souveraineté sur les systèmes d'information, les personnes et les activités cyber sur son territoire ou relevant de sa juridiction, dans les limites de ses obligations découlant du droit international. La pénétration non autorisée de systèmes français qui entraînerait la production d'effets sur le territoire français *via* des moyens cyberoffensifs par une entité étatique ou des acteurs non étatiques agissant sous les instructions ou le contrôle d'un État pourrait constituer une violation de souveraineté.

Dassault Systèmes et OVH « pour élaborer des plans visant à briser la domination des entreprises américaines en matière de *cloud computing* », en précisant que le « projet serait réalisé au niveau franco-allemand dans un premier temps, éventuellement au niveau européen ultérieurement », renouant ainsi avec une politique volontariste, qui, dans les années 1970, avait permis à l'Europe de résister à la suprématie américaine et russe en matière spatiale et aéronautique (Agence spatiale européenne, Airbus…). Traduire cette ambition dans les faits suppose d'importants investissements qui ne seront soutenus par l'opinion que si celle-ci comprend les réels risques d'une domination technologique étrangère : l'asservissement de nos économies et, à la clé, de nos libertés. Cela n'est pas acquis : beaucoup de gens, qui ont peur, à tort ou à raison, d'être espionnés par l'État, ne craignent apparemment pas de l'être par des entreprises privées ou des États étrangers.

152. – **La pandémie de Covid-19 a fait évoluer les mentalités et la souveraineté n'est plus un gros mot.** On lit notamment en exergue du volet du plan de relance consacré à la compétitivité : « La relance est la clé de la souveraineté économique et de l'indépendance technologique ». Aussi le plan de relance prévoit-il de consacrer 3,7 milliards d'euros au développement des *startups* et de la souveraineté technologique française, « afin d'accélérer le développement de l'écosystème numérique de la *French Tech* et de faire émerger des champions numériques français ».

D. – La nécessité de pouvoir agir militairement s'est imposée

153. – **Un renseignement national autonome est une condition de la souveraineté.** L'action militaire exige en effet d'abord une bonne information. Or le cybercrime a cela de commun avec le terrorisme et la prolifération que l'attribution est difficile, mais essentielle. Il est donc impératif de disposer de renseignement national autonome, sauf à reposer sur celui d'alliés qui peuvent ne pas être totalement transparents (rappelons combien il a été important pour la France d'avoir eu en 2003 un renseignement autonome sur les activités nucléaires de l'Irak). C'est d'ailleurs l'un des objectifs du Livre blanc de 2013 : « La capacité de se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs est devenue un des éléments de la souveraineté nationale ».

154. – **La France considère qu'une cyberattaque grave est une agression armée.** Elle soutient que le droit international s'applique au cyberespace en cas d'agression, avec les conséquences internationales qui en résultent. La stratégie internationale de la France pour le numérique de 2017 appelle les États à reconnaître la possibilité de saisine du Conseil de sécurité des Nations unies en cas de cyberattaque grave, celle de prendre des mesures techniques « nécessaires et proportionnées » et, en cas de cyberattaque visant une infrastructure critique et ayant des effets particulièrement graves, celle de la considérer comme une agression armée au sens de la charte des Nations unies, dont l'article 51 affirme le droit à la légitime défense. Mais, comme le relève par ailleurs la *Revue stratégique de défense et de sécurité nationale* de 2017, cette analyse n'est pas universellement partagée :

« Enfin, la fréquence, l'ampleur et la sophistication technologique des agressions augmentent sans cesse dans l'espace numérique, où les États se livrent à des affrontements constants, qui pourraient

à l'avenir relever du seuil de l'emploi de la force ou de l'agression armée, avec des conséquences collatérales potentielles pour les acteurs privés. **Si le principe de l'applicabilité du droit international à l'espace numérique et aux cyber-opérations, défendu par la France, fait l'objet d'un consensus croissant, certains États continuent de s'y opposer**. Par ailleurs, la question de ses modalités d'application et surtout du contrôle de leur mise en œuvre reste ouverte »[14].

155. – La nécessité de pouvoir conduire une action militaire dans le cyberespace est désormais admise. Le Livre blanc prévoyait dès 2013 « une capacité de réponse gouvernementale (…) sans s'interdire l'emploi gradué de moyens relevant du ministère de la Défense, si les intérêts stratégiques nationaux étaient menacés ». Depuis lors, la *Revue stratégique de cyberdéfense* présentée en février 2018 a défini une doctrine de gestion de crise cyber et clarifié les objectifs stratégiques nationaux de cyberdéfense. Elle prévoit notamment « le découragement des attaques par un ensemble de mesures de nature défensive, de résilience renforcée ainsi que de capacités de réaction et de réponse ». On y lit aussi que « l'arme cyber est un outil qui peut être particulièrement sélectif et dont les effets peuvent être réversibles. Utilisées pour garantir la supériorité dans le cyberespace, les capacités cyber permettent aussi aux armées de mener leurs opérations traditionnelles de manière plus efficace et moins coûteuse. La France a déjà investi dans ce domaine et la capacité cyber est désormais intégrée à toutes les opérations militaires ». Un commandement de la cyberdéfense a été créé en 2017 au ministère des Armées et la loi de programmation militaire 2019-2025 prévoit une augmentation significative des moyens alloués à la cyberdéfense avec un objectif de recrutement de 1 500 personnes supplémentaires, visant à porter à 4 000 le nombre de personnels affectés à ces enjeux au sein du ministère des Armées à l'horizon 2025.

E. – Quelques jalons

156. – Pour conclure, quelques jalons pour des propositions visant à défendre notre cybersouveraineté.

157. – Les États sont pertinents en matière de cybersouveraineté. Ce sont en effet les seuls sujets de droit international ; ils ont un pouvoir normatif interne et le monopole de la violence légale. Certains ont d'ailleurs pris des mesures nationales. Ce ne sont certes pas tous des démocraties, mais c'est possible. Ils posent *a contrario* une question terrible : la souveraineté numérique est-elle compatible avec la démocratie et le libéralisme économique ? C'est un faux dilemme dans lequel il ne faut pas se laisser enfermer. Même le très libéral droit européen reconnaît aux États membres de l'Union européenne le droit de limiter les échanges pour des raisons, entre autres, de sécurité publique[15]. Mais cela peut être inconfortable et coûteux et il vaut mieux ne pas être seul.

(14) *Revue stratégique de défense et de sécurité nationale* 2017, § 136, p. 47 (www.vie-publique.fr/sites/default/files/rapport/pdf/174000744.pdf).

(15) TFUE, art. 36 : « Les dispositions des articles 34 et 35 ne font pas obstacle aux interdictions ou restrictions d'importation, d'exportation ou de transit, justifiées par des raisons de moralité publique, d'ordre public, de sécurité publique, de protection de la santé et de la vie des personnes et des animaux ou de préservation des végétaux, de protection des trésors nationaux ayant une valeur artistique, historique ou archéologique ou de protection de la propriété industrielle et commerciale. Toutefois, ces interdictions ou restrictions ne doivent constituer ni un moyen de discrimination arbitraire ni une restriction déguisée dans le commerce entre les États membres ».

158. – Le territoire est essentiel. Le cyberespace est généralement ressenti comme une entité hors-sol et insaisissable. Mais il comporte une première couche matérielle qui doit donc être quelque part. Ce sera en général sur un territoire, sauf à imaginer un placement dans l'espace, qui serait alors vulnérable. Or, qui dit territoire dit souveraineté sur ce territoire d'un État qui peut, dans certaines conditions, soumettre ces équipements à ses pouvoirs normatifs et de contrainte. L'enquête sur une escroquerie informatique est ainsi en principe beaucoup plus simple si le serveur qui a acheminé le message est en France. Notons aussi que la convention de Budapest comporte un article 18 sur l'injonction de produire qui repose sur la compétence territoriale(16).

Le « groupe d'experts gouvernementaux » des Nations unies (GGE) a pour sa part édicté une norme qui pose la responsabilité de l'État en cas d'utilisation malveillante de son territoire : « Norme c – Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications ». On mesure l'importance de cette norme qui responsabilise l'État dont part géographiquement l'agression, que celle-ci soit effectuée sous son contrôle ou non. Illustrant l'importance du territoire, le rapport du Sénat relève que la politique russe de contrôle du cyberespace repose notamment sur l'obligation de stocker en Russie les données concernant les citoyens russes(17). La Chine interdit pour sa part aux entreprises étrangères de transférer leurs données électroniques vers leur siège national(18). À l'inverse, les États-Unis ont une « politique de la donnée basée sur une extraterritorialité juridique agressive ». Le *Cloud Act* facilite l'obtention par l'administration américaine de données stockées ou transitant à l'étranger, *via* notamment les opérateurs et fournisseurs de services en ligne américains(19). Si les intentions russes en matière de cybersurveillance ne sont vraisemblablement pas pures, cela n'implique pas que la méthode qu'est la localisation obligatoire de données sur le territoire russe soit en quelque manière condamnable. Serait-il « mal » d'imposer cette contrainte en France ? Sans doute pas, et nous l'avions d'ailleurs fait il y a une vingtaine d'années pour le *BlackBerry*, dont les serveurs étaient au Canada et au Royaume-Uni. Sous la pression des autorités françaises, *BlackBerry* avait fini par installer un serveur en France mais avait cru bon de le piéger.

159. – Le laisser-faire est, hélas, une option. La défense de la souveraineté, c'est cher et difficile et il serait en apparence plus simple de vivre tranquillement sous la protection d'une puissance dominante dans une sorte de nouveau pacte colonial où nous donnerions cette matière première que sont nos données en

(16) « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner : a. à une personne présente **sur son territoire** de communiquer les données informatiques spécifiées, en la possession où sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique ; et b. à un fournisseur de services offrant des prestations **sur le territoire de la Partie**, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services ».

(17) Sénat, Rapport cité, p. 26.

(18) *Ibid.*, p. 21.

(19) *Ibid.*, p. 20.

contrepartie de l'accès, exclusif, à ces marchandises de la nouvelle métropole numérique que sont les services. Les États-Unis et la Chine se seront partagé le monde et chacun vivra tranquille dans sa partie du Yalta numérique. À condition, bien sûr, que les frontières soient claires et stables. Mais où s'arrête l'Eurasie des « nouvelles routes de la soie » ? Peut-être dans la partie orientale de l'Union européenne ?

Comme à l'époque de la guerre froide, une forme de pacifisme ou de finlandisation pourra tenter une partie de l'opinion et, très sûrement, celle d'autres États membres de l'Union européenne qui, rappelons-le, compte aujourd'hui cinq États neutres. Plus que jamais, la formule de Sun Tzu est d'actualité : « La guerre peut être gagnée sans combattre, grâce à l'anéantissement de la volonté de se battre chez l'adversaire ».

160. – **L'Union européenne ne pourra pas nous défendre avant longtemps.** Elle ne sait pas le faire pour les frontières. Comment le ferait-elle sur un sujet aussi compliqué et dont les enjeux économiques sont tels ? On l'a vu lors de la pandémie : certains États de l'Union (pas la France) ont été prêts à vendre à un des GAFAM les données de santé de leurs citoyens relatives à la Covid-19. Il faut donc éviter le piège du slogan : « Nous sommes faibles parce qu'il n'y a pas assez d'Europe ». N'attendons pas qu'elle puisse nous défendre : il sera trop tard !

161. – **L'Union européenne peut néanmoins nous aider.** Elle le peut avec ce dont elle dispose aujourd'hui : profondeur stratégique, poids international, grand marché, compétence commerciale, puissance technologique et économique.

Elle dispose aussi d'une compétence normative qui peut être suscitée à bon escient. Même si le résultat est imparfait, l'expérience du règlement européen sur la protection des données illustre cette capacité. D'autres pans de la compétence communautaire pourraient être utilement mobilisés : la politique de protection des consommateurs, les négociations internationales sur les échanges de biens et de services ou le règlement sur le contrôle des concentrations.

Enfin, la coopération européenne, dans le cadre de l'Union ou pas, peut être un formidable levier pour des grands projets technologiques. Rappelons que **tous les grands projets technologiques européens, notamment ceux motivés par le souci d'indépendance, sont d'origine française :** Airbus, Ariane, ITER, Galileo.

162. – **Comment avoir une approche colbertiste adaptée à notre époque ?** Comment l'avoir sans création d'arsenal ou de manufacture en sachant que des expériences antérieures visant à l'émergence de « champions » ont été un échec, par exemple le projet *Andromède* de *cloud* souverain ? Comment utiliser, comme le fait si bien Israël, l'extraordinaire créativité de nos *startups* sans voir le fruit de leurs efforts partir à l'étranger ? Que devons-nous faire nous-mêmes en utilisant les succès des autres ? La Chine n'a-t-elle pas bâti sa politique numérique en utilisant les outils fournis par la technologie américaine, réactualisant la formule de Lénine qui prophétisait que « les capitalistes nous vendront la corde avec laquelle nous les pendrons » ? Et, *last but not least*, comment protéger nos investissements en ce domaine par une politique commerciale ajustée, politique commerciale dont nous avons transféré la compétence exclusive à l'Union européenne depuis le traité de

Rome ? Nous ne **pouvons pas tout faire.** Nous savons que nous ne pourrons pas tout faire ni tout contrôler. Les points sur lesquels l'effort de recherche et d'investissement devra porter doivent donc être sélectionnés attentivement. Parmi ceux-ci, les capacités de **détection** sont importantes. À l'image du statut que nous a donné le satellite *Graves* dans le domaine spatial, nous devons **disposer des outils nous permettant de rester dans le premier cercle des nations dans le domaine de la surveillance et de l'attribution cyber**. Les équipements de sécurité constituent une autre priorité. À cet égard, le développement d'un pare-feu entièrement national pourrait être envisagé. Nous devrions rendre obligatoire le stockage en France de données à définir concernant notamment ses citoyens, entreprises, administrations, services de santé et institutions de recherche. Enfin, et comme le relève la stratégie nationale pour le numérique, il est indispensable **de préserver un droit à réguler suffisant**, dans le cadre des négociations commerciales internationales notamment.

SECTION 2

LA CONCURRENCE DES ÉTATS AVEC LES OPÉRATEURS PRIVÉS

163. – Une souveraineté numérique malmenée. La souveraineté est sérieusement mise à mal dans le domaine du numérique avec le développement tentaculaire des géants de l'Internet désormais appelés GAFAM (Google, Apple, Facebook, Amazon et Microsoft) qui se sont vite accaparé le marché du numérique au niveau européen. Depuis le début de la pandémie de Covid-19, le débat sur la souveraineté s'est amplifié car les États ont perçu qu'ils dépendent de plus en plus d'autres pays pour leurs besoins vitaux.

I. – Des entreprises accaparant des domaines économiques régaliens

A. – Le constat

164. – Une prise de pouvoir. Les GAFAM, depuis une vingtaine d'années, ont progressivement pris le pouvoir dans le cyberespace au détriment des États qui, au nom de leurs compétences régaliennes, auraient dû davantage s'investir dans cet espace numérique.

Des groupes américains (GAFAM ou NATU – Netflix, Airbnb, Tesla, Uber) mais aussi chinois (BHATX-Baidu, Huawei, Alibaba, Tencent, Xiaomi) ou russes comme le moteur de recherches Yandex, se sont accaparées des parts de marché en captant des données numériques, ce qui leur donne un pouvoir supérieur aux États. Ils définissent leurs propres lois, à savoir leurs conditions générales, exploitent les données personnelles, confiées ou laissées à leur insu par les utilisateurs, dont l'agrégation forme le *big data*, véritable « or noir du XXIe siècle ».

165. – Une nouvelle colonisation. Face à ce constat, on évoque même une colonisation nouvelle[20] de l'Europe par ces puissantes entreprises. C'est dans ce contexte qu'a surgi la notion de souveraineté numérique, qui correspond à une réaction des États face cette hégémonie en particulier des GAFAM, avec notamment une supériorité en matière de ressources Internet et d'applications numériques. La question est devenue majeure suite à l'affaire *Snowden* qui a révélé l'espionnage des États-Unis à des fins économiques et politiques.

166. – Des stratégies offensives. On constate ainsi que les GAFAM ou leurs équivalents chinois, les BHATX, mènent depuis plusieurs années des stratégies offensives dans les domaines de l'intelligence artificielle, de l'analyse des données, de la robotique et d'autres branches du numérique.

167. – La question du télétravail. Un autre exemple est l'explosion du télétravail qui n'a été possible qu'en utilisant des logiciels quasi exclusivement américains : Microsoft, Google, Facebook, Zoom… qui ont atteint des records de fréquentation avec leurs plateformes. Ces nouveaux usages numériques posent d'évidents problèmes de souveraineté numérique et de confidentialité des données des entreprises et de l'État. La France et l'Europe, qui n'ont pas su faire émerger de géants du numérique, ont tout intérêt à favoriser le développement d'alternatives. Enfin, l'une des clés de cette révolution du télétravail réside dans la capacité d'avoir des réseaux performants, en ville comme dans les zones rurales, afin que le télétravail soit accessible à tous.

168. – Normalisation. En outre, la normalisation des usages numériques est souvent confiée à des acteurs privés, des organismes, 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'intérêt, ne sont pas 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.

La Compagnie des Indes est un précédent historique éclairant. Comme l'a montré Édouard Geffray[21], la comparaison entre Internet et l'espace maritime est un parallèle fécond. Dès lors, il est possible et instructif de tirer les enseignements de l'exemple historique de la Compagnie des Indes, dont la suprématie lui a permis de venir rivaliser avec les États de l'époque.

B. – Solutions pour restaurer la souveraineté numérique

169. – Hébergement des données en Europe. Il s'agit de faire en sorte que certaines données numériques des entreprises ou des individus soient hébergées dans leur pays d'origine et qu'elles soient soumises aux lois de ce même pays. Cet enjeu fut mis en évidence en 1978 grâce à la création de la Commission nationale de l'informatique et des libertés (CNIL).

(20) Catherine Morin Desailly utilise la même image (*L'Union européenne, colonie du monde numérique ?*, Commission des affaires européennes du Sénat, Rapport d'information n° 443, 2013).

(21) Ancien secrétaire général de la CNIL. Il est actuellement directeur général des ressources humaines des ministères de l'Éducation nationale et de l'Enseignement supérieur.

170. – **Création d'une réglementation protectrice.** La transformation numérique, dès les années 1990, fut l'occasion de créer de nouveaux cadres juridiques européens, tels que la directive sur la protection des données personnelles de 1995 et le règlement général sur la protection des données (RGPD) en 2016. Ce dernier interdit la fuite des données à caractère personnel hors de l'Union européenne, et c'est l'une des principales briques de compréhension de la souveraineté des données. Au niveau de l'Union européenne, aucune décision n'a été prise en ce qui concerne la mise à l'écart de Huawei même si quelques inquiétudes se manifestent de la part du vice-président de la Commission européenne, chargé du marché unique numérique. Chaque État de l'Union européenne est laissé libre de prendre une décision sur le sujet et les États européens semblent laisser la main aux grands opérateurs de télécommunication.

171. – **Renforcer les capacités de l'UE.** L'Union européenne doit se donner les moyens de développer son autonomie et son *leadership* en matière de numérique. Pour l'ANSSI, la souveraineté de l'Europe nécessite des efforts renouvelés en matière de développement capacitaire, de réglementation, de politique industrielle, ainsi qu'une gouvernance adaptée aux enjeux. Le renforcement des capacités de l'UE est impératif au sein des administrations des États membres, mais également aux niveaux du tissu économique, des citoyens et des institutions européennes elles-mêmes.

En outre, l'élévation du niveau de sécurité de l'espace numérique européen suppose une prise en compte des risques associés aux technologies et usages innovants dans les politiques publiques européennes sectorielles.

172. – **Exemple de mesures prises par les États-Unis.** Aux États-Unis, après avoir restreint le marché à Huawei en janvier 2018 pour des raisons de proximité de l'entreprise avec les services de renseignement chinois, les USA ont également demandé à leurs opérateurs télécoms d'exclure cette entreprise du territoire américain sur les technologies 5G. Les États-Unis s'étaient déjà opposés en 2007 au rachat du fabricant d'équipements réseaux 3Com par Huawei et BainCapital pour des raisons de sécurité nationale, face aux menaces de cyberespionnage.

173. – **La position française.** En France, la position adoptée par l'État est nettement moins catégorique que celle des États-Unis, et Huawei reste le bienvenu dans le pays. En effet, premier groupe chinois en France, présent depuis dix-huit ans, il vient d'ouvrir son cinquième centre de R&D à Grenoble. Le 14 décembre 2021, Huawei France recrute son directeur commercial chez Hewlett-Packard. L'État est très vigilant face à cet entrisme au sujet de la 5G dont le réel déploiement ne se ferait pas avant 2025. Cela reste un sujet très sensible touchant à la sécurité nationale notamment à proximité des principaux lieux de pouvoir. Au plus haut niveau de l'État, pour contrer Huawei, une surveillance discrète est opérée de manière confidentielle avec le dispositif Cerbère, et ce depuis 2015 mais repris et intensifié en 2018 sous l'égide du Secrétariat général de l'Élysée en collaboration étroite avec Bercy et six ministères. Le gouvernement a donc, entre négociation et surveillance discrète, défini les axes sur lesquels Huawei était autorisé à candidater et ceux où il n'était pas attendu. La France semble avoir opté pour une stratégie de

vigilance à l'égard des investisseurs et opérateurs en télécommunication. Il n'y a donc pas d'opposition directe vis-à-vis de Huawei, mais plutôt une volonté d'intervenir ponctuellement en exerçant des pressions pour que les opérateurs écartent Huawei des marchés sensibles.

174. – Stratégie de relance en France. Le plan France Relance[22], présenté par le gouvernement le 3 septembre 2020, comporte certes un chapitre complet dédié à la souveraineté numérique et un autre à la mise à niveau numérique de l'État, des territoires et des entreprises. Cela s'apparente à un tournant à 180 degrés de la part d'un gouvernement qui définit le retour à la souveraineté comme une condition de survie de l'économie française.

175. – Des monnaies numériques privées. Les cryptoactifs se définissent par leur caractère privé, totalement virtuel et par leur absence d'adossement physique ou financier. Il en existerait près de 1 600 aujourd'hui pour une capitalisation estimée à près de 270 milliards de dollars. Il existe une forte ambivalence sur les cryptoactifs : une attirance forte pour les innovations proposées mais un souci constant de protéger les investisseurs, les consommateurs et la stabilité du système financier.

L'émission d'une monnaie est une attribution centrale d'un État souverain et n'est pas du ressort d'une entreprise privée. Les cryptoactifs peuvent s'avérer, dans l'usage qui en est fait, positifs ou menaçants, en particulier si l'État souverain ne s'en empare pas de façon pertinente. Il risque alors de se voir concurrencé et finalement dépassé par des acteurs privés, sur lesquels la force de sa régulation pourrait se trouver amoindrie.

176. – L'exemple de Libra. De multiples cryptoactifs ont vu le jour ou sont en projet, comme par exemple Libra qui a pour objectif de créer une cryptomonnaie initiée par Facebook que rejoint, à l'origine, un consortium de vingt-huit grandes entreprises et ONG. Il est convenu que la monnaie sera gérée par une fondation sans but lucratif dont Facebook ne sera qu'une des organisations cofondatrices.

La France, l'Allemagne, l'Italie et les Pays-Bas ont appelé la Commission européenne à réguler les cryptomonnaies adossées à des actifs afin de protéger les consommateurs et de préserver la souveraineté des États dans leur politique monétaire.

Le Sénat, dans un rapport récent[23], préconise d'imposer à tous les acteurs impliqués dans l'émission et l'échange des cryptoactifs les réglementations auxquelles sont aujourd'hui soumises les institutions financières traditionnelles (licence bancaire, lutte contre le blanchiment des capitaux et le financement du terrorisme, accompagnement des investisseurs…). Il encourage les banques centrales nationales et la Banque centrale européenne à accélérer leurs efforts de recherche sur le déploiement d'une cryptomonnaie banque centrale, qui présenterait tous les avantages des cryptoactifs privés, tout en étant garantie par la puissance publique.

(22) www.gouvernement.fr.
(23) Rapport « Le devoir de souveraineté numérique » (www.senat.fr/rap/r19-007-1/r19-007-15.html).

177. – Offensive face au Libra. En réaction à l'annonce du projet Libra[24] de Facebook, qui inquiète légitimement les organismes monétaires officiels, la déclaration finale de la réunion du G7 des 17 et 18 juillet 2020 indique que : « Les *stablecoins* et les divers autres produits en cours de développement, dont des projets ayant potentiellement une portée globale et systémique comme Libra, soulèvent de sérieuses inquiétudes systémiques et de réglementation, qui doivent tous être traités avant que ces projets puissent être mis en œuvre ». Ainsi, pour pouvoir se lancer, le système de paiement fonctionnerait avec plusieurs devises numériques, dont l'euro. Les ministres des Finances des cinq pays ont déclaré que les *stablecoins* ne devraient pas être autorisés dans les vingt-sept États membres de l'Union tant qu'un texte les régulant ne sera pas adopté. La Commission européenne devrait présenter ses propositions prochainement.

II. – L'inadaptation du droit de la concurrence français et communautaire

178. – Problématique. L'essor de plateformes numériques d'envergure mondiale, le développement de nouveaux services fondés sur les technologies numériques (algorithmes, *cloud*, intelligence artificielle, *blockchain*), la disruption de certains secteurs de l'économie traditionnelle par de nouveaux types d'opérateurs (vente en ligne pour le commerce physique, plateformes de réservation en ligne ou de partage pour l'hôtellerie…) confrontent les autorités à de nouveaux défis dans la mise en œuvre du droit de la concurrence. Le pouvoir de marché considérable acquis par certains acteurs, fondé, selon les cas, sur leur expertise technologique, l'importance des effets de réseau, la collecte massive de données ou les économies d'échelle dont ils bénéficient, ainsi que les conséquences, parfois destructrices, des pratiques anticoncurrentielles mises en œuvre, ont conduit les autorités de concurrence à mener une réflexion approfondie sur la mise à jour de leur grille d'analyse, de leurs méthodes et des outils à leur disposition.

179. – Un droit plastique. Il convient de rappeler que l'Autorité de la concurrence constitue une instance particulièrement efficace pour maintenir la dynamique concurrentielle de l'économie numérique. Le droit de la concurrence est un droit plastique dont les concepts peuvent s'adapter à de nouvelles pratiques, sans nécessiter d'intervention du législateur. Les autorités de concurrence s'attachent, par une pratique innovante, à traiter de façon effective les problématiques posées par l'économie numérique, et à faire évoluer leur analyse à droit constant. Il n'en demeure pas moins que certaines règles pourraient être adaptées, à l'instar des projets « DMA » (proposition de règlement « relatif aux marchés contestables et équitables dans le secteur numérique », *Digital Market Act* [DMA]) et « DSA » (proposition de règlement « relatif à un marché intérieur des services numériques », *Digital Services Act* [DSA]), ainsi que de la proposition de réforme du contrôle des concentrations exposée plus loin dans la présente étude.

(24) https://libra.org/fr-FR.

SECTION 3

L'INDIFFÉRENCE ET L'IGNORANCE CITOYENNES

180. – Comment expliquer ce qui semble être une forme d'indifférence citoyenne à l'égard de la dimension numérique de la souveraineté ? Pour en saisir la réalité, deux points seront successivement abordés. Premièrement, il faut identifier pour ce sujet ce que l'on pourrait nommer la dimension « nationale » ou « populaire » de la souveraineté numérique, ce qui permet de compléter la caractérisation de cette dernière – si tant est que la notion de souveraineté se donne à penser de manière indissociable, au fil de son histoire, à la fois comme institutionnelle, nationale et populaire (V. *infra*, n^os^ 181 et s.). Deuxièmement, il convient de prendre la mesure des formes d'indifférence citoyenne et d'identifier le phénomène résiduel dit « de l'illectronisme » (V. *infra*, n^os^ 184 et s.). Dans un troisième temps, on mettra en exergue les efforts de la puissance publique pour remédier à ces difficultés (V. *infra*, n^os^ 190 et s.), ce qui conduit à l'hypothèse de repenser la souveraineté à partir des pratiques numériques (V. *infra*, n^os^ 195 et s.).

I. – Souveraineté institutionnelle, souveraineté populaire, souveraineté nationale

181. – Souveraineté populaire et souveraineté nationale. Tandis que la notion de souveraineté génériquement entendue renvoie à l'autorité de l'État et de l'Administration, ces deux autorités constituées, la **souveraineté populaire** concerne le peuple, qui, *via* son consentement, représente leur force constituante[(25)]. La notion de **souveraineté nationale** 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[(26)], 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[(27)]. Qu'elle soit appréhendée comme une communauté d'affects sensibles exprimés à travers l'attachement patriotique fondateur des révolutions modernes[(28)] ou comme une « communauté imaginaire » cimentant une appartenance collective fantasmée[(29)], 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 démocratique pour la dimension institutionnelle de la souveraineté.

(25) L. Jaume, *Le Discours jacobin et la démocratie*, Paris, Fayard, 1989.
(26) E.-J. Sieyès, *Qu'est-ce que le Tiers-État ?*, 1789, préf. J. Tulard, Paris, PUF, 1982.
(27) V. pour la conception « allemande » de la souveraineté de la nation en Allemagne : J. Gottlieb Fichte, *Discours à la Nation allemande*, 1807, trad. A. Renaut, Paris, Imprimerie nationale, 1992. Pour la conception « française » : E. Renan, *Qu'est-ce qu'une nation ?*, 1887, présentation R. Girardet, Paris, Imprimerie nationale, 1995.
(28) P. Raynaud, *Trois Révolutions de la liberté : Angleterre, États-Unis, France*, Paris, PUF, 2009.
(29) B. Anderson, *L'imaginaire national : réflexions sur l'origine et l'essor du nationalisme*, 1991, trad. P.-E. Dauzat, Paris, éd. La Découverte, 2002.

En d'autres termes, l'angle de vue adopté ici permet de pousser la métaphore entre la souveraineté politique et la souveraineté numérique jusqu'à son terme, ce qui offre le moyen de jauger de la pertinence de l'analogie. Cela offre en effet le moyen de répondre à ces questions : la notion de souveraineté numérique permet-elle de penser l'autonomie nationale entendue comme pouvoir constituant ? Si tel n'est pas le cas, de quelle nature est le pouvoir constituant du peuple numérique ? Est-ce que l'apparition des GAFAM et BHATX ne met pas radicalement et définitivement à mal la notion de nation et par conséquent celle de souveraineté nationale ?

182. – **La notion de souveraineté numérique.** Le problème est que la théorie classique de souveraineté reposait sur la notion d'autonomie de l'État telle que la doctrine de droit public l'avait conçue, inspirée par les philosophes classiques (Spinoza, Grotius) et par les expériences du pouvoir constituant, théorisées par les Pères fondateurs américains puis par les Constituants français. Or, les formes matérielles du pouvoir numérique d'aujourd'hui ne permettent pas une telle autonomie. Le cyberespace s'est même constitué sur une double fable antagoniste, celle de la puissance émancipatrice du marché et de l'essor du transnational. À l'origine d'Internet, l'utopie de la libre circulation de l'information, développée par exemple par John Perry Barlow dans le contexte de la culture *hippie*, a ouvert la voie à une posture libertaire et libertarienne érigeant la communauté des usagers contre le droit des États-nations, ainsi qu'on le peut le lire dans la *Déclaration d'indépendance du cyberespace* (1996). L'extraterritorialité de l'espace numérique apparaît fondatrice et fondamentale du point de vue de ce texte, qui vante une sorte d'autorégulation selon l'éthique de la réciprocité avec les libres contributions de chacun. De ce fait, la notion d'une souveraineté numérique semble un pur et simple oxymore.

À l'origine d'Internet, les citoyens ont vu dans le web un espace de jeux et de partages, dans une vision qui, avec le recul, peut sembler naïve. Dans le même temps, des acteurs économiques y ont vu une opportunité de capter de la valeur. Qu'ont vu pour leur part les États dans le web ? Est-ce que la prise de conscience des élites qui représentent les citoyens n'a pas été trop tardive ?

183. – **Les GAFAM, de nouveaux États ?** Les GAFAM ont en effet su s'approprier un bien commun et des données personnelles pour des raisons commerciales et, peu à peu, ont pris une place plus importante que les États. Certains comme Facebook ont créé des communautés tellement fortes que les responsables peuvent aller jusqu'à imaginer pouvoir revendiquer des prérogatives traditionnellement régaliennes comme celle de battre monnaie (projet Libra). Cela invite à se demander : qu'est-ce qu'un État ? Est-il constitué par des valeurs communes, une langue, une histoire, un territoire, une armée, une monnaie ? Qu'on le veuille ou non, ne faut-il pas admettre l'hypothèse que, parce qu'elles ont créé des communautés très larges et parfois soudées, les GAFAM sont une nouvelle forme d'État ? Et, à terme, l'appartenance à de telles communautés ne risque-t-elle pas de prendre le pas sur des valeurs nationales ? Le jour où les GAFAM auront imposé leurs règles fiscales aux États, ne pourrait-on pas imaginer qu'elles iront jusqu'à se revendiquer en meilleurs représentants de leurs usagers que les États de leurs citoyens, et négocier pour eux les règles de vie collective (fiscalité, protection et sécurité sociale…) ?

II. – Indifférence citoyenne à ces questions et « illectronisme »

184. – Des formes d'indifférence citoyenne se manifestent à l'égard du débat public qui porte sur cette thématique, et le caractère marqué à l'extrême droite de la notion de souveraineté nationale n'invite guère les élus de la République à approfondir la question. Mais plusieurs phénomènes, à la fois banals et massifs, contribuent à rendre ce débat nécessaire et urgent, parmi lesquels :

– l'achat et l'usage par les particuliers de matériels et de services massivement non français, ni européens, mais étrangers, majoritairement américains et asiatiques ;

– le recours massif à des plateformes numériques d'accès gratuit qui utilisent à des fins commerciales les informations mises en ligne, explicitement mais de manière oblique, notamment *via* les techniques du marketing digital ou numérique ou *e*-marketing ;

– et, corrélativement, un certain laisser-aller des usagers, tant à l'égard du respect des règles de savoir-être sur les réseaux que vis-à-vis de la sécurisation des informations personnelles.

Ces phénomènes provoquent un affaiblissement des acteurs hexagonaux ou européens du numérique, ainsi que l'expatriation des savoir-faire et de l'entrepreneuriat. L'offre hexagonale et européenne est inexistante et les préoccupations des citoyens semblent très éloignées des sujets de souveraineté nationale.

185. – L'illectronisme. Il convient également de prendre en compte le phénomène dit « de l'illectronisme », ou illettrisme numérique. En effet, aux usages peu rigoureux du numérique s'ajoutent des formes d'ignorance et d'exclusion. Selon l'Insee, en 2019, « 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. « 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 »[(30)]. Or, le gouvernement veut 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 et des citoyennes de savoir utiliser les ressources numériques courantes (Internet, traitement de texte…). On dit couramment que de telles compétences sont devenues presque aussi indispensables 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.

186. – Les raisons de l'absence d'équipement à domicile sont variables. Le manque de compétence (41 %), le coût du matériel (32 %) ou de l'abonnement

(30) *Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base : Insee Première* 2019, n° 1780, p. 1-2.

(27 %) sont les plus cités, 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 l'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).

187. – Pour autant, les compétences des Français sont dans la moyenne de l'UE. En France, en 2017, 43 % des individus de seize à soixante-quatorze ans (tranche d'âge commune à toutes les enquêtes européennes) avaient un score global de capacité numérique nul ou faible, ce qui place le pays dans la moyenne de l'Union européenne. Le Luxembourg et Pays-Bas sont en tête (entre 15 % et 20 % de non-usage et de compétences faibles ou nulles), alors que la Roumanie et la Bulgarie sont en bas du classement, en raison de la faible proportion d'usagers (63 % en Bulgarie et 64 % en Roumanie). Cette distribution reflète à la fois le niveau de développement économique des pays, leur pyramide des âges, leur densité de population et l'hétérogénéité de leur territoire.

188. – Les compétences numériques. Eurostat, direction générale de la Commission européenne chargée de l'information statistique à l'échelle communautaire, distingue quatre domaines de compétences numériques[31] : 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.*) ; et 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.

189. – Le développement de l'accès au numérique. Ainsi, les outils de mesure permettent de constater l'importance du développement de l'accès au numérique : en 2017, 8 % 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 quinze 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

(31) https://ec.europa.eu/eurostat/databrowser/view/tepsr_sp410/default/bar?lang=fr.

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 3 % du chiffre d'affaires des sociétés de 250 salariés 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[32].

III. – Les réponses de la puissance publique

190. – La réflexion et les actions de la puissance publique. Pour contrebalancer ces effets, une réflexion de fond est menée depuis plusieurs années par les sciences sociales[33] ; sur le plan national, des structures ont été dédiées et des actions ont été réalisées ou sont en cours 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. Elle fut créée par décret le 3 février 2015 et est 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, ainsi que la diffusion des outils numériques et le développement de leur usage auprès de la population. Elle comprend trois pôles responsables respectivement des trois missions suivantes : la mission « Très Haut Débit »[34], la mission *French Tech*[35] et la mission « Société Numérique »[36].

191. – La mission « Société Numérique ». Les activités de la mission « Société Numérique » visent explicitement à se situer au plus près des usagers-citoyens. Sa communication se veut 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 (seniors, familles à revenu modeste, personnes à faible niveau d'éducation ou sans emploi…) ». Initialement, elle a entrepris d'éditer les portails suivants, dont plusieurs sont aujourd'hui fermés : *NetPublic*, dont le but était d'aider le grand public à maîtriser les usages de l'Internet en développant des espaces publics numériques (EPN) ; *NetEmploi*, qui visait à aider les usagers à maîtriser les outils de la recherche d'emploi sur Internet ; *Le Portail des Métiers de l'Internet*, qui entendait favoriser une meilleure connaissance des métiers de l'Internet et des formations qui permettent d'y accéder ; *Ordi 2.0*, visant à favoriser la réutilisation d'ordinateurs

(32) Insee, *L'économie et la société à l'ère du numérique*, 2019.
(33) P. Brotcorne et G. 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 (www.cairn.info/revue-les-cahiers-du-numerique-2009-1-page-45.htm).
(34) www.amenagement-numerique.gouv.fr.
(35) https://lafrenchtech.com/fr.
(36) https://societenumerique.gouv.fr.

auprès des personnes défavorisées ; enfin *Internet sans crainte*[37], qui vise à protéger et à informer les mineurs sur les enjeux et risques liés à l'Internet, et qui est l'expression du pôle français du programme européen *Safer Internet plus* mis en place par la Commission européenne.

Ces programmes dédiés par l'institution publique sont mis en œuvre 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[38]. La crise sanitaire liée à la pandémie de Covid-19 a enfin vu le lancement de la plateforme *Solidarité numérique*[39], dont le but est d'accompagner les personnes en difficulté face aux outils numériques[40].

192. – **Les associations et les collectifs.** À cela s'ajoute l'action des associations et des collectifs qui luttent contre l'exclusion et la précarité numériques : nationaux comme Emmaüs Connect[41], région*aux* comme La Mêlée[42], ou de terrain comme Travailler et Apprendre Ensemble (TAE)[43] ; et également celle des *startups* comme *WeTechCare*[44], notamment responsable des *Cahiers de l'inclusion numérique*[45]. Peuvent être également cités des programmes reconnus d'utilité publique tels que Solidatech[46], lui-même étant lié au réseau TechSoup Global[47], fondé en 1987, réseau international de solidarité numérique pour les organisations à but non lucratif, qui se compose de soixante-huit partenaires en Afrique, Amérique, Asie-Pacifique, Europe et au Moyen-Orient et qui vise à renforcer l'impact des associations membres sur les problématiques sociétales locales et à favoriser un changement social mondial.

193. – **Quels sont les effets de ces actions pour la souveraineté numérique ?** L'enjeu qui se dessine ici est 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 a constitué la base de la diffusion des idées émancipatrices et a permis de cultiver l'esprit critique. À cette condition, il est possible de considérer les usagers comme

(37) www.internetsanscrainte.fr.
(38) V. le rapport de synthèse : www.enssib.fr/bibliotheque-numerique/documents/68347-rapports-et-recommandations-strategie-nationale-pour-un-numerique-inclusif.pdf. – V. le dossier de presse (2018) : https://societenumerique.gouv.fr/wp-content/uploads/2018/09/DP_SNNIVDEF2.pdf.
(39) https://solidarite-numerique.fr.
(40) www.vie-publique.fr/en-bref/274035-solidarite-numerique-nouveau-site-pour-lutter-contre-lillectronisme.
(41) https://emmaus-connect.org/exclusion-numerique.
(42) www.lamelee.com.
(43) https://ecosolidaire.org.
(44) https://wetechcare.org.
(45) www.inclusion-numerique.fr.
(46) www.solidatech.fr.
(47) www.techsoup.global.

un « public », selon le concept du philosophe pragmatique John Dewey[48] : l'accès aux nouveaux moyens d'expression, d'information et de communication constitue un nœud qui mêle intimement épistémologie, pédagogie, éthique et politique[49]. 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[50].

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 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[51]. L'expérience des espaces publics numériques en est aujourd'hui venue aux retours d'expérience[52]. On s'accorde notamment à reconnaître que l'acronyme « EPN » gagne aujourd'hui à être repensé comme « **espaces de pratiques numériques** » ou « EPN 2.0 »[53]. 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^e^ et XX^es^ 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 que l'on nomme en théorie politique la « perspective rationaliste sur la nation »[54] 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 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.

194. – Mobiliser les citoyens dans des formes de souveraineté post-nationale apparaît paradoxalement nécessaire si l'on veut fortifier ou recomposer une

(48) J. Dewey, *Le Public et ses problèmes*, 1927, trad. J. Zask, Paris, Gallimard, coll. « Folio essais », 2010.

(49) À propos de ce nœud, V. C. Gautier, *Le Public et ses Problèmes : le problème social de la connaissance*, Philosophical Enquiries : *Rev. des philosophies anglophones* 2015, n° 5 (www.philosophicalenquiries.com/numero5-article3Gautier.html).

(50) http://arsindustrialis.org/pharmakon.

(51) M. Lallement, *L'Âge du Faire, Hacking, travail, anarchie*, Paris, Seuil, 2015. – I. Berrebi-Hoffmann, M.-C. Bureau et M. Lallement, *Makers. Enquête sur les laboratoires du changement social*, Paris, Seuil, 2018.

(52) V. par ex. 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 (http://observatoire-reussite-educative.fr/thematiques/numerique-et-medias/Ressources-formation-contibutions-analyse/rapports-colloques-1/etude-epn-et-politique-de-la-ville). – L. Gervais, *Itinéraire d'un animateur d'espace publique numérique (EPN) : Cahiers de l'action* 2017/1, n° 48, p. 23-29 (www.cairn.info/revue-cahiers-de-l-action-2017-1-page-23.htm).

(53) https://movilab.org/wiki/Espace_de_Pratiques_Numériques. – A. Burret, *Démocratiser les Tiers-lieux : Multitudes* 2013/1, n° 52, p. 89-97 (www.cairn.info/revue-multitudes-2013-1-page-89.htm).

(54) D. Schnapper, *La Communauté des citoyens*, Paris, Gallimard, 1994. – P. Manent, *La Raison des nations : Réflexions sur la démocratie en Europe*, Gallimard, 2006.

souveraineté numérique « populaire », foyer de légitimité pour une souveraineté de type 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*, appartient à ceux qui peuvent plus ou moins l'imposer ou à ceux qui s'érigent en collectifs d'usagers, communautés de valeurs animées par l'engagement de ses membres.

Le problème est qu'en l'état actuel des pratiques numériques, ce dernier aspect ne suffit pas pour penser une forme pertinente de pouvoir constituant. Ainsi, le cyber-État qu'est quasiment devenu Google, selon l'hypothèse récemment imaginée par Marc Dugain dans son roman *Transparence*[55], ne pourrait offrir à ses ressortissants qu'une citoyenneté sans ancrage, une souveraineté en quelque sorte « hyper-postnationale » car nourrie par aucune terre, 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. Une citoyenneté qui n'est pas « enracinée »[56], et qui est même post-enracinée ou déracinée, est très dangereuse pour les libertés publiques mais aussi privées. 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 politiques ou commerciaux.

IV. – Conclusion : repenser la souveraineté à partir des pratiques numériques ?

195. – Si l'on veut penser la souveraineté numérique, il apparaît nécessaire de repenser le concept même de souveraineté à partir du numérique. Ce que l'on attend souvent de ce concept pour sanctuariser les économies nationales particulières, à savoir la régulation institutionnelle de niveau national, constitue désormais un objectif bien trop restreint, qui fait manquer l'essentiel. 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, peuvent s'opérer pour une 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.

(55) M. Dugain, *Transparence*, Paris, Gallimard, 2019.
(56) S. Weil, *L'Enracinement*, Paris, Gallimard, 1949.

196. – **L'apparition d'une souveraineté numérique populaire ou d'une nouvelle forme de souveraineté pour une nation numérique.** La notion classique de souveraineté, comme d'autres concepts hérités de la tradition politique moderne aujourd'hui débordés par les nouvelles technologies, tend lorsqu'elle est étroitement interprétée à masquer les nouvelles réalités socio-techniques, surtout celles qui émergent à travers les pratiques numériques. Pourtant à ce niveau se joue l'apparition d'une souveraineté numérique populaire ou d'une nouvelle forme de souveraineté pour une nation numérique. 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).

(57) P. Vion-Dury, *La Nouvelle servitude volontaire. Enquête sur le projet politique de la Silicon Valley*, Limoges, FYP éd., 2016.

TROISIÈME PARTIE

PROPOSITIONS

PROPOSITION N° 1

DÉFINIR ET PILOTER UNE STRATÉGIE DE CYBERSOUVERAINETÉ

RÉSUMÉ

La cybersécurité est désormais un pan essentiel de la mission régalienne de sécurité. Il ne saurait y avoir, en ce domaine comme en d'autres, de sécurité absolue, mais l'État a l'obligation d'optimiser la mise en œuvre de ses outils pour assurer au pays le plus haut niveau possible de protection. Il doit pour cela coordonner entre autres des moyens politiques, juridiques, administratifs, militaires, policiers, industriels, économiques et éducatifs. Cet éventail des modes d'action est un reflet de la présence d'une dimension cyber dans la quasi-totalité des activités. Cette mission ne saurait être dévolue à un seul département ministériel, même si tous doivent s'en saisir. Elle doit donc être menée au niveau du Premier ministre, tout en intégrant les acteurs non gouvernementaux dont l'apport est nécessaire. Il ne s'agit donc pas de créer un ministère, mais une politique appuyée sur une stratégie et dotée de moyens institutionnels et budgétaires substantiels.

DÉTAIL

197. – **Le constat : l'action dans le cyberespace est multidimensionnelle et n'est pas à ce jour pilotée, faute d'organes dédiés.** En dépit du poids déterminant pris par des entreprises privées et des organisations non gouvernementales, la régulation des activités cyber reste largement dépendante des États, sur lesquels repose le droit international. Ces activités interfèrent en effet avec nombre de domaines relevant de l'action de l'État : elles reposent sur des infrastructures qui sont situées dans un territoire, des entreprises dont le siège est quelque part et auxquelles s'appliquent des règles. Elles engendrent des flux financiers auxquels des lois ont vocation à s'appliquer. Elles ont des conséquences qui peuvent être très importantes sur l'économie, sur la vie des citoyens, sur l'exercice de la démocratie, voire sur la sécurité des individus, des organisations ou des nations.

Face à ces activités – et notamment à celles qui mettent en jeu la sécurité – les États ne sont pas démunis et certains ont pris des mesures qui, si elles ne sont pas

nécessairement mises en œuvre pour de bonnes raisons, n'en demeurent pas moins techniquement faisables.

198. – **La proposition : attribuer le pilotage d'une cybersouveraineté à un organe dédié.** Notre pays a, plus que beaucoup d'autres, une très large panoplie de moyens d'action à sa disposition : une capacité intellectuelle qui génère un foisonnement de créativité scientifique et entrepreneuriale, une puissance économique qui permet de faire des choix de politique industrielle, une diplomatie mondiale renforcée par son rôle au conseil de sécurité des Nations unies, un savoir-faire rare en matière de cyberdéfense et, désormais, une capacité militaire en ce domaine.

Pour autant, il ne peut pas tout faire : construire un Google français ou européen, développer une industrie autonome de composants, lutter sans coopération contre le cybercrime. Ce que pouvait faire Colbert pour la tapisserie ne peut pas l'être pour la maîtrise du cyberespace et il nous faut mettre en œuvre un colbertisme adapté. Celui-ci doit être fondé sur la définition de priorités au service desquelles l'État puisse concentrer la mise en œuvre des instruments puissants dont il dispose : diplomatique, réglementaire, technique, judiciaire, éducatif, budgétaire, militaire, sans oublier le bon usage de l'Union européenne. L'objet de la présente proposition n'est pas de dire quels doivent être ces choix, mais de proposer une méthode institutionnelle pour les définir.

Les organes de l'État appelés à participer à cette politique sont nombreux et aucun ne peut le faire seul. Le ministère chargé du numérique a un domaine de compétence important mais limité. Les grands ministères régaliens ont un rôle également essentiel. Le chef de cet orchestre ne peut être que le Premier ministre.

L'action de l'État en mer est multidimensionnelle. Elle est coordonnée par le Secrétaire général de la mer sous l'autorité du Premier ministre. On sait les nombreuses analogies qui existent entre le droit de la mer et celui du cyberespace, fondé lui aussi sur la liberté de navigation, mais avec aussi ses nations impériales, ses pirates et ses corsaires. Comme la souveraineté maritime, à la fois multidimensionnelle et vitale, la politique de cybersouveraineté, élément désormais central de l'indépendance nationale, doit être coordonnée et dirigée au plus haut niveau du gouvernement.

PROPOSITION N° 2

INVESTIR DANS LA RECHERCHE NUMÉRIQUE FONDAMENTALE FRANÇAISE ET EUROPÉENNE

RÉSUMÉ

Renforcer massivement la recherche fondamentale publique française et européenne dans le domaine des technologies numériques et la rendre plus attractive pour les chercheurs. Cela implique la création d'un fonds de financement spécifique à ce type de recherche, abondé notamment par le renforcement de la fiscalité à l'égard des GAFAM. Parallèlement, pour renforcer l'attractivité des pôles de recherche et pour valoriser le travail des chercheur·s·es, la France pourrait porter la création d'un grand prix international (type Prix Nobel ou médaille Fields) récompensant les chercheur·s·es, travaillant dans le secteur public et dont les recherches ont permis de donner naissance à des technologies permettant effectivement aux États de soutenir leur souveraineté numérique.

DÉTAIL

199. – **Le constat : depuis bien longtemps, la puissance d'un État se mesure à sa capacité à accueillir, à développer et à produire des progrès technologiques en investissant dans le domaine de la recherche fondamentale et appliquée.** La course au vaccin, lors de la récente épidémie de Covid-19, constitue sur le plan de la recherche en santé une bonne illustration des enjeux de souveraineté liés précisément à la puissance de la recherche d'un État. En ce qui concerne la souveraineté numérique, la question se pose aussi, pour les États, notamment parce que les technologies qui transforment effectivement aujourd'hui la vie de leurs citoyens – et qui construisent ainsi les formes de vie futures – sont développées et maîtrisées par de grandes entreprises privées, particulièrement les GAFAM, qui investissent massivement dans la recherche et le développement.

Pour retrouver ou conserver une souveraineté numérique, il ne suffit donc pas d'une volonté politique ou d'initiatives économiques, il faut aussi

réinvestir le terrain de la recherche fondamentale afin de retrouver l'initiative technologique.

200. – **La proposition : créer un fonds d'investissement pour soutenir la recherche fondamentale et créer les dispositifs de médiatisation et de valorisation de cette recherche fondamentale.** D'abord le financement. Les universités françaises, les laboratoires, les centres de recherche doivent pouvoir faire appel à un fonds dédié pour financer les recherches sur les technologies numériques afin de regagner une place de premier plan dans la course à l'innovation de technologies numériques souveraines. Cet investissement est nécessaire aussi pour rendre la recherche française attractive dans le contexte mondialisé et concurrentiel de la recherche fondamentale. Alors que la qualité de la formation des informaticiens et des chercheurs en informatique français est largement reconnue, il est regrettable que l'investissement de la nation dans cette formation ne lui soit pas davantage profitable par l'implication de ces ingénieurs et chercheurs dans des projets français.

Ce fonds d'investissement devrait être abondé par une part de la fiscalité émergente sur les bénéfices réalisés en France par les grands opérateurs du numérique. C'est une source de financement neutre pour l'État et susceptible d'entraîner un processus vertueux de réinvestissement du pouvoir de l'État.

Parallèlement à ce dispositif d'investissement dans la recherche fondamentale, la France pourrait porter la mise en place d'outils de médiatisation et de valorisation de cette recherche fondamentale, à travers la mise en place d'un grand prix international, visant à récompenser les travaux de chercheurs permettant aux États de réinvestir le champ de leur souveraineté sur le numérique. Outil d'attractivité pour les chercheurs, outil de *soft power* pour l'État français, ce prix serait aussi un élément de sensibilisation du grand public aux enjeux spécifiques de la maîtrise des technologies numériques.

PROPOSITION N° 3

STIMULER LES INVESTISSEMENTS PRIVÉS DANS LE NUMÉRIQUE

RÉSUMÉ

Pourtant cruciaux tant pour assurer l'émergence de fournisseurs européens de produits/services numériques que pour permettre aux entreprises plus traditionnelles de rester dans la course sur leur marché qui bien souvent se numérise, les investissements dans les compétences et équipements numériques sont trop faibles sur le Vieux Continent, notamment en France où ils sont près de quatre fois inférieurs pour une PME par rapport à son homologue américain. Le choix massif pour des solutions *cloud* non européennes a encore aggravé la faiblesse industrielle européenne en informatique. Il est temps de réagir en profitant de l'atout européen résidant dans sa forte épargne, qu'il faut orienter énergiquement vers l'investissement productif numérique. Pour ce faire, il est proposé :

– d'une part, d'élargir le dispositif de défiscalisation IR-PME, puis d'assouplir les critères d'admissibilité du crédit d'impôt recherche ainsi que celui des jeunes entreprises innovantes ;

– d'autre part, de favoriser la réimplantation d'infrastructures numériques d'entreprises françaises ou européennes sur le territoire de l'Union, en veillant à intégrer une dimension écologique pour éviter les impacts néfastes pour l'environnement d'une implantation massive d'infrastructures fortement polluantes.

Retrouvons l'esprit de bâtisseurs de nos ancêtres, investissons résolument dans le numérique pour pouvoir davantage choisir ses usages, qui pour le moment sont dictés par les *leaders* non européens en la matière !

DÉTAIL

201. – **Le constat : la faiblesse numérique européenne, symptôme d'un défaut d'investissement dans les équipements et les compétences en la matière.** Comme l'a montré cette étude (V. *supra*, n° 139, « Enjeu de domination économique, le cyberespace est un *far-west* très faiblement défendu par les uns, colonisé par les autres »), la faible puissance numérique européenne s'explique en partie par les investissements insuffisants en la matière, de la part des entreprises, mais aussi des épargnants qui,

au moins en France, n'orientent pas leur épargne vers l'investissement productif, en particulier dans le numérique. Quant aux entreprises françaises et européennes, la part de leur budget dépensée en équipements et compétences numériques est nettement plus faible qu'aux États-Unis, puisqu'elle était évaluée à 184 000 € en moyenne pour une PME en France, tandis qu'elle avoisine les 750 000 € outre-Atlantique. Cette disparité est aggravée par le passage au *cloud* qui, massivement adopté par les entreprises européennes, a accru la dépendance de ces dernières auprès des fournisseurs de services infonuagiques massivement étasuniens, en substituant en outre à la logique d'investissements (*Capital Expendidure* [CAPEX]) la logique d'un budget de fonctionnement (*Opérational Expenses* [OPEX]) et faisant ainsi passer les Européens du statut – coûteux mais pérenne – de propriétaire (de leurs infrastructures) à celui – prétendument plus économique, mais plus précaire – de locataire… De fait, ce contexte n'a pas favorisé la naissance de grands acteurs du numérique qui soient européens.

202. – **La proposition : stimuler l'investissement numérique (i) en élargissant le dispositif de défiscalisation IR-PME (ii) ainsi que celui du crédit d'impôt recherche (CIR), et (iii) en réformant la taxe foncière.** Parmi les pistes proposées par le rapport d'information dressé par MM. les Sénateurs Franck Montaugé et Gérard Longuet (remis à la présidence du Sénat le 1er octobre 2019 – V. p. 159 et s.), auxquelles les auteurs de la présente étude souscrivent, figurent celles consistant à élargir les dispositifs de défiscalisation IR-PME et du crédit d'impôt recherche, afin d'améliorer la position de la France pour attirer des porteurs de grands projets numériques. Ainsi, poursuivant en partie cette piste, la proposition du Cercle de la Donnée consisterait à :

– d'une part, encourager l'épargne française à s'orienter vers l'investissement productif numérique :

• d'abord, en élargissant le dispositif de défiscalisation IR-PME (lequel permet de bénéficier d'une réduction d'impôt en investissant dans le capital des PME communautaires, sous diverses conditions). Le taux de cette réduction d'impôt, égal à 18 %, avait été relevé à 25 % dans le cadre de la loi de finances 2020. Un décret paru au *Journal officiel* le 8 mai 2021 le prolonge à l'ensemble des versements effectués jusqu'au 31 décembre 2021. Ce taux pourrait être légalisé et pérennisé pour les entreprises du numérique (fournisseurs de produits et services numériques), ou pour toutes les entreprises qui souhaitent investir dans le numérique,

• ensuite, en assouplissant les critères d'admissibilité du crédit d'impôt recherche, qui permet d'imputer sur l'impôt sur les sociétés 30 % des dépenses inférieures jusqu'à 100 millions d'euros et 5 % au-delà, mais qui malheureusement est peu adapté à la matière numérique dans laquelle les innovations correspondent davantage à de nouveaux usages, peu à même de satisfaire aux conditions d'éligibilité de ce crédit d'impôt ; les indicateurs permettant d'évaluer les efforts en matière de R&D pour les entreprises du numérique pourraient être harmonisés et le périmètre des dépenses éligibles élargi pour intégrer l'innovation au sens large (marketing, *design*…),

• enfin, en simplifiant le dispositif de « Jeunes entreprises innovantes », à l'instar du CIR pour bénéficier aux entreprises du numérique ;

– d'autre part, à favoriser la RE (implantation d'infrastructures numériques d'**entreprises françaises ou européennes établies** sur le territoire français) en exonérant de taxe foncière les équipements de production et les équipements d'installation des sites industriels, ce qui permettrait de sortir indirectement du champ de la taxe foncière une part importante des équipements des *data centers*. **Cette mesure sera assortie d'une dimension écologique en imposant l'adoption d'infrastructures économes en consommation d'énergie (*Green Tech*), pour éviter que les territoires français et européen ne subissent lourdement les impacts écologiques néfastes d'une implantation massive de *data centers* fortement polluants.**

PROPOSITION N° 4

IMPOSER UNE SOUVERAINETÉ JURIDIQUE EUROPÉENNE POUR LES DONNÉES LES PLUS SENSIBLES

RÉSUMÉ

Le contrôle de son territoire et de ses lois étant l'un des attributs de la souveraineté, il peut aussi être l'un des outils à la disposition de l'État en matière de souveraineté numérique.

Les données numériques constituent désormais un actif stratégique pour un État, une entreprise, un citoyen. La confidentialité, l'intégrité et la disponibilité des plus sensibles d'entre elles sont une nécessité.

Or, la plupart des services mettent en œuvre et développent des technologies d'informatique en nuage (*cloud computing*) qui permettent d'héberger et de traiter les données *via* un accès en réseau. Le marché est dominé par des acteurs étrangers, ce qui pose un risque de captation des données, certains pays ayant adopté des législations à portée extraterritoriale leur permettant d'accéder aux données hébergées dans des serveurs informatiques situés dans d'autres pays.

L'objet de la présente proposition est de rendre obligatoires l'hébergement et le traitement en Europe, par des sociétés non exposées à des lois extra-européennes, d'un ensemble de données sensibles, à définir, concernant notamment des entités comme les administrations, les services de santé, les institutions de recherche, les entreprises et les citoyens. Cette mesure renforçant la sécurité technique et juridique de ces données contribuerait à notre souveraineté numérique.

DÉTAIL

203. – **Le constat : l'externalisation massive de l'informatique à des prestataires non européens a entraîné une exposition de nos données stratégiques en dehors de l'Europe, ce qui fragilise la souveraineté du vieux continent.** Il est nécessaire que les applications et les données considérées comme critiques ou sensibles pour une entité lui soient accessibles en permanence, que leur intégrité soit assurée et qu'elles ne soient pas consultées et exploitées sans l'accord de leur

propriétaire. Or avec le développement des échanges internationaux et l'évolution technologique, le volume des données produites par les systèmes d'information et leur traitement massif, nécessaire à des nouvelles technologies comme l'intelligence artificielle et le *big data*, conduisent à faire de plus en plus appel à des insfrastuctures[1], hébergements et logiciels utilisables à distance[2].

Le marché de cette informatique en nuage (*cloud*) est actuellement dominé par des acteurs étrangers de dimension internationale, notamment nord-américains et bientôt chinois. L'accès aux données pourrait être obtenu par l'application de lois extraterritoriales, comme le *Cloud Act*[3] adopté en 2018 aux États-Unis, qui prime, aux yeux des juges américains, sur la législation ou le droit contractuel européens.

204. – La proposition : imposer des conditions à toute opération portant sur certaines données essentielles, permettant que celles-ci soient uniquement soumises aux textes européens à l'exclusion de toute autre législation étrangère. Il s'agit d'éviter – autant que possible – l'application de lois étrangères (type *Cloud Act*) et de permettre aux juridictions européennes d'être seules compétentes ainsi qu'aux textes communautaires et/ou des États membres de l'UE de s'appliquer seuls.

Les entités concernées sont en premier lieu les opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE) pour lesquels des réglementations nationale et européenne sont déjà en place ; mais le périmètre doit être progressivement élargi aux administrations, aux entreprises petites et grandes, dont les *startups*, agissant dans des secteurs ou des domaines considérés comme prioritaires.

S'agissant des données, un examen serait nécessaire pour pouvoir les répartir en trois ensembles ou cercles.

Le premier cercle est celui des données et des applications les plus critiques ; elles seraient traitées exclusivement dans un « *cloud* interne », ou un réseau privé, physiquement localisé dans les emprises de l'entité, ou en dépendant directement. Ce premier cercle couvre notamment les systèmes d'information régaliens de l'État.

Le deuxième cercle est celui des données, des traitements et des applications de sensibilité moindre mais nécessitant un certain niveau de pérennité. Il pourrait être hébergé dans un « *cloud* dédié », des infrastructures dédiées situées chez des partenaires de confiance nécessairement européens.

Pour les données restantes, peu sensibles, il serait fait appel à un « *cloud* externe » accessible par le réseau Internet, avec des offres externes qui permettent de bénéficier de l'état de l'art et de ses meilleures innovations. Ces offres devraient cependant répondre à des critères minimaux en termes de fonctionnalité, de réversibilité et de sécurité et pourraient faire l'objet de labélisations en fonction de leurs caractéristiques notamment en matière de sécurité.

Les deux premiers niveaux (*cloud* interne et *cloud* dédié) devraient eux respecter les exigences réglementaires génériques et être conformes aux exigences du *cloud*

(1) IaaS (*Infrastructure as a service*).
(2) SaaS (*Software as a service*).
(3) *Clarifying Lawful Overseas Use of Data* (*Cloud*) *Act*.

de confiance telles que présentées en mai 2021 dans la stratégie nationale pour le *cloud* (visa SecNumCloud de l'ANSSI et critères de souveraineté) :

– remplir les exigences de sécurité associées au référentiel technique SecNumCloud ;

– localiser les infrastructures et les systèmes de traitement en France (en Europe) ;

– assurer les portages opérationnel et commercial de l'offre par une entité européenne, détenue par des acteurs européens.

205. – **Le développement d'une offre industrielle est une des conditions du succès.** La notion de *cloud* souverain développée *ex nihilo* en France de 2010 à 2015 a été un échec car elle correspondait à un objet pensé sur un plan strictement national tant pour la localisation (infrastructures situées en France) que pour les solutions techniques alors très limitées, voire inexistantes. L'approche actuelle est plus nuancée avec la mise en avant de l'« autonomie stratégique » nationale et européenne et l'adaptabilité des offres techniques, désormais existantes ou à développer, en fonction de l'acteur et des données concernés (les trois cercles).

La compétitivité française pour les solutions d'hébergement (IaaS) est reconnue mais notre pays est en retard pour les services et les applications (SaaS). Le développement des offres françaises et européennes doit être encouragé pour limiter, puis éviter les solutions « hybrides » associant logiciels américains et hébergement de données par des sociétés françaises[4] (ou européennes) qui, si elles préservent la souveraineté des données, entretiennent néanmoins une dépendance technologique.

Le projet GAIA-X initié il y a deux ans par l'Allemagne et la France est un pas dans la bonne direction. Il a pour objectif de construire une infrastructure de données fiable et sécurisée pour l'Europe avec les principes suivants : garantir la souveraineté des données, leur disponibilité, leur interopérabilité, leur portabilité. Pour autant, il convient d'être vigilant pour éviter l'arrimage à ce projet de sociétés américaines et chinoises, qui a déjà été évoqué.

(4) Exemples du partenariat de la société française d'hébergement OVH avec Google et de la création récente de Bleu, société de *cloud* associant les Français Orange et Capgemini à Microsoft.

PROPOSITION N° 5

ARMER LE DROIT DE LA CONCURRENCE FACE À L'ÉCONOMIE DE LA DONNÉE

RÉSUMÉ

Mis en place pour préserver une diversité sur le marché, le droit de la concurrence s'est montré insuffisant pour freiner la très forte concentration observée aujourd'hui chez les géants du numérique.

Convoitant les innovations d'usage et les vastes quantités de données que celles-ci permettent de collecter, les GAFAM n'ont eu de cesse, au gré de leurs acquisitions, de renforcer leur suprématie sur le marché, grâce notamment à la gratuité, car bien des services numériques ne sont pas payants de prime abord.

C'est sans doute ce qui explique en partie l'échec du cadre juridique actuel, dont les seuils pour déclencher le contrôle des concentrations s'expriment en chiffre d'affaires. Pour rendre au droit de la concurrence son efficacité, pourquoi ne pas prendre comme critère alternatif celui de la part de marché (y compris pour les marchés gratuits), en considérant également les quantités de données détenues par les parties ainsi que les finalités de réutilisation envisagées ?

Les modèles évoluent, le droit doit s'adapter !

DÉTAIL

206. – **Le constat : depuis l'avènement du numérique, se sont constitués des oligopoles sans précédent.** La concurrence, on le sait, doit être encadrée pour être pérenne, car à défaut elle n'est que le reflet de la lutte sans merci que se livrent les acteurs économiques et dont les plus puissants finissent par éradiquer leurs rivaux et dominer en maîtres absolus, au détriment des consommateurs. C'est tout l'objet du droit de la concurrence qui, en Europe, est partiellement de source communautaire, et qui, d'une part, prohibe certaines pratiques anticoncurrentielles (dont les ententes et les abus de position dominante) et, d'autre part, organise un contrôle des opérations de concentration. La justification de ce contrôle réside dans le fait que, à la différence d'une croissance interne qui reflète le mérite commercial d'une entreprise ayant été meilleure que ses rivales, la croissance externe peut résulter

d'une stratégie prédatrice par laquelle un acteur déjà puissant va choisir d'absorber, plutôt que de combattre, un compétiteur. Pour cette raison, depuis 1977 pour la France, puis 1989 pour l'Union européenne[1], le législateur a imposé que les opérations de concentration (fusion, prise de contrôle, création d'une entreprise commune)[2]) d'une certaine dimension (exprimée au moyen de seuils de chiffres d'affaires réalisés mondialement et dans l'Union européenne) soient préalablement notifiées aux autorités de concurrence, qui procèdent à un bilan économique et concurrentiel, au regard du marché pertinent, pour ensuite refuser ou autoriser (le cas échéant, sous réserve du respect de certains engagements) l'opération envisagée.

Or, rares sont ceux qui contestent l'anomalie numérique, c'est-à-dire l'extrême domination de certains acteurs : 90 % de parts du marché des moteurs de recherche pour Google, 3/4 de celui des réseaux sociaux pour Facebook, 98 % des marchés des systèmes d'exploitation pour les téléphones intelligents pour Google et Apple réunis, plus de la moitié du marché de la publicité en ligne pour Google et Facebook[3].

Comme cette étude l'a montré (V. *supra*, n° 87, « L'effet réseau est une menace pour la libre concurrence, et pour la souveraineté économique »), ces opérateurs ont pour point commun d'avoir pris pied sur le marché avec un produit d'appel (financièrement) gratuit pour favoriser leur adoption massive par les utilisateurs dont le nombre constitue ensuite le meilleur argument pour inciter les autres à choisir le même produit – ou un du même opérateur – par souci d'efficacité et au vu du parc installé. Or ces deux ingrédients détonants, qui ont fait recette chez les géants actuels du numérique (gratuité et effet réseau), ignorent le chiffre d'affaires, ce qui explique peut-être en partie le singulier échec de ce droit à préserver une concurrence équilibrée. Et le danger que fait courir ce constat peut être étendu à tous les secteurs car tous se numériseront à terme.

De fait, on observe chez les géants actuels du numérique un rythme très soutenu d'acquisitions : par exemple, Google a réalisé sept acquisitions majeures depuis 2006[4], soit une tous les deux ans en moyenne ; Facebook[5], Microsoft[6] ou encore Apple[7] ont suivi la même dynamique.

Ces acquisitions multiples peuvent inquiéter à plusieurs titres : le plus critique réside dans l'emprise grandissante, en perpétuelle expansion, qu'elles donnent aux

(1) Le législateur européen est intervenu bien plus que les législateurs nationaux sur le contrôle des concentrations. En droit communautaire, dans un premier temps, le contrôle ne s'exerçait qu'indirectement au moyen d'un examen d'une entente ou pratique concertée entre entreprises, ou encore d'un examen de l'abus de position dominante. Ce procédé ayant été jugé insuffisant, la Communauté a réussi à combler cette lacune avec le règlement n° 4064/89 du 21 décembre 1989, entré en vigueur en 1990 et relatif au contrôle des opérations de concentration entre entreprises.

(2) Selon l'article 3, § 1 du TFUE, une concentration n'est réputée réalisée qu'en présence d'un « changement durable du contrôle de l'entreprise ». Par « contrôle », l'article 3, § 2 explique qu'il faut entendre la possibilité d'exercer une influence déterminante sur l'activité de l'entreprise. Par « changement durable », deux cas de figure sont envisagés : la fusion de deux ou plusieurs entreprises et l'acquisition de la majorité des droits de vote dans le capital. L'article 3, § 4 vise spécialement l'hypothèse de la création d'une entreprise commune dans la définition de l'opération de concentration. En résumé, les opérations concernées sont les suivantes : la fusion, la création d'une entreprise commune et l'acquisition d'un contrôle.

(3) E. Claudel, *Le droit de la concurrence français à l'offensive : RTD com.* 2020, p. 806.

(4) Ainsi, Google a acquis : YouTube (vidéos) en 2006, Double clic (publicités en ligne) en 2007, Motorola (fabrication de smartphones) en 2011, Waze (services de navigation) en 2013, Nest (thermostats connectés) en 2014, Deepmind (apprentissage automatique et neurosciences) en 2014, Looker (stockage informatique et analyse de données) en 2019.

(5) Instagram en 2012, WhatsApp en 2014.

(6) Skype et LinkedIn en 2016.

(7) L'assistant vocal (Hey) Siri, en 2012, l'application météo Dark Sky en 2020, la plateforme Voysis (permettant d'optimiser les capacités des assistants vocaux) en 2020.

acteurs dominants, qui disposent dorénavant d'une puissance de marché inégalée, inquiétante pour la souveraineté économique des États.

207. – La proposition : élargir le contrôle des concentrations. Il est proposé :

– d'une part, d'ajouter un critère, alternatif à celui du chiffre d'affaires, correspondant à la part de marché[8] détenue par des entités parties à l'opération ; de la sorte, serait appréhendé le cas d'une opération visant une société générant un faible chiffre d'affaires, mais détenant de très conséquents volumes de données, révélateur d'un grand nombre d'utilisateurs et donc d'une forte part de marché, à l'instar d'Instagram[9] en 2012 (sur le marché des réseaux sociaux) ;

– d'autre part, d'imposer aux entités, parties à un tel projet de concentration, de déclarer les marchés connexes sur lesquels il est envisagé de prendre pied par la réutilisation des données et de respecter ensuite cette déclaration, sauf à effectuer une nouvelle notification aux autorités de concurrence donnant lieu à un nouvel examen ; on pensera, par exemple, à une entreprise en position dominante sur le marché des services de géolocalisation et acquérant une marque automobile, qui devrait dévoiler ses intentions si elle entendait se lancer sur le marché des véhicules connectés en profitant de ses données : de la sorte, pourraient être convenablement exprimées les préoccupations de concurrence lors de l'examen de l'opération qui pourrait, le cas échéant, être assortie d'engagements, comme celui d'ouvrir aux autres opérateurs du marché automobile un accès non discriminatoire.

(8) À noter que l'Autorité de la concurrence (française) s'est prononcée en défaveur d'une prise en compte de la « valeur de la transaction », dans la perspective d'une éventuelle réforme du cadre législatif actuel du contrôle des concentrations (communiqué du 7 juin 2018 : « (…) En l'état, l'Autorité considère que l'instauration d'un nouveau cas de contrôle des concentrations, fondé sur la valeur de transaction (comme décidé récemment en Allemagne et en Autriche) ne se justifie pas pour l'économie française : certes, il peut y avoir des rachats suscitant des préoccupations de concurrence, mais pour un nombre en définitive limité d'opérations problématiques, et le cadre d'un seuil en transaction ne permettrait pas nécessairement de traiter toutes les opérations potentiellement problématiques qui ne sont pas actuellement contrôlées. L'instauration d'un tel nouveau cas de contrôle systématique induirait ainsi une contrainte forte pour de nombreuses opérations de rapprochement ou rachat. L'Autorité écarte donc une telle hypothèse à ce stade, et suivra de près la mise en œuvre des dispositions adoptées en Allemagne et en Autriche, afin d'en tirer tous les enseignements »), www.autoritedelaconcurrence.fr/fr/communiques-de-presse/7-juin-2018-modernisation-et-simplification-du-controle-des-concentrations.

(9) Les autorités américaines ont donné leur feu vert, mercredi 22 août 2012, au rachat par le réseau social en ligne Facebook de l'application de photographie pour appareils mobiles Instagram, estimant que l'opération ne posait pas de problème de concurrence. La commission fédérale du commerce (FTC) a terminé son enquête « sans prendre aucune mesure », a-t-elle indiqué dans un communiqué. « La transaction peut donc se dérouler comme prévu », a-t-elle ajouté (*Le Monde* 23 août 2012), www.ftc.gov/news-events/press-releases/2012/08/ftc-closes-its-investigation-facebooks-proposed-acquisition.

PROPOSITION N° 6

CRÉER DES PROFESSIONS RÉGLEMENTÉES POUR LE NUMÉRIQUE

RÉSUMÉ

Lancés après-guerre, les pionniers de l'informatique, essentiellement américains, répondaient à une logique libérale peu favorable à la régulation. Le développement des entreprises de services numériques (ESN) et des intermédiaires de l'Internet (FAI, hébergeurs, plateformes) a suivi la même trajectoire.

Or, notre histoire nous enseigne que, à l'image du droit (avocats, notaires…) et du chiffre (commissaires aux comptes…) certaines professions du numérique devraient peut-être être instituées et réglementées : commissariat aux données, auditeurs d'intelligence artificielle, ingénieurs numériques…

Leur accès serait conditionné à une formation éprouvée, et leur exercice soumis au respect d'obligations légales et déontologiques précises. Ce serait un gage de lisibilité et de confiance pour tous ceux dont des pans entiers de l'activité dépendent du bon fonctionnement des outils numériques. C'est-à-dire désormais presque le tout à chacun.

Soyons ambitieux, contrôlons le numérique !

DÉTAIL

208. – **Le constat : l'insécurité numérique face à la faible régulation des fournisseurs de produits et services numériques.** Comme cette étude vient de le montrer, les atteintes portées aux droits des personnes et des organisations – y compris des États – sont nombreuses sur les réseaux, mais aussi plus généralement *via* tout outil numérique, à tel point que l'on parle même de « cyberguerre » (V. *supra*, n^os^ 102 et s., « La cyberguerre »). Si, sur le terrain politique, cette insécurité se traduit par la surveillance clandestine d'activités européennes stratégiques (affaire *Snowden*) – V. *supra*, n° 101, « Une efficacité contestée » –, elle se manifeste sur le terrain économique par des surcoûts engendrés par les failles, les dysfonctionnements ou l'inadaptation de certains outils et projets numériques, dont les conséquences financières et humaines peuvent s'avérer colossales. Ce fléau, qui touche

tous les secteurs et particulièrement les petites entreprises dont la surface financière ne permet pas de supporter un incident grave (et encore moins d'engager une procédure judiciaire, dans un tel cas), est aggravé, d'une part, par l'adoption massive et parfois sans discernement d'outils numériques qui, en raison de l'effet réseau qu'elle provoque (V. *supra*, n° 87, « L'effet réseau ») rend un très grand nombre d'organisations dépendantes de ces outils et, d'autre part, par la très grande disparité qui existe parmi les fournisseurs de produits et services numériques, en termes de compétence et de probité. Or, face à ce constat, on observe que ces fournisseurs ne sont pas – ou que très faiblement – régulés (par des règles spécifiques indépendamment du droit commun qui leur est applicable, comme à toute entreprise du marché) : les fournisseurs de produits (matériel/*hardware* – serveurs, ordinateurs, tablettes, smartphones… – logiciels/*software* dont les systèmes d'application et applicatifs, ainsi que les applications mobiles), les entreprises de services numériques (ESN) et les intermédiaires techniques de l'Internet dont notamment les hébergeurs (soumis à un régime de responsabilité allégé) et les plateformes (qui, au vu du poids économique et de l'influence de certaines d'entre elles sur les réseaux, apparaissent faiblement régulées).

209. – **La proposition : créer des professions réglementées pour le numérique.** La présente proposition comprend les dimensions suivantes :

– **tout d'abord**, il conviendrait de créer des professions chargées de garantir la conformité des systèmes d'information (SI) et de tout ce qu'ils comportent (données, logiciels, matériel…), au regard de la loi mais aussi de l'état de l'art (en termes de sécurité, en prenant en compte le niveau de risque propre à chaque organisation). Ces professionnels porteraient les titres :

• de « **commissaire numérique** », qui serait chargé :

(i) d'examiner annuellement les SI des organisations – qui, toutes, seraient contraintes de tenir une comptabilité numérique (description normée de leur SI, sur la base d'une sémantique agnostique de la technologie et d'une nomenclature standardisées, dont le niveau de détail devra être raisonnable) quelle que soit leur taille – dépassant certains seuils (volume de données détenues, nombre et/ou type d'applicatifs utilisés, *etc.*),

(ii) de révéler aux autorités les faits délictueux dont il aurait connaissance, à l'image du devoir d'alerte du commissaire aux comptes,

• d'« **auditeur d'algorithme** » qui contrôlerait, de manière approfondie, le bon usage de tout outil mettant en œuvre un algorithme, et :

- sur le plan juridique,

- mais aussi technique (en termes de sécurité physique, logique et peut être aussi éthique – en identifiant les risques de détournement de l'outil), en veillant notamment à conserver le caractère explicable et contrôlable du dispositif ;

– **ensuite**, les ESN se verraient imposer l'obligation de confier la responsabilité de tout projet à une personne détenant un titre académique « **ingénieur diplômé** » auquel serait ajoutée une mention « **numérique** » – à créer – et qui sanctionnerait un enseignement poussé en la matière. Tous (commissaires numériques, auditeurs d'algorithmes et ingénieurs numériques) prêteraient serment, en

début de carrière, devant une instance ordinale et auraient à répondre, devant elle, d'obligations juridiques et déontologiques spécifiques dont certains manquements graves pourront aboutir à leur exclusion de la profession ;

– **enfin**, à l'image de certains dispositifs de chiffrement, les fournisseurs de certains matériels et/ou logiciels seraient soumis à l'obligation d'obtenir une autorisation de mise sur le marché (AMM) / les réseaux (AMR), en particulier pour **certains usages exposant particulièrement la sécurité des utilisateurs, dont la liste serait édictée par le législateur**.

PROPOSITION N° 7

CAMPAGNE DE SENSIBILISATION CITOYENNE AVEC L'ÉDITION D'UN LIVRET D'INSTRUCTION CIVIQUE NUMÉRIQUE

RÉSUMÉ

Le rapport interministériel du procureur général de Riom, Marc Robert, intitulé « Protéger l'Internaute, Rapport sur la cybercriminalité » en 2014, est le premier travail de fond juridique consacré à la lutte contre la cybercriminalité. Relatif aux atteintes aux systèmes d'information et à leurs données ou à l'utilisation du vecteur Internet pour commettre des infractions, conscience est prise de la nécessité d'instruire, de former ou de sensibiliser tout type d'internaute, d'utilisateur, aux cybermenaces et donc aux moyens de s'en protéger afin d'en protéger autrui.

Toutefois malgré les conséquences tirées de ce rapport et des travaux animés par la DMISC[1] du ministère de l'Intérieur avec l'ANSSI, qui donnèrent « cybermalveillance.gouv.fr » (ACYMA), et en dépit des divers réseaux de sensibilisation existant, touchant les grosses entreprises, les petites et moyennes entreprises, les scolaires, *etc.*, les particuliers ne sont pas encore assez informés. Ils constituent alors une faille dans la cybersécurité collective nécessaire à la souveraineté notamment économique, numérique et politique du pays.

Cette vulnérabilité, par absence de connaissance de la menace et de ses impacts, doit être « patchée » ! Corrigée par un livret d'instruction civique numérique décliné, d'une part, en fonction des niveaux scolaires, écoles, collèges, lycées, universités ou supérieurs, afin de toucher ensemble ces classes d'âges et, d'autre part, à destination des adultes, même les plus âgés. Une campagne publique de sensibilisation citoyenne associant l'ANSSI, cybermalveillance.gouv.fr, des associations, tous les médias, et relayée par tous les ministères, accompagnerait l'édition de ce livret papier et numérique grâce à une démarche de mécénat d'entreprises éprouvée.

(1) Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces.

DÉTAIL

210. – Le constat : une faible culture des risques numériques dans une population qui s'approprie trop rapidement les nouveaux usages sans penser cybersécurité à l'aube de l'utilisation de milliards d'objets connectés. Beaucoup de programmes de sensibilisation touchent des entreprises mais peu les particuliers qui étalent pourtant leurs données comme des victimes consentantes. Aussi faut-il démarrer tôt les programmes pour, au fil des ans, faire progresser la nation en maturité. Les réflexes de base pour se protéger ne sont pas acquis, tels qu'un antivirus sur le smartphone et les mises à jour automatiques pour ne citer qu'eux. Il faut donc sensibiliser le grand public aux enjeux de souveraineté pour lui faire prendre conscience de l'importance de la cybersécurité. Si des réseaux de sensibilisation existent (ANSSI, cybermalveillance.gouv.fr, police et gendarmerie nationales et autres associations telles que ISSA France [*Security Tuesday*] ou le CESIN[2], le CLUSIF[3], *etc.*), ils touchent difficilement le grand public qui ne suit pas toujours les informations des institutions qui doivent s'adapter aux nouveaux canaux de communication. Les médias progressent dans quelques programmes sur les technologies ou rares sensibilisations de niveau du grand public tels que ceux de Raphaël Grably (BFM/RMC). Il est temps d'en finir avec un discours de prévention prétendument anxiogène, ce qui a limité la prise de conscience en minimalisant les menaces.

Aujourd'hui il est urgent qu'une campagne publique de sensibilisation citoyenne associant l'ANSSI (cybermalveillance, point de repère et de documentation) et relayée par tous les ministères, accompagne grâce à la mobilisation de la presse en ligne et audiovisuelle l'édition d'un livret « papier » et numérique grâce à une démarche de mécénat d'entreprises éprouvée.

211. – La proposition : éditer un livret d'instruction civique numérique à destination de publics d'âges différents lancé au moyen d'une campagne publicitaire publique et privée. La présente proposition comprend les dimensions suivantes :

– **l'objectif de conscientiser à la nécessité de cybersécurité, en fonction des publics**, pour arriver *in fine* à une cybersécurité attitude, naturelle, qui immunisera mieux les particuliers ce qui se ressentira partout ;

– **le plan d'action possible :**

• définition d'un contenu simple du ou des livrets civiques numériques,

• mobilisation des acteurs/contributeurs du contenu (cf. ISSA France),

• mobilisation des relais pour la campagne (Secrétariat d'État au numérique ; ministère de l'Éducation nationale, de la Jeunesse et des Sports ; ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation ; académies, presse, tous ministères et Service national universel, *etc.*) ;

• mobilisation des relais associatifs classiques et aussi SMLH[4], ONM[5] ;

(2) Club des experts de la sécurité de l'information et du numérique.
(3) Club de la sécurité de l'information français.
(4) Société des membres de la Légion d'honneur.
(5) Ordre national du Mérite.

• financement (acteurs mécènes pour levées de fonds, sachant que ce type de mécénat est déductible [ou peut être réduit] des impôts). Les entreprises privées seraient à même de s'engager sur des sommes de tous niveaux *via* les chambres de commerce et d'industrie, le MEDEF, la CGPME, Hexatrust par exemple.

La conscientisation doit permettre de préparer les esprits :

– des **petits** à la sécurité de leurs outils pour continuer à les utiliser correctement et tranquillement, et s'ils surfent sur Internet à les prévenir des dangers qu'ils courraient s'ils n'en étaient pas au courant ;

– des **adolescents** au même discours, mais adapté à leurs habitudes et outils afin de n'être pas une porte ouverte aux *hackers* et d'être un risque pour les autres ce qui leur coûterait de l'argent et des embêtements… Apprendre parallèlement la notion de souveraineté ;

– des **adultes** au risque que chacun constitue de ne pas s'intéresser à la cybersécurité, tant pour ses enfants et sa famille que pour son employeur et plus largement pour l'État, sous l'effet d'une indifférence qui non seulement facilite les appropriations frauduleuses de données et de fonds par les *hackers* voire l'espionnage de son entreprise ou son sabotage par les logiciels chiffreurs. Comprendre qu'en étant *cybersecure*, on participe à la défense de la nation car les chiffres de l'impact de la cybercriminalité sont très importants et appauvrissent le pays sur le plan macroéconomique.

Il n'y aura pas de souveraineté numérique si chacun n'en est pas acteur en défendant son propre environnement par un comportement de cybersécurité comme une seconde nature.

Paroles de partenaires du Cercle de la Donnée

Interview de Philippe Lavault, Secrétaire général de l'Agora 41

Propos recueillis en mai 2021

- **Pourquoi l'Agora 41 est-elle devenue partenaire du Cercle de la Donnée ?**

Partant du constat de Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), selon lequel le « cyber » n'est plus seulement une affaire d'ingénieurs mais touche désormais à la vie du citoyen, l'ANSSI a créé l'Agora 41 en octobre 2018, qui a pour mission de travailler sur des sujets périphériques à la cyber *stricto sensu*.

Il s'agit d'un club de réflexion et d'action, organisé autour de plusieurs groupes de travail (consacrés à des thématiques telles que « les talents », « les écosystèmes », « le rôle de l'État », « l'imaginaire de la cyber », « la régulation du cyberespace » ou encore « le cybermoi »).

Matthieu Bourgeois, par ailleurs membre fondateur et vice-président du Cercle de la Donnée, appartient au groupe « écosystème », au sein duquel la question de souveraineté était régulièrement évoquée.

Ainsi nous est venue l'idée que l'Agora 41 s'associe avec le Cercle de la Donnée pour produire un ouvrage global qui poserait les principes des interactions entre données et souveraineté numérique.

De par leur approche pluridisciplinaire, de par le fait qu'elles sont composées de personnalités diverses, de profils complémentaires, et nourrissent une vraie volonté d'ouverture à la société civile, nos deux entités se ressemblent et se correspondent.

À ce titre, l'ouvrage qui sortira à l'issue de nos travaux sera original, étant donné qu'il contiendra des propositions concrètes et pragmatiques que nous comptons bien diffuser auprès de l'administration et des décideurs, afin que ces réflexions et ces principes d'action infusent et se diffusent dans le contexte politico-administratif. Nous sommes un « cercle d'action » et, à ce titre, nous voulons avoir un effet ; notre objectif est bel et bien de servir et de faire bouger les lignes, et que nos réflexions débouchent sur de vraies décisions et implémentations.

- **En quoi la souveraineté numérique est-elle un enjeu majeur pour la France et l'Union européenne ?**

Le cyber prend aujourd'hui une telle place que sommes obligés de considérer une politique cybereuropéenne comme un élément constitutif de notre

souveraineté. Tout comme l'Union européenne a imaginé une politique étrangère et une politique de défense et de sécurité commune, elle doit désormais parvenir à constituer un quatrième pôle face aux États-Unis, à la Chine et à la Russie. Sans quoi, nous serons dépendants de l'un de ces pôles déjà constitués.

Le cyber pose de nombreuses problématiques, notamment industrielles ou encore de normes. Alors que, par exemple, la Chine vient d'édicter un arsenal normatif sur l'organisation de l'Internet, qui va créer un Internet chinois complètement fermé, la France et/ou l'Union européenne doivent porter des normes au niveau international sur ce sujet.

Dans le même temps, nous devons prendre en compte les GAFAM dans les négociations relatives à la politique cyber. On peut faire un parallèle avec l'apparition des organisations non gouvernementales au début des années quatre-vingt, qui ont constitué de nouveaux acteurs dans la gestion des conflits, face auxquels il a fallu créer un nouveau droit, celui de l'ingérence humanitaire.

On le voit bien, les enjeux cyber ont aujourd'hui une portée géostratégique. C'est pourquoi, au-delà de la résolution des conflits cyber, nous devons réfléchir à un système de régulation de ces conflits à grande échelle. On peut également s'interroger sur le droit d'ingérence cyber et sur la question de savoir si le cyber, à l'instar de la force nucléaire, peut avoir un « caractère égalisateur » tel que théorisé par Raymond Aron.

Les sujets à aborder sont d'envergure et il est clair qu'il y a énormément d'efforts à faire pour que l'Union européenne aille vers une souveraineté numérique. Pour autant, aujourd'hui, les oppositions sont telles entre les trois blocs établis que rien n'est joué et nous pouvons encore faire bouger les choses.

- **Au-delà de ces travaux sur la souveraineté numérique, quels sont les principaux enjeux de l'Agora 41 et de l'ANSSI en 2021 ?**

L'Agora 41 fête ses deux ans et, en parallèle de notre travail avec le Cercle, plusieurs réalisations sont en train de voir le jour. Elles ont toutes en commun de privilégier la démocratisation et la vulgarisation des sujets liés au cyber, afin de favoriser une prise en compte de ses enjeux par tous les publics. Nous voulons contribuer à faire prendre conscience que la cybersécurité est l'affaire de tous et ne doit pas être uniquement considérée comme un sujet technique, juridique, dangereux et inaccessible.

Un prix du « roman cyber Agora 41 » a été créé par le groupe « imaginaire », dont le jury sera présidé par Guillaume Poupard. Dix-neuf éditeurs participent à cette première édition dont le lauréat sera dévoilé en octobre.

Le groupe « cybermoi » a créé un questionnaire de Proust adapté au cyber et à sa compréhension auquel un éventail de personnalités varié (professeurs, artistes, influenceurs…) va répondre, sous forme d'interviews filmées qui seront largement diffusées ;

Le groupe « talents » réfléchit avec le Medef à la notion de « responsabilité numérique des entreprises » et travaille avec le ministère de l'Éducation nationale sur deux sujets : la notion de « cybercitoyenneté » et la féminisation des métiers du cyber.

Au niveau de l'ANSSI, les enjeux liés au numérique ne manquent pas, parmi lesquels :

- la préparation de la présidence française de l'Union européenne, dont les trois piliers en matière de cyber sont la nouvelle version de la directive « Sécurité des réseaux d'information » (SRI ou NIS en anglais), le développement d'un principe de solidarité (qui conduirait à s'unir pour répondre ensemble à l'attaque d'un des membres de l'Union) et la mise en place d'une unité cyber-conjointe ;
- le déploiement du cybercampus à Nanterre, une initiative lancée par le président Macron et soutenue par l'Agence, avec pour objectif de regrouper dans un lieu unique les différents acteurs français de la cyber (chercheurs, *startups*, administrations…), afin de favoriser la communication et le développement des collaborations ;
- le développement de la cybersécurité dans les territoires dans le cadre du plan de relance ;
- le développement d'un vivier de recherche stratégique lié au cyber, avec notamment la mise en place d'une session « Souveraineté numérique et cybersécurité » en collaboration avec l'Institut des hautes études de Défense nationale (IHEDN). L'idée étant d'avoir une approche stratégique, multi-disciplinaire du cyber qui est encore trop souvent appréhendé en silos en France.

En savoir plus sur l'Agora 41

Compte tenu de l'impact et des conséquences – effectives ou prévisionnelles – de la transformation numérique sur nos sociétés, c'est tout un écosystème, composé d'acteurs de la sécurité numérique mais aussi issus de l'ensemble de la société civile, qui se transforme et s'organise. Pour accompagner cette nouvelle dynamique, et répondre aux enjeux partagés par tous, il convient désormais d'aller plus loin pour favoriser les conditions d'un dialogue renforcé entre l'agence et des représentants de la société civile et de nos institutions.

C'est pourquoi l'ANSSI, autorité nationale en matière de cybersécurité et de cyberdéfense, reconnue dans son écosystème pour son expertise et son expérience, a lancé l'Agora 41. Cet espace de réflexion réunit quarante et une personnalités (chercheurs, universitaires, dirigeants, cadres, étudiants, *etc.*), que les enjeux de transformation numérique interpellent et mobilisent.

Les membres, au cœur du projet

L'Agora 41 est avant tout une tribune d'expression libre, multidisciplinaire qui propose à ses membres d'étudier des thématiques liées au numérique.

Pour mener une réflexion transverse et innovante, l'Agora tire parti de la diversité des expertises des personnalités bénévoles qui la composent. Ce sont donc les membres de l'Agora 41 qui la font vivre grâce à une réflexion commune et ouverte sur des thématiques transverses.

Les travaux de l'Agora 41

Animée par l'ANSSI, l'Agora s'est structurée sous forme de groupes de travail thématiques. Chaque membre a ainsi choisi un des cinq sujets proposés par l'ANSSI, qui ne couvrent pas son périmètre d'action : l'imaginaire, la régulation du cyberespace, les talents pour le cyberespace, l'écosystème ou le cybermoi.

Les fruits de leurs réflexions seront destinés à être partagés publiquement au sein de l'écosystème de la transformation numérique mais également plus largement avec toute personne intéressée par les enjeux du numérique.

Whaller

Interview de Thomas Fauré, Fondateur et *Chief Executive Officer* de Whaller

Propos recueillis en juin 2021

- **Pourquoi Whaller est-il devenu partenaire du Cercle de la Donnée ?**

Lorsque nous avons rencontré les membres du Cercle il y a plus de deux ans, j'ai été séduit par l'idée de connecter un écosystème autour de la donnée, un sujet vaste, dont chacun a une compréhension différente. J'ai beaucoup apprécié l'idée de réunir des profils variés qui peuvent ainsi s'éclairer mutuellement.

Nous sommes ravis notamment d'avoir pu, grâce à notre plateforme, permettre aux membres du Cercle de garder le lien pendant la crise sanitaire, notamment grâce à la digitalisation des « jeudis de la donnée », le rendez-vous mensuel de l'association.

Plus que jamais, je suis convaincu que les travaux du Cercle, notamment autour de la souveraineté numérique, et le travail de sensibilisation que vous menez auprès des décideurs politiques sont cruciaux pour aider à une prise de conscience devenue plus qu'urgente.

- **Quels changements en termes d'utilisation et d'usage de votre plateforme avez-vous pu constater avec la crise sanitaire ?**

Le premier confinement a été une véritable révolution, qui s'est traduite par une augmentation par quatre du trafic sur notre plateforme. À la suite de ce confinement, à l'automne 2020, nous avons assisté à une montée en puissance de l'utilisation de Whaller chez certains clients, qui se sont mis à vraiment le déployer et l'utiliser beaucoup plus largement.

Mais au-delà de cette accélération opérationnelle, nous avons surtout assisté à un raz-de-marée des GAFAM, un déferlement rendu possible, d'une part, par le fait – dans le cas de Microsoft notamment – que les outils proposés étaient compatibles avec un écosystème « SI » déjà existant et, d'autre part, par une piraterie concurrentielle d'acteurs comme Zoom qui ont proposé du gratuit à tout-va.

Ce déferlement me rend très inquiet.

- **Pourtant, il semble que la crise sanitaire a fait émerger le sujet de la souveraineté ?**

Certes, avec la crise la notion de souveraineté, tout à coup, ne s'est plus apparentée à un gros mot. On voit probablement de nouvelles lignes politiques se dessiner, le clivage gauche/droite étant possiblement remplacé par une opposition entre ceux qui défendent une vision mondialiste et ceux qui sont attachés à la souveraineté. Ce sujet, couplé à la notion de développement d'une économie « locale » (au niveau d'un pays), sera à mon avis un enjeu fondamental des prochaines présidentielles. Tous les pays du monde sont concernés, en premier lieu les pays qui hébergent les GAFAM et leurs homologues asiatiques.

Le véritable danger, c'est que les GAFAM font tout pour s'inscrire dans ces stratégies souveraines. Nous avons eu un exemple éclatant récemment avec cette annonce gouvernementale du *Cloud* dit « de confiance » qui engage certes des parties prenantes françaises (Orange et Cap Gemini), mais qui va surtout créer un cadre « de confiance » pour Microsoft et pour Google. Il n'y aura dès lors plus de concurrence possible, à l'instar de ce qui s'est passé pour le *Health Data Hub*.

Je reste combatif et optimiste, mais je suis inquiet de la naïveté de nos politiques, inquiet également pour le *software* français et européen, inquiet, en un mot, pour l'alternative. Revenons à un esprit de conquête et limitons l'expansion des GAFAM grâce à la législation.

- **Avez-vous senti une évolution des comportements à l'égard de la notion de souveraineté ?**

Du point de vue des utilisateurs, la prise de conscience des interlocuteurs est très variable et il est vrai que la notion de « souveraineté », si elle est effectivement souvent mentionnée, reste parfois au stade de l'incantation.

C'est d'ailleurs pour cela que nous n'en faisons pas un argument commercial en tant que tel, mais plutôt un sujet de communication par le haut (à travers nos prises de position dans les médias, nos tribunes…). Commercialement, notre argument c'est la technique, et il me semble que c'est une bonne chose car on ne peut prétendre à la souveraineté technologique sans être technologique. À titre personnel, je me suis remis depuis 2020 à coder chaque jour, car c'est notre ADN. Je suis un ingénieur, nous faisons de la technologie, seule voie selon moi pour acquérir une stratégie industrielle. C'est d'ailleurs parce que notre technologie *made in France* développée depuis dix ans est crédible que nous arrivons à nous battre au coude à coude avec les GAFAM.

On peut toutefois souligner que la récente prise de position de la Commission nationale de l'informatique et des libertés (CNIL) concernant l'utilisation de Zoom dans l'enseignement supérieur fait bouger les lignes et nous apporte beaucoup de prospects. Cette décision nous donne de l'espoir en termes de prise de conscience et de décisions stratégiques dans ce secteur.

- **Quelle est votre vision de l'évolution des réseaux sociaux d'entreprise ?**

L'e-mail a prédominé pendant vingt à trente ans, puis les réseaux sociaux d'entreprise ont bouleversé la donne il y a une quinzaine d'années. On assiste aujourd'hui à une convergence des usages de communication et aussi à une grande diversification des canaux. Il s'agit désormais d'avoir une plateforme pour gérer toutes ces communications, pour gérer le travail numérique, et j'ai la conviction que cette tendance sera pérenne. Cette évolution nous a d'ailleurs amenés à changer notre *baseline*, désormais « plateforme sociale et collaborative sécurisée ». En revanche, il est temps que nous construisions un modèle de travail européen. Adopter des outils anglo-saxons implique de développer des usages anglo-saxons, pour le meilleur et pour le pire. Chez Whaller, nous avons la conviction que le respect de la confidentialité, la sobriété numérique, l'équilibre vie professionnelle/vie personnelle, la limitation des interruptions font partie d'une façon de travailler à la française et nous nous efforçons de traduire cela dans notre plateforme.

J'appelle de mes vœux à une prise de conscience que l'outil induit l'usage et c'est pourquoi nous sommes particulièrement heureux d'être présents dans le milieu de l'éducation et de l'enseignement supérieur, car les élèves et étudiants utilisateurs d'aujourd'hui sont les citoyens de demain. Leur faire prendre conscience qu'ils doivent reprendre le contrôle sur l'usage du numérique me semble primordial.

En savoir plus sur Whaller : la plateforme sociale et collaborative sécurisée

Whaller est une solution française simple et complète qui permet de créer des réseaux sociaux et collaboratifs sécurisés.
Respectueuse des données de ses utilisateurs et garante de leur confidentialité, la plateforme s'adresse aux entreprises, organisations, administrations, établissements éducatifs, associations comme aux particuliers. La sphère, élément principal et distinctif de Whaller, est un espace sécurisé et dédié de partage, de discussion ou de collaboration. À partir d'un seul compte, l'utilisateur peut créer, administrer ou rejoindre une infinité de sphères indépendantes les unes des autres. L'utilisateur communique ainsi en toute confiance avec différents publics sans les confondre.
Whaller place la sécurité au cœur de son ADN :
– la protection des données est primordiale (pas de publicité ni d'exploitation de données) ;
– les entreprises peuvent choisir où sont stockées leurs données (SaaS ou *On-Premise*) ;
– la plateforme est conçue sur les bases de la *Privacy by Design*.
La structuration et la communication au sein de votre entreprise sont facilitées grâce aux sphères qui permettent :
– une meilleure scalabilité : sphères, organisations, fédérations pour une évolutivité permanente des plateformes de nos clients et une contextualisation systématique ;
– une solution multiréseaux : nos clients peuvent communiquer en interne et aussi avec des personnes externes ;
– une autre idée de la productivité : préserver l'attention de nos utilisateurs, en les rendant proactifs et en augmentant leur focus.
La plateforme Whaller peut être une solution clé en main ou sur-mesure pour nos clients (variété de fonctionnalités, typologies de réseaux, personnalisation complète, intégrations tierces, marque blanche, codéveloppement).

Interview croisée de Nicolas Vetriak, Président fondateur de Novaminds et de Matthieu Bourgeois, Vice-président du Cercle de la Donnée en charge des partenariats et Président du groupe de travail « Souveraineté numérique »

Propos recueillis en octobre 2021

- **La *data* est au cœur de votre ADN depuis votre création en 2014. Avez-vous senti un changement de perception, une prise de conscience collective concernant l'importance de la donnée dans les organisations et plus largement dans notre quotidien ?**

N.V. : Des réflexions ont été engagées au niveau européen et plus largement au niveau international sur les nouveaux enjeux en matière de *data*, tant sur les aspects défensifs (*reporting* réglementaire, gestion des risques, contrôle financier…) que sur les aspects offensifs (campagne marketing, pilotage d'activité, rentabilité, expérience client…). On parle beaucoup d'éthique de la donnée et des liens sont faits, de plus en plus, entre la donnée et la responsabilité sociétale des entreprises (RSE), notamment du fait d'une demande croissante de la collecte de données en lien avec l'environnement, le social et la gouvernance (ESG). Cette évolution, qui avait été engagée bien avant la crise sanitaire, s'est accentuée avec la crise. En faisant émerger de nouveaux modes de collaboration, de nouveaux modèles opérationnels et donc de nouveaux usages en matière de donnée, la pandémie a agi comme un accélérateur rendant la donnée de plus en plus présente dans notre quotidien.

Jusqu'à présent, les organisations étaient majoritairement dans une approche défensive concernant la gestion et l'exploitation de leurs données, en se concentrant sur les réponses réglementaires afférentes. On assiste aujourd'hui à l'émergence de stratégies plus offensives – en lien avec les nouveaux usages – avec pour objectif la création de valeur pour les utilisateurs, les clients, les partenaires et plus globalement la société civile. Ces nouvelles stratégies cherchent une prise en compte permanente des nouveaux enjeux en termes d'éthique, de protection des données et de souveraineté numérique.

M.B. : Notre groupe de travail consacré à la souveraineté est né au moment du confinement, période pendant laquelle on a assisté à un changement de paradigme. Alors que la vie physique passait par le filtre numérique, on a constaté une véritable explosion du volume de données échangées. Dès lors, la nécessité de protéger ces données est devenue plus évidente. Nous avons également ressenti, au sein de notre groupe de travail, un besoin important d'un réinvestissement de l'État. La puissance publique doit mieux protéger l'espace numérique, pour sortir de ce *far west* actuel, et qui n'est pas viable à long terme.

- **Vous partagez avec le Cercle la conviction de l'importance de produire des contenus de qualité pour partager vos idées et peser sur le débat public. C'est d'ailleurs tout l'objet de cette étude du Cercle consacrée à la souveraineté numérique. En quoi est-ce un enjeu important d'après vous ?**

N.V. : La souveraineté numérique est un enjeu majeur pour les organisations qu'il faut adresser au niveau européen, seul échelon adéquat pour pouvoir peser notamment face aux États-Unis et à la Chine. Dès lors, il convient de s'organiser au niveau européen pour trouver une réponse commune et harmonisée. Le cadre est en cours d'élaboration mais il reste beaucoup à faire ; il faut aller plus loin pour se prémunir contre l'hégémonie des puissances étrangères. Nous devons rester maîtres de notre souveraineté numérique.

Reste à déterminer les leviers dont nous disposerons pour garantir notre indépendance numérique. Au-delà d'un cadre juridique harmonisé au niveau européen, cela suppose aussi de mettre en place, à brève échéance, un ensemble de mesures concrètes et pragmatiques pour garantir l'indépendance numérique.

M.B. : Dans notre étude, nous avons résolument adopté une démarche volontariste, avec notamment trois propositions qui visent à instaurer une puissance en matière numérique : la première consiste à stimuler l'investissement numérique par des réformes fiscales, la deuxième à réformer le droit de la concurrence pour casser ces nouveaux trusts informatiques qui se sont formés depuis trente ans au profit des Américains et des Asiatiques. Enfin, notre troisième proposition est de créer des professions réglementées – à l'image des notaires, des avocats et des commissaires aux comptes du XIX^e^ siècle qui ont fait de la France et de l'Europe une grande puissance mondiale – et qui aujourd'hui manquent, nous semble-t-il, pour développer une filière de la donnée basée sur l'excellence. Il nous semble indispensable de sortir de l'économie informatique actuelle qui est fondée sur le *bug*. En tant que gros consommateurs de numérique, les Européens font les frais de cette logique économique, qui contribue à enrichir les fournisseurs de numérique, majoritairement américains. Nous croyons qu'il faut instaurer une comptabilité numérique, un commissariat au numérique, *etc.*, pour assainir les règles du jeu, séparer le bon grain de l'ivraie, fermer la porte de notre marché à des acteurs peu scrupuleux et également garder nos talents, notamment nos ingénieurs européens.

N.V. : Il faut aussi faire évoluer les mentalités, du côté des donneurs d'ordre, certes, mais aussi du côté du consommateur. Ce dernier sera-t-il prêt à payer plus ou à consommer différemment pour privilégier la souveraineté numérique et les intérêts de la nation et de l'Europe au détriment des solutions des puissances étrangères ?

M.B. : Sur ce point, nous pensons que les politiques feront ce que le citoyen demande. C'est pourquoi l'indifférence citoyenne est à notre avis la pire des choses contre laquelle il faut lutter. Dès lors que les citoyens voudront que les politiques se saisissent de ce sujet, ils le feront. C'est d'ailleurs l'objet d'une des propositions de notre étude.

- **Quels sont selon vous les autres enjeux majeurs concernant la donnée dans les prochaines années ?**

N.V. : Quand nous assistons aux pratiques de certaines puissances étrangères, avec notamment des faits de cybersurveillance, de violation de la vie privée…, nous pouvons nous demander si un label éthique et sécurité « *made in Europe* » n'est pas la clé pour inciter les consommateurs à privilégier des solutions qui garantissent la souveraineté numérique, la sécurité, la confidentialité, l'intégrité et l'éthique des données. Cette question de l'éthique sera de plus en plus prédominante avec le développement notamment de l'intelligence artificielle.

Par ailleurs, la question de l'*open data* et de la normalisation des échanges de données entre les organisations va devenir clé. Il n'y a pas encore de consensus clair en termes de normalisation, mais face à la croissance exponentielle du volume de données échangées, nous sentons poindre une prise de conscience et émerger des influences sur ce sujet.

Enfin, le lien naturel entre l'écologie et la RSE se dessine, mais le cadre réglementaire se renforce en la matière dans le même temps. Il y a de nombreuses incitations à la prise en compte des critères ESG dans les organisations que nous accompagnons.

M.B. : Nous venons de créer un groupe de travail consacré à l'écologie numérique, qui nous semble le prochain défi à relever. La question de la pollution numérique nous semble clé : longtemps considérée comme un élément virtuel, la donnée doit être au contraire pensée comme une ressource physique qui a des conséquences réelles sur notre environnement. Tous, nous allons devoir opérer une révolution copernicienne pour que « donnée » ne soit plus synonyme « d'illimité ».

En savoir plus sur Novaminds

Cabinet de conseil innovant, Novaminds est un acteur de référence en gouvernance de la donnée, conformité, gestion des risques et cyber-résilience. Novaminds accompagne les plus grands établissements du secteur financier dans la maîtrise de leurs transformations et des risques associés.

Novaminds propose des offres de services de pointe et des réponses sur-mesure dans un contexte de renforcement de la réglementation, de mutation et de digitalisation des entreprises et se positionne en *leader* d'opinion sur ses expertises.

Ses équipes pluridisciplinaires accompagnent leurs clients dans toutes les étapes de leur transformation, depuis la stratégie jusqu'à la mise en œuvre opérationnelle. Elles disposent d'une large expérience en matière de transformation et de gestion du changement.

Les experts de Novaminds apportent leur expérience et leur connaissance des meilleures pratiques du secteur financier avec, au cœur de leurs interventions, la donnée et l'apport des solutions technologiques nouvelles pour les directions.

Interview croisée de David Bessot, *Chief Strategy Officer* d'Adequacy, et de Matthieu Bourgeois, Vice-président du Cercle de la Donnée en charge des partenariats et Président du groupe de travail « Souveraineté numérique »

Propos recueillis en octobre 2021

- **Adequacy est partenaire du Cercle de la Donnée depuis sa création en 2018. Ces dernières années, et plus particulièrement ces derniers mois, on a senti les lignes bouger, notamment à la faveur du confinement. Toutefois, pensez-vous qu'il y a eu une prise de conscience collective de l'importance de la donnée dans les organisations et plus largement dans notre quotidien ?**

D.B. : Non, pas encore. Il me semble qu'en ce qui concerne le numérique, nous sortons tout juste de l'adolescence, de la pensée magique avec laquelle nous avons été élevés pendant vingt ans, qui consistait à croire que pour résoudre chaque besoin ou problème, il y avait une application. Or, après deux ans de confinement et de télétravail forcé, avec un flux de mails continu dans notre journée, de visioconférences qui s'enchaînent, on commence à se rendre compte de l'étendue du problème. Nous sommes en train de prendre conscience que notre utilisation du numérique crée une dette à trois niveaux. Une dette, tout d'abord, en matière de souveraineté, puisque si nous n'utilisons pas des applications françaises et européennes, nous prenons le risque de perdre la maîtrise de nos données. Une dette écologique, car aujourd'hui nous prenons conscience de l'impact écologique du numérique. Une dette enfin, au niveau humain, car nous nous sommes rendu compte, à travers cette crise sanitaire, que la collecte massive de données sensibles posait question. Nous sommes aux prémices d'une prise de conscience collective, mais nous n'avons pas encore compris à mon sens quelle était l'étendue du problème.

M.B. : Le confinement nous a fait prendre conscience de l'aspect inévitable du numérique, même pour les plus réticents d'entre nous. Nous avons constaté une explosion du volume des données, le *big data* devenant le *big*

big data, avec une donnée qui n'est pas normalisée et une multiplication des canaux de communication, qui entraînent de l'épuisement et de la perte d'efficacité. Nous sommes en train de comprendre le coût que le « tout numérique » a sur notre santé, notre fatigue et aussi, vaguement, sur notre souveraineté. Il y a deux ans, lorsque nous avons constitué notre groupe de travail, le terme « souveraineté » était synonyme de chauvinisme, voire de nationalisme, à contre-courant de l'idée dominante du libre-échange sans entrave. Avec la crise sanitaire, il y a une prise de conscience dans le débat public de la dépendance, de la fragilité et de l'exposition extrême de notre continent. On a déjà compris pour d'autres biens et services les problèmes causés par la libre circulation à tous crins ; nous sommes en train, avec un peu de retard, de comprendre la même chose concernant la libre circulation des données, qui pose des questions de surveillance massive, de dépendance et d'amenuisement des ressources. Le regard a changé, la souveraineté est désormais considérée avec intérêt, c'est devenu un concept *mainstream*.

- **Le Cercle de la Donnée et Adequacy partagent la volonté d'éduquer les consciences, ce qui peut paraître ambitieux. Qu'entendez-vous par là, concrètement ?**

  D.B. : Aujourd'hui, la transformation numérique est terminée ; tout le monde travaille avec des outils digitaux au quotidien. Nous entrons donc dans une nouvelle ère qui est celle de la donnée. Nous sommes un peu dans la même situation qu'au début du XX^e^ siècle avec l'arrivée de l'électricité, qui allait remplacer la lampe à huile en appuyant sur un bouton. Il me semble urgent qu'on réfléchisse ensemble et qu'on comprenne ce qu'on entend par la donnée. Éveiller les consciences sur ce sujet, c'est se construire une conscience éclairée de tous les usages que nous pouvons avoir de l'outil numérique et avoir présentes à l'esprit les questions que cela pose en matière de souveraineté, de géopolitique ou encore d'empreinte écologique. Dès lors que nous sommes – de par notre métier – concernés et mobilisés sur le sujet, je suis convaincu que nous avons un rôle social et sociétal à jouer. C'est ce que fait le Cercle de la Donnée à travers ses travaux sur la souveraineté, sur l'intelligence artificielle et demain sur l'écologie numérique. C'est ce que nous faisons à notre niveau chez Adequacy, en tant que prestataire, lorsque nous expliquons à nos clients que la contrainte juridique est plutôt quelque chose de bénéfique pour la population et pour le *business*, que l'écologie peut être intégrée dans une stratégie sans tomber dans le lobbying de la sobriété… Comprendre les impacts écologiques, la dette technique et les implications en matière de données personnelles, et intégrer cela dans la façon de prendre des décisions, c'est l'objectif d'un éveil des consciences. Il faut que les gens se construisent leur propre vision du numérique et arrêtent d'être guidés par les intérêts des industriels, qu'ils soient européens, américains ou chinois. Je suis convaincu qu'éveiller les consciences, c'est participer à ce chantier-là.

M.B. : Avant l'apparition de la technique vers 1800, l'humain était infirme et libre. Il est devenu depuis puissant mais très dépendant. Et s'il n'est pas éduqué, il ne fait pas bon usage de sa puissance et finit par se détruire lui-même et tout ce qui l'entoure. « Science sans conscience n'est que ruine de l'âme », écrivait Rabelais. Cette maxime est plus vraie que jamais, dans un monde où la technique a pris une telle place. Nous ne possédons aucune intuition venue de nos ancêtres sur ce sujet, nous n'avons aucun réflexe reptilien dans le numérique. L'éducation est donc absolument clé dans ce domaine. Nous devons nous éduquer nous-mêmes, sans quoi les usages sont infinis. Il peut alors en résulter de grands bénéfices, mais également de nombreux dégâts.

D.B. : Quand je vois que le « pass sanitaire » a suscité des débats sur l'utilisation de nos données (que l'on y soit favorable ou pas d'ailleurs), quand je vois que des députés se sentent concernés par la question de la souveraineté ou que la CNIL réfléchit à la façon de traiter nos données de santé, que les politiques commencent à s'interroger sur l'endroit où sont stockées les données, je me dis que les choses sont en train de bouger. Éveiller les consciences, c'est peut-être agir sur le temps court.

M.B. : Dans notre étude, nous avons fait le constat de l'indifférence citoyenne liée à ce manque d'éducation dont nous venons de parler, et qui a pour effet l'inaction politique. Rencontrer des parlementaires[1] a donc été très important pour nous, car nous souhaitons que les politiques reprennent l'initiative de la vision et des idées, qui ne doivent pas uniquement venir du peuple. Nous n'avons plus de temps à perdre, d'où l'importance, nous semble-t-il, de sensibiliser à la fois les politiques et les citoyens, qui sont aussi des électeurs.

- **Quels sont vos projets majeurs pour les mois ou années à venir ?**

D.B. : Chez Adequacy, nous avons pour ambition de proposer l'outil de gestion de données à caractère personnel le plus efficace au service du délégué à la protection des données (DPO). Nous sommes convaincus que le métier de DPO va évoluer et prendre de plus en plus d'ampleur, dans un contexte réglementaire qui va profondément modifier la façon dont les organisations gèrent leurs données. Pour ce faire, notamment, nous allons sortir prochainement un ouvrage intitulé *Les douze travaux du DPO*, qui a pour vocation d'être un livre de référence dans la durée et qui sera évolutif sur les dix prochaines années. Nous nous engageons sur cette période, tous les ans, avec nos équipes d'experts à mettre à jour ce document pour en faire un guide pour les personnes qui prennent la responsabilité de protéger les données personnelles des citoyens européens.

(1) Le groupe de travail a rencontré, dans le cadre de la rédaction de son étude, le député Jean-Michel Mis et la sénatrice Catherine Morin-Desailly.

Nous avons un autre projet intitulé « La *Junior Privacy* », qui consiste à accompagner les plus jeunes pour qu'ils entrent dans l'ère du numérique. C'est un projet pluriel regroupant plusieurs initiatives :

- l'accueil d'élèves de troisième pour éveiller la conscience de ces jeunes de quatorze ans aux sujets de la donnée et du numérique ;
- un programme de recherche que nous sommes en train de monter avec l'Université de Paris 8 pour comprendre la perception du droit par les jeunes sur les plateformes du numérique ;
- la création d'un compte Instagram qui vise à rencontrer les jeunes là où ils se trouvent pour leur permettre de se forger une culture générale autour de la donnée et du numérique.

M.B. : Pour 2022, le chantier auquel nous allons nous atteler sera l'écologie. Notre approche visera à faire émerger des usages vertueux de la donnée en changeant notre regard sur cette dernière. La donnée ne doit plus être vue comme quelque chose de virtuel, d'illimité, d'hyper-circulant, de non rival, de libre de droit, mais à l'inverse comme une ressource fragile qu'il faut gérer de manière durable. Un nouveau groupe de travail sur ce sujet vient de se constituer au sein du Cercle, dont les échanges et travaux déboucheront sur une nouvelle étude. Comme à chaque fois, nous allons redéfinir le sujet sous l'angle de la donnée, faire émerger les principaux défis liés à ce sujet, et bien sûr, proposer des solutions.

D.B. : Cette approche du Cercle est très intéressante car elle va permettre d'appréhender l'écologie du numérique non pas avec un regard purement technologique, comme c'est souvent le cas, mais selon une approche pluridisciplinaire, à l'image des compétences que regroupe ce *think tank*. Une approche peut-être plus humaine également, qui va finalement permettre de s'interroger sur l'impact de la donnée sur son environnement et sur le modèle de société que nous voulons.

En savoir plus sur Adequacy

Créée en 2016, Adequacy est une solution logicielle spécialisée dans le management des données à caractère personnel. Avec plus de 6 500 entités juridiques utilisatrices dans le secteur public comme dans le secteur privé, cette solution, 100 % développée en interne et hébergée en France, est un acteur majeur sur le marché de la conformité au règlement général sur la protection des données (RGPD) en France et en Europe.
Plus d'info sur www.adequacy.app.

Souveraineté numérique :
Essai pour une reconquête

Être souverain, c'est présider seul à ses destinées. Sommes-nous, français et européens, souverains sur les réseaux numériques ? Pouvons-nous y déployer librement notre diplomatie, nos politiques économiques et sociales, à l'abri des menaces d'espionnage et de captation de valeur mises en mouvement par d'autres États ou opérateurs privés ?

Il est permis d'en douter, si l'on est attentif à certains symptômes qui se manifestent aujourd'hui. Ceux-ci trouvent en partie leur cause dans la faiblesse de l'offre numérique européenne dont il résulte un déficit d'autonomie vis-à-vis d'autres puissances (étatiques mais aussi non étatiques) en suprématie sur l'espace numérique.

« Est maître des lieux celui qui les organise » dit l'adage. Or les réseaux numériques (dont Internet qui en relie un grand nombre d'entre eux) ne sont pas nés, pour la plupart, de la volonté des États européens, mais se sont au contraire développés de manière empirique et tentaculaire au gré des besoins de tous ceux qui l'exploitent. Et, en la matière, force est de constater que ceux qui ont forgé l'offre numérique ont essentiellement été des acteurs non européens, qui ont par conséquent dicté aux utilisateurs les usages servant leur modèle économique, voire idéologique.

Il est encore temps de réagir, et cela nécessairement à l'échelle européenne, seul niveau pertinent pour rivaliser avec les cyber puissances actuelles. L'occasion pour notre vieux continent de renouer avec son projet fédérateur, en bâtissant ensemble une puissance numérique. Des pistes sérieuses existent, à condition d'être ambitieux !

LES AUTEURS :

Cette étude est le fruit d'une collaboration entre des membres du Cercle de la Donnée (think tank interdisciplinaire réunissant des spécialistes soucieux d'éthique et d'excellence, produisant des travaux prospectifs sur le numérique et la donnée) et de l'Agora 41 (tribune de réflexion – lancée par l'Agence Nationale de Sécurité des Systèmes d'Information – libre, multidisciplinaire et originale réunissant 41 personnalités autour des enjeux de la transformation numérique).

ISBN : 978-2-9581579-0-6
Hors commerce