CERNA
Commission de réflexion sur l'Ethique de la Recherche en sciences et technologies du Numérique d'
ALLISTENE

La souveraineté à l'ère du numérique
Rester maîtres de nos choix et de nos valeurs

CERNA

Rédacteurs : Jean-Gabriel Ganascia, Eric Germain, Claude Kirchner

Octobre 2018

Table des matières

RÉSUMÉ

La révolution numérique en cours conduit à des questionnements éthiques inédits dont chacun est invité à se saisir. Issue de la philosophie politique où elle se restreint à l'idée de souveraineté nationale, la souveraineté peut se définir comme la capacité pour une entité de se donner ses propres règles ou, plus trivialement, comme « le pouvoir de pouvoir ». Ce concept de souveraineté demeure pertinent pour appréhender et analyser l'impact des sciences, technologies et usages du numérique. Cependant, nous devons le revisiter tant les problématiques soulevées par le numérique bouleversent le concept classique de souveraineté, en particulier celui de souveraineté nationale. Elles en modifient les conditions d'expression et en facilitent la contestation par des intérêts extérieurs. Loin de conduire à abandonner toute idée de souveraineté nationale, le numérique offre de nouveaux points de vue sur ce concept et amène à y intégrer différentes formes de souveraineté, qui incluent en particulier la question de la souveraineté sur les infrastructures, les souverainetés numériques des États, des organisations ou des citoyens, les souverainetés scientifiques, ou des souverainetés supranationales, comme la souveraineté européenne, qui apparaissent clairement aujourd'hui comme tout à la fois désirables et nécessaires.

Dans ce contexte, les enjeux éthiques qui apparaissent et que nous développons sont de deux ordres :

1. en l'absence de souveraineté, les choix résultant d'une réflexion rationnelle et de l'expression d'une volonté libre ne peuvent être mis en œuvre, la souveraineté est donc essentielle à une éthique appliquée ;
2. par ailleurs, le numérique transforme, mais ne supprime pas, l'expression classique de la souveraineté des peuples. L'ère numérique, malgré ses effets de globalisation, ne gomme ni l'expression des diversités culturelles ni le besoin et le droit des communautés humaines de se gouverner et se de forger un destin autour de valeurs, d'esthétiques et de choix politiques partagés.

Cependant, la coexistence de ces différentes formes de souverainetés amène inéluctablement à des conflits entre des souverainetés d'ordres différents, qu'il faudra surmonter. Cela conduira certainement à l'avenir à envisager des procédures inédites de résolution. Ce rapport ne porte pas sur ces procédures qui relèveront de choix politiques, mais s'attache avant tout à la caractérisation de ces nouvelles formes de souveraineté et aux enjeux qu'elles portent à l'horizon d'une société numérique.

Après l'introduction situant l'ensemble de la problématique, dans une première partie, nous rappelons les fondements historiques de la notion de souveraineté. La seconde partie développe les aspects conceptuels de la souveraineté en mettant en relief les points sur lesquels l'ère numérique conduit à une remise en question des notions traditionnelles, ce que nous développons dans la troisième partie. Nous explicitons dans une quatrième partie les souverainetés numériques d'une part et scientifiques d'autre part. Enfin, nous concluons en confrontant les enjeux éthiques et de souverainetés avec les réflexions géopolitiques contemporaines, la formation des citoyens et l'éthique scientifique.

Au travers du texte, chemin faisant, nous identifions d'une part les enjeux principaux liés au concept de souveraineté, nous énonçons des recommandations et faisons des suggestions, ces dernières sortant stricto-sensu des attributions de la CERNA tout en formant un ensemble cohérent avec les enjeux et nos recommandations. L'ensemble de ces éléments est résumé en fin de document.

INTRODUCTION

S'exprimant devant la 72e Assemblée générale des Nations Unies le 19 septembre 2017, le président des États-Unis cite pas moins de vingt-et-une fois les mots « *sovereign* » et « *sovereignty* »[1]. Il est difficile de ne pas voir dans cette insistance une réponse à la controverse du *Russiagate* où l'usage des technologies numériques est soupçonné d'avoir permis une ingérence russe ayant favorisé son élection. Donald Trump a à cœur de souligner qu'« *en Amérique, le peuple gouverne, le peuple dirige et le peuple est souverain* »[2].

Le même jour et devant le même auditoire, Emmanuel Macron affirme vouloir répondre à la vision fermée de la souveraineté de ceux qui « *croient que les murs et les frontières nous protègent* »[3], en plaidant pour une souveraineté qui n'oppose pas sécurité et ouverture sur le monde. Le Président de la République déclare ainsi : « *Ce qui nous protège, c'est notre souveraineté et l'exercice souverain de nos forces au service du progrès. C'est cela l'indépendance des Nations dans l'interdépendance qui est la nôtre* ».

Ces propos trouvent un écho tout particulier si on les rapporte aux enjeux de souveraineté posés par l'essor des technologies numériques dans un espace où l'on conçoit difficilement d'ériger des murs et des frontières, même si certaines tentatives se font jour à l'exemple du « Runet » qui se présente comme le segment russe d'Internet.

Les conséquences des bouleversements provoqués par les sciences, technologies, usages et innovations du numérique sont omniprésentes. La numérisation globale change l'expérience du monde qui nous entoure et exerce une pression formidable sur de nombreuses formes du rapport de l'humain au monde.

Souveraineté et éthique s'articulent de manière fondamentale, car sans souveraineté, il est difficile d'élaborer une réflexion éthique qui nécessite liberté de pensée, d'action et d'accès à la connaissance et, surtout, il est impossible de mettre en œuvre de manière claire et responsable les choix découlant de cette réflexion.

La CERNA a débuté ce travail au moment où la Loi du 7 octobre 2016 pour une République numérique envisageait la création d'un Commissariat à la souveraineté numérique[4]. Il nous est apparu alors indispensable de réfléchir ce que représentait réellement cette « souveraineté numérique » et aux enjeux éthiques que ce sujet portait.

Il est intéressant de noter que le récent rapport sur l'intelligence artificielle[5] de la mission du député et

---

1https://www.whitehouse.gov/the-press-office/2017/09/19/remarks-president-trump-72nd-session-united-nations-general-assembly

2« *In America, the people govern, the people rule, and the people are sovereign* ».

3http://www.elysee.fr/declarations/article/discours-d-emmanuel-macron-devant-la-72e-assemblee-generale-des-nations-unies

4Art. 29: *Le Gouvernement remet au Parlement, dans un délai de trois mois à compter de la promulgation de la présente loi, un rapport sur la possibilité de créer un Commissariat à la souveraineté numérique rattaché aux services du Premier ministre, dont les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège. Ce rapport précise les moyens et l'organisation nécessaires au fonctionnement du Commissariat à la souveraineté numérique;* https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=F5935AFABF3AE72BDB108134B84C9F8F.tpdila08v_2?idArticle=JORFARTI000033203122&categorieLien=id&cidTexte=JORFTEXT000033202746&dateTexte=

5« Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne » ;

mathématicien Cédric Villani ne parle jamais de « souveraineté numérique », mais l'englobe dans une problématique plus vaste de « souveraineté technologique et économique ». Lors de la restitution publique de ce rapport, le 28 mars 2018, le Président de la République, Emmanuel Macron, décrit la souveraineté nationale comme la capacité pour une Nation de définir par elle-même les normes auxquelles elle se soumet et non de se voir imposer ces règles de l'extérieur. Affirmer que « l'intelligence artificielle est un impératif de souveraineté »[6], nous amène immédiatement à poser la question de savoir si la souveraineté à l'ère du numérique a encore le même sens, ce que nous abordons précisément ici.

Si nous retenons la définition la plus simple de la souveraineté comme étant la capacité de se gouverner soi-même, une nation, une entreprise, une communauté scientifique a-t-elle encore la capacité de concevoir et d'appliquer les choix éthiques que cette entité collective définirait pour elle-même ? À l'échelle de l'individu, la problématique est similaire, même si l'on parlerait alors d'autonomie plutôt que de souveraineté.

La souveraineté, notion charnière et structurante du rapport d'autorité légitime entre les êtres humains dans un État de droit, est particulièrement affectée par cette évolution technologique rapide et globale. La notion est apparue à l'aube de l'âge moderne, avec des théoriciens politiques comme Jean Bodin au XVI^{e} siècle puis John Locke au XVII^{e} siècle et Jean-Jacques Rousseau au XVIII^{e} siècle. Sa transposition actuelle, dans l'hyper-modernité consécutive à la généralisation de l'emploi du numérique dans toute la société, soulève nombre de questions, ainsi :

- En quoi, la notion de souveraineté en général, concept politique ou philosophique étranger aux sciences du numérique, peut-elle s'appliquer au numérique ? En d'autres termes, peut-on imaginer qu'une **souveraineté numérique** s'impose, soit en renversant la souveraineté politique nationale classique et les frontières des États, soit en coexistant avec elles ?

- Comment, les concepts et les pratiques de la **souveraineté nationale**, peuvent-ils s'harmoniser avec des systèmes planétaires de circulation des données numériques qui semblent conduire à l'obsolescence de la territorialité ?

Les souverainetés, qu'il s'agisse des souverainetés nationales ou numériques, doivent-elles s'appuyer sur **des outils et des services numériques ou des gouvernances dédiés** ? Les notions de système d'exploitation ou de *cloud* souverains ont-elles un sens ? En quoi la gouvernance de l'Internet (ICANN, W3C, …) défie-t-elle la souveraineté nationale ?Il nous semble important d'apporter trois précisions pour bien délimiter le périmètre de notre réflexion.
Il ne faudrait pas attendre de ce rapport qu'il donne une valeur éthique, positive ou négative, à la souveraineté que nous considérons avant tout comme un concept. La rédaction du présent rapport nous a permis d'apprécier la valeur heuristique de ce concept qui nous est apparu particulièrement pertinent pour comprendre les enjeux politiques, sociétaux et naturellement éthiques soulevés par le déploiement massif des technologies du numérique.
Il ne faudrait pas non plus lire dans nos propos un plaidoyer en faveur de la souveraineté nationale. La valeur éthique que nous pourrions associer à ce type de souveraineté dépend grandement d'autres paramètres tel que le type de régime politique du pays concerné : la souveraineté d'une démocratie libérale ouverte et pluraliste, avec le jeu libre de différents contre-pouvoirs, n'est évidemment pas la souveraineté d'un régime autoritaire et dictatorial. Par ailleurs, nous parlons bien dans ce rapport de souverainetés au pluriel. Dans cette pluralité, c'est bien la recherche du bien commun qui donne la valeur éthique d'une souveraineté qu'elle soit étatique, scientifique ou d'une entreprise[7].
Enfin, notre sujet n'est pas celui de la « démocratie face aux enjeux du numérique », bien qu'il présente des liens évidents avec notre propos et qu'il soit à plusieurs reprises évoqué sans que nous

http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/184000159.pdf

6https://www.la-croix.com/Economie/France/Cedric-Villani-Lintelligence-artificielle-imperatif-souverainete-2018-03-29-1200927629

7Le code civil français affirme dans son article N° 1833 que « *toute société doit* (…) *être constituée dans l'intérêt commun des associés* » ; http://codes.droit.org/CodV3/civil.pdf, cf. p. 349. La « responsabilité sociale des entreprises » (RSE) peut être vue comme une forme d'extension de ce principe d'intérêt commun au-delà des seuls associés ou actionnaires.

nous y attardions. Il s'agit par exemple des débats sur la neutralité du Net confrontée aux enjeux de la cybersécurité. En France, du côté de la puissance publique, la réponse à cette question est aujourd'hui envisagée dans la mise en place d'une relation de contrôle « efficace et raisonnable »[8] de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) par l'Autorité de régulation des communications électroniques et des postes (ARCEP).

Nous proposons donc une contribution à la réflexion sur ces questions en rappelant d'abord les fondements historiques (partie I) et conceptuels (partie II) de la notion de souveraineté et en mettant en relief les points sur lesquels l'âge numérique conduit à une remise en question des notions traditionnelles (partie III).

Nous visons ensuite à éclairer concrètement les enjeux éthiques et politiques que recouvre l'affirmation par les États-nations de leur souveraineté dans l'espace numérique (Partie IV).

Nous concluons en formulant des recommandations pour permettre aux citoyens, aux scientifiques et aux responsables politiques ou entrepreneuriaux d'avancer dans leurs réflexions sur le numérique et sur ses enjeux éthiques afin de leur permettre d'agir au mieux de leurs convictions et de prendre leurs responsabilités.

8Expression utilisée par Guillaume Poupard, directeur général de l'ANSSI, lors de son audition du 8 mars 2018 devant la Commission de la défense de l'Assemblée Nationale ; http://www.assemblee-nationale.fr/15/cr-cdef/17-18/c1718053.asp

PARTIE 1 : Retour vers la définition historique et classique de la souveraineté

Avant de voir en quoi le numérique remet en question l'idée classique de la souveraineté comme fondation de l'identité sociale, culturelle et politique d'une communauté humaine, rappelons comment cette notion a émergé de notre histoire. Présente en théologie ou en philosophies politique et morale, elle fut introduite très tôt comme la base du droit international.

Au sens étymologique, est souverain, ce ou celui qui est au-dessus de tous les autres. En cela, Dieu dans une théocratie, le roi dans une monarchie absolue ou le peuple dans une démocratie, peut être celui qui détient l'autorité suprême et autonome qualifiée de pouvoir souverain.

1.1. D'une souveraineté d'essence divine…

L'adjectif « souverain » a qualifié un pouvoir spirituel, avant de se rapporter à une autorité temporelle. Au sens théologique, le souverain est cette entité qui, du point de vue métaphysique, est adéquate à soi, dont l'essence repose sur soi. Elle est autonome, totale, et close, puisqu'il n'y a rien au-delà. Ainsi, de la réflexion augustinienne à la théologie scholastique on voit l'existence d'un Dieu souverain posée comme étant la totalité du réel, rien n'étant en dehors de lui. Dans son *Éthique*, Spinoza caractérise Dieu qui est « cause de soi » comme un être disposant d'une souveraine intelligence et d'une souveraine puissance[9]. Comme nous le verrons plus loin, cette clôture peut aider à surmonter le paradoxe de la souveraineté numérique qui peut être entendue de deux manières différentes. D'une part comme une souveraineté nationale sur les infrastructures du numérique, ce qui aboutirait à ce qu'une maîtrise totale de la gouvernance de l'Internet par les États conduise à une logique de fermeture, de censure et de contrôle des frontières, etc. D'autre part comme une souveraineté du numérique sur les autres formes de souveraineté locale, en particulier nationale, ce qui conduirait à une ouverture et une réinscription du national dans le global.

Enfin, dans un registre encore différent, en philosophie morale, on parle de « Souverain Bien » pour désigner un bien supérieur à tous les autres. De même, un devoir est dit souverain s'il ne peut être comparé à d'autres raisons d'agir, car découlant d'une rationalité propre.

En Europe occidentale, l'époque moderne est marquée par la volonté des monarques de s'émanciper de l'autorité spirituelle du Pape. Au XVI^{e} siècle, l'un des premiers actes de la construction de l'État-nation[10] fut d'affirmer l'autonomie du pouvoir temporel national sur le pouvoir transnational de l'Église. En France, en 1539, le souverain François Ier impose par l'ordonnance de Villers-Cotterêts l'usage du français sur le latin comme langue du droit et de l'administration. Cette politique accompagne le courant du gallicanisme qui, dans la sphère religieuse, tend à imposer un contrôle politique national sur le pouvoir « ultramontain » du souverain pontife[11]. Notons que l'étymologie latine première de « pontife » fait référence au premier pont de la ville de Rome et que @pontifex est le titre du compte twitter du Pape, choix affichant une volonté de « faire le pont »[12]. Ce choix illustre la proximité de la souveraineté universelle et « déterritorialisée »[13] de l'Église catholique avec ce qui pourrait être aujourd'hui une caractéristique d'une souveraineté « fluide et omniprésente »[14] appliquée

9Baruch Spinoza, *Éthique*, Première Partie.

10Le terme État-nation désigne la juxtaposition d'un État, en tant qu'organisation politique, à une nation, c'est-à-dire des individus qui se considèrent comme liés et appartenant à un même groupe; https://fr.wikipedia.org/wiki/%C3%89tat-nation

11Dans le royaume britannique, ce mouvement sera encore plus radical avec la création en 1534 d'une Église indépendante de la papauté.

12https://fr.wiktionary.org/wiki/pontifex

13La souveraineté de l'Église catholique réside davantage dans l'appareil étatique du Saint-Siège que dans le micro-État du Vatican (moins de 1000 habitants sur un demi km^{2}) avec la plus petite armée du monde (110 gardes suisses pontificaux) et sans monnaie propre.

14À propos de la révolution numérique, la députée Laure de la Raudière évoque très justement « une dimension

au domaine du numérique.

1.2. … à la souveraineté de la nation

La souveraineté affirmée dans le champ religieux est différente du modèle rattaché à l'idée d'État-nation qui s'est imposé au XVII[e] siècle avec les traités de Westphalie[15]. Ces traités concrétisent un ordre international où chaque État est souverain dans le choix de sa politique religieuse (*ejus religio, cujus religio*)[16]. L'État est vu comme une entité imposant une religion unique dans ses frontières et exerçant un « monopole de la violence physique légitime »[17] sur ses sujets. Ce monopole s'impose à l'intérieur des frontières contre l'ordre féodal et se défend à l'extérieur avec une armée de plus en plus « nationale ».

La souveraineté de l'État-nation se traduira dans un absolutisme royal (théorisé par Jean Bodin en France au XVI[e] siècle, puis par l'anglais Thomas Hobbes au siècle suivant), avant d'évoluer vers une souveraineté de la nation qui prendra la forme du parlementarisme britannique ou d'une version plus radicale dans la France révolutionnaire.

Avec la genèse de l'État centralisé au début de l'âge moderne, on a eu recours à la notion de « souverain » pour désigner le prince, le roi ou la République (Gênes, Venise, Genève, etc.), incarnant l'entité abstraite collective au nom de laquelle les décisions publiques sont prises. L'établissement d'un appareil d'État avec ses institutions et ses grands commis aboutit à son autonomisation, à sa séparation de la personne du monarque au cours du XVIII[e] siècle. La notion se développe et s'épanouit à travers les réflexions de Bodin, Hobbes, et Locke, entre autres, avant de jouer un rôle central dans la pensée pré-républicaine de Rousseau. C'est surtout ce dernier qui précise, dans *Le contrat social*, cette idée régulatrice de « souverain » comme étant la personne collective d'où émane la « volonté générale ». Il oppose alors le peuple « souverain » aux individus ou aux entités constituées qui poursuivent chacun leurs intérêts particuliers.

Ainsi, la Déclaration des droits de l'homme et du citoyen de 1789 stipule, dans son article 3 que : « *Le principe de toute Souveraineté réside essentiellement dans la Nation. Nul corps, nul individu ne peut exercer d'autorité qui n'en émane expressément.* »[18]. Dans cette conception très française, l'autorité n'émane ni de groupes qui en tant que corps intermédiaires n'agissent que comme factions[19], ni d'individus, compris comme étant au service de leurs besoins particuliers. Cet article comprend donc la loi nationale comme expression de la volonté générale, elle-même manifestation de la souveraineté populaire.

Affichant sa filiation avec l'héritage révolutionnaire, la Constitution du 4 octobre 1958[20] stipule ainsi au début de son préambule : « *Le peuple français proclame solennellement son attachement aux Droits de l'homme et aux principes de la souveraineté nationale tels qu'ils ont été définis par la Déclaration de 1789, confirmée et complétée par le préambule de la Constitution de 1946, ainsi qu'aux droits et devoirs définis dans la Charte de l'environnement de 2004.* ». Puis, dans son article 3 « *La souveraineté nationale appartient au peuple qui l'exerce par ses représentants et par la voie du référendum.* ». Elle combine ainsi dans cet article les notions de souveraineté populaire et de souveraineté nationale qui s'exprime dans le cadre politique d'un « État » (principe cardinal de

---

d'omniprésence temporelle, spatiale et sociale » ; https://www.youtube.com/watch?v=Q_V9V3gpzXk&t=9s; cf. 8:26'

15Les traités de Westphalie de 1648 mettent fin à la guerre de Trente Ans. L'expression « système westphalien » désignera par la suite le système international né de ces traités.

16Ce qui peut se traduire par « tel prince, telle religion » ou encore « celui qui dirige le territoire détermine la religion de ses sujets ».

17Concept développé par Max Weber que l'on retrouve dans son ouvrage *Le savant et le politique* (1919).

18https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789

19C'est l'esprit de la loi Le Chapelier de 1791 qui interdit les corporations et associations professionnelles.

20https://www.legifrance.gouv.fr/Droit-francais/Constitution/Constitution-du-4-octobre-1958; texte mis à jour le 3 mars 2017.

l'Organisation des Nations Unies créée en 1945).

1.3. Une souveraineté nationale triomphante, mais doublement contestée

Certains courants politiques considèrent que le système démocratique représentatif trahirait l'expression « pure » de la souveraineté du peuple. Situés plutôt aux extrémités de l'échiquier politique, cette conception qualifiée par ses détracteurs de « populiste » se présente par ses partisans sous l'étiquette de « souverainiste ».

Qu'il soit qualifié de populiste ou de souverainiste, ce courant connaît aujourd'hui un regain de force, notamment en Europe. Il affirme renforcer le modèle d'« État-nation » dans un mouvement d'évolution pluriséculaire passant d'une souveraineté « de droit divin », à la souveraineté « de la nation » puis à la souveraineté « du peuple », cette dernière étant accompagnée d'une mystique qui n'est pas sans évoquer la première acception.

Cependant, l'« État-nation » se voit aussi remis en question par d'autres acteurs, qui ne le perçoivent pas comme le seul cadre possible d'expression de la souveraineté. Ses promoteurs plaident pour le passage d'un modèle rigide et centralisé vers un cadre plus fluide obéissant davantage à un principe de subsidiarité.

Si le modèle Westphalien de l'« État-nation » s'est imposé à l'Europe, puis au monde, il n'a jamais été exclusif. Il a coexisté avec des pouvoirs religieux ou économiques agissant comme de quasi-États qui ont évolué vers une déterritorialisation de l'exercice de leur souveraineté.

Dans le domaine religieux, l'Ordre de Malte est également un exemple de quasi-État aujourd'hui complètement « déterritorialisé ». Il jouit cependant d'une diplomatie officielle qui connaît ces dernières années un certain renouveau. Une ambassade de l'« Ordre souverain de Malte » a par exemple ouvert en 2017 en Allemagne. Dans le domaine économique, on peut rappeler l'exemple des Compagnies des Indes occidentales et orientales qui, en Europe, aux XVII^{e} et XVIII^{e} siècles, régissaient « souverainement » leurs comptoirs et les territoires ultra-marins placés sous leur contrôle. C'est tout particulièrement le cas des Compagnie des Indes orientales néerlandaise et britannique qui en ont offert de parfaits modèles[21].

Ces deux exemples correspondent à ce que l'historien Fernand Braudel qualifie d'« économie-monde » : l'ordre de Malte (comme les républiques maritimes de Venise ou Gênes) s'est développé dans l'espace méditerranéen et les Compagnies des Indes dans l'espace transocéanique. **L'espace marchand de l'« économie-monde numérique » n'est pas sans rappeler certains traits de ces exemples historiques**. Ils peuvent nous aider à mieux définir le concept de souveraineté qui, aujourd'hui, se caractérise principalement par ses objets et ses moyens d'exercice.

21On pourrait également citer d'autres modèles d'organisations économiques transnationales plus « souterraines » rivalisant avec les souverainetés étatiques, à l'exemple des triades et autres mafias pour lesquelles le numérique offre aujourd'hui de nouvelles ressources (ex. crypto-monnaies facilitant le blanchiment financier).

PARTIE 2 : Comment penser la souveraineté autrement ?

2.1. Définir le terme de « souveraineté » par ses objets…

Aujourd'hui mise en cause par le numérique et la mondialisation, l'idée de souveraineté nationale reste fondamentalement attachée à l'ancienne notion de souveraineté politique théorisée par Locke, Voltaire, Rousseau et d'autres. Il existe toujours des prérogatives qui sont reconnues comme relevant *a priori* de la compétence des États. Parmi celles-ci, on admet d'abord les fonctions régaliennes : sécurité intérieure, défense, renseignement, diplomatie, justice, finances, en particulier la politique monétaire et la perception de l'impôt et des taxes.

Certains pays comme la France considèrent que l'« éducation nationale » relève également d'une fonction souveraine de l'État, car elle offre aux futurs citoyens la possibilité de développer un sens critique et une maîtrise des outils méthodologiques d'accès à la connaissance et à la culture. Il faut sans doute y voir l'influence, assumée au plus haut niveau de l'État, d'un « *esprit des Lumières qui fait que notre objectif* (…) *est bien l'autonomie de l'homme libre, conscient et critique* »[22]. La problématique d'une mission régalienne d'« instruction publique » des nouvelles générations est aujourd'hui ravivée par le développement des technologies numériques. De même, certains pays comme la France pensent que l'organisation du système de santé demeure une prérogative de la souveraineté nationale.

La tradition française d'une conception élargie des fonctions régaliennes s'exprime à travers des compétences plus étendues : langue officielle, santé, environnement, transports et leurs infrastructures, solidarité (assurances sociales, retraites, chômage, etc.).

Non seulement le champ des sujets perçus comme relevant du cœur de la souveraineté d'une collectivité humaine peut varier, mais également leur hiérarchisation. L'exemple de la Catalogne illustre ainsi une orientation politique privilégiant la langue, la culture et l'éducation sur les sujets de politique monétaire ou de contrôle des frontières et qui correspond aussi au projet fédéraliste européen.

Cette approche de la souveraineté par ses objets nous conduit à revoir le concept classique de souveraineté **en nous attachant à la capacité du souverain, en tant qu'entité collective, à maîtriser pleinement les attributs dont il revendique avoir le contrôle** : territoires (frontières), armée, police, monnaie, langue, code civil, etc.

Le terme « maîtrise » est utilisé ici pour exprimer le fait que l'entité concernée est à la fois indépendante et reconnue comme telle par ses homologues et qu'elle possède aussi les moyens effectifs de l'exercice de son autorité.

La coexistence de ces différents ordres de souveraineté peut susciter des rivalités et engendrer des conflits, C'est le cas par exemple lorsqu'une entité supranationale supplante une entité nationale sur certaines prérogatives.

2.2. Tenir compte pragmatiquement des moyens de son exercice dans un monde globalisé

La souveraineté n'a de sens que si son détenteur a les moyens de ses ambitions. Dans le cas de la souveraineté nationale, celle-ci repose sur la maîtrise des fonctions régaliennes de défense nationale, de sécurité intérieure, de diplomatie et de justice[23] auxquelles on doit adjoindre la maîtrise de l'économie de marché en y incluant la collecte de l'impôt et dans une certaine mesure la monnaie. Typiquement, un État ne sera souverain que s'il détient par exemple des moyens crédibles pour défendre ses frontières (diplomatiquement ou par la force), maintenir l'ordre social et prélever l'impôt.

22Discours d'Emmanuel Macron devant le Parlement réuni en congrès, 3 juillet 2017 ; http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-devant-le-parlement-reuni-en-congres/

23En matière de justice, il y a un double niveau de souveraineté : une juridiction nationale peut être souveraine, mais il est également reconnu aux juges un « pouvoir d'appréciation souverain ».

La maîtrise de ces fonctions régaliennes a motivé l'acquisition et le contrôle des données, informations et connaissances et a donné lieu par exemple à la rédaction de doctrines nationales de domination de la sphère informationnelle (« *information dominance* » ou, plus diplomatiquement, « *information superiority* »). Les services de renseignement, les protocoles de communication et la cryptologie ont été, de tout temps, des moyens d'assoir la souveraineté nationale. Depuis le bâton de César jusqu'aux techniques de chiffrage contemporaines les techniques de conservation du secret et d'acquisition d'informations ont été (et sont encore largement) contrôlées par les États. Cependant, avec l'avènement des technologies de l'information et de la communication, en particulier avec le développement d'Internet, puis de ce que l'on appelle le numérique, à savoir d'une société toute entière pénétrée par ces technologies, la maîtrise de l'information, de sa transmission et de son traitement prend une importance bien plus considérable, puisqu'elle devient la clef de tous les échanges et de toutes les activités sociales. De ce fait, l'État n'a pas pu conserver, seul, la prérogative du chiffrage. Rappelons qu'en France ce n'est qu'en 1998, lorsqu'il fallait permettre aux banques d'offrir des services en ligne, que la cryptographie sans limite de résistance a été mise légalement à la disposition des citoyens et des entreprises. On voit qu'aujourd'hui la maîtrise des communications et du traitement de l'information est potentiellement accessible, dans les démocraties, à de multiples entités, depuis les grandes entreprises jusqu'aux simples citoyens[24].

Dans ce contexte, la souveraineté est à la fois mise en avant, contestée et confrontée à ses propres limites. Il existe des limites *doctrinales*, des limites *pragmatiques* (liées en particulier à la mondialisation), et des limites *technologiques*.

Les limites *doctrinales* tiennent essentiellement à une opposition entre deux traditions issues des Lumières, une tradition plus libérale, qui veut réduire au maximum l'emprise de l'État, sans toutefois le supprimer, face à une tradition plus étatiste qui donne à la souveraineté une plus grande extension, en conservant toutefois un espace privé. La tradition française est nettement étatiste. Mais, même dans la tradition la plus libérale, l'État assume toujours les fonctions régaliennes de défense, de sécurité intérieure, de justice, de finance et de diplomatie. Ainsi, en 2008, lors de la crise dite des *subprimes*, le gouvernement britannique est-il intervenu pour sauver les banques de la faillite. En revanche, un gouvernement libéral peut déléguer à d'autres entités plusieurs de ses compétences, comme la santé, l'éducation et parfois même des missions de sécurité et de défense (par exemple la société militaire privée Blackwater rebaptisée Academi en 2011).

La deuxième limite, *pragmatique*, tient à ce que les États ne vivent pas isolément : ils entretiennent entre eux des relations multiples qui viennent nécessairement limiter leur pouvoir. En cela les États n'ont jamais pu être totalement souverains et ils le sont moins encore aujourd'hui. La souveraineté nationale se trouve limitée par les conventions et traités internationaux, par le droit international et le droit de la guerre ainsi que par des renonciations volontaires des citoyens d'un pays à leur souveraineté pour participer à une entité supranationale plus étendue. C'est en particulier le cas en France, pour l'Europe. Ainsi dans le contexte très particulier du lendemain de la deuxième guerre mondiale le préambule de la constitution de 1946 a prévu que, sous réserve de réciprocité, « La France consent aux limitations de souveraineté nécessaires à l'organisation et à la défense de la paix. ». Et l'on accepte alors la règle selon laquelle « Les traités ou accords régulièrement ratifiés ou approuvés ont, dès leur publication, une autorité supérieure à celle des lois » (article 55 de la constitution). L'intégration européenne conduira ensuite à l'abandon de certaines prérogatives régaliennes de la nation, comme de « battre monnaie ».

La troisième limite est d'origine *technologique* et tient aux multiples dépendances des systèmes technologiques nationaux avec les systèmes internationaux. Le numérique est clairement l'un de ces systèmes et probablement le plus important, mais ce n'est pas le seul. Pensons par exemple aux systèmes de normalisation international, la conduite à droite ou à gauche, la largeur des voies de chemin de fer ou à la tension des systèmes électriques jusqu'aux RFC (*Requests For Comments*) de l'IETF ou du W3C[25]. Les frontières technologiques, pour ainsi dire, ne sont pas identiques aux

24Par exemple, en utilisant les messageries sécurisées comme Protonmail ou Telegraph, les bibliothèques de chiffrement comme PGP ou Veracrypt.

25L'IETF est l'*Internet Engineering Task Force* (IETF), un groupe de travail international informel qui depuis 1986 élabore des standards Internet. Le *World Wide Web Consortium* ou W3C a été créé en 1994 pour

frontières nationales.

2.3. Souveraineté ou autonomie ?

La souveraineté s'oppose à l'ingérence tout comme l'autonomie s'oppose à l'hétéronomie (« qui reçoit sa loi du dehors, au lieu de la tirer de soi-même »[26]). Souveraineté et autonomie sont des notions voisines mais, paradoxalement, c'est souvent au nom d'une « autonomie » régionale ou communautaire que la souveraineté nationale se trouve aujourd'hui contestée.

L'expression d'irrédentisme traduit plus précisément la question ancienne d'un territoire revendiquant de s'extraire de la souveraineté d'un État dont il fait partie pour acquérir une souveraineté propre. L'exemple de la Catalogne est encore une fois intéressant car il s'agit de revendications d'une souveraineté partielle (refus de la souveraineté espagnole mais acceptation d'une très forte délégation de souveraineté à l'Europe) et sélective, revendications qui se concentrent sur les éléments les plus centraux de l'identité d'une collectivité (langue d'usage et d'éducation, manuels scolaires, conception de la laïcité, etc.).

Les exemples de revendications « autonomistes » à l'intérieur même d'une nation peuvent nous aider à préciser et à mieux comprendre les différences entre autonomie et souveraineté.

Si ces deux notions sont évidemment reliées, la souveraineté implique la capacité à reconnaître l'indépendance et, par conséquent, la capacité à être représenté auprès des autres souverains en tant que détenteur d'un pouvoir reconnu et indépendant[27]. Du rapport à la transcendance des premiers usages du mot souveraineté, la notion a conservé une certaine sacralité. Une fois définies, les frontières des états modernes ont ainsi pris un caractère d'inaliénabilité[28]. Jusqu'à récemment, l'indépendance s'exerçait essentiellement sur un territoire géographique identifié. Aujourd'hui l'espace des données et celui des capacités de calcul viennent étendre les notions de territoires sujets de notre réflexion.

L'autonomie peut qualifier une collectivité comme un individu, voire un objet ou un ensemble d'objets (par exemple les voitures autonomes ou les essaims de drones), alors que dans son acception historique, la souveraineté est par essence collective.

En toute rigueur, on devrait réserver la notion d'autonomie pour une échelle individuelle (« libre arbitre ») et souveraineté pour l'expression d'une volonté collective. Mais nous sommes dans une situation où l'individu autonome aspire aussi à être indépendant grâce, en particulier, aux nouveaux outils numériques. On aboutit donc à consacrer une notion inédite (oxymore pour certains) de « souveraineté individuelle », notion déjà utilisée dans le discours politique en particulier, mais sur laquelle les rédacteurs de ce rapport ont des visions contrastées.

promouvoir la compatibilité des technologies du *World Wide Web*.

26Définition du Larousse : http://www.larousse.fr/dictionnaires/francais/h%C3%A9t%C3%A9ronome/39795

27« *Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State*. » Max Huber. Cour permanente d'arbitrage, sentence arbitrale, p.8, in https://pcacases.com/web/sendAttach/714

28En France, le principe d'inaliénabilité irrévocable et absolue du domaine royal fut affirmé par l'édit de Moulins de 1566.

PARTIE 3 : la notion classique de souveraineté de l'État-nation au défi du numérique

Par « le numérique » nous désignons ici les sciences, technologies, usages et innovations induits par l'identification, l'étude, le stockage, la transformation, la réception ou l'émission de l'information. En effet, l'information est au centre de cette révolution scientifique, technologique et humaine, au même titre que la matière, l'énergie ou le vivant au siècle précédent[29]. Les impacts du numérique sur notre réflexion philosophique, scientifique, technologique et sociétale transforment profondément nos sociétés contemporaines. Qu'en est-il de la notion de souveraineté ?

3.1. De l'utopie libertaire des premières heures d'Internet…

Une certaine notion de volonté populaire se trouve aux origines de l'ère numérique. Dès l'apparition des premiers concepts d'informatisation et d'Internet lors des années 1950 à 1980, et davantage au moment de la première itération du World Wide Web aux années 1990, le numérique a été regardé comme dévoilant l'horizon d'une certaine utopie politique, sociale et même spirituelle. Pour certains, le numérique pouvait devenir un espace dans lequel l'idéal de la volonté populaire s'exprimerait instantanément et donc se marier à une démocratie authentique à laquelle tous les citoyens participeraient en direct, de chez eux. Ainsi, a-t-on souvent évoqué l'idée d'« agora planétaire » en référence à l'agora dans la citée grecque, c'est-à-dire l'espace de discussion publique où s'élaborait la politique. Dans son fameux manifeste « *Declaration of Independence of Cyberspace*[30]» (1996) John Perry Barlow[31] annonce ainsi une nouvelle forme de souveraineté, un « nouveau domicile de l'esprit » au sein duquel les gouvernements du monde industriel n'auront aucune prise[32]. Barlow décrit un monde où les utilisateurs des données numériques possèderont une autonomie distincte en vertu de leur positionnement dans l'espace numérique et non pas en raison des normes ou des règles politiques des institutions démocratiques. Plusieurs institutions de gouvernance se sont créées par la suite dans la même logique, telles le W3C ou l'*Internet Engineering Task Force* (IETF), même si l'espace numérique s'est vite montré difficilement gouvernable, d'autant que les États-Unis, actuellement leader de ce nouveau secteur économique, n'ont pas souhaité abandonner une capacité d'influence si précieuse.

Comme nous venons de le rappeler plus haut et comme l'exprime très bien Michel Serres, le champ du numérique porte sur l'émission, la réception, le stockage et la transformation de l'information. Or, le domaine de l'information, et par là celui du numérique, est un secteur majeur d'exercice de la souveraineté, car celui qui maîtrise l'information surpasse ses concurrents dans sa capacité à savoir, à décider et à communiquer. Cet avantage est très explicitement l'objectif recherché par la doctrine de la domination dans la sphère informationnelle mise en œuvre en particulier par les États-Unis. Il est résumé par la citation de Barbara McNamara, directrice adjointe de la *National Security Agency*, qui affirmait en 1999 : « Tout en protégeant nos propres communications, la capacité de comprendre les communications secrètes de nos adversaires, capacité dans laquelle les États-Unis surpassent le reste du monde, donne à notre nation un avantage incomparable. »[33]. Cependant, si pendant longtemps l'information servait surtout au renseignement, pour disposer d'un avantage sur ces rivaux, aujourd'hui elle prend une dimension plus importante encore, puisqu'elle devient le support et la

29« *Information is information, not matter or energy. No materialism which does not admit this can survive at the present day.* » N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine* (1st. ed. 1948). Cambridge, MA: MIT Press, cf. p. 132.

30https://www.eff.org/cyberspace-independence

31John Perry Barlow (1947-2018), fondateur de l'*Electronic Frontier Foundation*.

32« *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.* » John Perry Barlow.

33« *The ability to understand the secret communications of our foreign adversaries while protecting our own communications, a capability in which the United States leads the world, gives our nation a unique advantage.* »

condition de toute vie sociale, qu'il s'agisse des échanges interhumains, des banques, des systèmes d'information hospitalier, de l'administration, etc.

Cette politique mobilise l'ensemble de l'appareil d'état américain comme l'affirme l'*Executive Order* N°12333 du 4 décembre 1981 dont l'énoncé de l'objectif débute ainsi : « L'effort de renseignement des États-Unis doit apporter au Président et au Conseil de sécurité nationale l'information nécessaire leur permettant de fonder leurs décisions en matière de diplomatie, de défense et de politique économique tout en protégeant les intérêts nationaux des États-Unis des menaces de sécurité étrangères. Tous les ministères et agences gouvernementales doivent coopérer pour atteindre cet objectif »[34].

L'information utilisée par les États pour contrôler leur territoire et l'activité de leurs ressortissants se distingue de l'information utilisée grâce aux technologies de l'information et de la communication par l'ensemble des citoyens. Si la maîtrise de l'information a toujours représenté un enjeu majeur pour la souveraineté nationale, l'élément nouveau tient à l'utilisation des technologies du traitement et de communication, d'où son importance cruciale à tous les niveaux de l'économie, de la vie sociale, des médias. Elle concerne tant les nations que les entreprises, les associations et les citoyens qui, au cœur de leurs foyers, peuvent participer à la vie de la cité.

3.2 … à des tentatives de démocratie directe

Les plateformes numériques proposent de nouvelles agoras d'échange qui visent à renforcer une expression libre et directe des citoyens. Elles concurrencent les organisations intermédiaires traditionnelles : syndicats, partis politiques, associations diverses. Il convient d'écouter avec attention la directrice de la communication de Google-France lorsqu'elle choisit d'illustrer la politique de « responsabilité sociétale » de son entreprise par trois exemples : l'aide à la révolution égyptienne de 2011 (le logiciel *Voice-to-tweet* développé par Google avec Twitter proposé aux citoyens égyptiens pour contourner la censure d'Internet), l'aide aux lanceurs d'alerte (sans autre précision) et l'action de la société Change.org[35].

Certes, on pourrait légitimement s'interroger sur le sort de ces initiatives dites « citoyennes » (l'internaute incarnant le « citoyen du monde ») dans le cas où elles se révèleraient en opposition avec la géopolitique de certains états ou des intérêts commerciaux (le cas des lanceurs d'alerte par exemple). Mais de manière plus significative, il nous semble intéressant de nous arrêter sur l'exemple de Change.org qui incarne un nouveau modèle de société philanthropique « à but lucratif »[36]. Son « *business model* » consiste en effet à mobiliser les sentiments moraux de la population afin d'acquérir une notoriété qui, dans l'économie numérique, représente une ressource valorisable. L'entreprise veut néanmoins incarner le parfait exemple du type d'initiative généreuse que la « démocratie du Net » peut produire. La plateforme de pétitions en ligne a bâti son succès sur des sujets populaires de protection de l'environnement, des droits de l'homme, de la santé. Mais elle se tourne aussi vers des sujets politiques comme la pétition demandant en 2013 la démission du gouvernement espagnol. Change.org étant une société marchande, sa valorisation repose sur sa capacité de mobilisation des opinions publiques acquise en soutenant des causes jugées « morales ».

Du point de vue de l'éthique, il conviendrait de s'interroger quand une société mercantile se pose en

---

34« *The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.* » ; https://www.archives.gov/federal-register/codification/executive-order/12333.html

35Intervention d'Anne-Gabrielle Dauba-Pantanacce, directrice de la communication de Google-France lors du colloque « L'héroïsme à l'ère de l'IA », à l'École militaire, le 18/12/2017. Il est intéressant de voir ainsi cette plateforme de pétitions en ligne mise en avant par la communication de Google, alors que les deux sociétés n'ont, à notre connaissance, aucun lien formel (si ce n'est la personne de Jennifer Dulski qui a quitté Google en 2013 pour prendre la présidence de Change.org).

36Tomio Geron, « The Business Behind Change.org's Activist Petitions », 5/11/2012 ; https://www.forbes.com/sites/tomiogeron/2012/10/17/activism-for-profit-change-org-makes-an-impact-and-makes-money/#6c1ce7e67ffa

parangon d'un modèle de souveraineté alternative. Le directeur de Change.org en France présente en effet sa société comme « une irruption citoyenne dans le débat public, un désir d'imposer des changements via les citoyens »[37]. Autour de l'idée que « grâce à la révolution numérique on peut mieux se faire entendre », il affirme que « l'objectif premier [de sa société] est " l'*empowerment*" c'est-à-dire de faire réaliser à chacun qu'il a un pouvoir. Tout ceci ne peut être géré par un algorithme… Il y a un accompagnement humain. ».

En hébergeant la pétition « *Loi travail : c'est toujours non, merci !* », cette entreprise (en collaboration avec Twitter et Facebook) assume de jouer le rôle d'acteur participant pleinement au jeu politique et affirmant proposer une alternative « moderne » aux partis politiques, syndicats et autres modèles associatifs. Change.org revendique aujourd'hui 9 millions d'utilisateurs et 2 millions de visiteurs uniques chaque mois. Que l'offre d'hébergement de Change.org comporte un accompagnement humain, c'est possible ; beaucoup d'algorithmes, c'est certain ; des outils numériques tels que ceux proposés par la société Nationbuilder[38], on peut aussi l'envisager.

Pour l'heure, la logique mercantile des entreprises œuvrant dans le domaine de l'« influence sociale » est présentée comme la meilleure garantie d'un accès non-partisan à leurs services. Effectivement, en France, les logiciels de la société Nationbuilder, par exemple, sont achetés et utilisés tant par Les Républicains, que La République En Marche ou le Parti Communiste Français. Mais, les choses évoluent et certains des grands acteurs du numérique assument désormais un engagement politique plus partisan.

Au début de la rédaction de ce rapport, il relevait encore du domaine de la prospective de s'interroger sur la problématique que poserait la candidature du fondateur et président de Facebook aux prochaines élections présidentielles américaines de 2020[39], alors que sa société détient une masse d'informations personnelles sur 200 millions d'utilisateurs aux États-Unis[40]. Le scandale Cambridge Analytica a montré qu'il convenait d'ores et déjà de réfléchir aux enjeux que posent aux démocraties, des États-Unis à l'Inde[41], l'accès asymétrique d'un candidat aux données personnelles d'une part significative de l'électorat. Il y a là assurément un défi éthique et politique majeur[42].

Plus généralement l'idéal d'une démocratie directe numérique pose le problème tant éthique que politique de sa légitimité. En effet le nombre d'expressions publiques numériques ne garantit pas leur représentativité tant les groupes organisés et maîtrisant bien le fonctionnement des réseaux sociaux sont à même de susciter des expressions orientées. De plus l'accessibilité de l'expression publique numérique reste marquée par des inégalités sur le plan technique et socio-culturel. Dès lors il convient de veiller aux conditions procédurales de construction de consensus entre groupes en conflits d'intérêts comme l'a souligné la philosophie de la « démocratie délibérative » initiée par John Rawls et Jürgen Habermas entre autres.[43]

37Olivier Pirot, « Change.org : les pétitions en ligne qui veulent changer le monde », *La Nouvelle République.fr*, 10/06/2017 ; https://www.lanouvellerepublique.fr/actu/change-org-les-petitions-en-ligne-qui-veulent-changer-le-monde

38http://nationbuilder.com/software

39Xavier de La Porte, chronique « Si Mark Zuckerberg devenait vraiment Président des États-Unis », *France Culture*, 17/01/2017 ; https://www.franceculture.fr/emissions/la-vie-numerique/si-mark-zuckerberg-devenait-vraiment-president-des-etats-unis

40https://www.statista.com/statistics/408971/number-of-us-facebook-users

41Barkha Dutt, « Even before Cambridge Analytica, India had already lost the data wars », *Washington Post*, 30/03/2018 ; https://www.washingtonpost.com/news/global-opinions/wp/2018/03/30/even-before-cambridge-analytica-india-had-already-lost-the-data-wars/?utm_term=.98a41d9037b4

42On peut en effet voir dans ce moment singulier, que Claude Lefort qualifie d'« épreuve d'une dissolution des repères de la certitude », le ressort d'une vie en commun autorisant la plus grande liberté d'opinion ; Philip Knee, « Claude Lefort, Montaigne et l'écriture de l'incertitude », *Revue d'histoire littéraire de la France* 2008/1 (Vol. 108), p. .21-36. DOI 10.3917/rhlf.081.0021

43https://en.wikipedia.org/wiki/Deliberative_democracy

3.3. Peut-on réduire la souveraineté numérique à un enjeu de chiffrement ?[44]

L'émission, la réception, le stockage, voire la transformation des informations sont de moins en moins contrôlés par des États souverains, ce qui pose, au-delà de la question de la souveraineté des États, des questions éthiques et légales qui paraissent tout à la fois nouvelles et complexes.

Ainsi, selon Pierre Bellanger, « *la souveraineté numérique est la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques.* »[45]. Mais aussi : « *Par le cloisonnement technique et matériel du modèle de la Chine ou de l'Iran, par le moyen d'une coordination au niveau national du chiffrement des données à intérêt national, pour une nouvelle forme de contrôle de frontière « chiffré », par un système d'exploitation en réseau faisant office de constitution, ou en insistant sur l'emplacement des applications et systèmes souverains—les serveurs--sur le territoire français et l'interdiction d'exportation des données*. »[46].

Quel est cet enjeu d'une nouvelle forme « chiffrée » de contrôle des frontières ? Techniquement, la communication d'informations, la préservation de l'intégrité ou de la confidentialité de données repose sur deux éléments essentiels : d'une part, la capacité d'un système informatique (SI) à garantir que les informations qu'il contient et les traitements qu'il effectue sont intègres et confidentiels ; d'autre part, la capacité à garantir que les communications issues du SI sont effectivement transmises, de manière confidentielle et intègre. Garantir les qualités d'un SI repose en particulier sur son système d'exploitation (SE ou OS, Operating System en anglais) et les qualités de ses composants matériels. On connaît aujourd'hui de multiples SE dont les noms les plus usuels sont Unix, Linux, Windows, MacOSX, ios, Android, VMS, Multics, CP/M, DOS et leurs multiples variantes. D'autres sont en cours d'élaboration, en particulier pour gérer des installations industrielles, des équipements ménagers, des voitures, les équipements de l'Internet des objets, etc. par exemple RIOT, Contiki, TinyOS.

La conception d'un SE « cybersécurisé » est un défi particulièrement complexe. Il n'existe pas aujourd'hui (en 2018) de SE qui soit prouvé, robuste et ayant des fonctionnalités suffisamment étendues pour en faire un SE largement utilisable. Mais l'état de l'art évolue rapidement et des fonctionnalités étendues sont actuellement disponibles, leur sécurisation reposant sur des capacités de chiffrement robustes et efficaces.

À cela, il faut ajouter qu'un SE ne suffit pas : des fuites peuvent s'organiser au niveau du BIOS *(Basic Input Output System*) ou, même au niveau du processeur. En conséquence, il faudrait d'une part repenser le SE et le BIOS ensemble pour fabriquer des machines « cybersécurisées », et d'autre part certifier le processeur lui-même.

Dans ce contexte scientifique et technique, la question peut donc s'analyser de deux manières différentes.

Première possibilité, les citoyens reconnaissent à l'État une position prééminente qui, pour des raisons de sécurité intérieure et de défense nationale, garantit la disponibilité d'un SE permettant d'assurer la souveraineté nationale. On se trouve alors dans la situation où des services de l'État seront, par exemple, à même de déchiffrer toutes les communications tout en assurant qu'elles ne soient pas déchiffrables par d'autres entités. Mais aujourd'hui, cette exigence de sécurité est contestée par l'exigence d'une protection maximale de l'intimité de la vie privée. Il conviendrait donc, dans ce cas, de trouver des garanties législatives et des procédures qui limitent cette intrusion de l'État dans les communications entre individus, organisations ou groupes. Cette première possibilité doit faire face à plusieurs difficultés que l'on voit d'ailleurs poindre dans le débat actuel sur l'utilisation de la cryptologie, dont les tribunes et rapports en 2017 de la CNIL[47] et du CNNum[48] se sont fait l'écho. En effet, elle implique d'assurer l'existence d'un tel SE souverain (avec le BIOS et le processeur), ce qui

44Cette partie a bénéficié de contributions de Didier Rémy, adjoint au directeur scientifique d'Inria.

45http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

46Pierre Bellanger, audition 19 octobre 2016.

47https://www.cnil.fr/en/node/23701

48https://cnnumerique.fr/wp-content/uploads/2015/04/2306_Rapport-CNNum-Ambition-numerique_sircom_print.pdf

est très difficile d'un point de vue technique. Par ailleurs, cette solution implique que tous les systèmes informatiques utilisent le même SE souverain, ce qui est extrêmement complexe techniquement avec des difficultés très concrètes. Ainsi, comment faire pour qu'un tel SE s'impose dans la population en remplaçant les SE plus ou moins propres à chaque marque (systèmes « natifs ») d'ordinateurs ou de téléphones ? Comment un SE souverain pourrait-il remplacer tous les SE qui sont nécessaires à l'Internet des objets ? Les expériences passées et récentes sur les logiciels libres de traitement de texte laissent assez dubitatif. En dépit d'une volonté affichée de passer au logiciel libre, l'administration a souvent envoyé des signaux contradictoires qui ont mis en difficulté tous les efforts. Par exemple, l'Agence nationale de la recherche (ANR) obligeait les candidats répondant à des appels à projets nationaux à utiliser des macros programmées dans la *Suite Office*, contraignant ainsi tous les postulants à acheter les logiciels de Microsoft. Un autre exemple est l'accord de partenariat signé le 28 novembre 2015 entre l'éducation nationale et Microsoft pour charger cette société de la formation des enseignants et des cadres de l'éducation nationale au numérique.

On converge donc vers une seconde possibilité où une souveraineté numérique nationale, « par le haut », est remplacée par la souveraineté numérique « par le bas », permettant à chaque utilisateur de rester maître de ses données et de ses communications dans une attitude volontariste assumée de chaque individu. Ceci peut reposer sur la disponibilité de SE (au pluriel) ayant les capacités à mettre en œuvre cette souveraineté numérique locale et dont la globalité est assurée par des communications chiffrées par des protocoles publics, dont les codes sont ouverts, vérifiables et vérifiés. La notion de « systèmeS d'exploitationS souverainS » trouve alors sa place dans ce contexte en mettant en place des SE en *open source* qui garantissent la sécurité publique et la souveraineté numérique, tout en préservant l'intimité de la vie privée. Outre les difficultés techniques à résoudre ce problème très contraint, se pose évidemment la question de l'accessibilité à des informations privées des services de renseignement, de police ou militaires à des fins sécuritaires (ex. anti-terrorisme, lutte contre la cybercriminalité, etc.).

Le chiffrement est incontestablement un enjeu très important de la souveraineté d'un État, mais le partage de cette capacité avec d'autres entités (communautés scientifiques, entreprises, voire le « quatrième pouvoir » qui est celui de la presse et des médias) semble une avancée démocratique récente[49] sur laquelle il serait dommageable de revenir. Par ailleurs, la souveraineté numérique ne saurait être réduite à cette seule question du chiffrement.

3.4. Quels attributs de la souveraineté classique peut-on encore protéger dans le monde numérique ?[50]

Que deviennent les attributs de souveraineté nationale dans un monde numérique et donc largement globalisé ?

L'une des limites pragmatiques à la souveraineté nationale vient du droit international et des traités passés entre États souverains. Or, le numérique exige des normes internationales, avec une circulation des informations libre et sécurisée. Sur ces principes, de grands acteurs privés prétendent de plus en plus rivaliser avec les États et assumer des fonctions qui faisaient jusqu'à une date récente l'objet d'un monopole régalien[51] :

- **Assurer la sécurité intérieure** : la reconnaissance faciale demande de disposer d'un grand nombre de photographies, ce dont, pour des raisons juridiques et techniques, la plupart des États ne disposent pas. En revanche, les réseaux sociaux peuvent sans difficulté assumer cette fonction. Par ailleurs, certains États exportent aujourd'hui leur savoir-faire technologique sécuritaire, par exemple la Chine vers l'Équateur.
- **Authentifier les personnes** : les réseaux sociaux proposent des services d'authentification permettant de certifier de l'identité d'un individu. Le Royaume Uni a par exemple envisagé un

49En France, l'utilisation de moyens de cryptés n'a été autorisé qu'à partir de 2004 et la Loi pour la confiance dans l'économie numérique.

50Cette partie a bénéficié de contributions de Didier Rémy, adjoint au directeur scientifique d'Inria.

51Jean-Gabriel Ganascia, *Le mythe de la Singularité : faut-il craindre l'intelligence artificielle ?*, éditions du Seuil, 2017, pp.107-126.

moment d'utiliser « l'identité Facebook » comme identifiant national. D'autres sociétés du Net proposent également ce type de service et vérification et de certification des identités (cf. https://www.civic.com).

- **Battre monnaie** : avec les crypto-monnaies comme le Bitcoin[52], mais aussi avec les monnaies locales restreintes à une communauté d'intérêt ou une communauté géographique, les monnaies nationales perdent leur exclusivité.
- **Établir le cadastre** : Google, par exemple, peut aider à percevoir l'impôt foncier dans certains pays comme en Grèce ou dans plusieurs pays d'Afrique où il n'existe pas. Établir les cartes utilisées internationalement, sans nécessairement une reconnaissance de l'ONU ou des pays concernés, peut empiéter considérablement sur la souveraineté nationale d'États en situation de conflits territoriaux[53].
- **Contrôler le trafic aérien** : l'aéroport suédois d'Örnsköldsvik devient fin avril 2018 le premier aéroport contrôlé depuis une distance de 150km, une technologie qui ouvre la possibilité de délocaliser les contrôleurs aériens (jouissant d'un statut de fonctionnaires en France) non seulement en dehors de l'aéroport, mais pourquoi pas, en dehors du pays.
- **Traiter les données de santé** : le traitement de données issues soit du système de santé, soit de réseaux sociaux (comme Twitter) ou encore de l'utilisation des données issues des moteurs de recherche entre complètement dans la mission régalienne de l'État en matière de santé.
- **Chercher en santé** : une société comme Calico ambitionne de décoder le génome pour trouver les gènes responsables des processus de vieillissement.
- **Attaquer et défendre** : des sociétés comme Zerodium proposent au plus offrant des attaques informatiques de type zero-day, c'est-à-dire inconnues jusqu'alors et par conséquent non détectées par la plupart des contremesures existantes, d'autres offrent des services de défense numérique des sites informatiques.
- **Chiffrer** : des sociétés spécialisées comme ProtonMail ou Telegram offrent des services de chiffrement de grande qualité, capables de rivaliser avec la plupart des moyens de chiffrement (ou de déchiffrement) y compris ceux développés par les États.
- **Établir et préserver des actes notariés** : des systèmes basés sur la technique de blockchain proposent des contrats de gré à gré qui par construction sont actuellement considérés[54] comme infalsifiables et pourraient à terme se substituer à certains actes notariés. Autre exemple, Creative Commons expérimente l'utilisation de techniques de blockchain pour enregistrer une œuvre ainsi que le nom de l'auteur, indiquer les conditions de la licence et suivre les modifications de l'œuvre sur internet.
- **Préserver le patrimoine** : la société Google a proposé en 2009 un accord de numérisation de l'ensemble des ouvrages de la BNF qui, controversé, n'a finalement pas été accepté.
- **Décider de la (ou des) langue(s) officielle(s)** : la langue des échanges, en particulièrement celle de l'administration relève de prérogatives régaliennes. Aujourd'hui, de plus en plus, les groupes privés imposent implicitement une connaissance de l'anglais qui devient un facteur d'intégration clef, car sans elle il devient très difficile de maîtriser les échanges.

À chacun de ces attributs de souveraineté sont associées des valeurs morales et donc des questions éthiques, des choix qui ne seront pas identiques d'un pays à l'autre. Ainsi, la définition

52La blockchain assure à chaque détenteur de bitcoins que l'argent qui est en sa possession est authentique et surtout qu'il est bien à lui, en ce sens qu'il n'a pas été cédé à d'autres et qu'il ne pourra pas l'être sans son consentement ; voir J.-G. Ganascia, « L'État peut-il rester tiers garant à l'heure de la blockchain ?», paru dans le magazine « L'ENA hors les murs » : https://www.aaeena.fr/group/l-ena-hors-les-murs/169/articles/l-etat-face-au-choc-numerique-mars-2018-n-478/23/04/2018/259

53Jean-Christophe Victor, *Le dessous des cartes, Asie itinéraires géopolitiques*, Tallandier et Arte éditions.

54Notons qu'à la date d'écriture de ce rapport, les propriétés des algorithmes du blockchain n'ont pas encore été analysées scientifiquement. Personne n'est donc en mesure aujourd'hui d'en garantir la robustesse à des attaques.

du patrimoine culturel et la sensibilité à sa préservation ne sont pas identiques à Paris, Santiago ou à Pékin[55]. De même, l'éthique médicale varie selon l'arbitrage entre libertés individuelles et intérêt collectif, arbitrage qui dépend dans une certaine mesure des cultures.

Ce n'est qu'après avoir établi le périmètre de ces attributs de souveraineté à protéger que l'on peut aborder les moyens et des conditions acceptables de leur protection.

3.5. Défendre seul ou à plusieurs la souveraineté numérique : la guerre avec d'autres moyens

Si le constat que nous venons de faire est partagé, un État doit-il y répondre seul ? Pour la défense, qui fut longtemps considérée comme le cœur même des compétences souveraines du pouvoir régalien, l'évolution est notable. Ainsi, en France, le dernier Livre blanc de la défense et de la sécurité nationale de 2013 affirme (nous soulignons) :

« Au niveau européen, en clarifiant le chemin que la France a décidé d'emprunter pour assurer sa sécurité, le Livre blanc vise à ouvrir avec les membres de l'Union un dialogue approfondi appelant une nouvelle ambition. Ce dialogue vise à ***substituer à des dépendances subies des interdépendances organisées, et à concilier ainsi souveraineté et dépendances mutuelles****. Au niveau global, il a pour objet d'expliciter comment la stratégie de la France s'insère dans la perspective plus large de la contribution de notre pays à un ordre international fondé sur la paix, la justice et le droit*. »[56].

Cette compréhension élargie du concept politique de souveraineté visant à « substituer à des dépendances subies des interdépendances organisées, et à concilier ainsi souveraineté et dépendances mutuelles » semble particulièrement intéressante pour aborder la question de la souveraineté numérique, mais est loin d'être universellement acceptée[57].

Quel que soit le périmètre privilégié (européen, franco-allemand, ou strictement national), nous sommes face à une question inédite de frontières numériques à préserver d'une ingérence étrangère dans une « guerre permanente ». Ainsi, les militaires rédigent désormais des doctrines de défense de l'« espace numérique national » qui, jusqu'à peu, était une *terra ingognita* du droit de la guerre.

Le centre de cyberdéfense coopérative de l'OTAN établi en Estonie a publié en 2013 une première édition d'un *Manuel de droit international applicable à la cyberguerre* (dit « *Manuel de Tallinn* »). Toujours sous la direction du juriste américain Michael Schmitt (colonel et professeur au *Naval War College*), la seconde édition de février 2017 intègre des problématiques se posant en temps de paix et traite notamment de l'application de la souveraineté au cyberespace. Il est très significatif de constater que la question de la souveraineté constitue le tout premier chapitre de l'ouvrage, la déclinant autour de cinq règles[58]. Le sujet du cyber-espionnage en temps de paix (règle 32) est également abordé.

Une question comme celle du renseignement, emblématique de la souveraineté étatique, permet de mesurer les différences « culturelles » qui peuvent exister aujourd'hui quant à l'acceptation de l'externalisation de certaines prérogatives étatiques à des sociétés commerciales privées. Ainsi dans le domaine éminemment régalien du renseignement, si l'ouverture au privé est très développée dans les pays anglo-saxons[59] (*US cyber command* ou le nouveau *National Cyber Security Centre* britannique) et en Israël, par contre, les positionnements français (DGSE) et allemands (BND) montrent clairement

55F. Koller, « Pékin rase son patrimoine pour les JO », *Le Temps, 4/12/2001 ; https://www.letemps.ch/culture/2001/12/04/pekin-rase-patrimoine-j-o*

56Livre blanc sur la défense et la sécurité nationale, 2013, p. 12 (souligné par les rédacteurs) ; http://www.defense.gouv.fr/portail/enjeux2/politique-de-defense/le-livre-blanc-sur-la-defense-et-la-securite-nationale-2013/livre-blanc-2013

57La Chine, par exemple, demeure marquée par le souvenir du XIXe siècle qualifié de « siècle de honte et d'humiliations » en raison du découpage de son territoire national en zones d'influence de puissances étrangères. Elle reste attachée à une conception stricte de la notion de souveraineté et au principe de non-ingérence extérieure. De même, dans ses relations internationales, la Chine n'accepte de participer à une intervention militaire de l'ONU que si le gouvernement du pays concerné donne son assentiment préalable.

58Cf. « *Sovereignty* » (p. 11-29), « *Rule 1: Sovereignty (general principle) / Rule 2: Internal sovereignty / Rule 3: External sovereignty / Rule 4: Violation of sovereignty / Rule 5: Sovereign immunity and inviolability* » ; http://assets.cambridge.org/97811071/77222/toc/9781107177222_toc.pdf

l'opposition de deux sensibilités en matière de souveraineté nationale.

Sur ce sujet du renseignement, il convient aussi de noter que des grandes entreprises du privé sont depuis quelques années tentées de créer leurs propres services de renseignement. Ceci illustre la manière dont certaines multinationales agissent désormais comme de quasi-États[60].

L'exemple du renseignement montre bien que les GAFAMI[61]– en raison de leur accès privilégié et massif à des informations confidentielles à « haute valeur de nuisance » – représentent une catégorie bien particulière. À l'évidence, à puissance financière équivalente, la problématique d'Alphabet-Google ou Microsoft se lançant dans le renseignement n'est pas de même nature que s'il s'agissait de l'industriel Toyota Motor ou de la banque Wells Fargo.

Dans son audition du 8 mars 2018 devant les députés de la Commission de la défense, le chef de la direction du renseignement militaire déclarait : « *Aujourd'hui, même les États sont dépassés par la puissance financière de certaines entreprises, comme Microsoft ou Google, qui peuvent consacrer à ces évolutions des moyens bien supérieurs*. »[62].

Mais même la position française qui tendait à maintenir à un niveau étatique l'ensemble des capacités offensives en matière de cybersécurité est en train d'évoluer. Le texte du projet de loi de programmation militaire examiné en première lecture, prévoit que les opérateurs de télé-communications pourront, « *pour les besoins de la sécurité et de la défense des systèmes d'information* », mettre en place des dispositifs de détection d'attaques sur leurs réseaux.

Le numérique nous conduit aujourd'hui à élargir le paradigme de la souveraineté en démultipliant ses porteurs, notamment aux entreprises.

59Même dans ces pays attachés à une tradition plutôt « libérale », la confiance dans le partenariat public/privé peut être contestée. Par exemple, le ministre suédois de la Défense, Peter Hultqvist, qui est actuellement sur la sellette à la suite d'une affaire de dissémination d'informations confidentielles – dont certaines concernent la défense –, après l'externalisation auprès d'IBM de l'entretien technique d'une base de données publiques (https://www.ttu.fr/suede-laffaire-derange).

60Voir sur ce sujet la controverse sur certains partenariats public-privé consentis par l'Organisation internationale de police criminelle (Interpol) et le très éclairant documentaire intitulé « *Interpol, une police sous influence ?* » ; https://www.arte.tv/fr/videos/061744-000-A/interpol-une-police-sous-influence

61GAFAMI pour « Google, Apple, Facebook, Amazon, Microsoft, IBM » dont l'équivalent chinois sont les BATX (Baidu, Alibaba, Tencent, Xiaomi). Ces sociétés ne sont pas les seules à collecter des données touchant au plus intime de chaque individu et on peut s'inquiéter de la sécurité des informations collectées par les applications de « réseautage social ». Voir à ce sujet l'article de Judith Duportail, « I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets », *The Guardian*, 26/09/2017 ; https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

62http://www.assemblee-nationale.fr/15/pdf/cr-cdef/17-18/c1718052.pdf

PARTIE 4 : Vers de nouvelles souverainetés et de nouveaux acteurs

Comme nous l'avons montré ci-dessus, la notion historique de souveraineté est aujourd'hui contestée tant par des personnes morales que physiques s'exprimant au nom d'idées et d'intérêts singuliers ou collectifs. On trouve clairement exprimées, nous l'avons vu, les notions de souveraineté collective (nationale, numérique, européenne[63], bien-être et santé, scientifique) mais aussi plus restreinte (à l'échelle d'une entreprise) voire individuelle[64]. Ce renversement de la vision classique de la souveraineté – conçue jusqu'à présent uniquement à l'échelle d'une collectivité humaine – constitue sans doute un changement de paradigme. Il s'agit d'une conséquence directe du processus de « ré-ontologisation » des notions induit par le numérique.

Nous développons dans cette partie ce que pourraient être la formalisation et la pertinence de notions de souveraineté numérique d'une part et de souveraineté scientifique d'autre part.

4.1. Des souverainetés numériques, au pluriel !

Outre la souveraineté nationale au sens classique/historique du terme, on parle aussi désormais de souveraineté européenne, de souveraineté scientifique, de souveraineté technologique, de souveraineté économique, de souveraineté individuelle[64] et bien sûr, de souveraineté numérique. Ainsi, dans la synthèse des quatrièmes *Assises de la Souveraineté Numérique : "Souveraineté numérique et cyber-sécurité"*[65] on peut voir présentés « *trois cercles de souveraineté* » :

« (…) Quels sens faut-il donner à la souveraineté ? La donnée est au cœur de l'espace numérique. Il faut la protéger. Les espaces de souveraineté sont différents :

1. *Souveraineté individuelle : qu'est-ce que l'on accepte de donner ? à l'État ? aux acteurs commerciaux ? Qu'est-ce qu'on n'a pas envie de donner : protection de nos vies privées, de nos mouvements, etc. Il faut réinventer la souveraineté.*
2. *Souveraineté de l'entreprise : la donnée est tout ce qui fait sa richesse. L'échange des données à travers le monde fait la richesse du commerce.*
3. *Souveraineté de l'État, la nôtre. Il faut absolument la protéger. »*

Le numérique et l'explicitation du rôle premier du concept d'information au même titre que la matière ou l'énergie ont révélé le nouveau « continent numérique » bien souvent appelé aussi « océan numérique » du fait de l'analogie avec son caractère omniprésent et de la similitude des aspects légaux relatifs aux mers et océans avec ceux sous-jacents au numérique[66]. On a donc vu émerger de nombreuses propositions de définitions et de mise en place de la souveraineté numérique.

En France, la problématique et le terme *souveraineté numérique* ont été introduits explicitement par

63« *Aussi si nous devons aujourd'hui refonder notre Europe,* […] *c'est pour vouloir refonder autour d'une* ***souveraineté commune****, c'est-à-dire d'une Europe qui protège nos concitoyens* […] ». http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-emmanuel-macron-lors-de-l-inauguration-de-l-historial-franco-allemand-de-la-guerre-14-18-du-hartmannswillerkopf-en-presence-de-frank-walter-steinmeier-president-de-la-republique-federale-d-allemagne

64« [Il faut] *intégrer la notion de souveraineté individuelle à la réflexion. Le citoyen ou l'entreprise doit pouvoir maîtriser ses données, avoir la pleine conscience de leurs valeurs, des enjeux, et également assurer une diffusion qui peut être consentie et rêvée.* », in *Synthèse des 4èmes Assises de la Souveraineté Numérique : "Souveraineté numérique et cybersécurité" ;* http://aromates.fr/public/Synthese%20ASN%202017.pdf

65Ces 4èmes Assises de la Souveraineté Numérique se sont déroulées à Paris, le 29 mars 2017, en présence de nombreux parlementaires ; http://aromates.fr/public/Synthese%20ASN%202017.pdf

66Le parallèle avec la métaphore marine pourrait même être poursuivi en associant le Net aux eaux de surface face au Darknet des fonds abyssaux…. On notera que le commandement des opérations cybernétiques dans les États-Majors est très souvent confié à des amiraux, que cela soit au Royaume-Uni, en France ou aux États-Unis !

Pierre Bellanger, d'abord dans un premier texte publié en ligne en 2011[67], repris dans la revue *Le Débat* puis largement développé en particulier dans son livre *La Souveraineté Numérique* publié en 2014[68]. La perte de souveraineté nationale que représente l'appropriation des données numériques par quelques entités étatiques ou entrepreneuriales y est vivement dénoncée. L'action de Pierre Bellanger a débouché sur une proposition d'amendement[69] acceptée lors du vote de la loi sur la République numérique promulguée le 7 octobre 2016, proposant l'étude de la création d'un Commissariat à la souveraineté numérique. Notons qu'ici, le concept de souveraineté est entendu au sens de souveraineté nationale, ce qui fait que la souveraineté numérique est une souveraineté de l'État sur le numérique.

Ceci étant, le concept de souveraineté numérique peut s'entendre dans un sens différent et désigner la capacité, pour une entité donnée (une nation, une entreprise, un individu), de maîtriser des attributs numériques (données, informations, connaissances, algorithmes) sur des objets dont elle revendique l'observation, voire le contrôle.

Le terme « maîtrise » utilisé ici (et ailleurs dans ce document) ne signifie pas nécessairement que l'entité détient (au sens d'une pleine propriété) les objets en question, et a fortiori les attributs numériques, ici les données, de ces objets.

Pour des pays comme la Russie ou la Chine, la maîtrise des données est clairement associée à l'obligation d'un stockage exclusif des données de leurs concitoyens sur le territoire national. Ce n'est le cas ni en France, ni en Europe où un volume important de données à caractère personnel sont transmises et stockées à l'étranger. Quand elles le sont aux États-Unis, le dispositif de « bouclier de protection des données » (Privacy Shield)[70] en vigueur depuis le 1er août 2016 ne préserve pas les citoyens européens de la surveillance massive et indiscriminée des données, ce qui est contraire au droit européen, mais autorisé par la législation américaine (à l'exemple du *Patriot Act*).

On voit que dans cette acception la souveraineté numérique, déclinée comme « **souveraineté numérique nationale** », c'est-à-dire comme souveraineté nationale sur le numérique, se heurte à l'intrication d'un monde globalisé régi par de multiples conventions et normes internationales. Le droit international sur les données rejoint la problématique déjà évoquée du droit maritime international. Plus prosaïquement, le fonctionnement de nos démocraties reposant de plus en plus sur une expression publique utilisant les médias numériques, la capacité de censure de certaines sociétés pose question (voir le débat en Allemagne sur l'application d'une loi obligeant Twitter, Facebook ou YouTube à supprimer les messages au contenu pénalement répréhensibles).

Dans un cadre à la fois infra-national et supra-national, la souveraineté numérique peut aussi se décliner en une « **souveraineté numérique entrepreneuriale** ». L'entreprise doit ici être considérée dans une définition large, qui est par exemple celle de l'INSEE[71], incluant aussi des organisations non-gouvernementales et des fondations. On a vu ci-dessus (section 3.4) qu'en particulier les GAFAMI (ou les BATX) pourraient prétendre à la maîtrise des données que ces sociétés possèdent ainsi qu'à la maîtrise des algorithmes qu'elles mettent en œuvre pour les collecter et les exploiter. Mais on voit aussi apparaître des revendications de souveraineté d'entreprises sur les données décrivant ou issues de leur savoir-faire et de leur activité de multinationales. Notons à cet égard que le règlement européen sur la protection des données personnelles (RGDP[72]) a pour objectif de faire obstacle à cette volonté de souveraineté numérique entrepreneuriale des grands acteurs de l'Internet. Au regard de l'expérience passée, il convient de rester vigilant sur les conditions de mise en œuvre du RGDP comme cela a été

67« De la souveraineté en général et de la souveraineté numérique en particulier », *les Échos ;* http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

68Pierre Bellanger, *La souveraineté numérique*, Éditions Stock, 2014, 264 p., ISBN 978-2918866213

69http://www.assemblee-nationale.fr/14/amendements/3318/CION_LOIS/CL129.asp

70https://www.cnil.fr/fr/le-privacy-shield

71Selon l'Institut national de la statistique et des études économiques : « *L'entreprise est la plus petite combinaison d'unités légales qui constitue une unité organisationnelle de production de biens et de services jouissant d'une certaine autonomie de décision, notamment pour l'affectation de ses ressources courantes*. » ; https://www.insee.fr/fr/metadonnees/definition/c1496

72Ce règlement, adopté en 2016, sera applicable à partir du 25 mai 2018.

encore récemment montré par la publication d'un *Code of Conduct for Cloud Infrastructure Service Providers* qui ne propose que des « recommandations non-contraignantes » pour la mise en application du RGDP[73].

Enfin, la notion de « **souveraineté numérique individuelle** » décrit la capacité des individus à maîtriser leurs données personnelles, médicales, pédagogiques (ex. scolaires, formation tout au long de la vie, etc.), mémorielles (photos, courriers, etc.) dans un contexte où la vision qu'ont les individus de la préservation de la vie privée dépend souvent de facteurs culturels et du niveau de maîtrise des outils numériques[74]. La prise de conscience de l'ampleur des données concernées se fait souvent au moment de l'annonce de piratage comme celui qui a affecté 3 milliards de comptes utilisateurs Yahoo en 2013 et, en 2016, les 57 millions d'utilisateurs de l'entreprise de VTC Uber. L'autonomie du sujet se heurte à la fois à la souveraineté nationale, comme cela a toujours été le cas dans les démocraties représentatives, et à la souveraineté entrepreneuriale, ce qui pourra engendrer des conflits dans le futur (on peut ainsi voir l'OpenAccess comme un moyen de se rebeller contre la souveraineté des entreprises, tout comme le DarkNet est aussi une forme d'opposition au contrôle souverain des États). Toutefois, si, dans les régimes démocratiques, les appareils judiciaires sont généralement en mesure de régler les conflits entre l'individu et l'État, surtout en Europe où il existe de surcroît une entité judiciaire à l'échelon supranational européen, il est beaucoup plus difficile de régler les conflits entre l'individu et les grands acteurs internationaux qui échappent aux emprises nationales.

La revendication de souveraineté dans ces trois catégories soulève des questions difficiles de droit, de légitimité et de mise en œuvre le cas échéant, on peut en prendre pour exemple le « non aboutissement » à l'heure actuelle (du moins à notre connaissance, en mai 2018) de l'étude commanditée par la loi du 7 octobre 2016 pour une République numérique sur l'opportunité de la mise en place d'un Commissariat à la souveraineté numérique.

Nous identifions donc les enjeux suivants :

E-1 La souveraineté numérique n'est pas simplement un enjeu politique ou économique, elle porte en elle des questions éminemment éthiques ;

E-2 Cet enjeu éthique concerne notamment le droit de chaque individu à préserver sa vie privée. La manière dont certaines entreprises du numérique considèrent que son aliénation serait aujourd'hui tacitement acceptée (selon le principe que le silence de l'usager vaudrait acceptation de toute utilisation ultérieure des données recueillies) n'est acceptable ni d'un point de vue éthique ni en terme de souveraineté nationale ou individuelle ;

E-3 Le dispositif de « bouclier de protection des données » (*Privacy Shield*) ou la prochaine mise en place règlement général sur la protection des données personnelles (RGDP) illustrent le rapport de force difficile existant avec des entreprises de droit américain (et l'extra-territorialité qui lui est attachée) qui nécessite de ne pas exclure la mesure radicale d'une obligation d'un stockage exclusif des données de nos concitoyens sur le territoire de l'Union européenne ;

E-4 Ce qui est vrai à l'échelle individuelle l'est tout autant à l'échelle collective ; que notre vision de la souveraineté collective se place à l'échelle nationale ou européenne, on doit s'inquiéter de la menace sur le fonctionnement démocratique de nos institutions ou d'ingérence dans les choix de société.

4.2. Le cas de la souveraineté scientifique

La « souveraineté numérique entrepreneuriale » n'est pas la seule à opérer dans un cadre à la fois infranational et supranational, la souveraineté numérique peut aussi se décliner en des formes de « souveraineté scientifique » qui intéressent tout particulièrement la CERNA dont le mandat est d'apporter une réflexion éthique à la communauté des chercheurs. Ainsi, nous traitons spécifiquement de ce sujet.

73Lettre envoyée par Isabelle Falque-Pierrotin (au nom du *Article 29 Working Party*) à Alban Schmutz (président du CISPE, le *Cloud Infrastructure Services Providers in Europe*) le 23 février 2018 ; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615033

74Jean-Marc Manach, *La vie privée, un problème de vieux cons ?,* Limoges, Éd. Fyp, coll. Présence, 2010, 224 p.

Aujourd'hui, la communauté scientifique valorise une certaine indépendance et aspire tout à la fois à l'autonomie de ses institutions et à la liberté de recherche[75]. Comme l'explique Caroline Wagner dans son ouvrage intitulé *The New Invisible College*[76], cette situation est récente : l'histoire des sciences et de leur financement montre que l'on est passé par des phases très contrastées. Au début du XX^{e} siècle et, en particulier après la Seconde Guerre mondiale, les États finançaient une science nationale, avec des fins à la fois économiques et militaires. Depuis le milieu des années quatre-vingts, avec les projets européens, le financement de la science est devenu de plus en plus supranational, ce qui fait que les communautés scientifiques ont désormais des agendas propres, indépendants de ceux des agents étatiques. Le numérique renforce encore l'autonomie des communautés scientifiques qui se concertent incessamment sur les réseaux et prennent des initiatives collectives. Qui plus est, aujourd'hui, les grands acteurs économiques privés, dont notablement ceux du numérique, ont eux aussi la possibilité de mettre en place des laboratoires de recherche. Certains peuvent être financés au moins autant que les grands centres publics de recherche en ayant des modes de rémunération et d'organisation de la recherche notablement différents. Ainsi, en bouleversant l'ensemble des approches et pratiques scientifiques, l'avènement du numérique contribue à introduire une notion de « souveraineté scientifique » et à se demander ce qu'elle signifie.

Par « **souveraineté scientifique** », on entend ici la maîtrise par les scientifiques, à divers titres collectifs (ex. laboratoire de recherche ou discipline scientifique), de toutes les informations qui leur sont nécessaires pour l'élaboration de connaissances, la réplication des travaux, pour le libre accès et la libre publication de l'ensemble des données, informations et connaissances issues de leurs travaux, dans le respect de la déontologie et de l'intégrité scientifiques.

Le numérique est directement issu des avancées scientifiques et technologiques élaborées depuis l'Antiquité avec une accélération considérable ces quelques soixante-dix dernières années. Il est cependant remarquable de constater, sans que nécessairement les scientifiques eux-mêmes en aient nécessairement conscience, combien ces avancées numériques transforment la méthode scientifique elle-même ainsi que l'environnement de la recherche scientifique. On assiste à une révolution scientifique qui affecte pratiquement toutes les disciplines scientifiques : là où la démarche expérimentale classique, depuis les débuts de l'âge moderne, passait par la conception d'un dispositif destiné à valider ou à invalider une théorie, on peut enregistrer désormais systématiquement toutes les données, que l'on traite ensuite avec des techniques numériques, sans idée *a priori* de la théorie. Cela correspond aux e-sciences et aux expérimentations *in silico*, c'est-à-dire sur des données, avec des puces de silicium.

La démarche ou méthode scientifique se voit donc étendue de deux nouveaux paradigmes : en plus de l'observation, de la conception de théories et de l'expérimentation, on dispose maintenant de capacités de simulation et d'analyse massive de données à des échelles qui transforment complètement toutes les disciplines. On peut par exemple faire évoluer une galaxie sous nos yeux, reconstituer les fragments épars de manuscrits, simuler un ordinateur quantique avant d'être capable de le réaliser physiquement, vérifier et dans certains cas calculer la preuve d'un nouveau théorème, etc. Pas une discipline n'échappe à cette révolution.

La science se nourrit et génère des masses considérables de données : les connaissances générées, les protocoles utilisés, les logiciels, les données issues des expérimentations ou des simulations, les échanges scientifiques issues de l'élaboration ou de la validation des connaissances. Cette multitude de données se présente sous des formes très différentes. Aux traditionnels textes documentant les connaissances (mémoires, thèses, articles et communications scientifiques) s'ajoutent désormais les téraoctets issus des observatoires astronomiques ou d'expériences en physique nucléaire, mais aussi d'analyse de textes, de vidéo et de sons à des fins d'analyse sociologique, ou de preuves formelles de protocoles ou de programmes. En outre, les données issues des échanges scientifiques prennent aujourd'hui des formes différentes via les discussions dans les réseaux sociaux scientifiques. Le partage éthique, intègre et déontologique de ces données constitue par conséquent un enjeu

75 Voir le rapport du COMETS n°2018-35 intitulé *Liberté et responsabilités dans la recherche académique* et approuvé le 31 janvier 2018.

76 Caroline Wagner, *The New Invisible College*, Brookings Institution Press, Washington D.C., 2008, 157 p.

important[77].

La publication des connaissances construites par les scientifiques et de leurs découvertes est emblématique des enjeux de souveraineté scientifique. La transformation numérique en cours soulève des questionnements déontologiques, d'intégrité et d'éthique.

Publier – c'est à dire rendre accessible à un certain public[78] une méthode, des discussions et les résultats obtenus via la démarche scientifique – est une part fondamentale de la mission des scientifiques. Publier signifie à la fois enrichir le bien commun que constitue la science[79], mais c'est aussi permettre aux autres de progresser en utilisant les nouvelles connaissances mises à disposition. Il s'agit d'exposer sa démarche et de permettre sa reproductibilité ou sa réfutation. C'est aussi, dans le contexte de « coopétition »[80] scientifique contemporain, donner la capacité d'évaluer la qualité du travail scientifique effectué par un individu, une équipe, un laboratoire, un centre de recherche, une université, une discipline ou un pays. On a ainsi vu naître l'utilisation de notions comme le facteur d'impact des revues scientifiques ou l'évaluation de l'influence des scientifiques via des mesures comme le H-index. Ces nouveaux outils ont permis de lancer des recherches sur les mesures les plus appropriées pour quantifier la portée des résultats scientifiques et de leurs auteurs.

Les premières revues scientifiques dans le monde occidental remontent au XVII^{e} siècle avec en 1665 la création à Paris du *Journal des Sçavans*[81] annonçant des nouveautés scientifiques, un périodique littéraire et scientifique édité aux frais de l'État. La même année, paraissent à Londres, les *Philosophical Transactions of the Royal Society of London*, première revue scientifique établissant les bases du mécanisme de revue par les pairs. Le service offert par les maisons d'édition aux scientifiques a ensuite évolué au bénéfice des chercheurs comme attesté par la lettre de remerciement enthousiaste envoyée en 1923 par 23 scientifiques dont Hilbert et Einstein à Ferdinand Springer[82]. Mais cette relation revient désormais au bénéfice très important des maisons d'édition ce qui a provoqué des réactions de plus en plus vives des communautés scientifiques (voir les appels de Budapest en 2002 et de Jussieu en 2017[83]).

L'*open access* et plus généralement l'*open science* sont des enjeux de souveraineté scientifique considérables car on assiste à une appropriation des données, informations ou connaissances scientifiques par des entités privées à but lucratif (comme les GAFAMI ou des maisons d'édition scientifique comme Elsevier, Springer, IEEE ou ACM) ou étatiques à but sécuritaire (comme la NSA). **Cette appropriation empêche des scientifiques ou des communautés scientifiques d'accéder aux connaissances leur permettant d'effectuer leur recherche au meilleur niveau international.**

Prenons le cas de la fouille de textes et de données (pratique souvent répertoriée sous le sigle TDM — *Text and Data Mining* —) qui nécessite l'accès à toutes les données, informations et connaissances disponibles pour en permettre l'extraction des informations nécessaires à la progression scientifique. Si, par exemple, un scientifique souhaite accéder à toutes les informations disponibles sur les

77Voir la recommandation du COMETS du 7 mai 2015 intitulé « Les enjeux éthiques du partage des données scientifiques » : http://www.cnrs.fr/comets/IMG/pdf/2015-05_avis-comets-partage-donnees-scientifiques-3.pdf

78En fonction de la technicité ou de la confidentialité des résultats, le public concerné peut-être la communauté scientifique ou des sous-ensembles de celle-ci, des communautés ciblées (par exemple les Responsables de la Sécurité des Système d'Information (RSSI) en cybersécurité) ou bien l'ensemble de la société (par exemple sur l'évolution du climat).

79Voir en particulier la révision par l'Unesco le 13 novembre 2017 de sa *Recommandation Concernant la Science et les Chercheurs Scientifiques*. Elle consacre en particulier les « libertés académiques » et la science comme « bien commun ». Actes de la Conférence générale 39^{ième} session, Paris, 30 octobre – 14 novembre 2017. Volume 1: Résolutions, pages 128-141. http://unesdoc.unesco.org/images/0026/002608/260889f.pdf#page=128

80Néologisme, contraction de « coopération » et de « compétition », qui exprime la volonté pour une entité, en particulier une entreprise, de partager certaines ressources (coopération), tout en conservant son autonomie.

81https://fr.wikipedia.org/wiki/Journal_des_savants

82Voir http://www.dam.brown.edu/people/mumford/images/MathAnn_FSpringer.jpg sur le blog de David Mumford http://www.dam.brown.edu/people/mumford/blog/2015/WakeUp.html

83http://www.budapestopenaccessinitiative.org/read et http://jussieucall.org

interactions électromagnétique-vivant, ces informations sont actuellement principalement contrôlées par des acteurs privés. Ces maisons d'édition veulent revendre l'accès à ces données alors que, d'une part, elles ont été construites et validées par la communauté scientifique elle-même et que, d'autre part, il n'y a aucune assurance que leur accès suive la déontologie scientifique (l'exhaustivité ou l'exactitude des données retournées par un éditeur lors d'une requête de TDM n'étant actuellement ni garantie ni vérifiable).

Un deuxième sujet de préoccupation concerne les données d'usage. En effet, les processus de revue par les pairs, les discussions dans les réseaux sociaux, les requêtes dans les moteurs de recherche génèrent des informations scientifiques précieuses qui ne sont pas aujourd'hui disponibles aux communautés scientifiques mais sont ici aussi préemptées par des intérêts spécifiques.

Un troisième exemple concerne la question de l'emploi scientifique jusqu'alors principalement maîtrisé par le milieu académique, et qui se voit aujourd'hui confronté à des intérêts spécifiques, accaparant à une échelle inédite, via des moyens financiers considérables, des scientifiques parmi les plus féconds.

Mentionnons enfin que les moyens mis à disposition des communautés scientifiques (capacités de simulation, d'apprentissage machine, de laboratoires d'expérimentation biologique, chimique ou physique) peuvent être aussi aujourd'hui contrôlés par des entités spécifiques à des fins économiques ou stratégiques.

Ces éléments mettent en perspective les enjeux éthiques issus des conflits de valeurs résultants de la mise en œuvre des souverainetés scientifique, nationale ou économique, chacune d'entre elles interférant aussi potentiellement avec les autres.

Nous identifions donc les enjeux suivants :

E-5 Le numérique transforme profondément l'approche scientifique et son environnement ; les questions de souveraineté scientifique qui s'ensuivent se combinent avec des enjeux éthiques cruciaux dans le développement de toutes les disciplines ;

E-6 Les implications de ces évolutions dans le cadre scientifique ont des conséquences profondes sur toutes les sociétés à l'échelle de la planète et sur l'évolution humaine.

Ces enjeux nous conduisent à formuler les recommandations suivantes :

R-1 De manière complémentaire aux formations à l'éthique et à l'intégrité scientifiques conduites dans les écoles doctorales, mettre en place des formations de tous les scientifiques à l'éthique et à la responsabilité scientifiques ;

R-2 Mettre en place les moyens de la souveraineté scientifique dans le secteur académique au niveau français et européen dans une perspective de science ouverte[84]. On visera en particulier à rendre systématique le dépôt dans HAL de toute la production scientifique dont au moins un auteur est affilié à un organisme de recherche français et à favoriser une telle approche au niveau européen et international ;

R-3 L'accès à toutes les données nécessaires à l'activité scientifique des institutions de recherche devra être rendu possible ; en particulier l'accès à la fouille de textes et de données (TDM) devra être assuré sans restriction à des fins scientifiques, le tout dans des conditions strictes et auditées d'éthique, d'intégrité et de déontologie scientifiques ;

R-4 Expliciter la façon dont les plates-formes collectant massivement des données (par exemple les GAFAMI et BATX) doivent ouvrir aux scientifiques ces données à des fins de science ouverte dans des conditions strictes d'éthique, d'intégrité et de déontologie scientifiques ;

R-5 Tenant compte des spécificités disciplinaires, établir, discipline par discipline, une politique d'ouverture équitable des données de la recherche en accord avec les institutions nationales et les grands acteurs de l'Internet ;

84La science ouverte (*open science* ou *open research* pour les anglophones) vise à rendre la recherche scientifique, les données, les connaissances et leur diffusion librement accessibles à tous les niveaux de la société.

R-6 Inviter les associations professionnelles des différentes disciplines scientifiques à expliciter leurs contributions au renforcement de la souveraineté scientifique ;

R-7 Les souverainetés nationales, numériques et scientifiques reposent sur la recherche en cybersécurité qu'il convient donc de développer très fortement ;

R-8 Avec le parrainage de l'Union Européenne et en collaboration des associations professionnelles scientifiques, l'académie des sciences et l'académie des technologies, mettre en place un prix international « éthique et souveraineté scientifique ».

4.3 Bien d'autres exemples !

Ce que nous venons de développer en tant que définition et conséquences des souverainetés numériques ou scientifique peut s'étendre à d'autres domaines tout aussi fondamentaux.

La souveraineté industrielle et technologique : il s'agit ici de la capacité d'un secteur industriel, d'une entreprise ou encore d'un Etat de maîtriser pleinement les attributs technologiques dont elle ou il revendique avec le contrôle. Aujourd'hui cette souveraineté croise souvent la souveraineté numérique de la même entité, incluant les données mais aussi les algorithmes nécessaires à la maîtrise des processus industriels. L'exemple de l'utilisation par Airbus des algorithmes développés par Palantir pour gérer la chaîne de construction des A350 est typique des questions qui peuvent se poser dans ce cadre[85].

La souveraineté dans le domaine de la santé : représente la capacité des individus (en bonne santé ou pas), d'établissements hospitaliers, d'un État, d'une spécialité médicale de maîtriser pleinement les attributs médicaux dont il ou elle revendique le contrôle. Ici encore, cette souveraineté croise la souveraineté numérique des mêmes entités, en particulier sur leurs données comme sur leurs procédures. Elle croise aussi la souveraineté nationale et repose sur la capacité à développer les corpus éthiques, déontologiques et législatifs permettant d'élaborer et d'assumer cette souveraineté.

La souveraineté sur les données : l'analogie avec le pétrole a souvent été mentionnée. La capacité de maitriser toutes les données est un enjeu de souveraineté fondamental comme cela a été souligné en particulier dans le rapport de Cédric Villani : « *La politique de la donnée doit enfin s'articuler avec un objectif de souveraineté et capitaliser sur les standards de protection européens pour faire de la France et l'Europe les championnes d'une IA éthique et soutenable.* »[86]. Cette souveraineté, qui est aussi la possibilité de maîtrise de cadre juridique s'appliquant à ces données, représente un sous ensemble de la souveraineté numérique qu'il est utile d'identifier en tant que telle. Notons que cette souveraineté peut s'exercer au niveau des individus ou d'une entreprise, d'un État ou encore d'entités telle que l'Union Européenne.

La souveraineté dans le domaine agricole : il s'agit ici de la capacité d'une filière agricole, d'une exploitation agricole ou de l'Union Européenne de maitriser pleinement les attributs dont elle revendique avec le contrôle. Ici aussi, cette souveraineté s'articule avec la souveraineté numérique de ces mêmes entités comme cela est souligné en particulier par l'OPECST[87].

Nous identifions donc l'enjeu suivant :

E-7 La souveraineté numérique croise dans nos sociétés actuelles la plupart voir toutes les autres souverainetés. Il en résulte une source importante de conflit.

85 https://www.palantir.com/build/images/media/Airbus-taps-Silicon-Valley-expertise-to-speed-production-of-A350.pdf

86 Rapport de Cédric Villani, p25.

87 La place du traitement massif des données (big data) dans agriculture : situation et perspectives. http://www.senat.fr/rap/r14-614/r14-6141.pdf

CONCLUSION : enjeux éthiques et recommandations

5.1 Souverainetés et éthique au cœur des réflexions géopolitiques contemporaines

Il a été beaucoup question de souveraineté et d'éthique lors du premier Forum parlementaire de l'Intelligence artificielle qui s'est tenu à Paris le 14 novembre 2017. Cette manifestation était coparrainée par les députés Cédric Villani et Laure de la Raudière qui a défini trois enjeux de souveraineté représentant, à ses yeux, une question politique et stratégique majeure :

- ✓ La souveraineté des États face aux tentations hégémoniques de certains d'entre eux ;
- ✓ La souveraineté des entreprises ;
- ✓ La souveraineté des individus qui passe par le droit à une vie privée[88].

Concluant les travaux du Forum, le ministre de l'Économie a affirmé que l'intelligence artificielle devait nous conduire dans les années à venir à relever un défi européen, mais aussi un « défi éthique »[89] avec « des problèmes éthiques considérables en matière d'information, en matière de maîtrise des données et (…) de souveraineté numérique ».

Il est intéressant de noter que le ministre de l'Économie lie très explicitement ce défi éthique à la défense d'une souveraineté numérique qui représente à la fois « un enjeu national et un enjeu européen ».

La députée Laure de la Raudière souligne l'importance de cet enjeu en affirmant que « l'éventuelle fin de la vie privée (…) serait la fin de la démocratie »[90].

Nous partageons ce constat dans la mesure où une communauté humaine qui n'aurait plus, ni la propriété de ses données personnelles, ni la maîtrise de l'information qui alimente son jugement, ni la capacité de traitement numérique de l'information, ne pourrait plus prétendre à former une « communauté de destin » agissant de manière autonome.

D'une certaine manière, le numérique montrera de la manière la plus crue si l'Europe peut prétendre ou non incarner un projet de souveraineté numérique d'une importance politique et stratégique proprement essentielle. Si l'Union Européenne échoue dans cette mission, **un échelon intermédiaire franco-allemand peut se révéler pertinent**, poursuivant autour d'un objectif pragmatique la coopération initiée il y a un peu plus d'un demi-siècle avec la signature du traité de l'Élysée. Comme l'a affirmé le Président de la République le 24 janvier 2018 à Davos : « Ceux [en Europe] qui veulent revenir à la souveraineté nationale ne doivent pas bloquer la porte aux plus ambitieux ».

Si la défense d'une souveraineté européenne ne pouvait se réaliser à l'échelle européenne, ou autour d'un axe franco-allemand, il faudra revenir à une solution nationale qui, pour un pays comme la France, semble peu adaptée au rapport de forces actuellement en place dans le monde.

Si nous observons des velléités de rétablissement d'un ordre westphalien de rapport de forces entre des pavillons nationaux, il existe également d'autres voies de gouvernance pour le numérique. À ce titre, le modèle des Conventions de Genève peut nous offrir une piste de réflexion intéressante.

Pendant la Seconde Guerre mondiale, la France a vécu l'occupation de son territoire et l'incapacité de son appareil étatique d'assurer sa première fonction régalienne de protection de ses citoyens. Cette expérience a stimulé une réflexion sur une protection des populations civiles ne relevant plus

88https://www.youtube.com/watch?v=Q_V9V3gpzXk&t=9s; cf. 10:36'

89https://www.youtube.com/watch?v=j5DIwcne85A; cf. 09:51' à 10'15

90https://www.youtube.com/watch?v=Q_V9V3gpzXk&t=9s; cf. 10:21'

exclusivement de la compétence de l'État-nation.

S'inscrivant dans la tradition du droit romain du *jus gentium* (droit des gens), cette réflexion a abouti à la signature le 12 août 1949 de la *Convention de Genève relative à la protection des personnes civiles en temps de guerre*. Celle qui fut qualifiée de « quatrième Convention de Genève » illustre une forme de renversement de la vision classique de la souveraineté avec des États qui anticipent leur possible impuissance (ici en temps de guerre) pour protéger leurs populations civiles. Une protection est reportée à l'échelle individuelle, une « souveraineté individuelle » d'un individu qui détient des droits de valeur universelle à faire valoir en dehors de toute appartenance à tel ou tel pays.

Aujourd'hui, il est significatif de noter que ce n'est pas un État ou un groupe d'États mais bien une entreprise multinationale privée, Microsoft, qui reprend le principe des conventions de Genève pour demander à l'appliquer au domaine du numérique[91].

Sans aller nécessairement jusqu'à un projet de « Convention de Genève du numérique », il semblerait judicieux de **lancer une initiative internationale visant à élargir le principe de « liberté de pensée et de conviction » à un droit, pour chaque individu, de contrôle des usages de la technologie pouvant porter atteinte à son intimité. Plus précisément il s'agit de préserver une capacité individuelle de développer une pensée singulière dans une sphère de l'intimité qui dépasse la notion juridique de « vie privée ».**

« Nous sommes entrés dans un nouvel âge de la propagande » pour reprendre les mots du ministre de l'Europe et des affaires étrangère[92]. L'« orchestration de stratégies digitales d'interférence » que dénonce Jean-Yves Le Drian ne se limite déjà plus seulement au champ de la « déstabilisation informationnelle » (dont les désormais fameuses *fake news*). Elles toucheront de plus en plus à la capacité même du citoyen digital de pouvoir formuler une pensée de manière raisonnablement autonome.

Il conviendrait donc de donner un sens nouveau au principe selon lequel « toute personne a droit à la liberté de pensée » énoncé dans l'article 18 de la déclaration universelle des droits de l'Homme du 10 décembre 1948 (repris dans l'article 9 de la Convention européenne des droits de l'Homme de 1950 et dans l'article 10 de la Charte des droits fondamentaux de l'Union européenne adoptée le 7 décembre 2000). Les rédacteurs de ces textes ne pouvaient imaginer que la technologie serait un jour capable de connaître le mode de pensée, la sensibilité, les plus intimes convictions non seulement d'un individu singulier, mais cela à l'échelle de dizaines ou de centaines de millions de personnes, voire de populations entières.

Les derniers chiffres de l'affaire Cambridge Analytica qui évoquent désormais quelque 87 millions de comptes[93] « siphonnés » nous montrent qu'il existe un danger réel pour une démocratie de ne pas maitriser l'accès aux données personnelles les plus intimes de ses citoyens. Ce scandale illustre également les risques inédits créés par des outils qui tirent de la connaissance des caractéristiques psychologiques et cognitives de millions d'individus une capacité d'influence sur leurs achats comme sur leurs votes. En cette année où nous célébrons les 70 ans de la déclaration universelle des droits de l'Homme, une initiative invitant les États parties à élargir le principe de « liberté de pensée et de conviction » semblerait particulièrement pertinente pour rappeler qu'on ne peut concevoir aujourd'hui de liberté de pensée sans une souveraineté numérique capable de permettre à chaque individu d'être autonome dans sa réflexion et souverain dans ses choix.

91On se rapportera au discours d'ouverture "*The Need for a Digital Geneva Convention*" prononcé par le president de Microsoft, Transcript of Keynote Address at the RSA Conference 2017, Brad Smith, à l'occasion de la *RSA Conference 2017* tenue à San Francisco le 14 février 2017; https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf

92Discours de M. Jean-Yves Le Drian prononcé en clôture de la conférence internationale sur les manipulations de l'information qui s'est tenue à Paris le 4 avril 2018 ; https://www.diplomatie.gouv.fr/fr/les-ministres/jean-yves-le-drian/discours/article/conference-internationale-societes-civiles-medias-et-pouvoirs-publics-les?xtor=RSS-1

93Chiffre donné par le directeur tecnique de Facebook, Mike Schroepfer, dans un post publié le 4 avril 2018 ; https://newsroom.fb.com/news/2018/04/restricting-data-access

Ce défi d'émancipation à l'échelle de chaque individu est en lien avec la capacité au niveau de la collectivité de pouvoir à la fois « partager et protéger », le projet même du « nouveau contrat mondial » promu par le président français lors du Forum de Davos. Il doit éviter, comme s'en est inquiété la chancelière allemande à cette même tribune, que « le développement disruptif du numérique ne casse les sociétés au risque que le XX^{e} siècle se répète ».

L'ère du numérique nous conduira peut-être à réinventer un nouvel *Habeas Corpus* qui ne soit plus uniquement centré sur la privation de la liberté physique du corps, mais aussi sur la liberté de l'esprit.

La liberté de penser individuellement étant relative, il faut l'associer à la reconnaissance de la liberté des groupes d'élaborer librement une pensée collective ou à affermir, par la controverse, des pensées individuelles. C'était tout particulièrement la fonction de la franchise universitaire (*libertas academica*) qui ouvre un espace de liberté dans les universités où la pensée se construisait en s'affrontant à différentes objections au cours de disputes privées. Avec le numérique, la transparence totale de tous les débats risque de supprimer cette protection, ce qui aurait des effets délétères. Il faut donc absolument préserver des espaces de liberté avant la publication pour permettre aux idées de se construire.

Dans un monde où les technologies numériques prennent une place croissante, leur potentiel de contribution positive au bien commun ne peut s'exprimer que si nous définissons clairement les règles garantissant les droits naturels et imprescriptibles de l'Homme définis en 1789 : la liberté, la propriété, la sûreté, et la résistance à l'oppression. Ces quatre notions ont un sens particulier à l'âge du numérique et permettent de préciser les enjeux non-négociables d'usages de la technologie portant atteinte à l'intimité et à la vie privée.

Nous suggérons donc de:

S-1 Lde lancer une initiative internationale visant à élargir explicitement au domaine numérique le principe énoncé par l'article 18 de la déclaration universelle des droits de l'Homme de 1948 selon lequel « toute personne a droit à la liberté de pensée », repris par l'article 9 de la Convention européenne des droits de l'Homme de 1950 et par l'article 10 de la Charte des droits fondamentaux de l'Union européenne de 2000[94] ;

S-2 Pparallèlement à cette initiative internationale, il convient de lancer une initiative européenne, ou plus pragmatiquement franco-allemande, qui se donnera les moyens de garantir l'intégrité et la confidentialité des données numériques et plus généralement de renforcer la recherche en cybersécurité et ses applications pour garantir l'expression de toutes les souverainetés qu'elles soient nationales, numériques, scientifiques ou individuelles ;

S-3 Iinciter les organisations œuvrant sur Internet dans le champ politique des « actions citoyennes » et de l'« influence sociale » (à l'exemple des organisations spécialisées dans le lancement de pétitions en ligne tels que Avaaz.org, Change.org, SumOfUs, etc.) à rendre transparentes, faciles d'accès et intelligibles les conditions d'utilisation des données personnelles et, en particulier, d'uniformiser une rubrique unique (regroupant les appellations variées de *data policy*, *privacy policy*, *confidentiality policy* et *information policy*).

5.2 Sensibilisation et formation des citoyens aux enjeux des souverainetés numériques

La réflexion sur la souveraineté numérique devrait nous conduire à étudier les moyens de renforcer la résilience de nos sociétés. Le 12 mars 2018, Mariya Gabriel, la Commissaire européenne à l'Économie et à la Société numériques, a reçu le rapport sur les *fake news* et la désinformation numérique qu'elle

94Si l'art. 18 du texte de 1948 ne crée pas d'obligation juridique pour les États signataires, ce n'est pas le cas de la Charte des droits fondamentaux qui, depuis la signature du traité de Lisbonne en 2007, possède une force juridique contraignante pour les États membres de l'Union européenne. Il est à noter que cette charte évoque déjà pour toute personne un « droit au respect de sa vie privée et familiale, de son domicile et de ses communications » (art. 7) et un « droit à la protection des données à caractère personnel la concernant » (art. 8).

avait commandé à un groupe d'une quarantaine d'experts[95]. Ce rapport invite les États membres de l'Union européenne à inclure dans leurs programmes éducatifs nationaux la connaissance de l'environnement médiatique et informationnel[96].

Nous estimons également qu'il existe un enjeu majeur de formation des citoyens qui pourrait se traduire de différentes manières :

- ✓ Dès l'école primaire[97], puis dans le secondaire, concevoir un enseignement qui sensibilisera aux enjeux de cybersécurité et de la maitrise des outils permettant de préserver la vie privée et d'alerter sur diverses formes de manipulation ou d'endoctrinement facilitées par les médias numériques.

  Cette proposition se rapproche de celle formulée dans le nouveau plan national de prévention de la radicalisation annoncé par le Président de la République qui appelle à « *Prémunir les élèves face au risque de radicalisation dans l'espace numérique et aux théories du complot en systématisant l'éducation aux médias et à l'information (EMI), tout en développant leur pensée critique et la culture du débat »*[98]. Cependant, nous nourrissons quelque inquiétude devant l'invitation à « *impliquer les acteurs de l'Internet dans la protection des citoyens* » (p. 10 du dossier de presse) de ce plan national « Prévenir Pour Protéger » si cette implication n'est pas assortie d'une réflexion approfondie sur ses enjeux éthiques et politiques. C'est en particulier le cas lorsque dans une « *lutte contre l'enfermement algorithmique* », cette collaboration s'assortit d'un appel à ce que les acteurs de l'Internet participent à « *promouvoir efficacement le contre-discours* » (mesure N° 14). Si l'on ne s'attaque pas au problème de l'indifférenciation et à la non-hiérarchisation de l'information – et sans effort de fonder une vérité sur un raisonnement rationnel –, tout contre-discours semble voué à l'échec, voire à devenir contre-productif.

- ✓ Poursuivre l'effort d'éducation dans le cadre d'un futur « service national universel » qui semble tout indiqué pour parler de cybersécurité, mais qu'il conviendrait de replacer dans un concept plus large de résilience. L'objectif serait en effet d'expliquer les enjeux sociétaux de la souveraineté à l'heure du numérique (en tenant compte des problématiques rappelées dans le point précédent).

- ✓ Au-delà de la formation des plus jeunes, cette sensibilisation devrait également trouver des moyens de toucher l'ensemble de la population (ce qui relève en particulier du rôle des médias mais aussi de la nécessaire implication de la communauté scientifique). À côté des initiatives de la société civile et les médias[99], il y a là aussi une mission régalienne d'un nouveau type qui renforcerait la résilience de nos concitoyens face aux « fausses nouvelles » ou *fake news* et autres actions de manipulation utilisant les médias numériques. L'action pionnière de certains pays

95 Rapport intitulé *A multi-dimensional approach to disinformation : Report of the independent High level Group on fake news and online disinformation*, 44 p. ; http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271

96 *Ibid*., p. 37.

97 En s'appuyant sur le retour d'expérience d'initiatives locales comme celle conduite par Rose-Marie Farinella auprès de classes de CM2.

http://www.cafepedagogique.net/lexpresso/Pages/2016/12/14122016Article636172963871740159.aspx

98 Dossier de presse, Mesure N° 9 p. 10, disponible sur :

http://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2018/02/2018-02-23-cipdr-radicalisation.pdf

99 À l'exemple, en France, du Décodex du *Monde* (http://www.lemonde.fr/verification/), de la « *Journalism Trust Initiative* » (JTI) lancée début avril 2018 par l'association Reporters sans frontières ou du podcast préparé conjointement par *France Info* et *France Culture* pour lutter contre les fausses nouvelles dans le domaine scientifique, qui devrait être accessible fin avril 2018 ;

http://www.lemonde.fr/economie/article/2018/03/19/franceinfo-et-france-culture-s-allient-contre-les-fake-news_5273020_3234.html

européens en la matière[100] mérite d'être étudiée[101].

Plusieurs entreprises annoncent aussi qu'elles travaillent sur le sujet de l'« *affective computing* » afin de mieux comprendre les mécanismes d'empathie et, ainsi, « de pouvoir lutter contre les *fake news* »[102]. D'autres prétendent détecter les faits erronés avec des logiciels dits de *fact checking*. À cet égard, on notera que le rapport[103] sur la désinformation que vient de publier la division CONNECT de la communauté européenne se fonde uniquement sur des solutions technologiques auxquelles ont contribué des représentants des grands acteurs de l'Internet, en particulier de Google, de Facebook et de Twitter. Il serait sans doute naïf de se reposer sur les seules entreprises du numérique pour défendre l'intérêt général, le droit et les valeurs des démocraties libérales. Le comportement fiscal de ces mêmes entreprises doit nous conduire à avoir un regard critique sur la sincérité de telles promesses. Sans compter qu'elles éludent trop souvent leurs responsabilités dans la diffusion des « infox » (*fake news* en anglais), puisque leur prolifération tient en partie au modèle économique fondé sur le « piège à clics », qui rétribue une information en fonction du nombre de clics qu'elle recueille.

Les recherches sur les mécanismes d'empathie permettent de vendre des produits et des services marchands ou de lutter contre des propagandes hostiles. Les marchés associés aux activités de modification des perceptions (*opinion shaping*) sont d'une ampleur assez asymétrique selon que sa finalité soit commerciale ou politique. Il est douteux qu'une entreprise privilégie un service d'intérêt général, même rémunéré, sur une activité économique plus lucrative.

Plus fondamentalement, il convient de rappeler que l'objectif stratégique des « *fake news* » diffusés dans les démocraties libérales n'est pas tant de créer une opinion, que de susciter du doute. La réponse des gouvernements ne peut pas rester dans le seul registre de l'émotionnel et abandonner toute volonté de reconquérir le terrain de la pédagogie et de l'argumentation rationnelle et scientifique.

Nous suggérons donc :

S-4 Ddès l'école primaire, puis dans le secondaire, concevoir un enseignement qui sensibilisera aux enjeux de cybersécurité et de la maitrise des outils permettant de préserver la vie privée et d'alerter sur diverses formes de manipulation ou d'endoctrinement facilitées par les médias numériques ;

S-5 Ddans le cadre d'un futur « service national universel » expliciter les enjeux sociétaux des souverainetés à l'heure du numérique ;

S-6 Een s'appuyant sur les médias et l'implication de la communauté scientifique, permettre de sensibiliser l'ensemble de la population pour renforcer la résilience de nos concitoyens face aux fausses nouvelles et aux actions de manipulation utilisant les médias numériques.

5.3 Souverainetés numérique, éthique, science et technologie

Comme nous l'avons vu, les souverainetés nationales, numériques et scientifiques induisent des enjeux éthiques et des responsabilités fondamentales.

En paraphrasant la tribune parue dans Le Monde numérique en décembre 2017[104], nous nous trouvons aujourd'hui dans une situation similaire à celle qui a amené la France à être pionnière avec la mise en

---

100 Voir le documentaire « Prague face à la propagande de Poutine » diffusé sur Arte le 14/11/2017 ou l'article de Pauline Moullot « Contre les « fake news », le tacle tchèque » paru dans *Libération* le 21/08/2017.

101 Sur ce sujet, voir le rapport n°2018-37 du COMETS paru en avril 2018 et intitulé *Quelles responsabilités pour les chercheurs à l'heure des débats sur la « post-vérité »*.

102 Selon Philippe Bournhonsque, directeur technique d'IBM-France, s'exprimant lors du colloque « L'héroïsme à l'ère de l'IA » qui s'est tenu à l'École militaire le 18/12/2017.

103 *A multi-dimensional approach to disinformation — Report of the independent High level Group on fake news and online disinformation*, Directorate-General for Communication Networks, Content and Technology, mars 2018, ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271

104 « Il faut créer un comité national d'éthique du numérique », LE MONDE | 14.12.2017 à 11h22 • Mis à jour le 15.12.2017 à 09h35. http://www.lemonde.fr/idees/article/2017/12/14/il-faut-creer-un-comite-national-d-ethique-du-numerique_5229661_3232.html

place en 1983 d'un CCNE pour les sciences de la vie et de la santé, ayant pour mission de réfléchir aux positionnements éthiques résultants de l'extension de nos capacités scientifiques et techniques dans ce domaine. Ce comité organise de façon lisible et construite, encadrée par la loi, le débat public. De ce fait ses avis consultatifs sont pris en considération par la société et par le législateur.

Il est donc essentiel de créer rapidement un comité consultatif national d'éthique pour les sciences, technologies, usages et innovations du numérique. En reprenant les termes de cette tribune : « *Il s'agit maintenant d'articuler le temps court, celui de la compétitivité industrielle et économique, avec le temps long, celui de l'être humain et celui d'un « futur désirable ». Ainsi ce CCNE du numérique, indépendant et consultatif, s'articulerait avec les comités industriels sectoriels. La maîtrise de ces enjeux est pour la France et l'Europe une question de souveraineté et de démocratie, faute de quoi notre continent dépendra de décisions qui seront prises ailleurs, selon des cultures ou des considérations éthiques, économiques, industrielles, sociales nous échappant.*

La France se doit donc d'être précurseur en la matière, comme elle le fut dans le domaine de la régulation des données personnelles et pour l'éthique des sciences du vivant et de la santé. Elle doit créer, dès à présent et sous l'égide de la présidence de la république, un Comité consultatif national d'éthique pour les sciences, technologies, usages et innovations du numérique. ».

Cette recommandation est également donnée dans le rapport de Cédric Villani déjà cité.

Comme nous l'avons élaboré dans la description de la souveraineté scientifique, des conflits importants peuvent naitre de visions différentes de la notion de progrès et des valeurs sous-jacentes au développement scientifique. Des contextes culturels ou politiques différents peuvent amener à mettre en œuvre des développements scientifiques dont l'éthique ne sera pas nécessairement partagée internationalement. On peut penser par exemple à des manipulations génétiques permises par des avancées en génomique et en bioinformatique et qui modifieraient significativement les capacités physiologiques ou intellectuelles humaines ou animales. Cela concerne en premier lieu l'éthique et les souverainetés nationales et scientifiques mais aussi l'ensemble de nos sociétés.

Nous suggérons donc de :

S-7 Ccréer un comité consultatif national d'éthique pour les sciences, technologies, usages et innovations du numérique ;

S-8 Ddévelopper une doctrine et une stratégie d'influence française et européenne et se donner les moyens de la défendre dans toutes les instances nationales et internationales (CE, Unesco, OMS, instances de normalisation et standardisation (ISO, AFNOR, IEEE,…)).

5.3 Résumé des enjeux, des recommandations et suggestions

Nous avons identifié tout particulièrement les **enjeux** suivants :

E-1 La souveraineté numérique n'est pas simplement un enjeu politique ou économique, elle porte en elle des questions éminemment éthiques.

E-2 Cet enjeu éthique concerne notamment le droit de chaque individu à préserver sa vie privée. La manière dont certaines entreprises du numérique considèrent que son aliénation serait aujourd'hui tacitement acceptée (selon le principe que le silence de l'usager vaudrait acceptation de toute utilisation ultérieure des données recueillies) n'est acceptable ni d'un point de vue éthique ni en terme de souveraineté nationale ou individuelle.

E-3 Le dispositif de « bouclier de protection des données » (*Privacy Shield*) ou la prochaine mise en place règlement général sur la protection des données personnelles (RGDP) illustrent le rapport de force difficile existant avec des entreprises de droit américain (et l'extra-territorialité qui lui est attachée) qui nécessite de ne pas exclure la mesure radicale d'une obligation d'un stockage exclusif des données de nos concitoyens sur le territoire de l'Union européenne.

E-4 Ce qui est vrai à l'échelle individuelle l'est tout autant à l'échelle collective ; que notre vision de la souveraineté collective se place à l'échelle nationale ou européenne, on doit s'inquiéter de la menace sur le fonctionnement démocratique de nos institutions ou d'ingérence dans les choix de société.

E-5 Le numérique transforme profondément l'approche scientifique et son environnement ; les questions de souveraineté scientifique qui s'ensuivent se combinent avec des enjeux éthiques cruciaux dans le développement de toutes les disciplines.

E-6 Les implications de ces évolutions dans le cadre scientifique ont des conséquences profondes sur toutes les sociétés à l'échelle de la planète et sur l'évolution humaine.

E-7 La souveraineté numérique croise dans nos sociétés actuelles la plupart voir toutes les autres souverainetés. Il en résulte une source importante de conflit.

Ces enjeux nous conduisent à formuler les **recommandations** suivantes :

R-1 De manière complémentaire aux formations à l'éthique et à l'intégrité scientifiques conduites dans les écoles doctorales, mettre en place des formations de tous les scientifiques à l'éthique et à la responsabilité scientifiques.

R-2 Mettre en place les moyens de la souveraineté scientifique dans le secteur académique au niveau français et européen dans une perspective de science ouverte. On visera en particulier à rendre systématique le dépôt en archive ouverte HAL de toute la production scientifique nationale et à favoriser une telle approche au niveau européen et international.

R-3 L'accès à toutes les données nécessaires à l'activité scientifique des institutions de recherche devra être rendu possible ; en particulier l'accès à la fouille de données (TDM) devra être assuré sans restriction à des fins scientifiques, le tout dans des conditions strictes et auditées d'éthique, d'intégrité et de déontologie scientifiques .

R-4 Expliciter comment les plates-formes collectant massivement des données (par exemple les GAFAMI et BATX) doivent ouvrir ces données à des fins de science ouverte dans des conditions strictes d'éthique, d'intégrité et de déontologie scientifiques.

R-5 Tenant compte des spécificités disciplinaires, établir, discipline par discipline, une politique de partage équitable des données de la recherche en accord avec les institutions nationales et les grands acteurs de l'Internet.

R-6 Inviter les associations professionnelles des différentes disciplines scientifiques à expliciter leurs contributions au renforcement de la souveraineté scientifique.

R-7 Les souverainetés nationales, numériques et scientifiques reposent sur la recherche en

cybersécurité qu'il convient donc de développer très fortement.

R-8 Avec le parrainage de l'UE et en collaboration des associations professionnelles scientifiques, l'académie des sciences et celle des technologies, mettre en place un prix international « éthique et souveraineté scientifique ».

Sortant du cadre premier des attributions de la CERNA qui est de s'adresser à la communauté scientifique française, nous estimons utile de formuler les **suggestions** suivantes, de nature plus politique et s'inscrivant dans un cadre international :

S-1 Lancer une initiative internationale visant à élargir explicitement au domaine numérique le principe énoncé par l'article 18 de la déclaration universelle des droits de l'Homme de 1948 selon lequel « toute personne a droit à la liberté de pensée », repris par l'article 9 de la Convention européenne des droits de l'Homme de 1950 et par l'article 10 de la Charte des droits fondamentaux de l'Union européenne de 2000.

S-2 Parallèlement à cette initiative internationale, il convient de lancer une initiative européenne, ou plus pragmatiquement franco-allemande, qui se donnera les moyens de garantir l'intégrité et la confidentialité des données numériques et plus généralement de renforcer la recherche en cybersécurité et ses applications pour garantir l'expression de souverainetés qu'elles soient nationales, numériques, scientifiques et individuelles.

S-3 Inciter les organisations œuvrant sur Internet dans le champ politique des « actions citoyennes » et de l'« influence sociale » (à l'exemple des organisations spécialisées le lancement de pétitions en ligne tels que Avaaz.org, Change.org, SumOfUs, etc.) à rendre transparent, facile d'accès et intelligible les conditions d'utilisation des données personnelles et, en particulier, d'uniformiser une rubrique unique (regroupant les appellations variées de *data policy*, *privacy policy*, *confidentiality policy* et *information policy*).

S-4 Dès l'école primaire, puis dans le secondaire, concevoir un enseignement qui sensibilisera aux enjeux de cybersécurité et de la maitrise des outils permettant de préserver la vie privée et d'alerter sur diverses formes de manipulation ou d'endoctrinement facilitées par les médias numériques ;

S-5 Dans le cadre d'un futur « service national universel » expliciter les enjeux sociétaux des souverainetés à l'heure du numérique.

S-6 En s'appuyant sur les médias et l'implication de la communauté scientifique, permettre de sensibiliser l'ensemble de la population pour renforcer la résilience de nos concitoyens face aux fausses nouvelles et aux actions de manipulation utilisant les médias numériques.

S-7 Créer un comité consultatif national d'éthique pour les sciences, technologies, usages et innovations du numérique.

S-8 Développer une doctrine et une stratégie d'influence française et européenne et se donner les moyens de la défendre dans toutes les instances nationales et internationales (CE, Unesco, OMS, instances de normalisation et standardisation (ISO, AFNOR, IEEE,…)).

REMERCIEMENTS ET PERSONNALITÉS AUDITIONNÉES

Nous sommes vivement reconnaissants aux personnalités suivantes que nous avons auditionnées sur ces sujets :

- *Pierre Bellanger*, président de SkyRock ;
- *Bernard Benhamou*, secrétaire général de l'institut de la souveraineté numérique[105] ;
- *Peter Burgess*, président de l'*Ethics Advisory Group* (groupe mis en place par *l'European Data Protection Supervisor*, Giovanni Buttarelli) ;
- *Guillaume Poupard*, directeur général de l'agence nationale de la sécurité des systèmes d'information ;
- *Henri Verdier*, directeur interministériel du numérique et du système d'information et de communication de l'État.

Outre ces auditions, nous avons organisé le lundi 3 juillet 2017, à l'institut Mines-Télécom, une journée CERNA intitulée « souverainetés et souveraineté numérique ». Nous remercions les intervenants de cette journée :

- Le vice-amiral d'escadre *Arnaud Coustillière*, qui occupait alors le poste d'officier général cyberdéfense du ministère des armées (actuel directeur général des systèmes d'information et de communication de ce même ministère) ;
- *Tristan Nitot*, ancien président de Mozilla Europe et qui occupait alors le poste de *Chief Product Officer* de Cozy Cloud ;
- *Pauline Türk*, professeur de droit public à l'université Nice Sophia Antipolis.

Nous tenons également à associer à ces remerciements les personnes venues assister à la journée du 3 juillet 2017 auxquelles il a été proposé de participer à quatre ateliers pour débattre de plusieurs thématiques au cœur de ce rapport. Ces débats ont été poursuivis lors d'une réunion de synthèse qui s'est tenue chez Inria à Paris l'après-midi du 20 novembre 2017.

---

105 http://www.souverainetenumerique.fr