

# Souveraineté numérique et cybersécurité de l'Europe

Thierry LEBLOND

Cet article rassemble les travaux conduits au cours du premier semestre 2021 dans le cadre d'un groupe de réflexion politique et écologique portant sur les questions de sécurité et de souveraineté numérique. Il aborde le sujet sous quatre angles : la sécurité environnementale, la souveraineté numérique des usages citoyens, la souveraineté numérique des opérateurs économiques et la souveraineté numérique des États.

**Thierry LEBLOND**

Thierry Leblond est membre du conseil EuroDéfense France, ingénieur général de l'armement, président et cofondateur de SCILLE, éditeur du logiciel de cybersécurité des données PARSEC, certifié par l'ANSSI, dédié au partage Zero Trust et anti-ransomware des données sensibles sur le cloud public.

## La souveraineté numérique : une question de volonté politique nationale et européenne

### *Les définitions de la souveraineté numérique*

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

*communications électroniques et nos données». De façon plus novatrice, d'autres relient la souveraineté numérique à la capacité de certains acteurs à se faire obéir, à imposer leurs lois, à apparaître comme devant être respectés dans l'espace numérique (Pierre Trudel, professeur à l'université de Montréal). Ou encore se réfèrent, pour l'appréhender, à l'appropriation de certains attributs de la souveraineté par les entreprises, grâce à leur position dominante sur le marché (Annie Blandin-Obernesser, op. cité*[1]*).* »

Nous renvoyons également au rapport Oliver Wyman (A Marsh & McLennan Company) « European Digital Sovereignty » publié en 2020 [2].

## *L'histoire de la souveraineté numérique de l'Europe s'écrit en ce moment*

Les positions dominantes des États-Unis et de la Chine en matière de technologies du numérique, notamment qu'il s'agisse du *Cloud* (informatique en nuage), des câbles optiques intercontinentaux, des réseaux numériques optiques ou aériens ou de la cyber-coercition condamnent-elles l'Europe à une position de vassalisation ?

L'Histoire n'est jamais écrite d'avance, car elle est le résultat de la volonté de la nation. Pourquoi, sinon par volonté de souveraineté, a-t-on, dans les années 1960, engagé avec le succès que l'on connaît aujourd'hui, des coopérations industrielles dans le spatial ou l'aéronautique comme Airbus et Ariane alors que des alternatives commerciales existaient de l'autre côté de l'Atlantique ? Pourquoi a-t-on engagé un programme de nucléaire civil ?

Pourquoi la Chine communiste, encore en « Révolution Culturelle » dans les années 1970, a-t-elle engagé dans les années 1990 un programme de reconquête qui fait d'elle aujourd'hui une puissance économique mondiale, numérique en tête ?

Tout est une question de volonté politique ! L'Europe estime que le Numérique est un enjeu stratégique [3] qui demande une vraie valeur politique. On a pu croire au cours des dernières décennies que les données numériques n'étaient que des biens marchands. Mais les nouvelles technologies de *Big Data*, d'Intelligence Artificielle (IA) ou de cybersécurité leur confèrent désormais une valeur stratégique. Une nation qui entend rester souveraine doit se doter des moyens de les maîtriser sur la durée quel qu'en soit le prix.

Au-delà des discours, quelles sont les actions concrètes de la France en tant que pays européen ? La situation est nuancée, car les signaux politiques sont contradictoires :

– d'un côté, dans le sillage de l'Union européenne et du plan de relance, la France se dote d'un grand plan d'investissement d'avenir dans les technologies de la transformation numérique et de la cybersécurité ; la direction interministérielle du Numérique, dans un contexte des lois extra-territoriales US, prend la décision majeure d'interdire aux administrations françaises d'utiliser la suite bureautique Office 365 opérée depuis le *cloud* étranger de Microsoft ;

– de l'autre côté, dans le contexte de la nouvelle stratégie « *Cloud* au centre », et alors qu'il existe une offre nationale avec OVH et Outscale 3DS, le gouvernement français salue la constitution d'alliances stratégiques entre des champions français des communications et de la sécurité et les GAFAM [4] pour construire des *clouds* dits « souverains » pourtant construits sur des technologies américaines : le projet « Bleu » entre Orange et Microsoft, puis le projet d'alliance entre Thalès et Google. Il poursuit également la captation annoncée des données de santé des Français autour du projet Health Data Hub opéré sur un *cloud* Microsoft. [5]

Parallèlement, elle fait allégeance aux GAFAM pour les données personnelles et sensibles de ses citoyens. L'Europe

(1) Türk (P.), 2020, « Définition et enjeux de la souveraineté numérique », article publié sur www.vie-publique.fr le 14 septembre : https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique

(2) Rapport Olivier Wyman (A Marsh & McLennan Company), «European Digital Sovereignty» publié en 2020 : https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf

(3) La commission européenne a engagé de nombreux travaux :
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC113826/ai-flagship-report-online.pdf
https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence
https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence
https://futurium.ec.europa.eu/en/european-ai-alliance/open-library/policy-and-investment-recommendations-trustworthy-artificial-intelligence
https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence
https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment
https://op.europa.eu/fr/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1/language-fr
https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_fr.pdf

(4) GAFAM est l'acronyme des géants du Web – Google, Apple, Facebook, Amazon et Microsoft – qui sont les cinq grandes firmes américaines qui dominent le marché du numérique, parfois également nommées les *Big Five*.

a-t-elle cette volonté politique de souveraineté dans les faits ? L'Europe investira-t-elle les 20 milliards d'euros par an nécessaires pour construire le *Cloud* européen de confiance qui est stratégique pour notre avenir ?

## Constats et enjeux

Les menaces sur notre souveraineté numérique européenne sont de quatre ordres :

1. La sécurité environnementale ;
2. La souveraineté numérique des usages citoyens ;
3. La souveraineté des opérateurs économiques ;
4. La souveraineté des États.

### *La sécurité environnementale ou la vision « terrienne »*

Le numérique est à la fois un outil et un défi pour la transition écologique.

#### *Une empreinte environnementale directe qui croît rapidement*

Chaque seconde, 400 personnes se connectent pour la première fois à Internet dans le monde. Pratiquement chaque habitant de la Terre y a accès, le plus souvent via son smartphone. La part du numérique dans les émissions de gaz à effet de serre a augmenté de moitié de 2013 à 2018. Selon le groupe de réflexion The Shift Project[6], le numérique émet, en 2019, 4 % des gaz à effet de serre du monde ; sa consommation énergétique s'accroît de 9 % par an qui se répartit en 55 % pour l'usage du numérique et 45 % pour la production des équipements.

En ce qui concerne les smartphones, 80 % des émissions de CO2 sont dégagées lors de leur phase de fabrication. L'utilisation (consommation de vidéo sur Netflix, échanges de mails, etc.) ne représente donc que 20 % du problème.

Outre les émissions de CO2, le numérique impacte directement notre environnement :

– la fabrication des terminaux numériques consomme beaucoup de métaux rares dont l'extraction a un impact sur l'environnement et la santé des ouvriers : utilisation de produits chimiques, d'eau …

– une fois parvenus en fin de vie, les objets numériques sont d'autant plus difficiles à recycler qu'ils sont complexes. Produisant des déchets d'équipements électriques et électroniques (DEEE) plus nombreux chaque année, ils aboutissent dans des décharges, parfois informelles, où ils contaminent leur environnement et, dans les pays en développement, les populations qui en vivent ;

– ils ont également un impact indirect sur les sols par l'épuisement des ressources abiotiques et sur l'eau par leurs effets d'eutrophisation et d'acidification.

#### *Les impacts environnementaux directs et indirects*

Les applications du numérique ont des impacts directs sur notre environnement en nous autorisant une meilleure efficacité énergétique : Blablacar nous permet de covoiturer facilement, Leboncoin nous permet de réutiliser quasi gratuitement les objets. Inversement, les réseaux sociaux et le *streaming* basés sur des serveurs centraux sont énergivores (comparativement à des technologies en *peer-to-peer* aujourd'hui en veille pour des raisons économiques et juridiques).

Les impacts indirects du numérique, ceux qui sont à venir, sont les plus importants et sont liés à l'effet de rebond. Ainsi, si l'efficacité énergétique, énergie dépensée par Go transféré, s'est améliorée, elle entraîne avec elle une augmentation du nombre de Go échangés aboutissant finalement à une consommation énergétique plus élevée.

#### *Une dépendance énergétique et matérielle croissante*

Les impacts environnementaux associés à l'électricité dépendent directement de la nature de l'énergie primaire employée (uranium, énergie fossile, vent, soleil, biomasse) et du moyen de production utilisé (centrale nucléaire, centrale thermique, éolienne, solaire, etc.).

### *La souveraineté numérique des usages citoyens*

La révolution numérique s'est installée dans nos sociétés et leurs organisations en plusieurs étapes. Progressant à

(5) Critiqué pour son hébergement de données par l'entreprise américaine, le projet soutenu par le gouvernement a retiré sa demande d'autorisation à la CNIL le 10 janvier 2022

(6) Déployer la sobriété numérique, *The Shift Project*.

la vitesse de la loi de Moore, c'est-à-dire le doublement de la puissance tous les 18 mois. Depuis les années 1980, chaque évolution s'impose comme un progrès pour l'Humanité sans qu'à aucun moment les pouvoirs politiques ne s'interrogent sur le prix à payer pour le Bien Commun. Or, selon Jacques Ellul, « *tout progrès se paie* [7] ».

Résumons ces étapes :

– 1980 : l'informatique et la bureautique individuelle ;

– 1990 : l'interconnexion par les réseaux ;

– 2000 : l'Internet, la virtualisation, les moteurs de recherche et le web ;

– 2010 : le *cloud* public, la mobilité, le *big data* et les réseaux sociaux ;

– 2020 : l'intelligence artificielle, les cyber-menaces, l'interconnexion généralisée, le ciblage individuel de la population.

L'être humain et la société ne maîtrisent pas les conséquences de ces révolutions numériques successives ; ils en subissent à la fois les bienfaits mais aussi de façon paradoxale les nuisances. Citons quelques enjeux majeurs :

1. Souhaitons-nous continuer dans l'accélération de notre référence temporelle où tout devient vitesse et instantanéité et où nous n'avons plus le temps du recul ?

2. Quel pouvoir voulons-nous laisser aux réseaux sociaux sur notre vie et nos libertés ?

3. Jusqu'à quel point laissons-nous les outils de mobilité (smartphones) prendre le pouvoir sur nos cerveaux ?

4. Comment maîtriser la généralisation du télétravail à domicile, conséquence directe du confinement sanitaire, entre nouvelle conquête sociale et nouvelle servitude ?

5. L'ubérisation est-elle compatible avec le Code du travail ?

6. Le numérique peut-il effacer la frontière du handicap ?

7. Comment vaincre l'analphabétisme numérique (« illectronisme »), nouvelle source d'inégalités ?

8. Quelle position nos sociétés doivent-elles adopter face à l'essor des crypto-monnaies ? Faut-il les réglementer [8] ?

## *Vers de nouvelles normes sociales ?*

L'épidémie de Covid 19 et les confinements qui en ont découlé ont incontestablement accéléré le passage au tout numérique :

– en France, au cours des deux premières semaines du confinement de mars 2020, on est passé de 800 000 à 8 000 000 de télétravailleurs réguliers – ce qui est le plus grand choc que le monde du travail ait jamais connu depuis l'exode rural à la fin du XIX$^{e}$ siècle ;

– la part des Français qui font leurs achats du quotidien en ligne a doublé en 15 jours ;

– en France, selon le directeur général de l'ANSSI, les cyberattaques « criminelles » ont été multipliées par 4 en 2020 [9].

Les phases de confinement risquent malheureusement de se banaliser au cours des prochaines décennies. Pendant ces périodes, le lien social, l'activité économique, les services publics ne pourront être maintenus qu'à travers le numérique. Le monde de demain devra apprendre à marcher sur deux jambes : transition environnementale et transformation numérique.

## *Télétravail*

La transformation numérique favorise la mobilité et l'utilisation du *cloud* public. Elle autorise ce nouveau modèle de travail qu'est le Télétravail, ou travail à distance, pour assurer la continuité de l'activité des entreprises.

L'environnement du télétravail est confronté à trois conditions que l'on doit dépasser :

1. La première condition, humaine, consiste à respecter la respiration sociale du groupe en organisant à intervalle régulier des rencontres ou séminaires d'équipe, car on ne peut travailler seul durablement ;

2. La deuxième condition est liée à l'organisation et au *management* qui doivent s'appuyer avec force sur les valeurs que sont la confiance, l'autonomie, l'envie de

(7) « Tout progrès se paie » Jacques Ellul : https://fr.wikipedia.org/wiki/Progrès
(8) https://www.lesechos.fr/finance-marches/marches-financiers/la-commission-europeenne-veut-reguler-les-crypto-monnaies-1248666
(9) https://www.bfmtv.com/economie/selon-l-anssi-les-cyberattaques-criminelles-ont-ete-multipliees-par-4-en-2020_AV-202101110353.html

progresser et le sentiment d'apprendre et de contribuer à un but supérieur [10];

3. La troisième condition concerne les outils de travail, qui doivent être à la fois collaboratifs, ergonomiques et sécurisés : une nouvelle manière de travailler pose de nouveaux défis sur la sécurité des données sensibles partagées, car nous sommes aussi dans un contexte croissant de cybermenaces.

Le 26 novembre 2020, un projet d'accord interprofessionnel pour une mise en œuvre réussie du télétravail (ANI) a été entériné par le Medef, la CPME et l'U2P côté patronat, et, côté syndicats par la CFDT, FO, la CFE-CGC, FO à l'exception de la CGT [11].

## *Impact des réseaux sociaux et des plateformes numériques sur notre société*

« *Jamais, dans l'histoire, il n'y a eu cinquante concepteurs (principalement des hommes blancs vivant à San Francisco entre 25 et 35 ans) prenant des décisions ayant un impact sur deux milliards de personnes.* » [Tristan Harris, éthicien, ancien cadre chez Google]

« *Progressivement, on intègre l'idée fausse que tout le monde est d'accord avec nous, parce que notre flux d'actualité ne montre que cela. Une fois dans cette disposition, on se fait aisément manipuler.* » [Roger McNamee, investisseur aux débuts de Facebook]

Les sources de revenus principales des plateformes en ligne sont les publicités. Pour maximiser leur profit, les plateformes ont donc intérêt à maximiser le temps passé de chaque utilisateur sur leur plateforme. On parle d'économie de l'attention.

Pour maximiser notre temps passé sur leurs plateformes, les réseaux sociaux utilisent des techniques qui exploitent nos failles psychologiques [12]:

– utiliser le circuit de la récompense de notre cerveau qui sécrète de la dopamine, exactement comme les drogues dures : alcool, héroïnes. Exemple des « like » ;

– l'addiction est un but recherché dès la conception de nos *smartphones* et applications : *Design* attractif, notifications *push* incessantes, *scrolls* infinis… Le *scroll* infini fonctionne, car il ne demande qu'un simple et rapide effort (*scroll*) pour obtenir une nouvelle récompense (nouveau post, nouvelle photo …). Les notifications sont désignées pour être envoyées de manière aléatoire, ce qui est beaucoup plus efficace que si elles étaient envoyées à intervalle régulier ;

– les algorithmes, pour maximiser notre temps en ligne, tendent à nous proposer du contenu qui correspond à nos opinions et à nos centres d'intérêt (bulles de filtrage), ce qui nous conforte dans nos opinions : biais de confirmation.

Ces différentes techniques ont les effets suivants sur notre société :

– segmentation et radicalisation de la société : tout le monde pense avoir raison, hystérisation des discussions ;

– perte de confiance dans les politiques et les scientifiques ;

– perte d'estime de soi;

– la vérité devient du côté des opinions plutôt que des faits.

C'est le message qu'a passé Frances Haugen, ex-employée de Facebook, lors de son audition du 5 octobre 2021 devant la Commission du commerce du Sénat américain : « *Facebook est devenu une entreprise valant mille milliards de dollars en faisant passer ses profits avant notre sécurité* ». Selon cette lanceuse d'alerte, « *Le Congrès doit changer les règles du jeu pour Facebook et mettre fin aux dégâts que cause l'entreprise* ».

## *Éducation, inclusion numérique et fracture numérique*

La pandémie Covid-19 a amplifié brutalement les inégalités et les enjeux des usages du numérique :

– inégalité dans l'accès aux équipements ;

– inégalités devant la qualité de la connexion ;

– manque de préparation des enseignants et des formateurs (appartenant majoritairement encore à des générations qui ne sont pas nées avec le numérique), passage brutal du « présentiel » à des méthodes en rupture d'enseignement à distance ;

(10) Conférence de Dan Pink sur la motivation au travail
(11) La Tribune "Télétravail : les principales mesures ont été validées par le patronat et les syndicats (mais pas la CGT)"
(12) Google Deck on Digital Wellbeing 'A Call to Minimize Distraction and Respect Users' Attention'

– développement de l'esprit critique des élèves dans un environnement numérique, sans la présence physique de l'enseignant : les nouveaux outils posent brutalement la question du sens de la transmission de la connaissance, car la dimension humaine de l'enseignement s'estompe. Peut-on transmettre le savoir par machine interposée si les hommes ne sont pas en relation directe ?

Elle interroge également sur les outils utilisés, l'autonomie et la responsabilité locale des enseignants sur le programme :

– faut-il considérer les outils numériques comme de simples dispositifs et ne pas se soucier de leur provenance, au risque de se livrer aux monopoles du numérique ?

– la crise sanitaire n'est-elle pas une opportunité de nous interroger sur le sens des outils, sur une pédagogie où l'individu n'est pas un consommateur du numérique, mais un acteur local de son écosystème ? Logiciels libres, développements agiles autour de composants libres sont des réponses où l'outil donne les moyens d'interroger notre relation à la connaissance ;

– à côté du « programme national officiel », quelle marge veut-on se donner sur l'autonomie locale des enseignants pour tenir compte des spécificités géographiques locales ? « Laissez-nous décider du programme ! ».

Outre l'article L. 123-4-1, qui ne s'applique qu'à l'enseignement supérieur, l'article 16 de la loi Lemaire qui s'applique à toute administration publique, notamment à l'enseignement scolaire public, n'est pas appliqué [13].

Dans le cadre d'un appel d'offres publié au mois d'août 2020, le ministère de l'Éducation nationale a débloqué des budgets pour le renouvellement de licences pour des produits Microsoft et des services associés. Le montant total de cet accord est estimé à 8,3 millions d'euros sur douze mois, renouvelable 48 mois afin d'équiper 800 000 postes de travail et 80 000 serveurs [14]. L'éducation nationale s'enfonce depuis longtemps dans sa dépendance à l'égard des GAFAM : Classroom, *iCloud*, Facebook et Office 365. La loi du 22 juillet 2013 relative à l'enseignement supérieur et à la recherche prévoit que l'on utilise en priorité des logiciels libres mais, dans les faits, il n'en est rien.

De plus, on confie les données personnelles et scolaires des élèves et des enseignants aux *clouds* (nuages de données) des GAFAM dont le modèle économique repose sur l'exploitation opaque des données en lien étroit avec la NSA, l'Agence nationale de la sécurité des États-Unis. Des critiques similaires sont portées sur le Health data hub confié à Microsoft ou sur le contrat « Open bar » négocié il y a quelques années entre le ministère de la Défense et la filiale irlandaise de Microsoft [15].

En novembre 2020, le Québec sortait un rapport sur l'état et les besoins de l'éducation 2018-2020 expliquant que la situation provoquée par la pandémie de Covid-19 a accentué la place du numérique et que toutes les personnes ne sont pas suffisamment outillées pour évoluer librement dans cette nouvelle réalité. Les inégalités observées ne portent pas uniquement sur l'accès à la technologie, elles concernent surtout les compétences requises pour utiliser cette technologie autrement qu'à des fins ludiques ou de consommation. Le système éducatif a la responsabilité de donner à chaque personne, à un moment ou l'autre de sa vie, l'occasion de développer la littératie numérique en question. Le Conseil formule trois orientations pour permettre au système éducatif d'assumer la responsabilité d'éduquer au numérique. Quelques extraits : « *L'école doit donner aux personnes l'occasion d'apprendre à se servir correctement des outils technologiques qu'elles auront à utiliser dans leur vie citoyenne et professionnelle. Cela déborde largement l'usage des ressources éducatives numériques et implique, par exemple, les connaissances requises pour faire un choix éclairé parmi les logiciels propriétaires et les logiciels libres* » ou encore : « *Pour éviter de dépendre des choix de l'industrie, l'État pourrait prendre en charge le développement de ressources éducatives en français et s'assurer qu'elles répondent aux critères de l'accessibilité universelle. Enfin, le recours aux logiciels libres devrait être encouragé* ».

## *Être citoyen, c'est comprendre le pouvoir du numérique sur nos décisions*

Les démocraties sont nées parce que les citoyens étaient capables de lire et de comprendre. Or, peu de gens sont capables de comprendre comment fonctionnent les systèmes numériques, par exemple les algorithmes d'intelligence artificielle, alors qu'ils se répandent rapidement et dictent une part croissante de nos choix. Les démocraties au XXIe siècle ne se sauveront que si elles sont capables de faire reculer ce qu'on appelle « l'analgorithmie », c'est-à-dire l'incapacité à lire et écrire un algorithme.

(13) L'article 16 de la loi République numérique n'est pas appliqué.
(14) Page 4 - question 1121 du 17/11/2020 : https://questions.assemblee-nationale.fr/static/15/questions/jo/jo_anq_202046.pdf
(15) Voir la question du député Philippe Latombe sur la dépendance de l'éducation nationale à l'égard des GAFAM.à l'attention de à M. le ministre de l'éducation nationale, de la jeunesse et des sports.

LES DÉMOCRATIES SONT NÉES PARCE QUE LES CITOYENS ÉTAIENT CAPABLES DE LIRE ET DE COMPRENDRE. OR, PEU DE GENS SONT CAPABLES DE COMPRENDRE COMMENT FONCTIONNENT LES SYSTÈMES NUMÉRIQUES, PAR EXEMPLE LES ALGORITHMES D'INTELLIGENCE ARTIFICIELLE, ALORS QU'ILS SE RÉPANDENT RAPIDEMENT ET DICTENT UNE PART CROISSANTE DE NOS CHOIX. LES DÉMOCRATIES AU XXIE SIÈCLE NE SE SAUVERONT QUE SI ELLES SONT CAPABLES DE FAIRE RECULER CE QU'ON APPELLE « L'ANALGORITHMIE », C'EST-À-DIRE L'INCAPACITÉ À LIRE ET ÉCRIRE UN ALGORITHME.

### *Impacts du numérique sur notre santé*

Les impacts du numérique sur notre santé sont compliqués à mesurer, car nous n'avons pas encore assez de recul et de nombreux autres facteurs ont un impact sur notre santé. Cependant il existe des études qui montrent les choses suivantes :

– une source préoccupante de stress et de charge mentale qui est une grande source de stress ;

– dépendance aux outils numériques (écran : un adolescent passe en moyenne 6 heures par jour sur un écran) ;

– l'infobésité et une moins bonne qualité de l'information entraîneraient une perte de repères et de confiance.

Les *Digital Therapeutics* (DTx), telles que celles imaginées par la société Lucine[16], proposent, par leurs approches originales et en rupture, de fournir aux patients des solutions thérapeutiques conduites par des logiciels pour prévenir, gérer ou traiter un large éventail de symptômes et pathologies physiques, mentales et comportementales. Concrètement, il s'agit d'activer les neurotransmetteurs du cerveau au moyen de stimulations visuelles et auditives pilotées par le numérique.

Si nous pouvons traiter la douleur par les technologies du numérique, cela ouvre le champ à d'autres voies pour agir sur nos neurotransmetteurs afin d'obtenir d'autres effets comportementaux.

## *La souveraineté numérique des opérateurs économiques*

### *Transformation numérique des organisations*

Avec la généralisation de la 5G qui interconnecte en direct tous les terminaux sur Internet et du *Cloud* Public, Internet devient un réseau d'entreprise géant. L'accès par Internet devient la norme quand l'Intranet et les réseaux privés deviennent des handicaps de mobilité. Les données circulent en texte clair et sont accessibles et manipulables par beaucoup trop d'acteurs tiers : gouvernements, *hackers*… Internet devient le terrain de jeu des pirates : la confidentialité et l'intégrité deviennent les nouveaux défis du partage des données.

Le *Cloud* Public et les applications en SaaS, « Low Cost », par leur agilité et leur scalabilité se généralisent et obligent à maîtriser la sécurité des données échangées, car les situations d'adaptation en mobilité sont de moins en moins prévisibles. Les infrastructures propriétaires ou dédiées vont devenir l'exception.

### *Retrouver une puissance économique numérique*

Les grands groupes américains du numérique, GAFAM, investissent six fois plus dans les *start-up*[17] de l'intelligence artificielle que leurs homologues français. Ces sociétés américaines grandissent plus par croissance externe que par croissance interne, et achètent souvent des entreprises européennes[18].

Nos entreprises ont besoin de pouvoir accéder plus facilement à la commande publique et aux capitaux pour accélérer leur croissance. Au-delà des aides à l'innovation, il faudrait par exemple réfléchir à promouvoir les technologies françaises/européennes par un dispositif de type « BETA » (sorte de « *Buy European Technology Act* ») et, d'une façon générale, mieux faire confiance aux petites entreprises innovantes.

Le plan de relance du numérique et de la cybersécurité entrepris par le gouvernement actuel dans le sillage de la politique de souveraineté de l'Union européenne va dans la bonne direction.

(16) Lucine : https://lucine.fr/
(17) *Startup* est un anglicisme à la mode pour dire « PME technologique ».
(18) Par exemple en cybersécurité, domaine souverain par excellence, la pépite Alsid, spécialiste de la sécurisation de l'Active Directory annonçait le 10 février 2021 son rachat par l'Américain Tenable pour 98 millions de dollars.

### *La collecte de données personnelles de citoyens et espionnage des données de sociétés*

Le règlement général sur la protection des données personnelles (RGPD) et la directive de sécurité des réseaux (NIS) du 6 juillet 2016 représentent sur le plan juridique une avancée notable et indiscutable dans la résolution des problèmes de confidentialité des données de certaines infrastructures nationales critiques. Elles ont clairement suscité l'attention des acteurs politiques et des industries de l'information hors des frontières de l'Europe. Le RGPD est même devenu un vecteur d'évolution culturelle profonde au sein des organisations, qui fera de la donnée un véritable « bien collectif » par rapport auquel chacun se sentira investi et redevable à son niveau, ne serait-ce qu'au niveau de son ou de ses terminaux ; cela constitue aussi, nous le verrons, un facteur de saine gestion des projets *cloud*[19] et *Big Data*.

Parallèlement, les GAFAM sont confrontés à des fuites massives de données personnelles, le Patriot Act d'octobre 2001 permet aux agences sécuritaires gouvernementales américaines d'obtenir des informations dans le cadre d'une enquête sur des actes de terrorisme, et le *Cloud Act* du 23 mars 2018[20], réplique politique au RGPD, permet, « *dans le contexte des enquêtes judiciaires* » un accès rapide aux données en s'adressant directement aux fournisseurs d'informatique en nuage plutôt qu'en passant par une demande de traités d'entraide judiciaire (MLAT).

Mais malgré cela, la volonté politique actuelle de la France en matière de souveraineté numérique n'est toujours pas au rendez-vous comme en témoigne le projet du « *Data Health Hub* », un guichet unique d'accès à l'ensemble des données de santé, confié à Microsoft, pour développer l'intelligence artificielle appliquée à la santé. Alors que ces données sont celles de tous les citoyens français et concernent l'ensemble des systèmes informatisés des acteurs français de la santé, ce projet ouvre aux GAFAM la porte de nos données de santé et au pouvoir financier qu'elles représentent. Suite à un référé-liberté, le Conseil d'État a reconnu le risque que les services de renseignement américains accèdent aux données personnelles de la plateforme ce qui, paradoxalement, ne l'a pas empêché d'autoriser la poursuite du projet, sous le contrôle de la CNIL[21].

### *Accélérer la réglementation européenne*

La souveraineté numérique nationale et européenne reste encore à construire, même s'il y a eu dans ce domaine des avancées incontestables sur le plan européen :

– l'adoption par le parlement du règlement 2016/679, le règlement général sur la protection des données applicable partout en Europe depuis le 25 mai 2018 constitue une première mondiale en termes de régulation ;

– l'invalidation par la Cour de justice européenne le 16 juillet 2020 par la décision « Schrems 2 », de l'accord transatlantique mal-nommé « Privacy Shield » qui autorisait le transfert vers les USA de données sensibles de citoyens européens a envoyé un signal fort en matière de lois extraterritoriales[22];

– l'*European Cybersecurity Act*, adopté par le Parlement européen le 12 mars 2019 puis par le Conseil de l'Union européenne le 7 juin, marque une avancée importante pour l'autonomie stratégique européenne avec un double objectif : l'adoption du mandat permanent de l'ENISA[23];

– le règlement « Electronic IDentification Authentication and trust Services » (eIDAS) de juillet 2014 qui est un règlement de l'UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein de l'Union européenne, déjà implémenté en Estonie, sur des technologies ouvertes ;

– le SWIPO, qui vise à faciliter le changement de fournisseur et le transfert des données entre systèmes informatiques ;

– la libre circulation des données en Europe ;

(19) *Cloud* ou *cloud computing*, informatique en nuage en français, correspond à l'accès à des services informatiques (serveurs, stockage, mise en réseau, logiciels) via Internet (le *cloud* ou nuage) à partir d'un fournisseur.

(20) *Clarifying Lawful Overseas Use of Data Act* (*CLOUD Act*) est une loi fédérale des États-Unis, promulguée le 23 mars 2018, autorisant les forces de l'ordre et les agences de renseignements américains à rapatrier l'ensemble des données personnelles en possession des multinationales américaines sur le territoire américain et ce, sans aucun consentement des personnes intéressées, dans le cadre des enquêtes criminelles (notamment terroristes) et en vue de la protection de l'ordre public. Cette dernière notion étant large d'interprétation, d'importants risques existent pour la protection des données personnelles des ressortissants européens alors même que les données sont hébergées officiellement dans des centres de données situés aux Pays-Bas. Cette possibilité de transfert s'avère contraire aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), particulièrement en matière de transfert des données.

(21) Critiqué pour son hébergement de données par l'entreprise américaine, le projet soutenu par le gouvernement a retiré sa demande d'autorisation à la CNIL le 10 janvier 2022

(22) La Cour de justice de l'Union européenne (CJUE), par sa décision du 16 juillet 2020 *Data Protection Commissioner Facebook Ireland Ltd contre Maximillian Schrems* invalida le bouclier de protection des données, « *privacy Shield* » , accord conclu le 2 février 2016 qui avait pour(...)

– et les futurs *Digital Services Act* et *Market Services Acts*, doivent donner d'ici 2 ans un cadre législatif à l'espace informationnel pour les 20 ans à venir.

## *Focus sur la souveraineté des données de santé face aux géants du numérique*

Les projections économiques de la santé incitent les acteurs économiques à se placer dans ce secteur[24], qu'il s'agisse des industries pharmaceutiques, telles que Iqvia[25], des start-up dans le domaine de la santé, mais aussi des géants du numérique, les GAFAM. De nouveaux écosystèmes de santé complexes, de forte valeur, en constants développements, accélérés par la mise en place de nouvelles technologies du numérique sans cesse émergentes, du développement de la 5 G, de l'interopérabilité de plus en plus possible des données, etc.

Les entreprises créent de nouveaux outils ayant un impact sur la santé, ce qui peut créer des formes inédites d'appropriation de la santé telles que, par exemple :

– la création d'applications et de services numériques en matière de diagnostics et préconisations de traitements (services payants en ligne gérés par des plateformes d'entreprises hors du territoire). Par exemple, Google a fait ainsi des progrès spectaculaires pour la détection du cancer du sein[26], de même que dans le domaine oculaire (rétinopathie diabétique[27]) ;

– des applications permettant d'envisager la probabilité de décès ;

– des applications prévoyant les probabilités de réadmission d'un patient dans un établissement de santé ;

– la mise en place d'une médecine personnalisée de plus en plus gérée par le patient lui-même par le biais de nombreuses applications numériques offertes par les géants du numérique, plus performantes que le secteur classique de la santé ;

– des prestations de soins innovants, notamment dans le domaine de la chirurgie.

Les géants du numérique se positionnent de plus en plus sur ce marché rentable, offrant d'importantes perspectives économiques. Pour ce faire, ils investissent à tout va dans ce secteur, notamment par le biais d'accords, de partenariats conclus, voire de rachats avec les *start-up* spécialisées dans le domaine de la santé numérique[28].

– partenariat entre Apple et Elli Lilly pour la détection de signes de démence[29];

– rachat par Google en 2019 de la société Fifbit (bracelets/ montres connectés collectant des données dont certaines de santé[30]) ;

---

(...) objet le maintien des accords commerciaux entre la Commission européenne et les États-Unis en assurant un niveau de protection renforcé des données à caractère personnel des ressortissants européens transférées vers les États-Unis . Cet accord faisait suite à l'arrêt « Schrems I», (...) ayant invalidé l'accord Safe Harbor qui permettait aux entreprises étatsuniennes s'y soumettant de transférer les données des ressortissants de l'Union vers les États-Unis. Sur le fondement de l'article 46 Paragraphes 1 et 2 du RGPD, elle précisa notamment que, « *dans le cas où les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers, celles-ci doivent bénéficier d'un niveau de protection substantiellement équivalent à celui garant au sein de l'Union européenne. À cet effet, l'évaluation du niveau de protection assuré doit, notamment prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union européenne, et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui, notamment ceux énoncés à l'article 45, Paragraphe 2 du règlement* ». Cet arrêt posa un coup d'arrêt aux transferts des données hors de l'Union européenne, notamment vers les États-Unis, si un niveau de protection équivalent n'était pas accordé par leur législation. Ceci n'empêche pas, par conséquent, les entreprises américaines de s'adapter aux exigences de la réglementation européenne concernant la protection des données personnelles (RGPD), et de tenir compte des clauses contractuelles.

(23) ENISA (European Network and Information Security Agency) : agence de l'Union européenne chargée de la sécurité des réseaux et de l'information www.enisa.europa.eu

(24) Allen (S.), 2019, Rapport «Global Heath care Outlook Laying a foundation for the futur », Deloitte : 2020 Global health care sector outlook

(25) *Cash Investigation*, « Nos données personnelles valent de l'or ! » diffusée le 20 mai 2021 : https://www.francetvinfo.fr/replay-magazine/france-2/cash-investigation/cash-investigation-du-jeudi-20-mai-2021_4605401.html

(26) Samuel (S.), 2020, « L'IA peut désormais surpasser les médecins dans la détection du cancer du sein. Voici pourquoi il ne les remplacera pas. Google a développé un nouvel algorithme impression pour l'analyse des rayons X », *Vox*, 3 janvier : Google's AI for detecting breast cancer beats doctors and radiologists

(27) *Deepmind*, Predicting eye disease with Moorfields Eye Hospital

(28) Cochard (S.), 2020, «Santé : 20 points clés à savoir sur les projets d'Apple, Google et Amazon », Hub Institute, 5 mars : Digital Health Repères Santé : 20 key points à savoir sur les projets d'Apple, Google et Amazon

(29) Farr (C.), 2019, « Apple et Eli Lilly en étudiant les données des Iphones et des montres Apple peuvent détecter des signes de démence », 7 août: Apple and Eli Lilly are studying whether data from iPhones and Apple Watches can detect signs of dementia

(30) Vynk (G. de), 2019, « Google achète Fitbit dans le cadre d'un d'accord de 2,1 milliards de dollars pour lutter montre l'Apple Watch », *Times*, 1er novembre, https://time.com/5716260/google-buying-fitbit/ ; Corot (L.), 2020, « Le rachat de Fitbit par Google validé par les autorités européennes », *Usine digitale*, 17 décembre : Le rachat de Fitbit par Google validé par les autorités européennes

– Apple Watch : détection de signes avant-coureurs [31], surveillance de la fréquence cardiaque ;

– application sur ipad, iphone, Apple Watch, ipad d'applications destinées à aider les professionnels de santé à prodiguer des soins médicaux personnalisés [32];

– lancement par Apple de Heath Records permettant le stockage de données de santé ;

– lancement par Google de l'application Heath Studies destinée à faciliter l'obtention de données pour la recherche médicale le 9 décembre 2020 [33];

– lancement en septembre 2019 de l'application Amazon Care, clinique en ligne permettant les consultations en ligne pour des soins primaires, des prescriptions et la livraison d'ordonnance dans la région de Seattle [34];

– lancement d'Amazon Pharmacy en 2019 après le rachat de la pharmacie sur Internet Pillpack en 2018 [35];

– lancement par Amazon en 2019 de « Transcribe Medical », permettant d'enregistrer les discussions entre le médecin et son patient et leur retranscription dans le dossier médical [36].

Les GAFAM concluent également des accords avec les autorités nationales de santé :

– accord d'Amazon avec le National Heath Service britannique lui permettant d'avoir accès aux informations de santé des citoyens [37];

– accord de Microsoft avec le *Heath Data Hub* français.

Ils créent des écoles ainsi que des laboratoires privés dédiés à la santé :

– Microsoft a inauguré la première école d'intelligence artificielle dédiée à la santé au CHRU de Nancy [38].

Voire collectent des données des personnes sans leur consentement :

– projet Nightingale rassemblant les données personnelles de santé de 50 millions d'Américains, sans leur information, ni leur accord [39].

Or, les développements sont tels que différentes mises en garde se sont succédé :

– de l'Institut Sapiens par le biais de Olivier Babeau le 5 juillet 2018 [40];

– de CBInsights concernant la perturbation de la chaîne d'approvisionnement des médicaments [41].

Les risques sont si importants que des actions commencent à être envisagées par les autorités dans le secteur de la santé comme par exemple les enquêtes sur la collecte massive de données de santé par Google aux États-Unis en 2019 [42-43]».

Nos responsables politiques et nos administrations peinent à reconnaître le risque majeur d'atteinte à la souveraineté nationale et européenne dans le domaine particulièrement sensible de la santé. Du moins, s'ils en ont pris conscience, peu ou pas de mesures concrètes ne paraissent avoir été prises pour y remédier. Lors la pandémie Covid-19, il leur a pourtant été possible de mesurer à quel point la France a perdu de sa souveraineté concernant l'approvisionnement

(31) Apple : Santé - Apple Watch
(32) Apple : Santé - Produits et plateforme
(33) Corot (L.), 2020, « Google lance une application pour faciliter l'obtention de données pour la recherche médicale », *Usine digitale*, 10 décembre, Google lance une application pour faciliter l'obtention de données pour la recherche médicale
(34) Amazon Care : Amazon Care: Healthcare built around you
(35) Farr (C.), 2020, « Amazon vient de déposer un tas de marques internationales pour Amazon Pharmacy, 22 janvier, *CNBC*, Amazon files trademarks for 'Amazon Pharmacy' in UK, Australia, Canada
(36) Farr (C.), 2019, « Amazon permet aux médecins d'enregistrer vos conversations et de les mettre dans vos dossiers médicaux », *CNBC*, 2 décembre, Amazon Web Services unveils Transcribe Medical software
(37) Walker (A.), 2019, « NHS donne à Amazon l'utilisation gratuite des données de santé dans le cadre de l'accord de conseil Alexa », *The Guardian*, 8 décembre , NHS gives Amazon free use of health data under Alexa advice deal
(38) Microsoft, Simon (C.), 2020, « 13e école IA Microsoft par Simplon : inauguration de la première promotion dédiée à la santé au sein du CHU de Nancy », 13 février, 13ème Ecole IA Microsoft powered by Simplon : Inauguration de la première promotion dédiée à la santé au sein du CHU de Nancy - News Centre
(39) Capeland (R.), 2019, « Le projet Nightingale de Google rassemble des données de santé personnelles sur des millions d'américains », *The Wall Street Journal*, 11 novembre, Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans
(40) Babeau (O.), 2018, « Gare au hold-up de Google sur la santé ! », Institut Sapiens, 5 juillet, Gare au hold-up de Google sur la santé !
(41) « Amazon dans la santé : la stratégie du géant du commerce électronique pour un marché de 3 billions de dollars », *CBInsight*, Rapport : Amazon Healthcare Strategy I CB Insights
(42) Copeland (R.), Needleman (S.E.), 2019, « Le projet "Project Nightingale de Google déclenche une enquête fédérale", Wall Street Journal, 12 novembre, Google's 'Project Nightingale' Triggers Federal Inquiry - WSJ
(43) Vitard (A.), 2019, « Une enquête s'ouvre sur la collecte massive de données de santé par Google aux États-Unis », Usine digitale, 13 novembre, Une enquête s'ouvre sur la collecte massive de données de santé par Google aux États-Unis

des masques, des médicaments, des équipements destinés à la respiration des malades du covid, et des vaccins, fabriqués par des sociétés étrangères hors du territoire. Cette situation de pénurie et de dépendance, qui a été à l'origine probablement du décès d'un certain nombre de patients, constitue une importante mise en garde. Il est indispensable que des mesures soient prises pour protéger la souveraineté de l'État français et la souveraineté européenne à l'égard des géants du numérique.

## *La souveraineté numérique des États*

### *Les attaques contre les valeurs démocratiques et européennes.*

L'Europe est ouverte et transparente puisque la liberté d'expression est protégée par l'article 10 de la Convention européenne des droits de l'homme. Cela procure un avantage à ceux qui utilisent les technologies du *Big Data*[44] et des réseaux sociaux pour déstabiliser nos institutions par l'arme de la subversion et de la désinformation.

La manipulation des élections américaines de 2016 et le scandale « Cambridge Analytica[45] », les pressions sur le déploiement du vote électronique malgré les incertitudes répétées sur sa fiabilité, la montée en puissance des « deep fakes » et de la haine sur Internet et les réseaux sociaux, favorisées par l'anonymat, sont autant de signaux qui doivent nous alerter et trouver une réponse politique.

Le limogeage mi-novembre 2020 de Chistopher Krebs, le directeur de l'agence de cybersécurité américaine, qui, en accord avec la déontologie, n'a pas accepté de relayer les allégations de fraudes électorales dénoncées sans preuves par le président Trump, les accrocs répétés dans tous les pays à la liberté de circulation au nom de la protection sanitaire de la population, montrent que la tentation de la dictature n'est jamais très loin.

Les valeurs démocratiques et européennes sont également attaquées par le fonctionnement même des réseaux sociaux qui contribue à conforter chacun dans ses opinions (biais de confirmation), segmenter notre société et éventuellement appauvrir, voire faire disparaître les discussions et débats. [cf. : *Impact des réseaux sociaux sur notre société*].

Le documentaire *Social Dilemma* illustre bien ces mécanismes).

### *Les cybermenaces contre les infrastructures et les activités stratégiques*

Ces cybermenaces sont devenues des réalités dont voici quelques illustrations :

– le 16 novembre 2019 : le CHU de Rouen, paralysé par un rançongiciel, a été contraint de revenir à « la bonne vieille méthode du papier et du crayon » ;

– le 27 juillet 2020 : la société Carlson WagonLit victime d'un rançongiciel a été bloquée deux jours et a dû payer 4,5 M$ de rançon pour récupérer ses données ;

– le 20 octobre 2020, Sopra Steria, entreprise de 46 000 personnes et 4,4 Md€ de chiffre d'affaires a arrêté très rapidement une attaque par le rançongiciel Ryuk qui a affecté le système d'authentification et entraîné le chiffrement d'une partie de ses données ;

– le 12 avril 2012, l'Élysée a mis en évidence une opération d'espionnage attribuée de façon formelle à nos alliés états-uniens ;

– le 23 décembre 2015, un piratage des systèmes industriels SCADA[46], basé sur le programme « BlackEnergy » et le logiciel malveillant KillDisk, a provoqué une importante coupure d'électricité le 23 décembre dans la région d'Ivano-Frankivsk, dans l'ouest de l'Ukraine ;

Entre 2014 et 2016, Frédéric Pierucci[47], cadre supérieur d'Alstom, président monde de la division chaudière, sur

(44) *Big Data* ou mégadonnées ou données massives, ce terme désigne les ressources d'informations dont les caractéristiques en termes de volume, de vélocité et de variété imposent l'utilisation de technologies et de méthodes analytiques particulières pour générer de la valeur

(45) Le scandale de Cambridge Analytica en mai 2018 a ébranlé Facebook, comptant plus de 2 milliards d'utilisateurs, qui auraient fourni à cette société les données personnelles de 87 millions de personnes pour qu'elles soient utilisées à des fins de manipulations pour la campagne présidentielle américaine de 2016. Le titre boursier de Facebook a baissé considérablement depuis cette affaire, environ moins 20 % entre avril et fin juillet 2018. Sur le sujet : Cherif (A.), 2018, « Cambridge Analytica : comment savoir si vos données Facebook ont été captées », *La Tribune*, 11 avril. Lien : https://www.latribune.fr/technos-medias/cambridge-analytica-comment-savoir-si-vos-donnees-facebook-ont-ete-captees-774929.html

(46) SCADA ou système de contrôle et d'acquisition de données en temps réel (anglais : *Supervisory Control And Data Acquisition*) est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques. C'est une technologie industrielle dans le domaine de l'instrumentation, dont les implémentations peuvent être considérées comme des *frameworks* d'instrumentation incluant une couche de type *middleware*.

(47) Voir Thinkeview du 8 juillet 2019 : « La France vendue à la découpe ».

la base de plusieurs Go de données et courriels espionnés, a été accusé de corruption par le gouvernement américain en vertu de lois extraterritoriales (FCPA), arrêté puis détenu plusieurs années aux États-Unis dans le contexte de la prise de contrôle par General Electric des turbines équipant nos centrales nucléaires.

La menace est à la fois endogène et exogène au réseau périmétrique privé (Intranet) et son coût mondial est chiffré à 4 Md$ en 2020 avec une croissance annuelle de 50 %.

Les outils informatiques d'origine étrangère soit logiciels (OS, IaaS, PaaS, SaaS[48]) soit terminaux (smartphones, PC), sont très largement diffusés dans l'ensemble de l'Union européenne, notamment au sein des administrations, des agences gouvernementales et des infrastructures d'importance vitale.

Ils sont largement contrôlés par des empires numériques multinationaux ou étrangers, en général peu enclins à la transparence et dont quelques-uns font parfois preuve, de manière notoire, de nocivité en matière de déstabilisation ou d'espionnage : ce sont autant de menaces supplémentaires pour les données et les activités stratégiques des institutions et acteurs économiques européens. Ces derniers font l'objet de contrôles à l'exportation ou de lois d'extraterritorialité qui menacent la sécurité de nos systèmes vitaux, de nos données confidentielles, et la sérénité de nos concitoyens.

### *Cyberguerre et délits numériques*

Le cyberespace est le cinquième milieu après la terre, la mer, l'air et l'espace. Le numérique est une révolution stratégique dans l'histoire des moyens offensifs. Le « cyber » devient un deuxième moyen alternatif, après la guerre, de « continuer la politique par d'autres moyens », pour faire référence à Clausewitz.

Le directeur de l'ANSSI, auditionné par le Sénat le 4 novembre 2020[49], déclare que la « *meilleure des défenses, c'est la défense* ». De fait, il est difficile d'imputer de façon certaine l'origine d'une agression cyber. Cependant, on se réserve la possibilité de réagir par une attaque sans la revendiquer comme dans le cas du logiciel malveillant Babar[50], voire via des intervenants tiers, en mode « corsaire de la République ».

À l'autre bout du spectre, prenant acte de la confusion permanente entre états de paix et de guerre, la doctrine « Gerasimov », théorisée en 2013 par le général Valeri Gerasimov, chef d'état-major des armées russes, préconise l'utilisation de moyens non-militaires pour atteindre des objectifs stratégiques.

Le cyber est un nouveau théâtre de guerre. Il donne un avantage décisif à l'attaquant qui peut recourir à des moyens économiques, dissymétriques et furtifs (impossibilité de trouver la provenance d'une attaque, ce qui pose la question de la nature de la réponse militaire à une agression de ce type).

L'utilisation offensive du cyberespace peut avoir lieu au niveau :

– des couches « physiques et matérielles » ou encore « logiques et applicatives » : cyber-espionnage, cyber-sabotage (attaque par Stuxnet des centrifugeuses d'enrichissement de l'uranium de l'Iran), cyber-intimidation (intrusion sans sabotage dans les systèmes de contrôle de nombreuses installations américaines de production et distribution électrique) ;

– des couches « sémantiques et cognitives »: les attaques informationnelles diffusent ou manipulent numériquement l'information ; publication de courriels piratés concernant Hillary Clinton, espionnage par nos alliés de l'Union européenne, de la chancelière Angela Merkel ou de l'Élysée.

En novembre 2020, le président du CIGREF a alerté le premier ministre dans une lettre rendue publique[51] : « Le Cigref alerte sur la multiplication des cyberattaques et la menace que cette hausse représente pour l'économie française. Et ce, alors que de plus en plus d'entreprises en France sont touchées par des attaques ».

## Quelle politique pour préparer l'avenir ?

Face à ces constats à 360°, quelles actions nous faut-il entreprendre pour améliorer notre sécurité et notre souveraineté numérique ? Quelles doivent être les réponses de notre nation européenne ?

(48) OS : *operating system* (système d'exploitation) ; IaaS : Infrastructure as a Service ; PaaS : *Platform as a Service* ; SaaS : *Software as a Service*.
(49) Audition du 4 novembre 2020 par la Commission des affaires étrangères, de la défense et des forces armées.
(50) https://fr.wikipedia.org/wiki/Babar_(logiciel_malveillant)
(51) CIO le 18 novembre 2020, « Le Cigref alerte contre le risque économique lié à la cybercriminalité » : https://www.cio-online.com/actualites/lire-le-cigref-alerte-contre-le-risque-economique-lie-a-la-cybercriminalite-12707.html

## *Pour contribuer à notre sécurité environnementale, être numériquement sobre*

### *Limiter les impacts environnementaux directs*

La proposition de loi REEN, adoptée par le Sénat le 12 janvier 2021 puis avec modifications, par l'Assemblée nationale le vendredi 11 juin 2021, a pour finalité de « Réduire l'empreinte environnementale du numérique en France ».

#### *Limiter l'impact de la production des appareils numériques*

Il faut développer les principes d'éco-conception lors de la fabrication. Par exemple, la directive européenne « Eco-Design », peu suivie et qui se focalise trop sur la consommation énergétique pourrait être renforcée : batterie amovible et standardisée, ports standards, modularité des appareils, pièces détachées compatibles entre appareils.

Nous pourrions aussi imposer une durée de production ainsi qu'un prix abordable pour les pièces de rechange. La loi AGEC impose l'indice de réparabilité depuis le 1er janvier 2021 et en 2023, une évolution est prévue pour introduire l'indice de durabilité.

– la convention citoyenne proposait de rendre obligatoire par une réglementation l'écoconception des sites web et services en ligne publics et des grandes entreprises ;

– elle proposait aussi de concevoir des applications et des logiciels plus sobres qui fonctionnent sans perte de qualité, sans changer de matériel. Il s'agit de changer certaines versions des applications pour les rendre moins consommatrices de ressources (en lien avec la mesure sur l'écoconception).

Ces mesures d'écoconception doivent être rendues obligatoires.

Aujourd'hui, certains composants ne sont pas recyclables, car trop complexes, en raison des alliages complexes de matériaux rares par exemple. Nous devons accroître le recyclage et le reconditionnement : les principes d'éco-conception permettent un recyclage plus simple, donc moins onéreux et plus important. Les filières du recyclage et du réemploi fournissant des emplois locaux, peu délocalisables, dans lesquelles des entreprises françaises sont déjà bien positionnées, on développera ainsi les filières de formation correspondantes qui créeront aussi des emplois locaux.

Nous pouvons enfin augmenter la durée de vie des équipements en allongeant la durée de garantie légale des équipements numériques à 5 ans.

#### *Limiter l'impact de notre usage*

Nous devons réduire nos besoins des services numériques surtout en réduisant la croissance de nos besoins :

– réglementer la fréquence des mises à jour et distinguer ce qui relève des mises à jour correctives : sécurité, dysfonctionnements… ; des mises à jour d'amélioration du logiciel. Les mises à jour évolutives ne sont en général pas nécessaires, elles sont la plupart du temps à l'origine de « ralentissements » constatés. Les mises à jour correctives devront quant à elles rester des mises à jour légères. Le Parlement européen fait déjà cette distinction dans sa résolution du 25 novembre 2020 « Vers un marché unique plus durable pour les entreprises et les consommateurs » ;

– imposer la réversibilité des mises à jour non nécessaires, pendant deux ans après installation, afin de permettre à l'utilisateur de revenir à une version antérieure plus performante ;

– la loi de Moore sur la croissance exponentielle de la puissance de calcul des machines n'est plus valable depuis quelques années. Or, cette croissance était une des causes de l'obsolescence rapide des matériels, parce que les performances offertes devenaient rapidement insuffisantes par rapport à ce que des machines neuves pouvaient proposer ;

– former les développeurs au principe d'éco-conception.

Nous devons sensibiliser la population à l'impact environnemental de nos usages numériques et ralentir la croissance de nos besoins et de leurs renouvellements en adoptant par exemple un système de bonus-malus, comme pour les voitures (REEN).

Nous devons freiner le marketing qui pousse à « l'achat de la dernière innovation » par exemple les offres d'équipements à « 1 euro » contre un réengagement de 24 mois.

Il faudra aussi poser la question de la finalité de chaque innovation et éviter de mettre les contraintes de cette action sur les utilisateurs, car si la démarche est perçue comme coercitive, elle ne sera pas suivie d'effets.

### *Limiter les impacts environnementaux indirects*

Face à l'effet rebond, il faudra mettre en place une évaluation de la pertinence environnementale systématique lorsqu'une solution numérique est considérée.

### *Limiter notre dépendance énergétique et industrielle*

Dans ce domaine, la marge de manœuvre est faible ; faute de pouvoir ouvrir des mines de métaux rares en France pour assurer une exploitation respectueuse de l'environnement et des travailleurs et assurer un minimum d'indépendance, il faudra, *a minima*, relocaliser la fabrication des processeurs nanométriques, des terminaux numériques ou composants numériques.

## *Pour que le numérique soit au service de l'humain (et non l'inverse), en maîtriser les usages*

### *Télétravail en tant que nouvelle réalité sociale*

Le retour en arrière n'est socialement plus possible, il convient d'acter l'autonomie des salariés professionnels, de légaliser le télétravail et, par corollaire, de déléguer au professionnel salarié la gestion de son propre temps de travail.

Parallèlement, il faut acter le droit à la déconnexion en dehors des heures de travail.

### *Éducation au numérique*

Nous allons devoir abroger les contrats-cadres avec les GAFAM, et compte tenu de l'importance de l'enseignement dans la formation à la société numérique de demain, doter l'Éducation nationale d'une stratégie *open source*, coordonnée avec la stratégie générale de l'État, et d'une structure dédiée à son application. À ce titre, la création d'une mission indépendante, OSPO (*Open Source Programme Office*) chargée du suivi de la politique *open source* de l'État conformément à la proposition du CNLL (Union des entreprises du logiciel libre et du numérique ouvert) est reprise dans le rapport du député Bothorel [52] sur la politique publique de la donnée, des algorithmes et des codes sources.

### *Talents numériques*

En 2021 on estime qu'un CDI sur dix sera signé dans une *start-up*. Inversement, les créations d'emplois y sont à 90 % des CDI : aucun autre secteur n'en concrétise autant en raison de la pénurie durable de profils désirés. Les études montrent que les postes les plus difficiles à pourvoir se trouvent dans le secteur de la vente. Ce ne sont pas des profils surdiplômés : la pénurie pourrait assez facilement être résorbée et ainsi créer des emplois de qualité.

D'un côté, Paris-Saclay est la meilleure université de mathématiques au monde, on y forme les meilleurs spécialistes en intelligence artificielle. Dans n'importe quel laboratoire d'intelligence artificielle dans la Silicon Valley, il y a un Français formé en France.

De l'autre, on constate le succès d'écoles qui forment massivement au numérique comme Epitech, l'École 42, qui sont des initiatives privées. Mais l'offre de formation des « ouvriers du code » ou bien des « vendeurs de produits technologiques » reste trop parcellaire. Sans les milliers d'ouvriers qui l'ont construite, il n'y aurait pas de Tour Eiffel.

Si un jour on veut ériger un symbole mondial du numérique, il ne faudra pas juste avoir « Villani, médaille Field ». Il faudra avoir « Villani, médaille Field » et des milliers d'ouvriers du code pour construire effectivement le monument.

Il est grand temps pour l'État de réhabiliter le « T » d'IUT [institut universitaire technologique].

### *Liberté d'expression et transparence des algorithmes*

Il faut renforcer la protection et l'anonymat des lanceurs d'alerte et des détecteurs de failles numériques « zero day » en créant par exemple un guichet national dédié.

Il faut également rendre obligatoire la publication de tous les algorithmes de tri sur tous les réseaux sociaux, ou de tous les outils de traitement des données personnelles.

### *Inclusion numérique*

Nous devons aborder la question de la sobriété numérique sous l'angle social pour ne pas, sous couvert de sobriété

(52) Rapport Bothorel sur la politique publique de la donnée, des algorithmes et des codes sources remis le 23 décembre 2020 : https://www.gouvernement.fr/remise-du-rapport-sur-la-politique-publique-de-la-donnee-des-algorithmes-et-des-codes-sources

numérique, faire reculer les droits humains notamment dans les pays les plus pauvres.

## *Numérique, énergie et gaz à effet de serre*

Il est peut-être possible de contraindre la consommation énergétique par un mécanisme de type « Compte Carbone [53]», d'appliquer une démarche d'écoconception pour la fabrication des appareils numériques qui facilitera, dans un premier temps, la réparation et la maintenance et, dans un second temps, maximisera le recyclage ; de découpler mise à jour de sécurité et mise à jour logiciel qui contribue à l'obsolescence programmée ou de décarboner les villes [54] et d'y construire une économie circulaire [55].

Nous devons réinventer les circuits courts du numérique, avec un circuit de réparation ou un circuit de reconditionnement localisé en France. Au lieu de changer son smartphone tous les 3 ans, on doit être en mesure de le faire réparer. Pour cela, il faut à côté de chez soi quelqu'un qui puisse fournir ce service. Au niveau national, cela permettra :

– de développer une industrie verte ;

– de réduire les émissions dues aux transports ;

– d'éviter l'extraction de minerais supplémentaires.

L'État doit donner l'exemple en utilisant des smartphones reconditionnés plutôt que de faire des méga-contrats avec Hewlett Packard ou Microsoft. En mettant en place une filière nationale du reconditionnement, on traiterait une grosse partie du problème. Il ne s'agit pas de recyclage : le reconditionnement est beaucoup plus efficace.

Il se trouve que les *leaders* mondiaux du reconditionnement sont français : Back Market, Recommerce. C'est une chance, car il sera plus facile d'agir que s'ils étaient chinois ou coréens.

## *Santé*

L'analyse des données de santé par les technologies dites « d'intelligence artificielle » et la protection des données personnelles de santé sont incompatibles tant que le chiffrement homomorphe ne sera pas opérationnel à grande échelle. Il convient donc de faire un choix :

– privilégier la protection des données personnelles de santé par chiffrement de confiance nulle et mettre un terme aux projets centraux d'analyse massive des données de santé sur systèmes centraux qui sont incompatibles avec la sécurité de ces données ;

– interdire que les données de santé soient manipulées ou hébergées par des entités non souveraines ou soumises aux lois extraterritoriales étrangères ;

– inciter les entreprises françaises à créer des produits et services complètement autonomes des GAFAM, à l'exemple de la Chine qui a pu rattraper son retard en agissant de cette manière, ceci suppose de passer par des systèmes autres développés par le biais de la recherche et de l'innovation ;

– inciter les *start-up* françaises à déployer leurs produits sur les territoires français et européens par le biais de marchés publics préférentiels ;

– inciter les professionnels de santé à acheter des produits numériques aux entreprises françaises par le biais de primes ou d'exonérations fiscales ;

– inciter au rapatriement de sociétés françaises en santé localisées à l'étranger ;

– inciter à la création d'entreprises françaises pour les produits de santé de première nécessité (médicament, matériaux de prise en charge des patients) ;

– taxer plus fortement les produits et services provenant des GAFAM et autres entreprises étrangères, y compris ceux des entreprises françaises et européennes recourant à leurs services pour créer leurs systèmes en raison de la dépendance générée lorsqu'ils n'ont pas les codes d'accès.

(53) https://fr.wikipedia.org/wiki/Compte_carbone
(54) Net Zero Carbon Cities: An Integrated Approach
(55) Circular Trailblazers: Scale-Ups Leading the Way Towards a More Circular Economy

## *Protéger nos valeurs démocratiques et se prémunir contre les opérations d'influence et de manipulation*

Nous devons réguler l'anonymat sur les réseaux sociaux et notamment rendre obligatoire la vérification d'identité lors de l'inscription.

Nous devons également obliger la tenue de registres de diffusion pour les publicités personnalisées afin de tracer la promotion de tout contenu et éviter que les publicités ou contenus mensongers disparaissent après avoir produit leur effet sur l'opinion.

L'Europe s'apprête à dépenser 750 milliards d'euros, dont 20 % doivent aller à la transformation numérique de nos entreprises et de nos administrations. À l'image de ce qui a été fait aux États-unis, la mise en place d'un BETA (*Buy European Technology Act*) aidera nos champions à acquérir leur autonomie financière sur le marché européen, faute de quoi ces milliards risquent de profiter en premier lieu aux GAFAM.

Même si beaucoup a déjà été fait dans ce domaine, il faut établir un lien plus fort entre la commande publique, entre l'État et les écosystèmes d'innovation de type « start-up ». La commande publique et l'accompagnement de l'État sont indispensables pour transformer progressivement des *start-up* prometteuses en géants mondiaux du numérique.

Construire une alternative aux GAFAM nécessite de faire des choix politiques assez puissants. Une stratégie intéressante serait aussi de capitaliser sur notre « Mittelstand numérique européen » composé de sociétés, petites certes, mais très spécialisées, très expertes, de vrais *leaders* dans leur segment de marché. On parle sans arrêt d'écosystème « technologique », d'écosystème « d'innovation », d'écosystème « de *start-up* ». Or, on oublie que fondamentalement il n'y a pas d'écosystème durable sans biodiversité. Et il est important d'avoir des champions technologiques qui incarnent un système de valeurs parce que cela facilite la constitution d'un tel écosystème.

Si l'on veut construire des géants du numérique européens, il faudra enlever les obstacles qui empêchent les effets d'agrégation et les effets de réseaux.

Positionnons-nous sur les prochaines révolutions technologiques et voyons comment certains de nos géants économiques, qui ont la force de frappe financière, peuvent s'en emparer.

Enfin, nous devons interdire sans ambiguïté toute forme de vote électronique pour les consultations, référendums, scrutins organisés par la puissance publique, car cette technologie ne sera jamais en mesure de garantir, vis-à-vis du citoyen, la fonction de transparence des urnes physiques dépouillées manuellement sous la surveillance visuelle d'assesseurs.

## *Défendre nos infrastructures vitales et nos entreprises stratégiques contre les attaques cyber*

L'Europe doit contribuer à créer une agence internationale de la cybersécurité.

Il faut également promouvoir le chiffrement de bout en bout ou *end-to-end*[56] avec détention souveraine des clés[57], et, pour certains services (correspondance, santé par exemple), le chiffrement des données avec auto-détention des clés (les données mêmes stockées dans le *cloud* ne sont déchiffrées que dans le terminal de l'utilisateur et demeurent ainsi inexploitables par des tiers).

Dans le contexte de la politique « Cloud au Centre » de l'État, il convient de favoriser l'émergence de véritables infrastructures numériques souveraines (composants matériels et services de base) et non des chevaux de Troie basés sur des composants technologiques sous licence étrangère.

Il convient d'encourager le développement de services numériques de base tels que messagerie, agenda,

(56) Le concept de chiffrement de bout en bout ne veut rien dire. Tous les services proposés sur Internet supposent de confier ses données à un tiers de confiance. C'est cette situation qu'il faut faire évoluer pour davantage de souveraineté. La question centrale est : « qui détient les clés ? ». Si le partenaire fournisseur de service (infogéreur ou administrateur ou opérateur réseau) détient les clés des données (en confidentialité/chiffrement ou en intégrité/signature) alors c'est lui le point faible de la sécurité. La sécurité idéale, c'est quand l'utilisateur final est le seul à détenir et à gérer les clés de ses données.

(57) La marge de manœuvre de nos services de renseignement repose sur le générateur d'aléa de la clé. Tout dépend de la finalité du service : soit gouvernemental, soit ouvert (ex : libsodium et pyNaCl). Le but de ce système est d'éviter la pêche au chalut sur toute la population (métadonnées) et de limiter l'action aux cibles spécifiquement visées par les services de renseignement.

carnets d'adresses, sauvegarde de fichiers et de services de connexion intermédiés (similaire à connexion via facebook/apple) au travers d'avantages fiscaux significatifs pour les opérateurs fournissant chacun de ces services indépendamment de tout autre, s'engageant à ne collecter aucune donnée sur les utilisateurs, publiant leurs codes sources et domiciliant l'ensemble de leurs activités dans le territoire de l'Union/France (territoire de l'avantage fiscal).

Notre politique industrielle doit encourager le développement de composants cœur de réseau, terminaux, logiciels pilotes et systèmes d'exploitation « libres, transparents et souverains » au travers d'avantages fiscaux et de taxes perçues sur la mise en service de matériels dotés de capacités de télécommunication.

Nous devons aussi créer un référentiel de certification européen pour les terminaux numériques et des systèmes d'exploitation auquel serait soumis tout produit ou service selon sa classe de sensibilité stratégique.

Il faut également étendre les pouvoirs d'enquête et de signalement des agences comme l'ANSSI ou des organes de contrôle comme la CNIL en les dotant de moyens renforcés pour pouvoir mener leurs enquêtes. Dans ce contexte, les lanceurs d'alerte et leur anonymat doivent être mieux protégés.

## *Protéger les citoyens européens contre la collecte de données personnelles et sensibles par des puissances étrangères et protéger les sociétés européennes contre le cyberespionnage*

De même que la contrefaçon de monnaie est une atteinte à leur souveraineté monétaire, nos États doivent sans ambiguïté criminaliser l'évasion de données sensibles et personnelles vers des *clouds* non européens et rendre obligatoire la publication des algorithmes de sélection des informations et des personnes.

Ils doivent investir dans les technologies souveraines européennes plutôt que dans les technologies contrôlées par des puissances étrangères où assujetties à des lois extra-territoriales non européennes.

## *Organiser notre réponse militaire face aux stratégies d'usages des outils non-militaires pour atteindre des objectifs stratégiques*

Bernard Barbier, expert en cybersécurité et ancien directeur technique de la DGSE, propose de créer[58], sur le modèle israélien ou britannique[59-60], une Cyberforce européenne en s'appuyant sur le pivot France-Allemagne ou encore de construire des cyber campus rassemblant les forces armées, les universités et les entreprises (écoles d'ingénieurs et universités, grands groupes, PME et *start-up*) pas seulement dans le domaine du cyber mais pour l'ensemble des activités en France[61] ■

(58) *Le Monde* du 28 janvier 2020 « Cybercoercition : un nouveau défi stratégique » : https://www.lemonde.fr/idees/article/2020/01/28/cybercoercition-un-nouveau-defi-strategique_6027444_3232.html

(59) La création de la National Cyber Force est une évolution majeure dans la capacité de cyberdéfense britannique. L'objectif est de perturber et casser les moyens des cyber attaquants, qu'ils soient des mafias, des criminels ou des États. Alors que la vision française est « La meilleure défense c'est la défense » risque de nous amener vers une ligne « Maginot numérique » facile à contourner, sommes-nous capables de mener une telle (r)évolution stratégique ?

(60) LinkedIn le 9 mai 2021 « Face à la cyber coercition , la réponse britannique: la National Cyber Force » : https://www.linkedin.com/pulse/face-%C3%A0-la-cyber-coercition-r%C3%A9ponse-britannique-national-barbier/

(61) Si des grandes écoles telles que par exemple l'X vont dans ce sens, les universités françaises sont à la traîne, ce qui est grave et dangereux. Grave pour la formation des jeunes, dangereux car les entreprises se privent d'une grande part de la recherche et de l'innovation.