N° 7

SÉNAT

SESSION ORDINAIRE DE 2019-2020

Rapport remis à M. le Président du Sénat le 1er octobre 2019

Enregistré à la Présidence du Sénat le 1er octobre 2019

RAPPORT

FAIT

au nom de la commission d'enquête (1) sur la **souveraineté numérique**,

Président
M. Franck MONTAUGÉ,

Rapporteur
M. Gérard LONGUET,

Sénateurs

Tome I : Rapport

(1) Cette commission est composée de : M. Franck Montaugé, *président* ; M. Gérard Longuet, *rapporteur* ; M. Patrick Chaize, Mmes Sylvie Robert, Catherine Morin-Desailly, MM. Yvon Collin, M. André Gattolin, MM. Pierre Ouzoulias et Jérôme Bignon, *vice-présidents* ; Mme Viviane Artigalas, MM. Jérôme Bascher, Bernard Bonne, Mme Martine Filleul, MM. Christophe-André Frassa, Loïc Hervé, Laurent Lafon, Rachel Mazuir, Stéphane Piednoir, Mmes Sophie Primas, Frédérique Puissat et M. Hugues Saury.

SOMMAIRE

Pages

PRINCIPALES RECOMMANDATIONS

La souveraineté nationale fonde le pacte républicain, pacte par lequel le citoyen accepte une discipline collective fondée sur la loi, en contrepartie d'une protection.

La souveraineté nationale, pour ne remonter qu'à la fondation de la République en septembre 1792, n'a jamais été certaine, quelle que soit la nature des défis qu'elle devait affronter.

Aujourd'hui, la question de la souveraineté numérique est totalement actuelle, car si l'ère numérique est à la fois une chance et une certitude partagée dans le monde entier, elle constitue pour la France, comme pour les pays de l'Europe, un triple défi éthique, de sécurité et de liberté économique.

D'abord, en effet nos sociétés sont confrontées à une mise en cause sourde de leurs valeurs : l'homme est moins un citoyen et un sujet de droit, mais de plus en plus une somme de données à exploiter. Ce n'est pas notre conception de la personne humaine, ce n'est pas non plus le modèle de société que nous portons et dans lequel s'incarnent nos valeurs de respect de tous et de chacun. La souveraineté numérique est donc la condition nécessaire et indispensable à la préservation de ces valeurs.

Des actions ont été entreprises depuis plus de 15 ans pour la restaurer ou la préserver. Point cependant de stratégie globale lisible qui fédèrerait les énergies et les efforts. Votre commission d'enquête souhaite y remédier en proposant :

- un principe et une méthode :
    - le principe est que la souveraineté numérique est un devoir national et, à ce titre, engage nos compatriotes, toutes responsabilités confondues ; aussi serait mis en place un « Forum national du numérique », structure temporaire qui permettrait de donner le coup de collier nécessaire pour sortir de la situation peu satisfaisante dans laquelle les attributs traditionnels de la souveraineté nationale et nos valeurs démocratiques sont malmenés ;
    - la méthode serait la présentation par le Gouvernement et l'adoption par le Parlement d'une loi d'orientation et de suivi de la souveraineté numérique (LOSSN). La discussion parlementaire et le vote d'une loi d'orientation triennale permettront au Parlement d'exercer pleinement son rôle de gardien de la souveraineté numérique nationale.

Cependant, dès maintenant, des mesures précises et urgentes dans le domaine de la protection des données, une réforme de la réglementation visant le renforcement de notre souveraineté numérique et une action sur les leviers de l'innovation et du multilatéralisme doivent être menées.

1. Définir une stratégie nationale numérique au sein d'un Forum institutionnel temporaire du numérique

La stratégie gouvernementale pour la défense de la souveraineté numérique est dispersée entre souveraineté et libertés publiques, sécurité et défense, et présence économique effective sur un marché nécessairement mondial, ce qui la rend peu lisible. Les ministères et grands opérateurs publics doivent impérativement mieux articuler leurs efforts et leurs actions en faveur de la souveraineté numérique, posée comme un enjeu fédérateur. Il convient d'associer à cette réflexion les collectivités territoriales, responsables de l'aménagement numérique du territoire, la recherche et l'industrie, le public et le privé.

Nous avons, au cours de nos travaux, constaté qu'il manquait, au-delà des actions menées, engagées ou projetées, une impulsion fédératrice. Ce n'est ni un secrétaire d'État au numérique, ni le Gouvernement, ni l'industrie, ni les prestataires de service qui peuvent seuls définir la stratégie nationale numérique dont notre pays a besoin. C'est grâce à un travail collectif, alliant les forces et expériences de chacun, et s'appuyant sur l'excellence de la recherche française, sur l'inventivité de nos territoires, sur l'exigence des associations de défense des citoyens, sur le dynamisme des fleurons économiques français, qu'il sera possible de mobiliser nos forces, et elles sont réelles, au service de notre souveraineté numérique.

Nous proposons la transformation du Conseil national du numérique en un Forum de concertation temporaire, force de propositions et d'impulsions fédératrices, pour renforcer l'approche transversale et interministérielle du numérique. D'une durée de vie limitée à deux ans, il permettrait au Gouvernement et au Parlement de réaliser les arbitrages nécessaires à la défense de notre souveraineté numérique.

2. Inscrire l'effort pour la souveraineté numérique dans le temps en votant une loi d'orientation et de suivi de la souveraineté numérique (LOSSN)

Une loi d'orientation et de suivi de la souveraineté numérique devrait découler des travaux du Forum : à l'image de la loi de programmation militaire, elle garantirait davantage de lisibilité et de stabilité aux entreprises, et mettrait en œuvre un pilotage public plus rigoureux des innovations dans les secteurs et technologies essentiels à la défense de la souveraineté numérique française. Le suivi de l'exécution de la LOSSN par le Parlement garantirait la gestion politique de ces choix stratégiques. Le Parlement s'exprimerait à cet effet de manière régulière.

Cette loi, triennale, définirait une stratégie claire sur les infrastructures du numérique avec deux piliers urgents : l'attractivité de notre territoire pour les câbles sous-marins, les centres de données et la fibre optique, et l'accélération de la couverture numérique du territoire. Elle favoriserait également les technologies numériques d'avenir et les domaines dans lesquels la France a une carte à jouer pour devenir un leader européen et mondial. Ces domaines, définis dans le cadre du Forum, ne se résumeraient pas aux seules technologies de rupture, mais viseraient également le développement des hautes technologies dans lesquels le savoir-faire français est déjà reconnu et incarné par de grandes entreprises françaises dont le rachat, qui plus est, est peu envisageable contrairement à celui de start-up innovantes.
Cette loi inclurait le financement de solutions répondant aux attaques qui visent notre modèle de société et qui fragilisent notre souveraineté : fournir une carte d'identité électronique ; *élaborer une cryptomonnaie publique sous l'égide de la Banque centrale européenne et à laquelle pourraient collaborer les banques centrales des pays non membres de la zone euro (ex. Suisse, Royaume-Uni, Suède, Danemark)* ; obtenir au sein de l'OCDE une taxation commune des multinationales du numérique, avec un principe d'imposition fondé sur le lieu de consommation ; généraliser la solution de la banque centrale européenne pour les paiements transfrontières.

3. Protéger les données personnelles et les données économiques stratégiques

Cet objectif se déclinerait en deux grands axes :

Restituer à chacun la maîtrise de ses données
Sur la base d'un premier bilan du droit à la portabilité des données personnelles (existant depuis la loi « République numérique » et consacré par le RGPD), il conviendrait de soutenir et d'étudier la faisabilité technique et opérationnelle d'une obligation d'interopérabilité (bénéfices, coûts, impact sur le consommateur et l'innovation), y compris comme mesure de régulation asymétrique imposée aux grandes plateformes systémiques, le Gouvernement associant les régulateurs nationaux (ADLC, CNIL) et présentant au Parlement la position qu'il compte défendre au niveau européen sur ce sujet central pour nos concitoyens.

Défendre les données stratégiques de nos entreprises contre l'application de lois à portée extraterritoriales
Une obligation de localisation des données sur le territoire national peut être justifiée par des motifs de sécurité publique, mais ce n'est qu'une solution imparfaite ; il convient de cartographier et de faire émerger des solutions pour l'hébergement et le stockage des données sensibles autour de prestataires français et européens non soumis aux législations étrangères à portée extraterritoriale.

Parallèlement, il est essentiel d'opposer fermement notre législation nationale et européenne au *Cloud Act* ou à toutes autres normes se voulant porteuse d'un ordre juridique extraterritorial. La loi dite de « blocage» doit être renforcée, sur la base de rapport du notre collègue député Raphaël Gauvain afin que les entreprises françaises ne soient plus démunies face aux procédures américaines, notamment (mise en place d'une déclaration aux autorités françaises, accompagnement par une administration dédiée et durcissement des sanctions encourues).
S'il convient d'encourager la conclusion rapide d'accords de coopération entre l'Union européenne, ses États membres et les États-Unis dans le cadre du *Cloud Act*, il faut aussi réfléchir à l'opportunité d'étendre les sanctions prévues par le RGPD aux données non personnelles stratégiques des personnes morales, pour sanctionner les intermédiaires qui transmettraient aux autorités étrangères des données en dehors de ce mécanisme d'entraide administrative ou judiciaire.

4. Adapter la réglementation aux défis numériques

Cet objectif se déclinerait en quatre grands axes :

Muscler le droit de la concurrence aux niveaux national et européen
Le droit de la concurrence n'est plus adapté aux spécificités de l'économie numérique et devrait, par conséquent, être amendé. Il faut faciliter le recours à des mesures conservatoires, lorsque l'urgence le justifie, et réviser le champ de contrôle des concentrations, par exemple en introduisant un nouveau seuil basé sur la valeur de rachat. Enfin, la France doit transposer au plus vite la directive ECN +, qui permet aux autorités de prononcer des injonctions structurelles (ex. cession d'une branche) dans le cadre des sanctions en cas de pratiques anticoncurrentielles.

Utiliser l'information : la « régulation par la donnée »
Les autorités de régulation souhaitent réguler par la donnée, c'est-à-dire s'appuyer sur la puissance de l'information pour réguler le marché. Il s'agit de collecter les informations de toute origine, y compris citoyenne, pour détecter les signaux faibles et les risques systémiques. L'analyse de ces données permet ensuite de mieux éclairer les choix des acteurs publics et des utilisateurs, et d'anticiper les réactions négatives de ces derniers. Le but de cette approche est moins de sanctionner les entreprises concernées que d'orienter le marché. Pour ce faire, les autorités de régulation doivent se doter des compétences, humaines et technologiques, nécessaires. La démarche concertée présentée le 8 juillet 2019, de plusieurs régulateurs (l'Autorité de la concurrence, l'AMF, l'Arafer, l'Arcep, la CNIL, la CRE et le CSA) en ce sens est un premier pas décisif qui doit être soutenu.

Étudier la faisabilité de nouvelles régulations sectorielles…
Ces nouvelles régulations sectorielles incluraient, après étude d'impact et de faisabilité, la neutralité des terminaux, l'accès sous le contrôle du régulateur aux données essentielles à l'exercice d'une activité, la transmission des informations pertinentes des plateformes aux autorités publiques ou encore l'accès aux méthodes et données sous-jacentes des algorithmes.
Donner accès à certaines données permet en effet de favoriser la concurrence et l'innovation. Dans ce cadre, les entreprises devraient être incitées à partager et à mutualiser leurs données privées, avec l'État comme tiers de confiance. Sur l'ouverture des données, l'approche ne peut être globale et la décision doit être prise au cas par cas.

…voire d'obligations proactives, spécifiques et multisectorielles pour les acteurs systémiques du numérique : la régulation « ex-ante ».
Identifier les acteurs essentiels du numérique pourrait se faire grâce à un faisceau d'indices permettant de définir leur caractère « systémique »[1]. De nouvelles obligations applicables à ces acteurs numériques systémiques pourraient être définies de façon proactive. Les pistes retenues par votre commission d'enquête portent sur la mise en œuvre d'une obligation de transparence de l'activité et d'une obligation de ménager dans des conditions équitables l'accès d'autres acteurs pour certains types de données. De même, le renforcement de la portabilité des données et de l'interopérabilité des plateformes doit être recherché. L'auditabilité et la redevabilité[2] des algorithmes utilisés doivent être des objectifs du législateur. Cela suppose de permettre l'accès des chercheurs ou d'organismes publics à ces algorithmes pour évaluer et garantir leur transparence, leur intelligibilité, leur conformité à la loi, la non-discrimination, et leur loyauté.

5. Utiliser les leviers de l'innovation et du multilatéralisme

Cet objectif se déclinerait en deux grands axes :

Encourager les innovations aux niveaux national et européen
Sans innovation, pas de souveraineté numérique. Des pistes existent pourtant pour améliorer notre pilotage des innovations, pour attirer le capital financier nécessaire et pour favoriser les liens entre entreprises et

[1] *Existence d'effets de réseaux massifs ; maîtrise d'un volume considérable de données non réplicables ; situation incontournable sur un marché multi-faces ou capacité de l'acteur à définir lui-même les règles de marché ; aptitude de l'acteur à placer le régulateur en forte position d'asymétrie d'information ; effets globaux sur la collectivité hors champ économique et pouvoir d'influence sur des pans sensibles du lien social - discours haineux,* fake news*, protection des données personnelles, cybersécurité, etc.*
[2] *La redevabilité des algorithmes est entendue comme un « devoir de rendre compte », qui inclut deux composantes : le respect de règles, notamment juridiques ou éthiques, d'une part ; la nécessité de rendre intelligible la logique sous-jacente au traitement des données, d'autre part.*

recherche privée : revoir, au niveau européen, le régime des aides d'État ; utiliser le levier de l'achat public; élargir la dépense fiscale IR-PME pour soutenir le capital-risque ; clarifier les conditions du crédit d'impôt recherche pour les entreprises du secteur numérique ; créer un portail unique permettant aux entreprises de visualiser l'ensemble des dispositifs existants ; renforcer la place des entreprises au sein des centres de recherche publics.

Porter la vision française de la souveraineté numérique dans les enceintes multilatérales

Alors que sa souveraineté est concurrencée, la France doit défendre sa présence au sein des organismes internationaux. À ce titre, renforcer la mobilisation des acteurs français et européens du numérique dans les organismes de normalisation multilatéraux est une action prioritaire. Les désengagements récents, qui semblent presque fortuits, sont signes de l'absence de pilotage d'une stratégie nationale de préservation de la souveraineté numérique nationale. Le réinvestissement des agoras de normalisation est indispensable.

De même, la promotion à l'international de la vision française de cybersécurité se décompose en deux items : le droit international est applicable au cyberespace, et l'attribution d'une cyberattaque est une décision politique souveraine et ne peut être faite par une structure multinationale, qu'elle soit interalliée comme l'OTAN ou autre. La défense de ce principe est essentielle à la pleine restauration de notre souveraineté numérique.

AVANT-PROPOS

> « *Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Au nom du futur, je vous demande à vous du passé de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté où nous nous rassemblons.* » (John P. Barlow, 1996)[1]
>
> « *Je trouve enthousiasmant le potentiel du Libra, et je suis fier que ce soit Facebook qui en ait pris l'initiative ici, aux États-Unis. Je crois que si l'Amérique ne mène pas l'innovation dans le secteur de la monnaie numérique et des paiements, d'autres le feront. Si nous n'agissons pas, nous pourrions bientôt voir une monnaie numérique contrôlée par d'autres acteurs dont les valeurs sont radicalement différentes des nôtres.* » (David Marcus, Facebook, chef du projet de monnaie virtuelle *Libra*, 2019)[2]

Mesdames, Messieurs,

Développé initialement sur des bases théoriques libertaires et libertariennes, dont la célèbre déclaration d'indépendance du Cyberespace de John P. Barlow en 1996 résonne comme le manifeste le plus enthousiaste, bâti sur une architecture technique décentralisée permise par les progrès de la technologie, Internet a connu depuis le milieu des années 2000 des évolutions notables : recentralisation du web, autour de systèmes fermés et de technologies propriétaires, développement des applications, « plateformisation », et surtout émergence de grands acteurs privés bénéficiant de puissants effets de réseaux au soutien de leurs offres de nouveaux services et outils numériques.

Ces entreprises géantes du numérique, les « Gafam »[3] américains, les « BATX »[4] chinois, dépassent désormais celles des secteurs traditionnels en

---

[1] *Déclaration d'indépendance du Cyberespace, John P. Barlow, février 1996 (traduction Hache).*
[2] *Hearing before the United States Senate committee on banking, housing, and urban affairs, July 16, 2019, Testimony of David Marcus, Head of Calibra, Facebook.*
[3] *Google, Apple, Facebook, Amazon et Microsoft.*
[4] *Baidu, Alibaba, Tencent et Xiaomi.*

termes de valorisation financière et atteignent un nombre d'utilisateurs inédit dans l'histoire (Facebook revendique ainsi 2,4 milliards d'utilisateurs actifs chaque mois).

Loin de l'utopie égalitaire et individualiste des débuts, le cyberespace est bien aujourd'hui le lieu où s'exercent les conflits d'intérêts, les luttes d'influences et de logiques économiques et sociales antagonistes, bref le retour sous des formes nouvelles de la très classique compétition pour la prise de pouvoir. Les États, avec l'appui plus ou moins ambigu de ces géants numériques, développent ainsi des stratégies de domination, d'indépendance ou d'autonomie dans le cyberespace.

À l'échelle de nos concitoyens, le déploiement désormais généralisé des outils numériques pose aussi un véritable défi démocratique pour l'expression de la volonté générale. Ces outils peuvent troubler le jeu politique en facilitant de nouveaux modes d'actions pour des tentatives d'ingérence ou de manipulation spécifiques et ciblées : le vol de données d'un QG de campagne et leur dissémination publique lors de l'élection présidentielle de 2017 en témoigne chez nous, et, à l'échelle mondiale, l'affaire dite « Cambridge Analytica » montre le danger de méthodes peu scrupuleuses de recueil massif, d'analyse et de recoupement des données aux fins d'influence sur les choix politiques.

Plus généralement, l'absorption de l'attention par des techniques ciblant avec une redoutable précision chaque seconde de « temps de cerveau disponible » peut laisser craindre, à terme, une réduction du temps d'exercice des fonctions mêmes de citoyen – en 2018, en moyenne, un Français consacrait ainsi 18 heures par semaine à internet… Force est de reconnaître souvent le désarroi du pouvoir politique face à une société dont le numérique change profondément le comportement et les modes de participation démocratique, en particulier chez les jeunes générations.

Comment, dans ce contexte, et face à de redoutables concurrents, conserver une capacité autonome d'appréciation, de décision et d'action pour l'État dans le cyberespace ? Comment garantir une « autonomie informationnelle » suffisante à nos concitoyens de plus en plus dépendants d'intermédiaires techniques au fonctionnement souvent opaque ?

Créée par le Sénat le 9 avril 2019, à l'initiative du groupe Les Républicains, notre commission d'enquête a bénéficié dans ses réflexions de l'audition de 63 [1]personnes entendues sous serment au cours de plus de 70 heures d'échanges. Elle s'inscrit dans la lignée des travaux engagés sur

[1] *Devant votre commission d'enquête, 39 personnes ont prêté serment. Les Président et Rapporteur ont procédé à l'audition de 24 personnes supplémentaires, dont 8 d'entre elles ont été entendues lors du déplacement à Bruxelles de votre commission d'enquête.*

ces sujets depuis quelques années[1] par plusieurs collègues appartenant à toutes les sensibilités politiques de notre assemblée.

Elle s'est attachée à identifier, d'une part, les champs fondamentaux de notre souveraineté numérique, qu'elle soit individuelle ou collective, pour esquisser, d'autre part, les moyens de la reconquérir, qu'ils relèvent de la règlementation ou de la mise en œuvre de politiques publiques. Pour ce faire, votre rapporteur a procédé sans naïveté ni résignation.

Pas de résignation, d'abord. Car malgré le caractère immatériel du web et du « cyberespace », le réseau internet qui en permet le déploiement garde cependant toujours un ancrage territorial donnant prise à la puissance publique : le réseau dépend en effet d'actifs physiques stratégiques indispensables (centres de données, câbles,…) qui nécessitent des investissements considérables et relèvent, au moins pour partie, d'ordres juridiques nationaux ; les équipements actifs et les protocoles utilisés (pour la communication des données ou leur chiffrement) répondent à des normes techniques négociées au sein d'instances internationales ; les entreprises dominantes du numérique ont elles-mêmes des nationalités (Gafam aux États-Unis et BATX en Chine) et sont également soumises aux contraintes de législations locales, à portée souvent extraterritoriale, voire concurrentes (*Cloud Act* vs. RGPD) ; les technologies (intelligence artificielle) et les ressources humaines (ingénieurs, programmeurs…) se développent grâce à un écosystème de recherche et d'innovation dans lequel la puissance publique nationale a toute sa part (financements publics, lien avec les industries de défense ou les agences d'innovation, programmes de formations et universités).

Aucune porte n'est dès lors fermée pour la préservation de la souveraineté numérique française : la technologie et les logiciels, algorithmes compris, ne nous marginalisent pas, même si nous sommes – comme souvent en haute-technologie et en sciences – sur le fil du rasoir. Les infrastructures nous sont accessibles – c'est même un paradoxe : l'argent public français, national et local, public et privé, finance des réseaux universels et accessibles à tous, assurant ainsi le développement des Gafam, premiers utilisateurs des autoroutes de l'information ! Enfin, si le marché des services numériques est dominé par les grands acteurs Nord-Américains, ils ne sont pas tous, loin s'en faut, en position durablement dominante, en théorie du moins.

Pas de naïveté non plus, cependant : les équilibres entre puissances placent aujourd'hui l'Europe, et la France, dans une position bien

[1] *Outre les rapports de la mission d'information* « L'Union européenne, colonie du monde numérique ? » *(en 2013) et de la mission commune d'information* « L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne » *(en 2014), dont notre collègue Catherine Morin-Desailly* était rapporteure*, près d'une dizaine de rapports de l'Office parlementaire d'évaluation des choix scientifiques et technologiques s'inscrivent dans ces thématiques (un résumé synthétique de ces rapports figure en annexe).*

particulière. Pour les Etats-Unis, il s'agit d'affirmer une souveraineté mondiale, forts de la création du net à l'origine libertarien – mais financé par la Défense, au prix de l'acceptation des monopoles – pourtant si contraires à la pratique historique des Etats-Unis –, et d'une chasse permanente et mondiale aux talents et aux pépites – puisque « le gagnant prend tout ». Pour la Chine et la Russie, l'affirmation de souveraineté se décline de façon différente, plus défensive et parfois plus subtile.

Cette situation géopolitique laisse peu de place pour une stratégie européenne encore mal définie : entre le duopole Chine-USA des géants numériques, nos capacités d'investissements restent marginales, l'accent est donc mis sur la défense de valeurs (une conception exigeante de la vie privée), et le principal levier reste, par défaut, de négocier l'accès des entreprises à un marché intérieur convoité de près de 500 millions de consommateurs. De même, la défense que promeut la France face aux menaces cyber et à la cybercriminalité est la reconnaissance de l'application des principes du droit international dans le domaine cyber et du multilatéralisme – dont l'Appel de Paris résume l'ambition. Elle tente de gagner ses partenaires européens à ces lignes d'action et promeut, sans angélisme, la coopération entre pays amis, avec la réserve adaptée aux secteurs vitaux et stratégiques.

Dans ce contexte de compétition intense entre États dans le cyberespace, votre commission a abordé les scénarii permettant de répondre aux menaces pesant sur notre souveraineté et se traduisant par la remise en cause de l'ordre économique, de l'ordre juridique, et du système fiscal et monétaire.

Elle envisage enfin la façon dont peut s'exercer la souveraineté numérique - capacité de l'État à agir dans le cyberespace – dans ses deux dimensions :

- la faculté d'exercer une souveraineté dans l'espace numérique, qui repose sur une capacité autonome d'appréciation, de décision et d'action dans le cyberespace – et qui correspond de fait à la cyberdéfense ;

- et la capacité de garder ou restaurer la souveraineté de la France sur les outils numériques afin de pouvoir maîtriser nos données, nos réseaux et nos communications électroniques.

Enfin, votre commission d'enquête propose un principe et une méthode d'action : un rendez-vous triennal, des mesures précises et urgentes dans le domaine de la protection données, une réforme de la réglementation visant le renforcement de notre souveraineté numérique et une action sur les leviers de l'innovation et du multilatéralisme pour garantir la souveraineté numérique nationale dont le Sénat se veut être le gardien.

I. QUELS SCÉNARII FACE AUX MENACES PESANT SUR NOTRE SOUVERAINETÉ ?

A. LA COMPÉTITION INTENSE ENTRE ÉTATS DANS LE CYBERESPACE

La maîtrise des données a de profondes répercussions économiques et a permis l'émergence d'acteurs économiques capables de rivaliser avec les États. Elle est également un enjeu géopolitique et les stratégies nationales déployées par les États eux-mêmes entrent en concurrence. Selon le rapport intitulé « *L'Europe : sujet ou objet de la géopolitique des données* »[1] : « *Les données ne doivent plus seulement être comprises comme un sujet juridique et commercial, mais comme un* ***enjeu de politique internationale à part entière*** ».

Le cyberespace a ceci de particulier qu'il est le seul espace stratégique créé de la main de l'homme. Ce monde immatériel apparaît comme un monde à conquérir ou, *a minima*, dans lequel exercer sa puissance, au même titre que le monde matériel, d'abord terrestre, puis maritime, et enfin aérien, a été pendant des siècles le lieu d'affrontements pour la suprématie. Le lieu de ces confrontations est désormais en grande partie immatériel et situé hors des frontières physiques des États, dans un espace sans territoire, mais non sans matérialité.

Le cyberespace se compose en effet d'une couche matérielle qui correspond à l'ensemble des appareils, serveurs, routeurs, ordinateurs qui permettent l'interconnexion des machines ; d'une couche logique ou logicielle qui couvre les éléments de communication entre les machines elles-mêmes, autrement dit les protocoles, ou bien entre les humains et les machines, c'est-à-dire les logiciels. Ces deux premières couches forment l'organisation technique du cyberespace et définissent la manière dont les réseaux fonctionnent. La troisième couche, dite sémantique ou informationnelle, correspond à l'ensemble des informations qui transitent au travers des deux premières. Cette segmentation en trois couches justifie une différence d'approches nationales selon la culture du cyberespace que l'on choisit de privilégier[2].

Les États-Unis ont pensé le développement du cyberespace concomitamment à leur positionnement comme leader de ce nouvel espace stratégique. Le modèle américain ultra-libéral, porté et portant ses acteurs privés, nouvelles compagnies coloniales du monde numérique pour filer la métaphore utilisée en son temps par notre collègue Catherine Morin-Desailly, est souverain, dominant les secteurs clés, imposant ses normes, favorisant ses acteurs économiques au détriment des usagers.

---

[1] *De Thomas Gomart, Julien Nocetti et Clément Tonon, IFRI, juillet 2018.*

[2] *Cf. audition de Nicolas Mazzuchi, chargé de recherche à la Fondation pour la recherche stratégique, devant votre commission le 23 mai 2019. Votre rapporteur n'a pas souhaité segmenter ses analyses et propositions en fonction de chacune de ces couches, préférant une approche transversale.*

S'y opposent des modèles chinois et russe, autoritaires, segmentant l'espace numérique pour en avoir un parfait contrôle à l'intérieur des frontières physiques du pays. Ce modèle est-il réellement souverain ?

Enfin, face à ces stratégies, celles de la France et de l'Europe apparaissent parfois idéalistes et peu pragmatiques. L'Europe et la France sont souvent présentées comme l'enjeu du cyberespace, avec un marché de 500 millions de consommateurs. Sont-elles encore des acteurs ?

1. La politique américaine : la recherche d'un leadership incontesté

Les États-Unis ont structuré leur vision stratégique et géopolitique du cyberespace sur son architecture technique, définie par ses deux premières couches, avec 90 % des communications dans le cyberespace circulant de manière sous-marine *via* des câbles, et un recours aux serveurs racines pour faire fonctionner Internet. C'est une vision libérale, avec des segments fixes détenus par le *Department of Defense* sur les serveurs racines, comme le serveur qui appartient au laboratoire de recherche de l'armée américaine, ou le serveur propriété de la NASA. L'État américain exerce ainsi un contrôle matériel très fort, l'action privée s'exerçant surtout sur les couches logicielle et sémantique.

Le contrôle des données est l'axe prioritaire tant du « redéveloppement » économique américain, structuré autour des géants économiques, que sont les Gafam, que de la stratégie américaine de sécurité, appuyé par les pouvoirs très importants confiés à la National Security Agency (NSA)[1]. Cette priorité prend appui sur la longue tradition d'*open door policy* ou liberté de circulation des données défendue par Washington visant à l'ouverture des marchés au profit du maintien de la prééminence américaine, à la fois militaire et économique[2]. Pour autant cette stratégie ne paraît plus aussi simple à mener qu'elle a pu l'être par le passé.

a) Des relations complexes entre les Gafam et l'État américain

Aucun autre pays que les États-Unis n'a aussi étroitement intégré l'utilisation, voire la captation des données au sein de sa stratégie économique et de sa politique de sécurité. Cette politique a été très favorable au développement d'un écosystème d'innovation et de développement économique dans le secteur numérique, qui a abouti à l'émergence des géants américains numériques. Les aides de l'Agence pour les projets de recherche avancée de défense (*Defense Advanced Research Projects Agency* - DARPA) au secteur numérique ont été déterminantes dans l'émergence de cet écosystème. Les effets combinés de la crise de 2008, entraînant la

[1] *Dont les pratiques ont été dénoncées par Edward Snowden en 2013.*

[2] *Cf. audition par votre commission de Julien Nocetti, chercheur à l'Institut français des relations internationales.*

disparition des entreprises les plus fragiles et laissant les autres sans concurrents, et d'un modèle économique basé sur l'effet de réseau ont favorisé la constitution de monopoles, voire de conglomérats.

Les États-Unis sont attachés au principe de libre-concurrence et ont su à plusieurs reprises au cours de leur histoire démembrer les monopoles économiques qui s'étaient formés dans le domaine de l'exploitation pétrolière puis plus tard dans celui des télécommunications. Dans le cas du numérique, pourtant, ce n'est que récemment que des critiques ont émergé sur la concentration des acteurs du cyberespace et encore ne sont-elles pas unanimement partagées par la classe politique américaine. Des actions ont toutefois été engagées en justice en septembre 2019 à l'encontre de Facebook et de Google. De fait, les relations du pouvoir américain avec les Gafam et les autres entreprises numériques est ambigu.

Les autorités s'attribuent sous Obama la propriété d'Internet, dans un nationalisme numérique assumé et quasi messianique lorsque la secrétaire d'Etat, Hillary Clinton promettait en 2010 d'abattre le rideau de fer numérique en référence au vaste système de censure en ligne chinois qui était déployé. Prompt à les soutenir à l'international, en agitant des menaces de représailles après l'adoption de la taxation des géants du numérique ou en présentant le RGPD comme anticoncurrentiel[1], l'actuel président américain ne présume pas du soutien de ces entreprises. Les Gafam sont en effet traditionnellement identifiés comme des soutiens du parti démocrate, au sein duquel se tient pourtant le débat sur leur démantèlement.

Mais, en fait, la frontière entre les Gafam et l'État américain est « *particulièrement poreuse, les liens interorganisationnels et interpersonnels qui unissent ces deux mondes concourent à la structuration d'un « complexe techno-étatique », technocratique, même, au sens quasi étymologique du terme* »[2]. Selon Charles Thibout, chercheur associé à l'IRIS : « *Pour prendre l'exemple de Google, entre 2005 et 2016, l'entreprise a embauché près de 200 membres du gouvernement américain, dont une majorité à des postes de lobbyistes, et, concomitamment, une soixantaine de ses employés ont rejoint la Maison Blanche, les agences gouvernementales ou le Congrès. Entre 2015 et 2018, Alphabet a déboursé près de 70 millions de dollars en lobbying à Washington : 82 % de ses lobbyistes enregistrés sur la période 2017-2018 travaillaient auparavant soit à la Maison Blanche, soit dans des agences gouvernementales, soit au Congrès.* ».

---

[1] *La protection des données personnelles étant présentée comme un frein à l'accès des petites et moyennes entreprises au marché numérique.*

[2] *Selon la tribune de l'IA en Amérique : les Gafam mènent la danse stratégique de Charles Thibout, publiée le 30 janvier 2019 sur le site de l'IRIS https://www.iris-france.org/129644-de-lia-en-amerique-les-gafam-menent-la-danse-strategique/ :* Les raisons de cette coalescence sont nombreuses : elles reposent sur des cercles de sociabilité communs (réseaux d'anciens étudiants de grandes universités, fondations, clubs), des communautés idéologiques homologues (néolibéraux, libertariens, objectivistes, transhumanistes) et des pratiques de lobbying et de *revolving doors* finement organisées par les multinationales.

Selon Félix Tréguer, chercheur, membre fondateur de La Quadrature du Net, ce phénomène tient finalement plus de la fusion que de la concurrence entre l'État et les Gafam[1].

b) Une politique de la donnée basée sur une extraterritorialité juridique agressive

Au-delà du lien supposé ou réel entre les autorités politiques et ces entreprises, le conflit qui a opposé Apple au gouvernement américain est symptomatique d'une bataille pour la souveraineté entre l'État américain et les entreprises américaines du numérique : Apple, en 2015, a refusé de livrer au FBI les clés du chiffrement de l'iPhone de l'auteur de la fusillade de San Bernardino[2]. En 2016, c'est Microsoft qui a refusé de livrer au FBI les courriels d'un trafiquant de drogue, hébergés sur des serveurs situés en Irlande. La réquisition directe, sans coopération judicaire internationale, semblait illégale à Microsoft et susceptible de nuire encore à la confiance de ses clients, déjà entamée par le *Patriot Act* et les révélations de Snowden.

Le *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) a été la réponse légale des pouvoirs publics américains aux réticences des entreprises du numérique. Cette loi facilite l'obtention par l'administration américaine de données stockées ou transitant à l'étranger, *via* notamment les opérateurs et fournisseurs de services en ligne américains. Cet acte législatif contraint les entreprises numériques américaines à accepter la pleine souveraineté numérique des États-Unis. Lors de leurs auditions par votre commission en juillet et septembre 2019, les représentants des Gafam ont fait preuve d'une grande prudence et ont fait valoir leur volonté de protéger les données de leurs utilisateurs et clients. Ainsi, entendu par votre commission le 18 juillet 2019, M. Marc Mossé, directeur juridique et affaires publiques de Microsoft Europe a déclaré : « *La position de Microsoft devant la Cour suprême – visant à protéger les données stockées en Europe – demeure, même si le cadre a évolué. Nous protégeons les données de nos clients : premièrement en répondant aux autorités qui nous sollicitent qu'il faut demander ces données directement aux*

---

[1] *Selon un texte adapté d'une intervention au colloque* Réglementer la liberté d'expression au nom du débat public, *qui se tenait à l'Institut de Recherche Philosophiques de Lyon (IRPhiL) les 29 et 30 novembre 2018, publié le 25/02/2019 sur le site des blogs de Médiapart https://blogs.mediapart.fr/felix-treguer/blog/250219/vers-l-automatisation-de-la-censure-politique :*
« Si l'on pense l'État non pas comme un bloc aux contours clairement identifiés (à la manière des juristes) mais davantage comme un ensemble de pratiques et une rationalité que Michel Foucault désignait comme la « gouvernementalité », alors il est clair que ce que ces évolutions donnent à voir, c'est l'incorporation de ces acteurs privés à l'État ; c'est la cooptation de leurs infrastructures et la diffusion de leurs savoir-faire dans le traitement et l'analyse de masses de données désormais cruciales dans les formes contemporaines de gouvernement. C'est donc une fusion qui s'opère sous nos yeux, bien plus qu'une concurrence entre les États et les Gafam qui chercheraient à se substituer aux gouvernements. »

[2] *Un couple de tireurs a ouvert le feu, le 2 décembre 2015, dans un centre social du comté de San Bernardino en Californie, tuant 14 personnes. Le FBI a eu recours à des hackers pour briser le chiffrement.*

clients, deuxièmement en avertissant nos clients si nous sommes saisis d'une telle demande, et troisièmement en envisageant fortement de nous opposer à une telle demande en cas de conflit de loi précis et clair. »

2. La Chine : une politique numérique globale aux résultats encore incomplets

La Chine comme la Russie ont développé des politiques visant à garantir leur souveraineté numérique et à s'émanciper de l'hégémonie américaine. Ces politiques, éloignées des valeurs occidentales démocratiques, connaissent un succès mitigé mais ne doivent en rien être négligées.

Au modèle américain s'oppose le modèle chinois, autoritaire, segmentant l'espace numérique pour en avoir un parfait contrôle sur son sol, interdisant aux entreprises étrangères de transférer leurs données électroniques vers leurs sièges nationaux, utilisant les données personnelles de ses citoyens pour asseoir la domination du parti communiste chinois. Ce modèle est-il réellement souverain ?

a) Le basculement de la Chine vers le cyberespace

La puissance numérique chinoise a cru très fortement. En matière de capacités de de *cloud computing*, la Chine arrive en seconde position, derrière les États-Unis et connaît une croissance d'activité extrêmement forte, de sorte qu'elle tend à remettre en cause la toute-puissance américaine dans ce champ. Le nombre d'utilisateurs d'Internet entre 2000 et 2016 s'est nettement rééquilibré en faveur de la Chine[1]. Ainsi, en 2000 sur 412,8 millions d'utilisateurs d'Internet : 122 millions étaient situés aux États-Unis, 77 millions dans l'Union européenne, 38 millions au Japon, 22 millions en Chine, 21 millions en Corée du Sud, 16 millions au Canada et 9 millions en Australie. Le Brésil, le Mexique et la Malaisie comptaient chacun 5 millions d'utilisateurs et l'Inde 6 millions. En 2016, Internet comptait 3,4 milliards d'utilisateurs dont 733 millions localisés en Chine, 414 millions dans l'Union européenne, 391 millions en Inde et 246 millions aux États-Unis. Le Brésil recensait 126 millions d'utilisateurs et le Japon 118 millions. La Russie qui comptait moins de 5 millions d'utilisateurs d'Internet en 2000 en totalisait 106 millions en 2016. Viennent ensuite le Mexique avec 76 millions,

[1] *Source : Dossier « une bascule vers l'Asie » de Martin Untersinger, réalisé avec l'aide d'Alix Desforges, Frédérick Douzet, Jérémy Robine, Loqman Salamatian, chercheurs de l'Institut français de géopolitique (Université Paris-VIII) et de la Chaire Castex de cyberstratégie (IHEDN), à l'issue du colloque international* Cartographie du cyberespace*, organisé en mars 2018, et avec l'aide de Kavé Salamatian associé au laboratoire LISTIC de l'Université de Savoie, à Datasphère de l'INRIA et à l'Académie des Sciences de Chine, publié à l'adresse suivante sur le site du Monde : https://www.lemonde.fr/mmpub/edt/zip/2018/07/23/113436857-58150bec479c4da6fa4f66fec35e46554ceb122f/index.html*

l'Indonésie avec 66 millions, la Corée du Sud et le Nigéria avec chacun 48 millions puis la Turquie avec 46 millions et l'Iran avec 43 millions.

Nicolas Mazzuchi, entendu par votre commission d'enquête[1] a rappelé que cette évolution ne devait rien au hasard : les Chinois ont su mesurer l'importance de mener une politique de puissance dans le cyberespace. Il a ainsi rappelé que « *la Chine est venue au cyberespace dans la seconde moitié des années 90, à ses propres conditions. Elle a d'emblée adopté la segmentation du cyberespace en trois couches et a décidé de devenir souveraine sur ces trois couches, tout au moins dans son propre espace national. La Grande Muraille dorée opère un contrôle des données sur la première couche, sous la forme d'un gigantesque pare-feu permettant à l'État chinois de contrôler, avec une efficacité importante, tout ce qui entre et sort de l'espace informationnel chinois.*

Au niveau de la deuxième couche, la population chinoise peut bénéficier des services d'opérateurs nationaux qui offrent en version locale et facilement contrôlable, avec une législation obligeant à stocker les données sur le territoire national, l'équivalent de ce que proposent les opérateurs internationaux. On retrouve ainsi répliqués les grands Gafam (Google, Apple, Facebook, Amazon, Microsoft), avec, par exemple, Baidu pour Google, Alibaba pour Amazon, ou Sina Weibo comme Twitter local.

Pour ce qui est de la couche sémantique, une armée d'opérateurs sont payés pour effectuer des contrôles destinés à empêcher l'émergence de critiques sur le système politique et social chinois. L'État chinois affiche ainsi sa volonté de garder la mainmise sur toute l'architecture de son cyberespace, permettant à la Chine de s'insérer dans le cyberespace à ses propres conditions. ».

b) Une souveraineté numérique chinoise encore relative

Les BATX[2] rivalisent avec les Gafam, et cette politique a permis à la Chine de garder les deux tiers de son trafic national numérique sur son sol[3]. De plus, le contrôle de la population par les technologies numériques se met en place avec un système de notation sociale dont l'acceptabilité par les sociétés occidentales démocratiques paraît à l'heure actuelle inenvisageable[4].

---

[1] *Cf. Audition par votre commission de Nicolas Mazzuchi, chargé de recherche à la Fondation pour la recherche stratégique le 23 mai 2019.*

[2] *Pour Baidu, Alibaba, Tencent et Xiaomi, les géants du Web chinois.*

[3] *À titre de comparaison, en France, moins de 25 % du trafic Internet reste dans le pays soit environ 200 millions des sites Web visités par mois. Le reste du trafic se dirige vers des sites américains soit environ 650 millions de visites par mois.*

[4] *Voir notamment les articles :* Comment le Xinjiang est devenu le laboratoire high-tech du contrôle social*, de The Wall Street Journal - New York, de Josh Chi et Clément Bürge publié le 19/12/2017 –*
https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355?mg=prod/accounts-wsj et En Chine, les personnes avec une faible "note sociale" ne pourront plus prendre l'avion ou le train *de Claire Tervé, publié sur le huffingtonpost.fr le 19/03/2018.*
https://www.huffingtonpost.fr/2018/03/19/en-chine-les-personnes-avec-une-faible-note-sociale-ne-pourront-plus-prendre-lavion-ou-le-train_a_23389304/

Pour autant de nombreux analystes mettent en doute la capacité de la Chine de tenir à long terme sa « muraille de Chine numérique ». Deux éléments viennent corroborer ceci :

- si la Chine parvient bien à garder son trafic numérique sur son sol, seuls 24 % des visites sur les sites Web aboutissant aux États-Unis, les composants publicitaires contenus par les pages Web, appelés « trackers »[1] aboutissent pour 87 % d'entre eux aux États-Unis,

- la chaîne de valeur numérique chinoise n'est pas à l'abri des décisions américaines. La décision de bannir le géant chinois Huawei du sol américain et, autant que faire se peut, du sol des pays alliés des États-Unis, a montré l'importance des liens d'interdépendance tissés entre la Chine et les États-Unis. Cette interdépendance est complexe et handicape à la fois la Chine et les États-Unis comme l'ont montré les récents soubresauts de l'industrie des semi-conducteurs.

c) Politique économique dirigiste et arsenal juridique au service de la souveraineté numérique de la Chine

La Chine a pris modèle sur l'ancien schéma occidental de l'administration technicienne qui fit, jadis, le succès de l'Europe et des États-Unis[2]. Elle a ainsi défini les grandes lignes de sa politique de puissance dans le plan quinquennal 2015-2025 « *Made in China* » et le 13e plan quinquennal 2016-2020. Pékin vise l'autonomie et la souveraineté dans de nombreux domaines, notamment : les nouvelles technologies de l'information, la robotique, le secteur aérospatial, les biotechnologies, les véhicules électriques et de basse consommation. L'intelligence artificielle est également un secteur prioritaire aux termes du 13e plan.

Pékin n'est pas encore parvenu au degré d'autonomie et de souveraineté défini par ses documents de programmation mais poursuit ses efforts : en finançant par exemple la recherche et l'innovation dans les

[1] *Ces trackers transmettent des informations concernant les internautes avec l'objectif de leur adresser des publicités ciblées.*

[2] *Voir la tribune* De l'IA en Amérique : les Gafam mènent la danse stratégique *de Charles Thibout, précitée.*

domaines stratégiques du numérique tels que l'intelligence artificielle ou la politique spatiale[1].

De même, la Chine vise à s'émanciper de l'hégémonie américaine dans le domaine des câbles sous-marins. En 2021, dans le cadre du projet « PEACE » (pour *Pakistan and East Africa Connecting Europe*) participant de la stratégie des nouvelles routes chinoises de la soie, la France devrait accueillir à Marseille le premier câble chinois. Long de 12 000 km, il relira le Pakistan, Djibouti, le Kenya, l'Égypte et la France.

Les autorités chinoises rationnalisent leurs acteurs dans le domaine des câbles sous-marins avec le rachat par le groupe Hengtong, plus gros fabricant mondial de câbles optiques terrestres et sous-marins, de 51 % du capital de Huawei Marine Networks, filiale de câbles sous-marins de Huawei, co-détenue avec Global Marine[2], et quatrième producteur mondial de câbles derrière l'Américain TE Subcom, le Japonais NEC et le Français Alcatel Submarine Networks. Ce rachat va permettre l'émergence d'un acteur économique puissant.

Autre corde à l'arc chinois : la mise en place d'un arsenal juridique propre à garantir la relocalisation des données chinoises en Chine.

En 2016, la Chine a ainsi adopté une loi sur la cybersécurité qui, au nom de la protection de la sécurité nationale et de la vie privée, offre une très large marge de manœuvre aux responsables de la sécurité et aux organismes de réglementation pour surveiller internet. Des politiques dites de cryptosécurité ont également prévu l'interdiction d'utiliser des équipements terminaux de fabrication américaine à certaines occasions et à certains endroits.

---

[1] *La politique chinoise des nouvelles routes de la soie s'étend au numérique et au domaine spatial : le déploiement accéléré d'une couverture satellitaire globale chinoise, semblable au GPS américain, à l'horizon 2020, étendrait les services, chinois, de navigation, de communication et d'e-commerce le long des nouvelles routes de la soie. La Chine incite ainsi les pays adhérant à sa politique à recourir à ses services pour lancer leurs satellites, soutenant financièrement ces projets et proposant des services « tout-en-un » comprenant la fourniture du satellite et le lancement par la fusée chinoise Longue Marche-5. En 2017, un satellite algérien a ainsi été mis en orbite par une fusée chinoise. Des contrats ont été conclus avec le Cambodge et l'Indonésie. Le premier alunissage chinois sur la face cachée de la Lune en janvier 2019 crédibilise la politique chinoise spatiale. Rapport n° 520 (2017-2018) du 30 mai 2018 de Pascal Allizard et Gisèle Jourda, au nom de la commission des affaires étrangères, de la défense et des forces armées, intitulé* « Pour la France, les nouvelles routes de la soie, simple label économique ou nouvel ordre mondial ? ».

[2] *Cet homologue britannique d'Orange marine, héritier de la flotte câblière de Cable & Wireless (C&W) et de British Telecom (BT), est actionnaire à 49 % de Huawei Marine. À terme, Hengtong pourrait logiquement se porter acquéreur des parts détenues par Global Marine. Fin 2018, l'actionnaire principal de Global Marine, le fonds d'investissement HC2, a annoncé qu'il réfléchissait à se retirer en partie ou en totalité de son capital. Selon l'article* Pourquoi l'essor du chinois Hengtong va obliger Paris à accélérer la fusion d'Orange marine et d'ASN *? d'Emmanuelle Serrano publié sur le site La lettre A le 04/07/2019.*
https://www.lalettrea.fr/entreprises_tech-et-telecoms/2019/07/04/pourquoi-l-essor-du-chinois-hengtong-va-obliger-paris-a-accelerer-la-fusion-d-orange-marine-et-d-asn,108364096-evl

Le 1er janvier 2017, le Gouvernement chinois a annoncé un plan visant à reconquérir la souveraineté chinoise sur internet exigeant notamment des entreprises de télécommunications qu'elles ferment tout accès aux VPN[1], moyen de contourner les mesures numériques isolationnistes chinoises. Le 1er juin 2017, est entrée en vigueur la loi sur la cybersécurité imposant aux entreprises actives dans la collecte de données personnelles et dans les infrastructures de réseau de stocker physiquement lesdites données sur des serveurs localisés en Chine. Un délai de grâce de 19 mois était prévu pour permettre aux entreprises de se mettre en conformité avec cette législation. Les Gafam ont signé des accords de partenariats avec des sociétés chinoises, à l'exception d'Apple qui a ouvert un centre de données en Chine.

La *Cyberspace Administration of China* (CAC) a rédigé un nouveau règlement en mai, qui stipule que si l'acquisition de produits et de services perturbe l'infrastructure de l'information clé, ou entraîne des pertes importantes de renseignements personnels et de données importantes, ou pose d'autres risques de sécurité, elle doit être signalée au bureau de révision de la cybersécurité de la CAC.

Si la Chine n'exerce pas une souveraineté numérique complète, elle met en œuvre des moyens dirigistes voire autoritaires pour y remédier.

3. La Russie : une stratégie numérique autoritaire adaptée à ses moyens et ses ambitions

a) La Russie investit les couches du cyberespace à sa portée

Selon Nicolas Mazzuchi, l'espace euro-Atlantique a négligé l'importance de la couche sémantique d'internet, qui a fait un retour fracassant, avec l'invasion de la Crimée par la Russie, puis le scandale Cambridge Analytica[2]. Il estime que « *la Russie au contraire a investi sur la couche sémantique du web au point de parler d'« espace informationnel » pour désigner le cyberespace. (…) [le modèle russe] se concentre sur la capacité d'avoir*

---

[1] *Pour* Virtual Private Network. *Un VPN est un logiciel de sécurité qui construit un réseau privé au sein d'internet, également appelé tunnel, qui permet de se connecter en toute sécurité et confidentialité à un serveur à distance, partout dans le monde, pour envoyer et recevoir des données. La confidentialité des données est garantie par l'encryptage (effectué par le logiciel VPN) entre l'utilisateur et le serveur. Le VPN permet de fait de contourner la censure mise en place par les pouvoirs chinois. Il était, avant cette loi, fréquent de lire dans les conseils aux voyageurs des recommandations visant à télécharger un VPN sur ses terminaux avant de se rendre en Chine, afin de pouvoir continuer à accéder au web sans restrictions. Les opposants au régime chinois étaient réputés faire également usage des VPN.*

[2] *Cette société est au centre d'une affaire de vol de données révélée par le Guardian, le New York Times et The Observer, qui a éclaboussé autant la Maison Blanche que Facebook. Cette filiale de SCL Group, entreprise britannique spécialisée dans le conseil en communication et l'analyse de données, a été accusée d'avoir utilisé des données de 30 millions à 70 millions d'utilisateurs de Facebook, recueillies sans leur consentement, en vue de manipuler les élections présidentielles américaines de 2016.*

des opérateurs informationnels qui émettent en langue russe, au-delà des frontières russes, dans un espace post-soviétique relativement étendu. Ce modèle fait force de sa faiblesse en se concentrant sur la couche internationale au détriment des deux couches techniques. ».

L'action des pouvoirs russes se concentre sur cette couche informationnelle d'internet. Cette stratégie pourrait s'expliquer par un certain pragmatisme, la Russie ne disposant pas de champions mondiaux dans le domaine numérique au même titre que les Gafam ou les BATX. Pour autant, les récentes avancées russes en informatique devraient leur permettre de ne plus dépendre ni de Microsoft ni d'Intel pour leurs systèmes sensibles[1]. Si ses acteurs industriels ne sont pas de premier rang international, ils parviennent apparemment à développer des outils autonomes.

Sur la couche sémantique, la Russie a également des acteurs nationaux : Mail.ru – propriétaire du « Facebook russe » VKontakte – et Yandex, moteur de recherche dominant le marché russe, qui a lancé son Yandex.phone en 2018, produit de moyenne gamme d'un coût modéré. Mail.ru a récemment annoncé une alliance avec le géant chinois de l'e-commerce Alibaba, tandis que Yandex s'est associé avec la première banque du pays, Sberbank, pour la création d'une société commune dans le commerce en ligne, valorisée à un milliard de dollars.

b) Elle déploie un arsenal juridique visant à garantir sa souveraineté

La Russie a, de fait, mis en œuvre une politique très autoritaire pour protéger sa souveraineté numérique dans le cyberespace. À partir de 2012[2], et en réaction aux mouvements de contestation citoyens, la censure d'Internet a été centralisée et organisée. Des règles de localisation des données des ressortissants russes ont été définies : le stockage doit s'effectuer exclusivement sur des serveurs situés physiquement en Russie. De même, les activités de surveillance du web sont facilitées par l'accroissement des pouvoir du Service Fédéral de Surveillance des Télécommunications, des Technologies de l'Information et des Moyens de

---

[1] *Ainsi, la holding Électronique « Rosselektronika », partie de Rostec, champion russe des technologies militaires, est un acteur majeur des hautes technologies en Russie dans le domaine militaire comme civil (créant notamment des circuits intégrés, d'électronique quantique). Un microprocesseur appelé Baïkal, devrait être produit en Russie pour les structures gouvernementales, évitant d'éventuelles "backdoors" de la NSA dans les microprocesseurs américains. Il serait mis en œuvre par l'alliance de Rosnano (fond d'investissement visant à développer, en partenariat avec des entreprises privées, la production d'équipements de haute technologie en Russie, en particulier dans les domaines de l'énergie, des nano-matériaux, des biotechnologies, de l'ingénierie mécanique, de l'optoélectronique etc.), Rostec et T-platforms (son dernier superordinateur est le 22e plus puissant du monde, il produit également des caisses enregistreuses).*

[2] *Les débats parlementaires ont été particulièrement longs, et la loi qui devait initialement entrer en vigueur le 1er septembre 2014 a soulevé de fortes protestations au sein de l'industrie qui ne pouvait immédiatement appliquer les nouvelles dispositions prévues. La Douma a repoussé au 1er septembre 2015 l'application de la loi, avec quelques aménagements.*

Communication, le Roskomnadzor. Le blocage des adresses internet et l'inspection des paquets de données deviennent monnaies courantes.

En 2015, le Roskomnadzor a pu exiger de Reddit[1], puis de Google, Facebook et Twitter qu'ils censurent des centaines de pages de leurs utilisateurs, en s'appuyant sur la « loi des blogueurs », adoptée en 2014, qui interdit l'anonymat des blogueurs et autres internautes ayant une influence sur la population par leurs écrits. La sanction encourue par les entreprises visées est la suspension d'accès à leurs services par les utilisateurs russes[2].

En 2016, les lois Yarovaya[3] visant à renforcer la lutte antiterroriste comportaient également un volet numérique prévoyant de très lourdes obligations pour les entreprises assurant la diffusion de contenu sur internet. Elles doivent désormais conserver pendant un an, sur le territoire russe, les données relatives à la réception et à la transmission d'appels, de messages textuels, de photos, de contenus audio et vidéo. À la demande des organes de sécurité, les messageries des réseaux sociaux utilisant des systèmes complémentaires de chiffrement des messages, tels que WhatsApp et Telegram, doivent fournir les clés permettant le déchiffrage des contenus.

Ce dispositif a encore été complété par deux lois votées à l'été 2017 interdisant l'utilisation des VPN, contrôlant les applications de messagerie instantanée (les opérateurs doivent désormais coopérer dans l'identification de leurs utilisateurs et bloquer les messages à la demande des autorités) et censurant les moteurs de recherche, obligés de retirer toute référence aux sites bloqués en Russie.

Enfin, au début de l'année 2019, pour se prémunir des cyberattaques les plus destructrices, la Russie a entamé l'examen d'une loi destinée à créer dans le pays un « Internet souverain ». Ce texte était présenté comme une réponse au « *caractère belliqueux de la nouvelle stratégie américaine en matière de cybersécurité adoptée en septembre 2018* »[4]. Les autorités cherchent un moyen de couper Internet sur leur territoire afin, disent-elles, de mettre à l'abri leurs infrastructures stratégiques qui pourraient continuer de fonctionner en cas d'interruption des grands serveurs mondiaux. Dans cette perspective, les fournisseurs russes d'accès Internet devront également s'assurer de la mise en place, sur le réseau, de « moyens techniques » fournis par le Roskomnadzor, permettant un contrôle centralisé du trafic pour contrer les

---

[1] *Reddit est un réseau social « viral » c'est-à-dire que les contenus sont déterminés par les utilisateurs et non des éditeurs. Si Google est l'endroit où sont effectuées les recherches; Reddit est l'endroit où l'on peut voir ce que les utilisateurs ont trouvé et aimé.*

[2] *Le Roskomnadzor a le pouvoir d'exiger des opérateurs russes de bloquer l'ensemble du site Wikipédia.*

[3] *Du nom de la députée qui l'a portée : Irina Yarovaya. LinkedIn a été bloqué en novembre 2016 sur décision des tribunaux russes pour non-respect de la loi russe sur les données personnelles.*

[4] *Voir l'article* La Russie cherche à créer un internet indépendant*, Le Figaro.fr avec AFP publié le 12/02/2019 à l'adresse suivante :*
http://www.lefigaro.fr/flash-actu/2019/02/12/97001-20190212FILWWW00051-la-russie-cherche-a-creer-un-internet-independant.php

menaces éventuelles. Ce contrôle centralisé, perçu comme un moyen d'intervenir directement, à la place des opérateurs, dans la gestion du réseau pour bloquer du contenu interdit en Russie, a fait l'objet de nombreuses critiques.

Disposer d'un Internet souverain rend plus crédible d'éventuelles actions nuisant au réseau mondial, dans la mesure où les dispositions nationales permettent de se prémunir des conséquences désastreuses d'une cyberattaque de grande ampleur.

c) La Russie affiche une capacité de déstabilisation profonde du web

Comme le précisait Julien Nocetti lors de son audtion : « *certains pays, tels que la Russie, ne se privent pas d'exploiter la dimension physique d'Internet sous un angle stratégique. C'est un enjeu de souveraineté majeur pour l'Union européenne.* ».

Le 16 avril 2018, les experts américains et britanniques ont fait état d'une « *cyberactivité malveillante d'acteurs soutenus par l'État russe* » dont « *les cibles sont principalement les gouvernements et les organisations du secteur privé, les fournisseurs d'infrastructures cruciales et les fournisseurs d'accès à Internet* »[1]. Depuis de nombreuses années, en effet, les pouvoirs russes sont accusés d'espionner les infrastructures critiques des pays occidentaux en vue d'élargir l'arsenal des outils utilisés en cas d'attaque hybride[2]. En janvier 2019, le ministre britannique de la défense alors en poste a accusé Moscou d'espionner les infrastructures britanniques afin de trouver comment dégrader son économie, détruire ses infrastructures et d'identifier un élément permettant de provoquer un chaos total au sein du pays. En mars 2019 encore, un rapport de l'*US Computer Emergency Readiness Team* (US CERT) affirmait que des pirates informatiques agissant pour le compte du gouvernement russe avaient : « *procédé à une reconnaissance en réseau du système contrôlant des éléments clés de l'économie américaine et tenté de couvrir leurs traces en supprimant les preuves de leur infiltration* »[3].

Le Kremlin a donc refaçonné l'internet russe selon sa propre vision autoritaire, centralisée voire agressive. Sa souveraineté numérique s'exprime par la volonté d'afficher, d'une part, une capacité de résilience pour son propre territoire et, d'autre part, une capacité de nuisance sérieuse pour le réseau mondial.

---

[1] *Voir l'article* Les États-Unis et la Grande-Bretagne accusent la Russie de se livrer à une « cyberactivité malveillante » *de Laurent Lagneau, publié le 17 avril 2018 sur le site opex360.com à l'adresse suivante :*
http://www.opex360.com/2018/04/17/etats-unis-grande-bretagne-accusent-russie-de-se-livrer-a-cyberactivite-malveillante/

[2] *Une attaque hybride ou guerre hybride comporte d'autres volets que les volets militaires traditionnels, notamment des cyberattaques, des sabotages, d'infrastructures numériques ou autres, la propagation de fausses informations, etc.*

[3] *Article précité du site opex360.com.*

Dans ce contexte, les réponses européenne et française à cette compétition dans l'expression d'une souveraineté numérique agressive, qui n'est pas que le fait de la Russie, en témoignent par exemple les cyberattaques menées par la Corée du Nord, dont certains experts estiment qu'elles lui permettent de financer le développement de son arsenal nucléaire[1], peuvent sembler limitées. La souveraineté de nos États est pourtant déjà l'objet de nombreuses menaces qui tiennent plus à l'organisation du web et de ses acteurs qu'à la compétition internationale évoquée ci-dessus[2].

B. ÉTABLIR LA CONCURRENCE SUR LES MARCHÉS NUMÉRIQUES

Les grands acteurs de services sur internet (moteurs de recherche, réseaux sociaux, systèmes d'exploitation, plateformes de services, fournisseurs de solutions d'informatique en nuage…)[3], dont l'activité est par nature mondialisée, peuvent être amenés à remettre en cause la souveraineté des États, constat que notre collègue Catherine Morin-Desailly avait appelé « *l'hypercentralisation de l'Internet autour de géants qui défient les États* »[4]. Certains, à l'instar du Professeur Annie Blandin, n'hésitent pas à qualifier ces acteurs « *d'entreprises souveraines* »[5].

Certes, le rapport de force n'est pas encore aussi écrasant, mais rien n'interdit de penser qu'il puisse le devenir, car c'est exactement le projet de certains entrepreneurs du numérique, qui bénéficient sur les États du double avantage de la cohérence (le succès de leur projet) et de la continuité (tant que les actionnaires continuent d'espérer la « victoire finale »). Les Gouvernements n'ont ni la même cohérence ni la même continuité : le citoyen vote, mais le consommateur agit souvent en contradiction de ce que

---

[1] *Voir à ce sujet l'article* Le programme nucléaire nord-coréen carbure aux cyberattaques *publié le 07/08/2019 sur le site France 24 à l'adresse suivante : https://www.france24.com/fr/20190807-cyberattaque-coree-nord-gain-financement-missile-nucleaire-onu faisant état d'un rapport confidentiel de l'ONU sur ce thème.*

[2] *À laquelle la réponse tient notamment en une cyberdéfense efficace présentée ultérieurement dans le présent rapport.*

[3] *Deux acronymes désignent en général les grands acteurs américains du numérique. Le premier comporte l'ensemble des acteurs les plus importants : les « Gafam » (Google, Apple, Facebook, Amazon, Microsoft) et le second rassemble des acteurs financièrement moins importants mais déjà rentrés dans la vie quotidienne de très nombreux foyers à travers la planète : les « Natu » (Netflix, Airbnb, Tesla, Uber).*
Les géants chinois du numérique sont généralement désignés par l'acronyme « BATX » (pour Baidu, Alibaba, Tencent, Xiaomi), auquel on ajoute désormais souvent le H de Huawei.

[4] L'Europe au secours de l'internet ? *Rapport d'information n° 696 (2013-2014) de Mme Catherine Morin-Desailly, fait au nom de la mission commune d'information sur la gouvernance mondiale de l'Internet, juillet 2014.*

[5] *Annie Blandin,* Les entreprises souveraines de l'internet : un défi pour l'Europe, *in Droits et souveraineté numérique en Europe, 2016. Elle y écrit :* « Nous proposons de qualifier de souveraines les entreprises qui détiennent un pouvoir de marché tel qu'elles se dotent des attributs de la souveraineté, d'un véritable pouvoir de gouvernement ».

son vote exprime ! Les caractéristiques des Gafam et la façon dont ils sapent la souveraineté des États font l'objet d'une annexe au présent rapport.

Dans le domaine économique, on constate que le numérique favorise les concentrations, qui elles-mêmes ouvrent la voie à des pratiques anti-concurrentielles, ce qui minore en partie le potentiel économique de la France en restreignant la concurrence et l'innovation. C'est pourquoi il n'est plus possible d'attendre : il convient d'adopter un cadre de régulation économique adapté au XXIe siècle.

Toutes les pistes d'action décrites dans les sous-parties suivantes démontrent qu'une action politique concrète, pragmatique et crédible est possible. Elle l'est d'autant plus que **le gigantisme de ceux qu'on appelle aujourd'hui les « Gafam » constitue paradoxalement une opportunité pour le politique**, dans la mesure où toute atteinte à leur image de marque peut avoir un effet substantiel sur leur cours de bourse[1]. La « régulation par le cours de bourse » est donc une arme dont l'État ne doit pas se priver ! De même ces géants peuvent-ils révéler leurs faiblesses lorsque les convictions éthiques des salariés les obligent à modifier leurs orientations commerciales[2].

1. Une économie du monopole qui minore le potentiel économique de la France

a) Effets de réseau et rendements d'échelle, ferments d'une économie du monopole

Comme l'explique Jean Tirole[3], **deux facteurs poussent à la concentration des utilisateurs sur une ou deux plateformes numériques**, et donc à la concentration sur les marchés de plateforme (sur les notions de plateforme et de marché biface, voir l'encadré ci-dessous) : les effets de réseau[4] et les rendements d'échelle. Les travaux récents ajoutent à ces deux items le rôle de la **détention en masse de données** comme démultiplicateur de ces deux éléments, celle-ci constituant une importante barrière à l'entrée.

---

[1] *C'est ce qu'a démontré le scandale de Cambridge Analytica, bien que le cours de bourse de l'entreprise concernée, soit presque revenu, six mois plus tard, à son niveau antérieur à la polémique.*

[2] *Suite à la protestation de Facebook, ses salariés, en mars 2018, après la révélation de l'implication de l'entreprise dans un projet d'intelligence artificielle porté par le Pentagone, Google a finalement décidé de ne pas renouveler sa collaboration avec le ministère de la Défense américain (voir, par exemple, l'article de Wired,* « Google won't renew controversial Pentagon AI project », *1er juin 2018).*

[3] *Jean Tirole, Économie du bien commun, PUF, 2016.*

[4] *Ou « externalités de réseaux ».*

Qu'est-ce qu'un marché biface ?

Le modèle économique des entreprises du numérique repose sur l'utilisation de données captées par les plateformes en échange d'une « fausse » gratuité du service mis à disposition. Une plateforme ou **marché biface** est selon Jean Tirole[1] « *un marché où un intermédiaire permet à des vendeurs et des acheteurs d'interagir*[2] ».

La plateforme doit attirer les deux faces du marché en tirant profit de leurs intérêts respectifs. Lorsque l'une des deux faces du marché (par exemple, les utilisateurs) n'est pas prête à payer pour un service mais que l'autre y est en revanche parfaitement disposée (par exemple, les annonceurs) et qu'il existe entre les deux faces d'importantes externalités (par exemple, l'utilisation des données des utilisateurs pour offrir aux annonceurs de la publicité ciblée), il est alors possible de **proposer des services gratuits d'un côté tout en monétisant ces services de l'autre**.

Ainsi, les utilisateurs bénéficient gratuitement de nombreux services – moteur de recherche, messagerie en ligne, cartographie … – grâce auxquels les annonceurs peuvent obtenir des publicités ciblées.

Les **effets de réseau** peuvent se résumer par la formule suivante : plus il y a d'utilisateurs, plus le service a de la valeur. L'exemple le plus parlant est sans doute celui du réseau social : il n'a d'utilité que si nos proches s'y trouvent.

Les effets de réseau peuvent être directs – lorsque l'utilité du réseau pour l'utilisateur grandit à mesure que le nombre d'utilisateurs augmente – ou indirects – lorsque l'utilité du réseau pour les utilisateurs d'un côté de la plateforme augmente avec le nombre d'utilisateurs de l'autre côté de la plateforme[3]. Ces effets de réseau n'existent que si la possibilité de passer d'un service à l'autre ou l'utilisation de plusieurs services en même temps (« *multi-homing* ») ne sont pas restreintes.

Les **rendements d'échelle** se caractérisent quant à eux par le fait que le coût fixe du développement d'un produit se réduit à mesure que le nombre d'utilisateurs grandit. Ainsi, dans le monde numérique, le coût marginal de production tend à être quasi-nul.

---

[1] *Jean Tirole, Économie du bien commun, PUF, 2016.*

[2] *Par exemple, un système d'exploitation (iOS ou Android pour les téléphones intelligents, Windows ou Linux pour les ordinateurs personnels) est une plateforme qui permet à des développeurs d'applications d'interagir avec leurs utilisateurs. De même, un moteur de recherche est une plateforme permettant aux utilisateurs et aux annonceurs d'interagir.*

[3] *Comme l'avait rappelé le rapport de la mission commune d'information de Gaëtan Gorce, Catherine Morin-Desailly,* L'Europe au secours de l'internet : démocratiser la gouvernance de l'internet en s'appuyant sur une ambition politique et industrielle européenne*, juillet 2014), ces effets de réseau sont décrits par Pierre Bellanger, dans son ouvrage sur la souveraineté numérique, à travers la loi de Metcalfe, selon laquelle* « la valeur d'une machine est proportionnelle au carré du nombre de machines auxquelles elle est connectée ». *Pierre Bellanger précise que cette loi peut être étendue aux réseaux en ces termes :* « la valeur d'un réseau est équivalente au carré du nombre de ses utilisateurs ».

C'est pourquoi on constate souvent que « *le gagnant prend tout*[1] ». On observe ainsi une **tendance à la constitution de monopoles puis de conglomérats**. La taille sans précédent des Gafam peut se vérifier à leur nombre d'utilisateurs, leur capitalisation boursière[2], leur chiffre d'affaires[3] ou encore leur part mondiale de marché, mais il ne faudrait pas non plus oublier la forte ascension des acteurs chinois du numérique[4].

L'un des fondateurs de PayPal et de l'entreprise Palantir, **Peter Thiel**[5], qui siège également au conseil d'administration de Facebook, **a même théorisé la nécessité de bâtir un monopole** : selon lui, « *monopoly is the condition of every successful business* »[6]. L'auteur propose un mode d'emploi du monopole réussi : commencer sur un marché de niche afin d'y être en position dominante avant de s'étendre à des marchés proches. C'est, par exemple, le cas d'Amazon, qui a débuté avec un service de librairie avant d'étendre son magasin en ligne à d'autres marchés.

De fait, de **nombreux marchés numériques sont dominés, au niveau mondial, par un ou deux Gafam**[7] :

- Google représente plus de 90 % du marché des **moteurs de recherche**[8] ;

- Facebook dispose de près des trois quarts du marché des **réseaux sociaux**[9] ;

- Google (Android) et Apple (iOS) disposent respectivement de 76,03 % et de 22,04 % du marché des **systèmes d'exploitation pour les téléphones** intelligents ;

---

[1] *« the winner takes all ».*

[2] *La valorisation boursière cumulée des Gafam dépasse 4 000 milliards de dollars, soit plus de deux fois et demi celle de la totalité du CAC 40.*

[3] *Le chiffre d'affaires d'Amazon en 2017 était l'équivalent de la TVA française, première recette fiscale de l'État.*

[4] *Alibaba (l'Amazon chinois) et Tencent (conglomérat de services en ligne, qui détient notamment l'application WeChat, comparable à la fois à Facebook, Skype, WhatsApp, Paypal et Instagram) étaient valorisées au 1er juillet dernier respectivement à 438 et 430 milliards de dollars, soit les septième et huitième capitalisations mondiales.*

[5] *Peter Thiel, Zero to One, 2014.*

[6] *L'auteur remet par ailleurs en cause le bien-fondé de l'appréhension de la concurrence par les économistes, et considère qu'il s'agit d'une relique de l'histoire, tant les « monopoles créatifs » sont de « puissants moteurs » de changement pour la société.*

[7] *Les chiffres cités proviennent, sauf indication contraire, du site internet suivant : http://gs.statcounter.com. Ils datent de juin 2019. Il convient de noter que la notion de part de marché est délicate à appréhender pour les entreprises du numérique dont le modèle repose sur la gratuité sur l'une des faces du marché, d'où des estimations qui peuvent varier selon la source utilisée. De même, la notion de marché pertinent donne lieu à de longs développements dans les décisions des autorités de la concurrence – les marchés considérés sont donc en l'espèce simplifiés.*

[8] *92,62 % en juin 2019. En prenant uniquement sa part de marché sur les téléphones intelligents, celle-ci atteint 95,58 %.*

[9] *73,91 %, contre 13,16 % pour Pinterest, 6,18 % pour Twitter et 1,43 % pour Instagram.*

- Microsoft (Windows) et Apple (OS X) disposent respectivement de 78,43 % et de 13,53 % du marché des **systèmes d'exploitation pour les ordinateurs** personnels, Linux ne représentant que 1,6 % du marché ;

- Google (Chrome) détient près de 65 % et Apple (Safari) 15,15 % du marché des **navigateurs web** ;

- Google et Facebook détiennent plus de la moitié du marché de la **publicité en ligne**[1] ;

- Amazon représente près ou plus de la moitié du marché du **commerce en ligne** dans de nombreux pays[2] ;

- Amazon (33 %), Microsoft (16 %) et Google (8 %) représentent plus de la moitié (57 %) du marché des **infrastructures de services d'informatique en nuage**[3]…

Cette dynamique conduit également à la constitution de **conglomérats**, une entreprise étant en mesure d'augmenter ses activités sur un segment de son activité en jouant du pouvoir de marché qu'elle détient sur un autre produit ou marché – c'est par exemple le cas d'*Amazon Web Services* (AWS) pour sa plateforme de marché Amazon. C'est ce que les économistes appellent les « *economies of scope* », que l'on pourrait traduire par « **économies de gamme » ou « de diversification** » : les grandes plateformes offrant déjà de multiples services sont plus efficaces lorsqu'elles pénètrent un nouveau marché. Ce qui conduit, de façon croissante, à constater une **concurrence entre écosystèmes**[4] – lesquels peuvent d'ailleurs être constitués de plusieurs services en ligne, mais aussi de services en ligne adjoints à des terminaux (téléphones intelligents, assistants vocaux…).

Ces positions ne seraient pas acquises, « *la concurrence étant à portée de clics* ». S'il est indéniable que certains grands acteurs du numérique ont pu se faire dépasser par le passé – comme, par exemple, le réseau social MySpace – ces entreprises, dont l'ampleur est inédite, ont désormais les moyens d'éviter l'apparition d'une concurrence libre et non faussée.

b) Des abus de position dominante et des stratégies de croissance externe agressives.

Si la position dominante n'est pas en soi condamnable en droit positif, on a déjà pu observer de **nombreux abus de position dominante de**

---

[1] *eMarketer, Net Digital Ad Revenue Share Worldwide, by Company, 2016-2019 ; https://www.emarketer.com/Chart/Net-Digital-Ad-Revenue-Share-Worldwide-by-Company-2016-2019-of-total-billions/205364.*

[2] *47% aux Etats-Unis selon eMarketer. Selon Foxintelligence, sa part de marché serait de 50% en France – mais Kantar Worldpanel l'estime, selon une méthodologie différente, à 17,3%.*

[3] *Synergy research group, Communiqué de presse,* Cloud Service Spending Still Growing Almost 40% per Year; Half of it Won by Amazon & Microsoft*, 26 juillet 2019. Le cabinet utilise la notion de* "Cloud infrastructure services market".

[4] *Voir, sur ce point, le rapport de Jacques Crémer, Yves-Alexandre de Montjoye et Heike Schweitzer intitulé* Competition policy for the digital era*, publié début 2019.*

la part des géants du numérique. Dès 1969, IBM a été contrainte, aux États-Unis, de séparer ses activités logiciel et services de son activité matérielle. En 2000 et en 2008, Microsoft a dû découpler, en Europe, son système d'exploitation Windows des services comme le navigateur *Internet Explorer* et le lecteur *Media Player*.

Plus récemment, Google a été condamnée par la Commission européenne à **plus de 8 milliards d'euros d'amende en trois ans** pour atteinte aux règles de la concurrence avec les applications AdSense[1], Android[2] et Shopping[3]. Au premier semestre 2019, l'Autorité française de la concurrence a prononcé des mesures d'urgence dans le litige opposant Google à la société Amadeus sur le marché de la publicité en ligne[4]. De même, l'autorisation accordée à l'entreprise Facebook de racheter WhatsApp et Instagram fait l'objet de critiques.

La dynamique monopolistique des marchés peut constituer une **incitation pour les plateformes à recourir à des pratiques anti-concurrentielles**. Par exemple, pour Benoît Thieulin, ancien président du Conseil national du numérique, rapporteur de l'avis « Pour une politique de souveraineté européenne du numérique » adopté par le Conseil économique, social et environnemental : « *les plateformes, qui sont en situation de quasi-monopole naturel, disposent d'un* ***droit de vie et de mort sur tout un ensemble d'acteurs****. Il leur suffit de modifier les API*[5] ». Ce phénomène est parfois désigné par les termes de « *plateforme régulatrice* »[6]. Le positionnement d'Amazon qui, d'une part, en tant que place de marché, revend pour le compte de commerçants, et d'autre part, en tant que plateforme de commerce en ligne, revend directement des produits qu'elle achète, soulève également des interrogations quant aux potentielles atteintes à la concurrence qu'il génère - Amazon est d'ailleurs visée par une enquête de la Commission européenne ouverte en juillet dernier afin de déterminer si l'utilisation de données sensibles provenant de détaillants indépendants utilisant sa place de marché enfreint les règles de concurrence de l'Union[7]. Comme l'a noté notre collègue Pascale Gruny dans son récent rapport sur

---

[1] *Commission européenne, communiqué de presse, 20 mars 2019. L'amende infligée est de 1,49 milliard d'euros.*

[2] *Commission européenne, communiqué de presse, 18 juillet 2018. La sanction infligée est de 4,34 milliards d'euros.*

[3] *Commission européenne, décision du 27 juin 2017. La sanction infligée est de 2,44 milliards d'euros.*

[4] *Autorité de la concurrence, Décision n° 19-MC-01 du 31 janvier 2019 relative à une demande de mesures conservatoires de la société Amadeus.*

[5] *Les API (*Application Programming Interface*), ou interfaces de programmation applicative, sont un ensemble de méthodes et de fonctions servant de façade à un logiciel pour offrir des services à d'autres logiciels. Plus simplement, elles sont des interfaces mises à disposition par les plateformes pour permettre à des tiers d'innover à partir de leurs ressources. Facebook, par exemple, propose un grand nombre d'API aux développeurs, comme celle permettant de répandre le bouton «* like *» sur internet.*

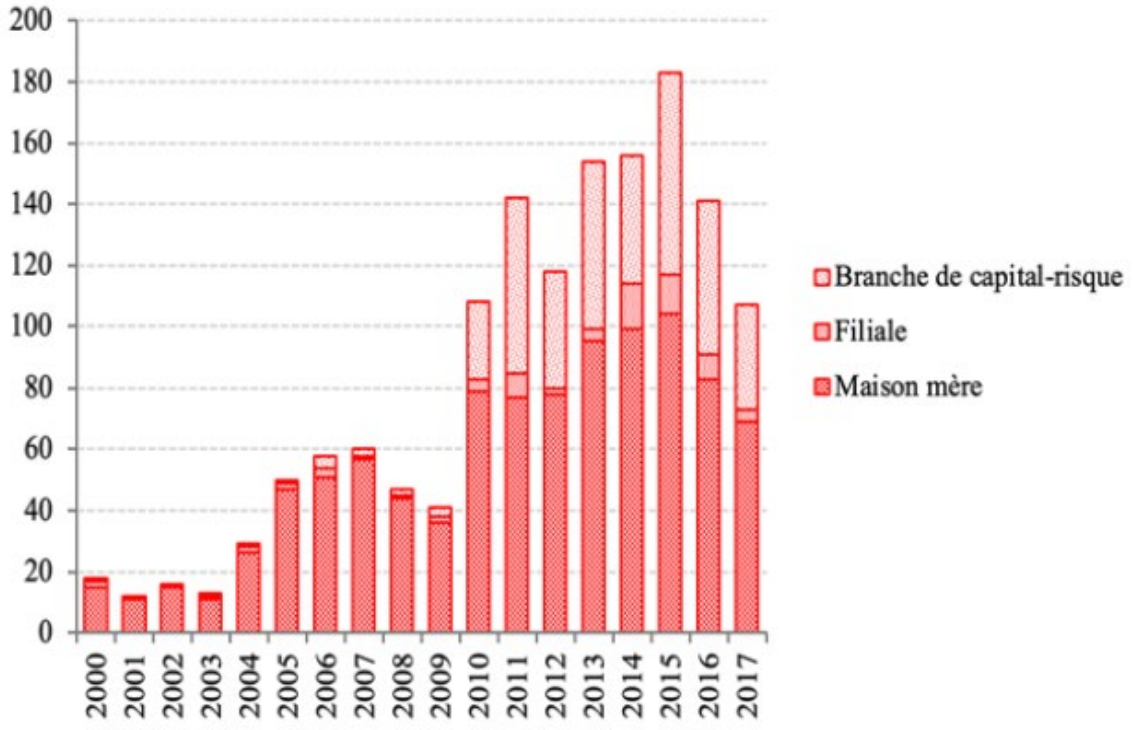
[6] *Voir, par exemple, le rapport Crémer précité.*

[7] *Commission européenne, communiqué de presse du 17 juillet 2019.*

l'accompagnement de la transition numérique des PME[1], une étude de la Commission européenne montre que, parmi les PME européennes ayant recours à des places de marché en ligne pour vendre leurs produits et services, « *près de 50 % des entreprises (…) se heurtent à des problèmes. Quelque 38 % des problèmes rencontrés dans les relations contractuelles demeurent non résolus, et ce n'est que difficilement que l'on résout 26 % d'entre eux. Cela entraîne directement des pertes de ventes d'une valeur comprise entre 1,27 et 2,35 milliards d'euros* ». Ont également pu être répertoriés des comportements préjudiciables aux consommateurs, comme le fait pour Apple de brider volontairement les performances des composants de certains de ses téléphones intelligents pour en préserver la batterie vieillissante[2].

Cette situation de position dominante sur certains marchés permet d'amasser suffisamment de trésorerie[3] pour procéder à de **nombreux rachats d'entreprises** ainsi qu'à un grand nombre de prises de participations.

Acquisitions et prises de participation des dix plus grandes entreprises américaines du numérique (en nombre de transactions)



Source : fondation pour l'innovation politique, d'après les données de la plateforme Mergermarket, 2018.

[1] *Rapport d'information n° 635 (2018-2019) de Mme Pascale Gruny, fait au nom de la Délégation aux entreprises du Sénat,* Accompagnement de la transition numérique des PME : comment la France peut-elle rattraper son retard ?, *juillet 2019.*

[2] *Voir, par exemple, l'article de Numerama,* Apple ne bride pas que les vieux modèles d'iPhone : le 8, 8 Plus et le X aussi, *3 novembre 2018.*

[3] *Le cas emblématique est celui d'Apple, qui disposait, au deuxième trimestre 2019, d'une trésorerie de 210 milliards de dollars… soit près de la moitié du budget de l'État français !*

Cette politique de croissance externe des géants numériques **peut être qualifiée d'agressive**, car elle conduit, dans certains cas, à l'acquisition de jeunes entreprises qui défient leur position dominante – c'est ce qu'il est convenu d'appeler les « ***acquisitions prédatrices*** »[1], qui visent à s'approprier clientèle, technologies et ressources humaines.

Parallèlement, les grandes entreprises numériques rachètent les *start-up* et entreprises très innovantes dans les segments naissants des nouvelles technologies. On remarque également, sur le graphique précédent, l'importance croissante des prises de participation *via* leurs véhicules internes d'investissement, ce qui permet aux géants du numérique de s'assurer un accès privilégié aux innovations développées par les entreprises cibles.

Quelques exemples emblématiques d'acquisitions par les géants américains du numérique

Google a racheté Android en 2005 et Youtube en 2006. Plus récemment, l'entreprise a acquis le service d'aide aux déplacements Waze en 2013 et DeepMind, le spécialiste britannique de l'apprentissage automatisé et des neurosciences, en 2014.

Facebook a racheté le réseau social Instagram en 2012 et la messagerie instantanée WhatsApp en 2014.

Microsoft a racheté la messagerie en ligne Skype et le réseau social LinkedIn respectivement en 2011 et 2016.

Apple a acquis l'entreprise Hey Siri pour développer son assistant vocal en 2010.

Une telle politique de rachat oriente les choix des entrepreneurs : au lieu de faire croître leur entreprise pour devenir un géant numérique, ils espèrent leur rachat par un géant. Cela peut aboutir à ce que des entreprises développées en France et soutenues par des capitaux publics soient rachetées par des entreprises étrangères qui s'en approprient les fruits[2].

Enfin, le rapport de la fondation pour l'innovation politique précité souligne deux autres éléments qui constituent autant d'indices de la diminution de l'intensité concurrentielle sur les marchés des nouvelles technologies :

- **les profits** des géants technologiques américains ont été **sans commune mesure avec ceux d'autres industries sur les vingt dernières années** ;

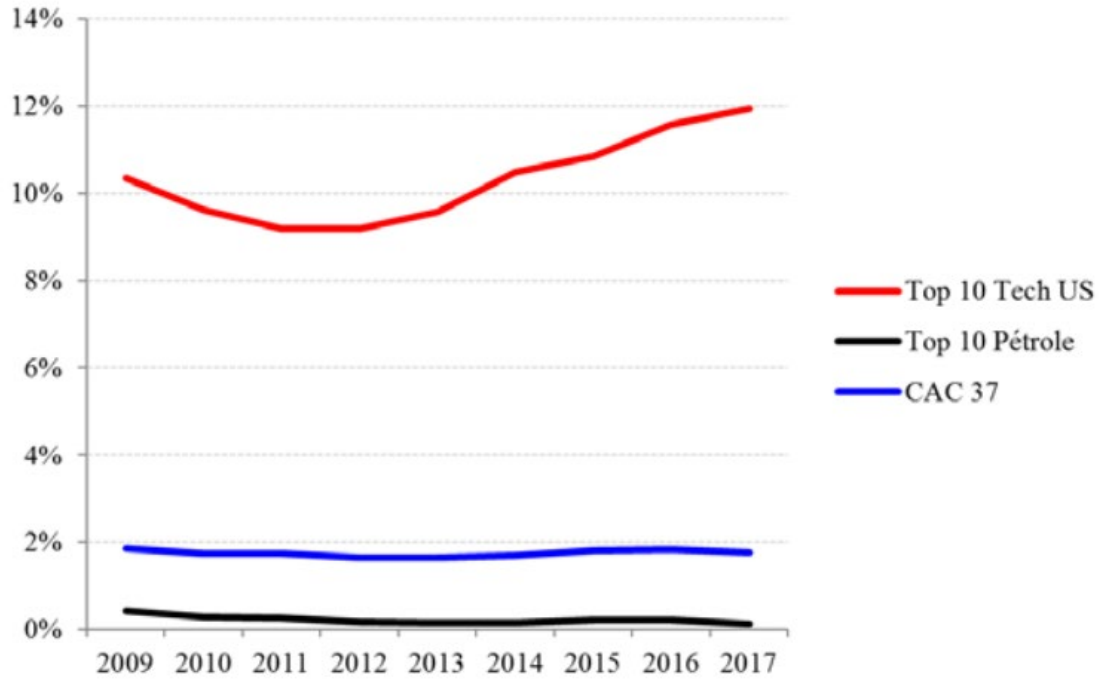
- leur importante trésorerie leur permet également d'engager de **colossaux efforts de recherche et développement** (R&D) au regard des

[1] *Le concept de « killing acquisitions » avait déjà été développé dans le domaine de l'industrie pharmaceutique. La presse a révélé des échanges de courriels internes à Facebook affirmant que l'objectif du rachat d'Instagram était bien de « tuer » la concurrence (voir New York Post,* Facebook boasted of buying Instagram to kill the competition*, 26 février 2019).*

[2] *Ce point est discuté dans le E de la deuxième partie du présent rapport.*

industries plus classiques, avec des ratios d'investissement cinq à six fois supérieurs comme le démontre le graphique ci-dessous.

Comparaison des dépenses de R&D (en % du chiffre d'affaires)



Source : fondation pour l'innovation politique, 2018.

c) Une minoration du potentiel économique de la France

Comme le remarquait la résolution du Sénat *Pour une réforme des conditions d'utilisation des mesures conservatoires en droit européen de la concurrence*, adoptée à l'initiative de notre collègue Catherine Morin-Desailly, la souveraineté numérique « *ne peut être exercée que par le biais d'un tissu économique et entrepreneurial dynamique qui doit être protégé des abus de position dominante ou des situations monopolistiques suscitées par les grands groupes étrangers* »[1].

Les pratiques anti-concurrentielles massives sont le fait d'entreprises étrangères et ont pour effet de miner le potentiel de développement économique des entreprises locales qui pourraient leur faire concurrence. Dans sa contribution écrite, le Cigref, s'exprimant au nom des entreprises utilisatrices de services numériques, a par ailleurs souligné la dépendance des entreprises domestiques aux géants du numérique étrangers[2], donnant lieu à des pratiques commerciales parfois illégitimes. Elles peuvent

[1] *Résolution européenne pour une réforme des conditions d'utilisation des mesures conservatoires prévues par le règlement (CE) n° 1/2003 du Conseil relatif à la mise en œuvre des règles de concurrence, 8 septembre 2017.*

[2] *« Les grandes organisations utilisatrices de solutions et services numériques n'ont bien souvent d'autre choix que de recourir à des fournisseurs nord-américains, et demain chinois. »*

également porter préjudice aux consommateurs de notre pays en termes de prix, de qualité de service ou de protection des données personnelles. Au-delà des dysfonctionnements du marché, c'est donc bien **la souveraineté économique qui est menacée par de tels agissements**, à savoir la possibilité pour chaque entrepreneur domestique de développer son activité dans des conditions de concurrence satisfaisantes. Il ne s'agit pas de nier que les géants du numérique fournissent des services toujours plus performants, mais de mesurer que la puissance économique ne doit pas se muer en domination.

C'est pourquoi il convient d'examiner les voies et moyens de restaurer la concurrence et la possibilité d'entrer sur les marchés de l'économie numérique.

2. Le nécessaire renouvellement du droit de la concurrence.

Depuis l'été 2018, le Gouvernement a lancé, sous l'égide du Conseil national du numérique, les « États généraux des nouvelles régulations du numérique ». Au premier semestre 2019, une consultation ouverte a été mise en œuvre. Hormis la publication de certaines synthèses[1], **les États généraux n'ont pourtant, à ce jour, pas débouché sur la moindre mesure concrète**, ce que les présidents de l'Autorité de la concurrence et de l'Autorité de régulation des communications électroniques et des postes ont déploré devant votre commission.

Pourtant, un **consensus** semble se dégager sur la nécessité de mettre en œuvre une **régulation économique plus efficace du numérique**, comme en témoignent les nombreux rapports récents sur le sujet[2] et les auditions de votre commission.

Le Sénat tire depuis plusieurs années la sonnette d'alarme. **L'inaction ne doit plus être une option.** Il convient d'en finir avec l'esprit de défaite : les utilisateurs européens sont le premier marché économique pour les Gafam. C'est une force qui ne doit pas être sous-estimée. Il faut, au contraire, utiliser ce puissant levier.

a) La piste du démantèlement ne semble pas apporter de garanties suffisantes

La piste du démantèlement des géants du numérique est de plus en plus sérieusement évoquée outre-Atlantique, notamment par les élus démocrates, et particulièrement Elisabeth Warren, sénatrice et candidate à

---

[1] *Une synthèse de la consultation publique sur les thèmes « Adaptation des règles de concurrence et de régulation économique » et « Observatoire du numérique » a été publiée en mars dernier.*

[2] *On peut notamment citer, au niveau européen, le rapport de Jacques Crémer, Yves-Alexandre de Montjoye et Heike Schweitzer intitulé* Competition policy for the digital era*, publié début 2019, et au Royaume-Uni, le rapport du panel d'experts sur la concurrence numérique intitulé* Unlocking digital competition*, publié en mars dernier.*

l'investiture démocrate pour l'élection présidentielle de 2020. Elle est également défendue par Chris Hughes, le co-fondateur de Facebook, ou encore par le professeur de droit Tim Wu[1]. Le démantèlement de Google avait été demandé par le Parlement européen dès 2014[2]. Ses modalités concrètes sont cependant rarement précisées.

Si les précédents de la Standard Oil en 1911 et d'AT&T en 1982 sont régulièrement invoqués, on rappellera que Microsoft avait failli être démantelée lorsque, en juin 2000, un tribunal l'avait ordonné. La décision avait cependant été révisée en appel et l'entreprise a finalement pu passer un accord avec le Gouvernement américain en 2001… ce qui est parfois considéré comme **l'acte introductif du renoncement de la politique américaine de la concurrence**.

Comme l'a cependant rappelé Isabelle de Silva devant votre commission, cette piste ne doit pas être considérée comme la panacée d'une politique de concurrence 2.0. En effet, nombreux sont ceux qui considèrent que, **tel l'Hydre de Lerne, l'entreprise, même scindée, poursuivrait le développement de sa puissance[3]**. Selon le secrétaire d'Etat en charge du numérique Cédric O, « *l'enquête durera cinq à dix ans, et ne règlera pas tous les problèmes. Même si Facebook était divisé en dix entités, il resterait 240 millions d'utilisateurs dans chaque entité...* »[4].

Enfin, il est souvent avancé que réguler sévèrement les Gafam ou les démanteler favoriserait l'émergence des géants chinois du numérique[5] au-delà du marché asiatique. Si cet élément ne doit pas être déterminant, dans la mesure où la sévérité des autorités de la concurrence devrait être la même qu'il s'agisse des entreprises américaines, chinoises, ou européennes, il convient cependant de reconnaître qu'en l'absence de « Gafam européens », les BATX pourraient bénéficier de l'affaiblissement des Gafam sur le marché européen. Ceci est d'autant plus vrai que le démantèlement par le pouvoir chinois des BATX, au nom du respect du droit de la concurrence, est plus qu'improbable à ce jour.

---

[1] *Tim Wu,* The curse of bigness, Antitrust in the new gilded age, *2018. Tim Wu est également connu comme le penseur du concept de neutralité du net.*

[2] *La résolution du Parlement européen du 27 novembre 2014 sur le renforcement des droits des consommateurs au sein du marché unique numérique appelait la Commission européenne à* « envisager des propositions afin de séparer les moteurs de recherche des autres services commerciaux ».

[3] *Cette position est en particulier celle de la Commissaire européenne à la concurrence Magrethe Vestager, qui s'exprimait ainsi en mars dernier, lors d'une conférence de presse à Washington :* « Il y a un risque que, même si nous démantelons ces sociétés, elles redeviennent grosses très rapidement avec les effets de réseau ».

[4] *Propos tenus lors de son audition par la commission de la culture, de l'éducation et de la communication du Sénat, le 24 juillet dernier.*

[5] *Voir, par exemple, la tribune de Nicolas Bouzou,* Démanteler les Gafam : un cadeau à la Chine, *Le Figaro, lundi 12 août 2019.*

Les autorités américaines ont cependant lancé, depuis quelques mois, plusieurs actions à l'encontre des géants du numérique. Une commission de la chambre des représentants a ouvert une enquête sur la concurrence sur les marchés du numérique[1]. Le ministère de la Justice (DoJ) a lancé une vaste enquête sur les éventuels abus de position dominante des plus grandes sociétés du numérique[2]. La *Federal Trade Commission* (FTC) a condamné Facebook au paiement d'une amende record de 5 milliards de dollars[3]. Le 6 septembre 2019, neuf procureurs des Etats fédérés ont annoncé l'ouverture d'enquêtes à l'encontre de Facebook[4] sur le fondement du droit de la concurrence. Le 9 septembre 2019, 50 procureurs des Etats fédérés empruntaient la même voie concernant Google[5]. On assiste donc à un mouvement en faveur d'une plus grande régulation, ce qui crée des conditions politiques favorables à l'action de ce côté-ci de l'Atlantique.

b) Un renforcement du droit de la concurrence apparaît nécessaire

Comme l'ont démontré les récentes sanctions infligées à Google, le droit de la concurrence européen et français permet de traiter de nombreux cas d'abus. Mais un consensus semble émerger en faveur de l'introduction de certains **ajustements de l'arsenal juridique**.

À droit constant, **une notion « *quelque peu oubliée ces dernières années* »,** selon la présidente de l'Autorité de la concurrence, **celle d'abus d'exploitation** dans l'examen des pratiques anti-concurrentielles[6], devrait être davantage utilisée. Elle permettrait de répondre au « *cas de Booking prélevant des commissions sur les gains des hôteliers, ou bien d'Apple facturant une commission aux créateurs d'applications* ». Mme de Silva a également estimé que « *face aux problématiques qui découlent de l'utilisation des données, notre interprétation de ce droit doit être plus innovante que par le passé. À cet égard, la décision prise par l'équivalent allemand de l'Autorité de la concurrence peut être citée. Elle a abouti à la condamnation de Facebook pour une utilisation disproportionnée des données des utilisateurs, qui excédait largement ce qui est*

[1] *Communiqué de presse,* Judiciary Committee Launches Investigation into Competition in Digital Markets*, 3 juin 2019.*

[2] *Communiqué de presse,* Justice Department Reviewing the Practices of Market-Leading Online Platforms*, 23 juillet 2019.*

[3] *Communiqué de presse, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, 24 juillet 2019.*

[4] *Facebook est accusé de chercher à acquérir un monopole des médias sociaux empêchant l'émergence de concurrents après le rachat d'Instagram pour 1 milliard de dollars en 2012 et celui de WhatsApp pour 19 milliards en 2019.*

[5] *Une enquête antitrust a été ouverte contre l'entreprise accusée de déminer tous les aspects de la publicité et de la recherche sur internet.*

[6] *La notion de pratiques anti-concurrentielles recouvre les abus de position dominante (interdites par l'article 102 du traité sur le fonctionnement de l'Union européenne) et les ententes (prohibées par l'article 101 du même traité).*

nécessaire au bon fonctionnement du réseau social. La captation illégitime des données peut donc être sanctionnée, comme nous le démontre cette décision »[1].

Le rapport de Jacques Crémer, Yves-Alexandre de Montjoye et Heike Schweitzer intitulé *Competition policy for the digital era*, publié début 2019, plaide principalement pour une **actualisation des méthodes** utilisées par les autorités de la concurrence **à droit constant**. La direction générale des entreprises s'inscrit dans cette démarche et a souligné l'intérêt de deux recommandations de ce rapport : donner plus de poids, dans l'analyse concurrentielle, **au critère du dommage concurrentiel** et prendre en compte **l'accès aux données** dans la mesure du pouvoir de marché. À l'échelon européen, le ministre de l'économie et des finances a plaidé, devant votre commission, pour que la Commission européenne appréhende la notion de marché pertinent au niveau mondial plutôt qu'à l'échelle européenne.

Encourager les autorités de protection de la concurrence à adapter leurs méthodes aux spécificités de l'économie numérique.

Des **modifications du droit en vigueur apparaissent également nécessaires**.

Une résolution européenne adoptée par le Sénat à l'initiative de notre collègue Catherine Morin-Desailly[2] plaide en faveur d'un **assouplissement du droit européen relatif aux mesures conservatoires** applicables en cas de pratique anti-concurrentielle. Il s'agit :

- d'assouplir les critères de définition du risque d'atteinte à la concurrence résultant de la pratique en cause (« préjudice grave et irréparable ») pour prévoir le constat d'une **« atteinte grave et immédiate »** ;

- d'alléger l'obligation pour la Commission d'établir un « constat *prima facie* d'infraction » en lui substituant celle du constat que la **pratique relevée porte une telle atteinte** ;

- et **d'élargir le champ des intérêts protégés** justifiant des mesures provisoires en ne visant plus seulement l'atteinte aux règles de concurrence mais également « *à l'économie générale, à celle du secteur intéressé, à l'intérêt des consommateurs ou à l'entreprise plaignante* ».

---

[1] *Voir le communiqué de presse en anglais du Bundeskartellamt en date du 7 février 2019 :* Bundeskartellamt prohibits Facebook from combining user data from different sources.

[2] *Résolution européenne pour une réforme des conditions d'utilisation des mesures conservatoires prévues par le règlement (CE) n° 1/2003 du Conseil relatif à la mise en oeuvre des règles de concurrence, 8 septembre 2017. Ce constat a d'ailleurs été corroboré pour les autorités nationales par un référé de la Cour des comptes en date du 14 mars 2019 (*Politique de la concurrence – L'action de l'autorité de la concurrence et de la direction générale de la concurrence, de la consommation et de la répression des fraudes*), qui dénonce un délai de traitement de cinq ans en moyenne par l'Autorité de la concurrence.*

Cette recommandation[1] est toujours d'actualité et a depuis été confortée par un récent rapport d'inspection sur la politique de la concurrence[2].

Permettre à la Commission européenne de recourir plus facilement à des **mesures conservatoires en cas de pratique anti-concurrentielles, lorsque l'urgence le justifie**.

La **directive européenne dite « ECN + »**[3], publiée en janvier 2019, sur les pouvoirs des autorités nationales de concurrence, constitue un progrès, car elle permet à ces autorités de prononcer des **injonctions structurelles** – par exemple, l'obligation de céder une branche d'activité – dans le cadre des sanctions qu'elles infligent du fait de pratiques anti-concurrentielles. Il conviendrait de procéder rapidement à sa transposition[4].

Transposer rapidement la directive ECN +.

Un ajustement du **droit des concentrations**[5] apparaît également nécessaire. Ce droit permet aux autorités de la concurrence d'empêcher un rapprochement d'entreprises dont les effets pourraient être anti-concurrentiels. Afin de lutter efficacement contre les acquisitions « prédatrices », la présidente de l'Autorité de la concurrence a rappelé, devant votre commission, qu'elle propose « *de compléter la loi française pour les entreprises du numérique, en abaissant les seuils de chiffre d'affaires impliquant l'obtention d'une autorisation* »[6].

Il pourrait également être intéressant d'introduire un **nouveau seuil basé sur la valeur de rachat** qui peut être un meilleur indicateur que le

---

[1] *Il s'agit de modifier l'article 8 du règlement (CE) n° 1/2003 du Conseil du 16 décembre 2002 relatif à la mise en œuvre des règles de concurrence prévues aux articles 81 et 82 du traité.*

[2] *Inspection générale des finances, Conseil général de l'économie, de l'industrie, de l'énergie et des technologies,* La politique de la concurrence et les intérêts stratégiques de l'Union européenne, *avril 2019.*

[3] *Directive (UE) 2019/1 du Parlement européen et du Conseil du 11 décembre 2018 visant à doter les autorités de concurrence des États membres des moyens de mettre en œuvre plus efficacement les règles de concurrence et à garantir le bon fonctionnement du marché intérieur.*

[4] *L'article 211 de la loi PACTE prévoyait sa transposition par voie d'ordonnance, mais cette disposition a été censurée car considérée comme un cavalier législatif par le Conseil constitutionnel dans sa décision n° 2019-781 DC du 16 mai 2019.*

[5] *Au niveau européen, les règles en matière de concentration sont déterminées par le règlement (CE) n° 139/2004 du Conseil du 20 janvier 2004 relatif au contrôle des concentrations entre entreprises. Pour une description du droit français des concentrations, voir la page suivante, sur le site internet de l'Autorité :*
http://www.autoritedelaconcurrence.fr/user/standard.php?lang=fr&id_rub=296&id_article=1018

[6] *Ces seuils sont déterminés par l'article L. 430-2 du code de la concurrence.*

chiffre d'affaires. En effet, alors que WhatsApp réalisait un chiffre d'affaires de l'ordre de 20 millions de dollars, Facebook l'a acquis pour 19 milliards de dollars[1]. Un tel critère est déjà en vigueur en Allemagne et en Autriche[2].

Le rapport d'inspection précité sur la politique de la concurrence propose d'instaurer **un contrôle *ex post*** des concentrations pour lesquelles le **ratio de la valeur de la transaction au chiffre d'affaires** de l'entreprise achetée suggère un possible enjeu concurrentiel[3]. Lors des auditions de votre commission, le ministre de l'économie et des finances s'est d'ailleurs déclaré favorable à un contrôle *ex post* des opérations de fusion entre entreprises européennes.

Afin de lutter contre les « acquisitions prédatrices » et les effets de concentration, une **révision du champ d'application du contrôle des concentrations** apparaît nécessaire.

3. L'émergence de nouvelles régulations sectorielles, et d'un cadre général de régulation *ex ante*

a) De premières initiatives encourageantes amenées à être complétées ?

Plusieurs initiatives législatives récentes, et pour certaines encore en cours de discussion, ont contribué à renouveler la régulation des acteurs du numérique (désignés soit de façon classique comme intermédiaires techniques – hébergeurs, fournisseurs d'accès, moteurs de recherche – soit au travers de la création de nouvelles catégories juridiques – « plateformes », « fournisseurs de service numérique »…). **Il s'agit ainsi de leur imposer, de façon proactive, de nouveaux types d'obligations pour un objectif donné d'intérêt général** qui englobe et dépasse la simple application des règles du droit de la concurrence (protection du consommateur, préservation de la liberté d'expression, de la libre expression du suffrage…).

Ces initiatives ont pour point commun d'imposer au moins en partie des obligations de transparence et de moyens à certains acteurs majeurs ou systémiques (*via*, par exemple, la définition de seuils élevés de connections depuis la France ou de volume de chiffres d'affaires). Elles constituent ainsi **les premières bases d'une régulation proactive et dédiée à l'encadrement des acteurs systémiques du numérique** (elles sont présentées dans l'encadré suivant)**.**

---

[1] *On peut également citer le cas du rachat de Waze par Google, qui avait cependant fait l'objet d'un examen par l'autorité de la concurrence britannique.*

[2] *Voir Bundeskartellamt et Bundes Wettbewerbs Behörde,* Guidance on transaction value threshold for mandatory pre-merger notification*, juillet 2018.*

[3] *Rapport d'inspection précité, intitulé* « La politique de la concurrence et les intérêts stratégiques de l'Union européenne ».

De premiers exemples d'obligations proactives sectorielles

Pour s'assurer de la **protection des consommateurs**, la loi pour une République numérique du 7 octobre 2016 impose une obligation de loyauté, de clarté et de transparence des plateformes (cette disposition est précisée plus loin dans le présent rapport).

Pour contribuer au respect par les intermédiaires numériques de leurs **obligations sociales et fiscales**, la loi relative à la lutte contre la fraude du 23 octobre 2018 renforce la responsabilité sociale des plateformes et crée des obligations déclaratives sur les revenus des utilisateurs.

Pour protéger l'i**ntégrité des processus électoraux** nationaux contre les manipulations et les infox (« fake news »), la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information impose la transparence des publicités à caractère politique en période électorale et crée une obligation générale de coopération, sous le contrôle du Conseil supérieur de l'audiovisuel (CSA).

Dans le domaine de la **lutte contre les abus de la liberté d'expression**, plusieurs initiatives sectorielles sont également en cours d'examen, tant au niveau national (proposition de loi visant à lutter contre la haine sur internet) qu'au niveau européen (proposition de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne).

Alors que certains de ces régimes sont désormais en place depuis plus d'un an, **votre rapporteur invite le Gouvernement à présenter un premier bilan de leur application**.

Dresser un **bilan** des premières initiatives de régulations sectorielles des acteurs systémiques du numérique.

D'autres dispositifs de régulation des géants du numérique ont également été proposés. Lors des débats relatifs à la loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques, **le Sénat** avait adopté un amendement proposé par notre collègue Catherine Morin-Desailly et cosigné par notre collègue Bruno Retailleau qui confiait à l'Arcep une **mission de régulation des moteurs de recherche**[1]. Une résolution européenne[2] adoptée par le Sénat à l'initiative de notre collègue Catherine Morin-Desailly a appelé « *à mettre en place des agences d'évaluation et de notation des plateformes* ».

Partant du constat selon lequel « *notre situation démontre un échec cuisant de toutes les autorités publiques à créer un véritable jeu concurrentiel dans le secteur entre les plateformes du numérique* », le président de **l'Arcep** a rappelé, devant votre commission, le **projet de régulation des terminaux**

[1] *Amendement n° 995 rectifié, de Mme Morin-Desailly, MM. Retailleau, Bizet et Lenoir, Mme Jouanno et les membres du groupe Union des Démocrates et Indépendants – UC.*

[2] *Résolution européenne pour une stratégie européenne du numérique globale, offensive et ambitieuse, 30 juin 2015.*

(ordinateurs, *smartphones*, enceintes, voitures ou télévisions connectées) proposé par l'Autorité[1]. Ce projet consisterait à étendre aux terminaux la portée du **principe de neutralité du net** établi au niveau européen[2] et transposé en droit français par la loi pour une République numérique. Ce principe, selon M. Soriano, permet de « *réguler la tuyauterie d'internet* » (les réseaux déployés par les opérateurs de communications électroniques), mais reste aveugle sur « *les robinets* » (les terminaux). On peut ainsi lire dans le rapport de l'Autorité que le principe « *du libre choix des contenus mis à disposition ou consommés en ligne* », doit « *s'appliquer non seulement au niveau des réseaux, mais également au niveau des terminaux* ». Le cas d'application par excellence est celui des systèmes d'exploitation des téléphones intelligents : ce marché est structuré en un duopole détenu par Google et Apple. Cette domination donne lieu à des pratiques restreignant le choix des utilisateurs, comme un filtrage des applications par les magasins d'application ou l'impossibilité de désinstaller des applications préinstallées, ce qui rend le marché captif.

Un régulateur devrait être chargé de mettre en œuvre ce principe, en élaborant, pour reprendre les termes utilisés par le président de l'Arcep devant votre commission, « *un agenda avec des objectifs précis et en vérifi(ant) sa bonne application en continu* », en collectant des informations auprès des acteurs et en réglant les différends pouvant naître entre les utilisateurs et les fournisseurs de terminaux, systèmes d'exploitation, magasins d'application ou assistants vocaux.

Votre rapporteur estime qu'une telle piste mérite d'être étudiée. Elle rejoint d'ailleurs les recommandations des rapports de notre collègue Catherine Morin-Desailly sur *l'Union européenne, colonie du monde numérique*[3] et sur *l'Europe au secours de l'Internet* ainsi que celles du Conseil national du numérique[4] selon lesquelles le **principe de neutralité devait être étendu aux services et applications sur internet**. Il conviendrait de s'assurer de sa compatibilité avec le droit européen (notamment la libre circulation des services) et avec le droit constitutionnel (notamment la liberté d'entreprendre).

Étudier la faisabilité de **l'extension du principe de neutralité du net aux terminaux**.

---

[1] *Voir, par exemple,* Arcep, Les terminaux, maillon faible de l'ouverture d'internet, *février 2018.*

[2] *Règlement 2015/2120 du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert.*

[3] L'Union européenne, colonie du monde numérique ?, *Rapport d'information n° 443 (2012-2013) de Mme Catherine Morin-Desailly, fait au nom de la commission des affaires européennes, déposé le 20 mars 2013. Lien vers le rapport :* https://www.senat.fr/notice-rapport/2012/r12-443-notice.html

[4] *Avis n° 2013-1 Net Neutralité du 1er mars 2013.*

b) Établir un cadre général de régulation ex ante *des acteurs systémiques*

Tirant les enseignements de ces premières initiatives et prenant acte du fait que si les adaptations du droit de la concurrence sont nécessaires et doivent être menées à terme, ces mesures ne pourront toutefois pas répondre à elles seules à toutes les problématiques de souveraineté numérique, il semble désormais souhaitable d'**adopter un cadre général de régulation *ex ante*** des acteurs systémiques du numérique.

L'idée **d'imposer des obligations proactives, spécifiques et multisectorielles aux acteurs systémiques du numérique** commence à être explicitement envisagée au sein de l'administration – elle est expressément préconisée dans les réflexions menées par certains corps d'inspection[1], et elle est réclamée par la société civile comme par les régulateurs – en témoignent les conclusions des « Etats généraux des nouvelles régulations du numérique »[2]. Dans la résolution européenne précitée, le Sénat appelait d'ailleurs à « *adopter de nouvelles règles destinées à encadrer spécifiquement les plateformes numériques structurantes pour l'économie* »**.**

Votre rapporteur note que c'est un sujet sur lequel le secrétaire d'État au numérique, M. Cédric O, s'est montré ouvert devant notre commission, puisque selon lui : « *Le sujet n'est pas de savoir s'il faut une régulation spécifique sur les données, sur la vie privée, sur les contenus haineux, sur les rapports entre fournisseurs et sous-traitants, etc.* ***Dès lors qu'un acteur est une brique de base de l'économie, alors une régulation systémique****, qui peut ressembler à la régulation bancaire,* ***à base de supervision, de régulateur technique dédié et de capacité technologique du régulateur au bon niveau, doit être développée****.* »

Comme l'ont relevé tous deux les présidents de l'Arcep et de l'Autorité de la concurrence, **il est regrettable qu'aucune suite concrète n'ait encore été donnée à l'heure actuelle à ces préconisations** ni aux riches propositions formulées dans le cadre des Etats généraux des nouvelles régulations du numérique, **le Gouvernement semblant renvoyer au seul échelon européen la responsabilité d'agir en la matière**. Votre rapporteur estime à tout le moins que les travaux de la direction générale des entreprises (DGE)[3] pour identifier les acteurs systémiques du numérique et définir les types de règles qui pourraient leur être imposés devraient être menés rapidement à leur terme et publiés (l'encadré suivant détaille les modalités de mises en œuvre de ces deux objectifs).

---

[1] « Les limites de l'application [du droit de la concurrence] suscitent beaucoup de débats aujourd'hui et conduisent à penser d'autres modalités de régulation, comme par exemple une régulation proactive asymétrique des acteurs du numérique, sur le modèle mis en place dans le secteur des télécoms » (La politique de la concurrence et les intérêts stratégiques de l'UE, *rapport au ministre de l'économie et des finances, IGF-CGE, juin 2019).*

[2] « *Envisager une régulation sectorielle et proactive des acteurs systémiques du numérique* », https://egnum.cnnumerique.fr

[3] *Comme son directeur l'a indiqué en réponse à plusieurs questions écrites.*

Imposer des obligations proactives, spécifiques et multisectorielles aux acteurs systémiques du numérique :

- **Identifier les acteurs essentiels du numérique** et **établir un faisceau d'indices permettant de définir leur caractère « systémique »** ; en ce sens, une série d'indicateurs pourraient être envisagée (existence d'effets de réseaux massifs ; maîtrise d'un volume considérable de données non réplicables ; situation incontournable sur un marché multifaces ou capacité de l'acteur à définir lui-même les règles de marché ; aptitude de l'acteur à placer le régulateur en forte position d'asymétrie d'information ; effets globaux sur la collectivité hors champ économique et pouvoir d'influence sur des pans sensibles du lien social – discours haineux, *fake news*, protection des données personnelles, cybersécurité, etc.) ;

- **Définir de nouvelles obligations établies de façon proactive dont le respect devrait être assuré, en sus des règles de concurrence** (transparence de l'activité ; obligation de ménager dans des conditions équitables l'accès à d'autres acteurs pour certains types de données ; renforcement de la portabilité des données et de l'interopérabilité des plateformes ; auditabilité – accès des chercheurs – et redevabilité des algorithmes utilisés - transparence et intelligibilité, conformité à la loi, non-discrimination, loyauté…).

4. Un renforcement de la transparence de l'économie numérique.

a) Accroître la transparence : une tendance affirmée

La réglementation récente tend vers davantage de transparence dans les relations des plateformes avec les consommateurs et les professionnels. Des dispositions normatives aux niveaux français et européens ont en effet été adoptées ces dernières années pour renforcer l'information des consommateurs puis des professionnels ayant recours aux plateformes. Il conviendrait de s'assurer de leur bonne mise en œuvre.

(1) La transparence envers les consommateurs : le nécessaire bilan d'application de la loi pour une République numérique.

La loi pour une République numérique[1] impose aux plateformes des **obligations de loyauté et de transparence** afin de permettre aux **consommateurs** d'accéder à des informations claires, objectives et

[1] *Articles 49, 50 et 52, complétés par les décrets n° 2017-1434 du 29 septembre 2017 relatif aux obligations d'information des opérateurs de plateformes numériques, n° 2017-1435 du 29 septembre 2017 relatif à la fixation d'un seuil de connexions à partir duquel les opérateurs de plateformes en ligne élaborent et diffusent des bonnes pratiques pour renforcer la loyauté, la clarté et la transparence des informations transmises aux consommateurs et n° 2017-1436 du 29 septembre 2017 relatif aux obligations d'information relatives aux avis en ligne de consommateurs.*

transparentes. L'objectif est de mieux **équilibrer les relations entre plateformes et consommateurs** :

- les plateformes qui valorisent des contenus, des biens ou des services proposés par des tiers, tels que les moteurs de recherche, réseaux sociaux ou comparateurs, doivent préciser les **critères de référencement et de classement** qu'elles utilisent ;

- les sites publiant des **avis** de consommateurs doivent préciser s'ils ont été vérifiés et selon quelle **méthodologie** ;

- les places de marchés et sites d'économie collaborative doivent fournir des **informations essentielles qui peuvent orienter les choix des consommateurs** : la qualité du vendeur, le montant des frais de mise en relation facturés par la plateforme, l'existence d'un droit de rétractation, l'existence d'une garantie légale de conformité ou encore les modalités de règlement des litiges.

Par ailleurs, les plateformes affichant plus de 5 millions de visiteurs uniques mensuels sont tenues, depuis le 1er janvier 2019, d'**adopter de bonnes pratiques** visant à accroître la clarté, la transparence et la loyauté de leurs offres en ligne.

Votre rapporteur **déplore le délai de mise en œuvre de la loi** : bien que celle-ci date du 7 octobre 2016, le décret d'application de la disposition relative aux bonnes pratiques n'est entré en vigueur qu'au 1er janvier 2019, soit près de deux ans et trois mois après l'adoption de la disposition législative. Il note qu'un premier bilan est en cours à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), et souhaite que ce dernier soit communiqué rapidement au Parlement.

Dresser rapidement le bilan de l'application des principes de loyauté et de transparence des plateformes issus de la loi pour une République numérique.

(2) La transparence envers les professionnels : l'entrée en vigueur à venir du règlement européen dit « *Platform-to-business* ».

Le règlement dit « *Platform-to-business* »[1] publié au journal officiel de l'Union européenne le 11 juillet 2019 vise à renforcer la transparence des plateformes pour leurs utilisateurs professionnels.

Il prévoit deux grandes séries de mesures pour équilibrer les relations entre plateformes et entreprises : en amont, des **obligations d'information et de transparence** – sur les clauses contractuelles, sur les paramètres utilisés par les algorithmes de classement ; en aval, des

[1] *Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne.*

dispositifs de résolution des litiges et de médiation entre plateformes et professionnels – système interne de traitement des plaintes, désignation d'un médiateur, possibilité pour les associations représentatives et des organismes publics de saisir les juridictions en vue de faire cesser ou d'interdire tout manquement aux exigences édictées par le règlement.

Ce règlement entrera en vigueur le 12 juillet 2020. La Commission doit encourager l'élaboration de codes de conduite pour garantir une bonne application du règlement. En France, **le Gouvernement a coordonné l'élaboration, avec les grandes places de marché, d'une charte** signée en mars dernier[1] qui contient de nombreuses dispositions proches de celles du règlement, en attendant son entrée en vigueur. Mais la principale plateforme concernée, à savoir Amazon, n'en est pas signataire ! Il en est de même pour le géant chinois Alibaba. Il faudra donc finalement **attendre l'entrée en vigueur de la réglementation au niveau européen pour que les géants du secteur soient concernés.**

Le règlement constitue la **première pierre d'un édifice de transparence de l'économie numérique au niveau européen**. Cependant, il se limite à la transparence, **sans envisager d'agir sur les pratiques –** ce qui justifie d'ailleurs, par exemple, la proposition formulée par l'Arcep relative à la régulation des terminaux déjà évoquée. Il ne permet pas non plus d'aborder **les distorsions de régulation entre le commerce physique et le commerce en ligne** : l'absence de contraintes imposées au géant du numérique Amazon[2] contraste avec la lourdeur des règles pesant sur la grande distribution physique. Il est aujourd'hui **urgent d'harmoniser le cadre fiscal[3] et réglementaire** dans lequel ces deux formes de commerce évoluent. Enfin, il convient de saluer l'action du ministère de l'Économie[4] tendant à supprimer des clauses contractuelles que la place de marché d'Amazon impose à ses partenaires commerciaux et qui créent un déséquilibre significatif dans les droits et obligations des parties[5].

---

[1] *Charte des acteurs du e-commerce, 26 mars 2019.*

[2] *Au contraire de contraintes, ce sont même des facilités qui sont accordées à Amazon par les collectivités locales lorsque l'entreprise souhaite implanter un entrepôt, selon une forme de chantage décrit, par exemple, dans une série d'articles récents du site Reporterre.net (Reporterre.net, Le plan secret d'Amazon en France, 2 juillet 2019).*

[3] *Une mission sur ce thème avait été confiée à l'inspection générale des finances en 2018. Ses conclusions n'ont pas été rendues publiques.*

[4] *Voir, par exemple, le communiqué de presse du ministère de l'économie et des finances en date du 4 septembre dernier intitulé «* pratiques commerciales des plateformes numériques : le tribunal de commerce de Paris sanctionne Amazon dans le cadre d'une procédure initiée par Bruno le Maire et lui impose de revoir ses conditions générales d'utilisation *». Le tribunal de commerce de Paris a ainsi condamné le groupe Amazon à modifier sous six mois et sous astreinte plusieurs clauses des conditions générales d'utilisation de sa place de marché et à payer une amende de 4 millions d'euros.*

[5] *Conformément aux termes de l'article L. 442-6 du code de commerce. Une action similaire a été engagée à l'encontre d'Apple et de Google le 14 mars 2018.*

Étudier l'harmonisation du cadre fiscal et réglementaire du commerce et du e-commerce.

b) Auditer les algorithmes plutôt que les rendre publics

Les algorithmes sont sujets à de nombreux biais. Ils font également l'objet d'une attention croissante au regard de leurs potentiels effets anti-concurrentiels[1]. Notre collègue Joëlle Garriaud-Maylam a d'ailleurs récemment interrogé le Gouvernement[2] sur l'éventuelle création d'une autorité de régulation des algorithmes. À ce jour, cette question n'a pas reçu de réponse.

Plusieurs voix s'élèvent pour demander la publication des algorithmes. Mais, comme l'a rappelé Claire Mathieu lors de son audition devant votre commission[3], un algorithme peut être protégé en tant qu'information par le secret des affaires[4], selon les modalités prévues par la loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires. De plus, une fois publié, un algorithme peut être contourné. Les entreprises connaissant les critères de référencement, et particulièrement celles disposant d'une puissance de calcul suffisante, pourraient leurrer l'algorithme pour améliorer leur classement. Enfin, ce sont surtout, d'une part, **la connaissance des données et des résultats**, et d'autre part, celle des **principes et méthodes** de constitution de l'algorithme qui permettent une meilleure compréhension de son fonctionnement. Le rapport de notre collègue député Cédric Villani sur l'intelligence artificielle rappelait que, quand bien même les algorithmes seraient rendus publics, les algorithmes d'apprentissage profond (*deep learning*) sont soumis au **phénomène de la « boîte noire »** : on connait les données d'entrées et les données de sortie, mais on n'en comprend pas le fonctionnement interne.

L'explicabilité de ces algorithmes est pourtant bien l'une des conditions de leur acceptabilité sociale. S'il ne paraît ni réaliste ni judicieux de prévoir la publication des algorithmes, il faut en organiser **l'auditabilité** afin de garantir le respect des règles de concurrence, la protection des données, etc.

Cela **suppose que les autorités publiques se dotent des moyens humains et techniques** en ce sens. Le rapport du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies intitulé *Modalités de régulation des algorithmes de traitement des contenus* et publié en mai 2016 recommandait d'ailleurs, sur le modèle américain de l'*Office of Technology*

[1] *L'Autorité de la concurrence française et le Bundeskartellamt allemand ont lancé, en juin 2018, un projet conjoint sur les algorithmes et leurs enjeux pour l'application du droit de la concurrence (source : communiqué de presse du 19 juin 2018).*

[2] *Question écrite n° 11170, 27 juin 2019.*

[3] *Audition du 12 juin 2019.*

[4] *Sauf à être intégré dans un logiciel protégé par le droit d'auteur ou dans une invention protégée par un brevet, auxquels cas il bénéficie du régime du droit d'auteur ou du brevet.*

Research and Investigation crée en mars 2015 au sein de la *Federal Trade Commission*, de créer un **bureau spécialisé des technologies de contrôle de l'économie numérique,** chargé de développer et de mettre en œuvre des techniques de contrôle adaptées à un ensemble de thèmes nouveaux de l'économie numérique. Ce bureau, qui serait par exemple localisé au sein de la DGCCRF[1], pourrait être saisi par l'ensemble de la communauté intéressée, notamment les autorités administratives indépendantes.

Sur ce point, le rapport de notre collègue député Cédric Villani envisageait la constitution d'un corps d'experts publics assermentés en mesure de procéder à des audits, qui pourraient être saisis à l'occasion d'enquêtes ou de contentieux administratifs ou judiciaires. Reconnaissant qu'aujourd'hui, « *personne dans l'État n'est capable de parler avec les programmateurs de Facebook* », le secrétaire d'État en charge du numérique a considéré, devant votre commission d'enquête, que « *l'État doit être au bon niveau technologique pour comprendre, tester, décoder voire infirmer le fonctionnement des algorithmes* ».

Votre rapporteur note avec intérêt que le Gouvernement a fait de la transparence des algorithmes l'un de ses axes de politique de l'innovation : c'est l'un des « **grands défis »**[2] sélectionnés par le Conseil de l'innovation de juillet 2018 ayant vocation à être financé par le fonds pour l'innovation et l'industrie à hauteur de 30 millions d'euros sur trois ans porte précisément sur « *la sécurisation, la certification et la fiabilisation des algorithmes* »[3].

Prévoir **que les autorités compétentes** (qu'elles soient judiciaires ou administratives) **puissent accéder**, dans le cadre de leurs fonctions, **aux principes et méthodes de constitution des algorithmes ainsi qu'aux données sur lesquels** ils se basent pour éviter l'asymétrie d'information entre les régulateurs et les régulés. Créer au sein de la DGCCRF un bureau idoine.

c) Favoriser la régulation par la donnée

Le 8 juillet 2019, sept autorités administratives indépendantes ont publié[4], sous l'égide de l'Arcep, une note sur la **régulation par la donnée**. La

[1] *Direction générale de la concurrence, de la consommation et de la répression des fraudes.*

[2] *Sur le modèle des agences de l'innovation américaines, qui privilégient la réalisation de défis plutôt que l'octroi de subventions selon une grille d'analyse calée sur les secteurs économiques existants. L'ambition de ces défis est de permettre la création de nouveaux marchés sur lesquels la France pourrait prendre l'avantage.*

[3] *La stratégie économique en intelligence artificielle publiée le 3 juillet dernier décrit ainsi ce défi :* « ce défi vise à assurer la transparence et l'auditabilité des systèmes autonomes à base d'IA, d'une part en développant les capacités nécessaires pour observer, comprendre et auditer leur fonctionnement et d'autre part, en développant des approches démontrant le caractère explicable de leur fonctionnement ».

[4] *L'Autorité de la concurrence, l'Autorité des marchés financiers, l'Autorité de régulation des infrastructures ferroviaires et routières, l'Arcep, la CNIL, la Commission de régulation de l'énergie et le Conseil supérieur de l'Audiovisuel.*

régulation par la donnée viendrait ainsi compléter les outils traditionnels du régulateur. Au lieu de prescrire aux acteurs économiques un comportement, il s'agit de **créer un réseau d'informations et d'incitations pour réduire les asymétries d'information et démultiplier l'impact de l'action du régulateur** en mobilisant les utilisateurs et leurs relais.

Comme l'a rappelé le président de l'Arcep lors de son audition par votre commission, une telle régulation aurait deux objectifs :

- amplifier la capacité d'action du régulateur, notamment dans une logique de supervision, à travers une la détection de signaux faibles et de risques systémiques comme le fait par exemple déjà l'Autorité des marchés financiers ;

- éclairer les choix des utilisateurs et mieux orienter le marché, comme le fait par exemple l'Arcep en publiant les données relatives à la couverture numérique du territoire.

Concrètement, cette politique doit être menée par le recueil de données auprès des opérateurs contrôlés – ce qui suppose un pouvoir du régulateur pour imposer la transmission de données –, les signalements des utilisateurs et les applications d'externalisation ouverte (*crowdsourcing*).

Il convient, à nouveau, de souligner que la mise en place d'une politique efficace de régulation par la donnée suppose cependant que les **régulateurs se dotent des compétences humaines et des moyens techniques**.

Votre rapporteur soutient cette démarche et appelle à sa généralisation.

d) Renforcer l'observatoire de l'économie des plateformes en ligne créé au niveau européen

Votre rapporteur souhaite rappeler, à titre préalable, que l'article 29 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique prévoyait la remise d'un rapport du Gouvernement au Parlement, dans un délai de trois mois à compter de sa promulgation, sur la possibilité de créer un **commissariat à la souveraineté numérique**. Aucun document n'ayant été adressé aux assemblées parlementaires en près de trois ans, votre rapporteur en a demandé communication au titre de ses pouvoirs de contrôle sur pièce et a eu la surprise de constater que ce rapport avait bien été rédigé en mars 2017 sans pourtant qu'aucune suite ne lui soit donnée, qu'aucune évaluation des propositions ne soit entreprise, ni même que le Parlement ne soit informé de son existence[1]… C'est pourquoi votre rapporteur a souhaité le publier en annexe au présent rapport.

[1] *Rapport étudiant la possibilité de créer un commissariat à la souveraineté numérique, mars 2017 (ce document figure en annexe du présent rapport).*

Afin de renforcer l'information disponible sur les pratiques des entreprises du numérique à l'égard de leurs utilisateurs – professionnels ou non, le Gouvernement a mis en consultation, dans le cadre des états généraux, la proposition de créer, désormais, un « **observatoire du numérique** ».

Cette proposition n'a pas fait consensus, notamment en raison de l'existence d'un observatoire au niveau européen.

L'observatoire européen sur l'économie des plateformes en ligne

Le 26 avril 2018, la Commission européenne a publié une décision installant un Observatoire sur l'économie des plateformes en ligne. Composé de 15 membres, il est rattaché à une direction générale de la Commission Européenne, qui en assure le secrétariat. Il a tenu sa première réunion le 27 septembre 2018.

Sa mission est de conseiller et de mettre son expertise à disposition de la Commission européenne sur l'évolution de l'économie des plateformes en ligne, en particulier sur les potentielles pratiques abusives dans les relations commerciales entre les plateformes et leurs utilisateurs professionnels. Il peut notamment se pencher sur les décisions prises par algorithmes, l'accès et l'utilisation des données, la rémunération des résultats de recherche, la transparence dans les relations d'affaires, le traitement différencié des biens et services…

Il existe pour l'instant assez peu de données sur l'activité de l'observatoire : l'entreprise *Open evidence* a remporté un appel à projets pour réaliser une étude sur l'économie des plateformes en ligne… qui devrait s'étendre jusqu'à 2021 !

Ainsi, s'il ne fait aucun doute qu'il est nécessaire de renforcer l'information disponible des autorités publiques sur les grands acteurs du numérique, les modalités de mise en œuvre de cette orientation restent ouvertes. Il semble, dans ce contexte, plus avisé de permettre aux régulateurs et aux administrations compétentes d'imposer aux opérateurs de leurs **transmettre toute information nécessaire à l'exercice de leurs compétences**, sur le modèle de ce qu'a fait l'Arcep en matière de couverture du territoire dans une logique de régulation par la donnée[1].

Avant de créer un observatoire des plateformes, il est préférable de **généraliser l'obligation de transmission d'informations pertinentes** aux autorités publiques par les plateformes.

Au niveau européen, en revanche, il pourrait être envisagé, comme suggéré par Benoît Thieulin devant votre commission, de **renforcer l'observatoire des plateformes pour en faire une agence européenne d'évaluation des plateformes** réunissant des équipes d'ingénieurs « *afin de savoir précisément*

[1] *Voir, par exemple, la décision n° 2018 – 0169 de l'Autorité de régulation des communications électroniques et des postes en date du 22 février 2018 relative aux contenus et aux modalités de publication de cartes de couvertures des réseaux et des services d'accès à internet en situation fixe, et aux modalités de transmission des informations sous-jacentes.*

ce qui se passe dans ces boîtes noires que sont les plateformes ». Cette proposition rejoint celle formulée en 2015 par le Conseil national du numérique dans son rapport *Ambition numérique*, qui préconisait de créer une agence de notation européenne de la loyauté des plateformes.

C. PRÉSERVER NOTRE ORDRE JURIDIQUE EN RENFORÇANT NOTRE MAÎTRISE DES DONNÉES ET NOTRE CAPACITÉ À RÉGULER LES PLATEFORMES

1. La souveraineté de l'État remise en cause par la « révolution des données »

a) Les données, matière première du cyberespace

Les données, et tout particulièrement les données personnelles, sont **la matière première de la société de l'information**. À ce titre, elles représentent **un enjeu économique stratégique** et forment désormais, non pas le « pétrole »[1] mais bien un « terreau » – selon l'image reprise devant notre commission par Mme Marie-Laure Denis, présidente de la CNIL – pour l'activité de tous les grands acteurs de l'économie numérique[2].

C'est en effet **la nature particulière des données qui fait toute la singularité de la révolution numériqu**e : contrairement aux précédentes grandes transformations industrielles fondées sur la découverte et l'exploitation de ressources physiques nouvelles mais limitées, **les gisements de données ne se tarissent pas avec le temps ou l'usage qui en est fait**.

D'une part, la numérisation croissante et la dématérialisation irréversible de pans entiers des secteurs des biens et services contribue à alimenter constamment **une production exponentielle de données** : cette dernière est le fruit de l'activité des individus eux-mêmes (les citoyens par leur activité sur les réseaux sociaux, les consommateurs par leurs achats en ligne), mais aussi des entreprises et des institutions (à travers leurs activités de production, de gestion ou d'administration), et elle découle même passivement des capteurs analysant de façon routinière et automatisée notre environnement quotidien (objets connectés, « véhicules intelligents »…)

D'autre part ces données constituent **un bien « non rival »**, au sens économique du terme : le fait qu'elles soient utilisées – analysées, recoupées

---

[1] *En ce sens, voir l'introduction du rapport du groupe de travail franco-britannique sur l'économie de la donnée (2016), consultable en ligne à l'adresse suivante : https://www.modernisation.gouv.fr/sites/default/files/fichiers-attaches/rapport_revolution-donnee_juillet2016_vf.pdf*

[2] *Le rapport sur la fiscalité du numérique précité rappelait que* « les données, en particulier les données personnelles sont au cœur de tous les modèles d'affaires de l'économie numérique. Chacun diffère dans les modalités de collecte et de traitement de ces données. Mais tous en font levier pour améliorer leur offre, réaliser des gains de productivité, diversifier leurs activités ou renforcer leur position sur les différentes faces du modèle d'affaires ».

– une fois par un acteur n'empêche normalement pas une utilisation simultanée, voire ultérieure, par un autre acteur.

La valorisation de ces données résulte essentiellement de leur traitement et de leur mise en relation : agrégation, rapprochements de jeux de données de sources diverses, analyses, extrapolations. Prise isolément, une donnée ne génère en effet généralement que très peu de valeur.

Aux capacités de recueil et d'accumulation de données désormais sans précédent correspond ainsi **le développement de nouvelles technologies de traitement par les grands acteurs du numérique** : agrégation à très grande échelle et traitements massifs (*big data*), algorithmes comprenant des mécanismes d'apprentissage automatique (*machine learning*), recours à l'intelligence artificielle… Or l'**exploitation massive de données est permise par la diminution du coût** de traitement déjà décrite dans le rapport de la mission commune d'information sur l'Europe au secours de l'Internet[1]. Comme l'a souligné M. Thierry Breton, président-directeur général d'ATOS, lors de son audition, le coût du stockage des données et de la puissance de calcul continuent à diminuer drastiquement grâce aux progrès technologiques[2].

La valeur générée par la « révolution des données » tient aux nouvelles possibilités offertes aux acteurs économiques :

- création de **nouveaux services numériques**, mais également, même pour les secteurs traditionnels de l'économie, **gains d'efficacité dans la production de biens ou la prestation de services** (par l'amélioration de l'allocation des ressources et la réduction des coûts de transaction)[3] ;

- possibilité de **personnalisation extrême** des services afin d'en accroître la qualité ou la rentabilité (adaptation et ciblage de l'offre, profilage publicitaire), analyse prédictive visant à étayer la prise de décision ou l'investissement…

---

[1] *Catherine Morin-Desailly, L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne, juillet 2014. Ce rapport rappelait notamment les deux lois ayant permis, selon Pierre Bellanger, cette explosion des données, à savoir la loi de Moore, d'une part (selon laquelle* « à prix égal, la capacité de calcul d'un microprocesseur, matérialisée par la densité de transistors sur une puce, double tous les dix-huit mois – ce qui est également vrai pour la bande passante et pour la mémoire de stockage des données »*), et le calcul de Grötschel, d'autre part (selon lequel* « la vitesse de calcul des machines, grâce à la croissance de l'efficacité des algorithmes – séquence d'instructions d'un programme informatique – progresse quarante-trois fois plus vite que la loi de Moore »*).*

[2] *« La progression de cet espace [informationnel] obéit également à la Loi de Moore, selon laquelle les capacités des microprocesseurs sont multipliées par deux tous les dix-huit mois, tandis que les coûts en sont divisés par deux ».*

[3] *Selon l'OCDE, les entreprises utilisant des innovations basées sur l'utilisation de données bénéficient d'une productivité 5 à 10% plus élevée que les autres (OCDE, Big data : bringing competition policy to the digital era, novembre 2016).*

- accentuation des **positions dominantes** et constitution de **barrières à l'entrée** de nouveaux acteurs ; renforcement des effets de **captivité du consommateur** (en réduisant la mobilité des utilisateurs d'un service qui possède toutes leurs données).

Nature et statut juridique des données personnelles : un attribut incessible de la personnalité

Une donnée est une parcelle d'information[1]. Le numérique est le format particulier que prend cette information – elle correspond alors à un certain nombre de *bits* (composés de 0 et de 1) pour son traitement par les outils informatiques.

Au plan économique, il s'agit d'un bien non rival (dont l'usage par une personne ne dégrade pas celui d'une autre personne) et au faible coût de production.

Les données numériques peuvent relever de régimes juridiques variés, comme « information publique » (code des relations entre le public et l'administration) ou comme « données à caractère personnel » (loi du 6 janvier 1978 dite « Informatique et Libertés ») comprises selon le droit européen comme « *toute information se rapportant à une personne physique identifiée ou identifiable* »[2].

Même si leurs traitements peuvent être *de facto* « contrôlés » par les entités qui les collectent, **les données ne font pas, en droit français, l'objet d'une « propriété »**[3].

La loi Informatique et Libertés de 1978, comme le RGPD désormais à l'échelle de l'Union européenne, s'inscrivent en effet dans **une logique de droits attachés à la personne**. La possibilité de disposer d'une vie privée y est appréhendée comme un droit qui se situe à l'essence même de la personne, fondamental pour sa dignité et le libre développement de sa personnalité.

Cette conception de la donnée personnelle constitue ainsi l'affirmation de convictions éthiques et humanistes : Une marchandisation des données personnelles constituerait un frein à l'exercice effectif du droit à l'**autodétermination informationnelle**, notamment en ôtant aux individus la capacité à révoquer leur consentement, une fois leurs données vendues.

[1] « Une donnée est une description élémentaire, typiquement numérique pour nous, d'une réalité. C'est par exemple une observation ou une mesure. À partir de données collectées, de l'information est obtenue en organisant ces données, en les structurant pour en dégager du sens. En comprenant le sens de l'information, nous aboutissons à des connaissances, c'est-à-dire à des faits considérés comme vrais dans l'univers d'un locuteur, et à des lois (des règles logiques) de cet univers » *Serge Abiteboul,* Sciences des données : de la logique du premier ordre à la Toile*, leçon inaugurale prononcée le jeudi 8 mars 2012, Collège de France, Chaire d'Informatique et sciences numériques.*

[2] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit « RGPD ».*

[3] *En revanche, les bases de données bénéficient d'une protection juridique particulière (en application du code de la propriété intellectuelle), qui permet d'interdire l'extraction ou la réutilisation sans autorisation du contenu de la base. L'article L. 112-3 du code de la propriété intellectuelle définit les bases de données comme « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen ».*

b) Les défis de la « révolution des données » pour notre ordre juridique

Les modèles économiques des grands acteurs dominants (gratuité d'accès, collecte massive, utilisation et valorisation des données personnelles, vente de publicités ciblées) passent aujourd'hui par **la mise en œuvre de stratégies d'évitement leur permettant d'échapper aux contraintes traditionnelles de notre ordre juridique**.

Leur développement, fondé sur la recherche du plus grand nombre d'utilisateurs (pour ses effets de réseau), a en effet tout intérêt à se faire indépendamment des frontières nationales : l'interconnexion des réseaux de communication et les technologies le permettent désormais naturellement, et **la gratuité apparente de ces nombreux services renforce leur attractivité,** comme le relève justement M. Bernard Benhamou : « *[la gratuité] a été conçue comme la meilleure manière de créer le plus rapidement possible un auditoire qui soit le plus large et le plus captif possible* ».

La gratuité sur internet

La gratuité n'est pas nouvelle : certains médias se sont développés sur ce modèle grâce aux revenus publicitaires. Elle est **permise par le modèle économique des marchés bifaces et les rendements d'échelle, qui incitent à donner la priorité à la captation de nouveaux utilisateurs –** quitte à ne pas se rémunérer dans un premier temps, avant de monétiser l'activité dans un second temps[1].

Toutefois, cette gratuité n'est qu'apparente : **les données sont issues du « travail gratuit » des internautes**, qui les déposent à mesure qu'ils consultent des pages sur internet[2]. La frontière est brouillée entre l'acte de consommation et l'acte de production, dans la mesure où c'est le consommateur qui fournit des moyens de production au producteur. Cette activité est au cœur du modèle d'affaire des géants du numérique.

Votre rapporteur note que **l'absence de paiement entraîne des addictions extraordinairement fortes à certains services, usages contre lesquels ni les cadres juridiques ni les volontés politiques nationales ou européennes ne pèsent plus grand-chose**. Cette véritable torsion du capitalisme classique vers une « économie de l'attention »[3] a d'ailleurs fait l'objet de travaux spécifiques du Conseil national du numérique comme Mme Annie Blandin, universitaire qui en est membre, en a alerté votre commission lors de son audition.

---

[1] *Que ce soit par la publicité ou en adoptant un modèle dit « freemium », qui consiste à fournir des services améliorés pour ceux qui sont prêts à payer.*

[2] *Le « travail du clic » a été étudié par le sociologue Antonio A. Casilli, qui rassemble sous cette notion à la fois le travail gratuit des utilisateurs mais aussi les microtravailleurs payés pour cliquer, depuis leurs domiciles ou dans des « fermes à clic », cf. Antonio A. Casilli,* En attendant les robots. Enquête sur le travail du clic*, 2019).*

[3] *Voir notamment Tim Wu,* The attention merchants, The epic scramble to get inside our heads*, 2016. Les conséquences néfastes ont récemment été décrites par Bruno Patino « La civilisation du poisson rouge, Petit traité sur le marché de l'attention » avril 2019.*

En outre, **ces acteurs établis pour l'essentiel à l'étranger peuvent résister par des complexités administratives aux tentatives de légiférer des Etats dans lesquels ils opèrent.** Ces « entreprises souveraines » **créent ainsi des normes propres** (leurs conditions générales d'utilisation – CGU ; certaines incorporant une définition autonome des « standards de la communauté » véritable charte encadrant la liberté d'expression sur les réseaux sociaux), au point, comme le relève Me Olivier Itéanu[1], qu'invoquer une violation des CGU sur certaines plateformes est souvent plus efficace qu'attendre le traitement d'une plainte formelle par les autorités nationales compétentes.

Certains acteurs du numérique sont même susceptibles d'être en France **les vecteurs – consentant ou non - d'ordres juridiques étrangers** : les géants américains sont tenus à l'application des régimes de sanctions extraterritoriales ou des règles d'accès aux preuves électroniques (comme le *Cloud Act*) et de grands acteurs industriels du numérique chinois restent marqués par une certaine porosité avec les intérêts militaires de leur pays.

Enfin, pour nos concitoyens, c'est **un véritable défi démocratique dans l'expression de la volonté générale** que pose parfois le déploiement généralisé des outils numériques. Ils peuvent en effet venir troubler le jeu politique en facilitant de nouveaux modes d'actions pour des tentatives d'ingérence ou de manipulation spécifiques et ciblées : le vol de données d'un « QG de campagne » et leur dissémination publique lors de l'élection présidentielle de 2017 a pu en témoigner en France. À l'échelle mondiale, l'affaire dite « Cambridge Analytica » montre le danger de méthodes peu scrupuleuses de recueil massif, d'analyse et de recoupement des données aux fins d'influence sur les choix politiques. Lors de son audition devant notre commission, M. Christophe Castaner, ministre de l'intérieur, a souligné que, sous réserve de l'achèvement des analyses et retours d'expérience, aucun dysfonctionnement n'avait été constaté ni aucune attaque significative identifiée lors des élections européennes. Notre vigilance, soutenue par l'expertise de l'Anssi (Agence nationale de la sécurité des systèmes d'informations) en la matière, reste pour votre rapporteur une impérieuse nécessité.

Quel Gouvernement, fût-il libéral, pourrait s'accommoder d'un système qui risque à terme de rendre sans effet les prescriptions de son ordre juridique ?

2. Développer l'identité numérique garantie par l'État

Exemple frappant de cette remise en cause de l'ordre juridique, **l'authentification des personnes**, privilège de l'État, est **de plus en plus contestée par des entreprises privées**, au premier rang desquelles Facebook

[1] *Audition du 9 juillet 2019.*

et Google. Leurs solutions d'identification, ensuite réutilisables sur d'autres sites internet privés, généralement pour des utilisations non sensibles, **sont devenues le premier moyen de prouver son identité sur internet**. Les acteurs concernés nient toute volonté de supplanter les États et affirment simplement fournir à leurs utilisateurs les services dont ils ont besoin.

Ces solutions présentent à terme **le risque de devenir des identités numériques d'usage**[1], d'autant qu'il a été souligné devant votre commission qu'**aucun outil proposé par l'État ne saura s'imposer s'il n'est pas au moins aussi facile d'utilisation, aussi efficace et aussi pratique que ceux proposés par les entreprises du numérique**. Henri Verdier, ambassadeur pour le numérique, estime pourtant « *qu'à l'avenir, l'un des grands rôles des États pourrait être de garantir les 'communs'* », dont fait partie l'identité numérique[2].

Cependant, **la France a jusqu'ici moins proposé de solutions qu'elle n'a tenté d'encadrer les initiatives privées**. La loi pour une République numérique[3] dispose qu'une identité numérique fournie par le secteur privé est fiable si et seulement si elle répond au cahier des charges établi par l'Anssi. Au niveau européen, le règlement eIDAS[4] instaure un cadre juridique pour l'utilisation des services de confiance en distinguant les niveaux de sécurité requis en fonction de ces services et en imposant l'interopérabilité des méthodes nationales d'identifications numériques[5]. Des pays tiers ont demandé à en faire partie et à partager les normes européennes. Dans la compétition qui les oppose aux acteurs privés, cette **capacité à dire le droit** demeure un atout pour les États, concurrencés dans l'exercice de cette prérogative souveraine.

Les instruments d'identification aujourd'hui proposés par l'État ne constituent pas à proprement dit une « identité numérique ». FranceConnect, conçue par la direction interministérielle du numérique et du système d'information et de communication de l'État (Dinsic), est un **agrégateur d'identités :** l'usager utilise l'identité numérique d'un fournisseur (ex. impots.gouv.fr) pour s'authentifier auprès de fournisseurs de services intégrant le bouton FranceConnect.

---

[1] *Un risque sur lequel a insisté Mme Claire Landais, Secrétaire générale de la défense et de la sécurité nationale, lors de son audition devant votre commission le 23 mai 2019.*

[2] *Audition de M. Henri Verdier, ambassadeur pour le numérique, devant votre commission le 4 juin 2019.*

[3] *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, créant l'article L136 du code des postes et des communications électroniques.*

[4] *Règlement n° 910/2014 du Parlement européen et du Conseil 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, dit règlement « eIDAS ».*

[5] *Pour un panorama complet des services concernés et de la mise en œuvre du règlement, voir le site de l'Anssi : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/*

Complémentaire, le **projet AliceM**[1] (Authentification en ligne certifiée sur mobile), développé par le ministère de l'intérieur et actuellement en phase de test, est **encore loin, dans sa première version, de répondre aux ambitions d'une identité numérique souveraine**. Son objectif est de permettre aux usagers de « prouver » leur identité en ligne et de pouvoir accéder, grâce à leurs téléphones, à certains services publics habituellement accessibles par FranceConnect. L'authentification s'appuie sur une reconnaissance faciale statique (photographie du passeport) et dynamique (vidéo). L'objectif du ministère de l'intérieur est de proposer un parcours unique d'authentification afin d'offrir, à terme, une carte d'identité numérique[2]. Toutefois, aucune date de lancement n'a encore été précisée, d'autant plus que l'application suscite certaines réticences quant à sa gestion des données personnelles[3].

Dans ce domaine, votre rapporter relève que **la France accuse un retard certain vis-à-vis de ses partenaires européens**, 23 d'entre eux ayant mis en place une identité numérique. Devant votre commission, le ministre de l'intérieur, M. Castaner, a lui-même reconnu que « *nous n'étions pas en avance sur ce sujet* » et que « *d'autres pays pourraient nous donner des leçons dans ce domaine* ». L'exemple le plus fréquemment cité est celui de l'Estonie, où les cartes d'identité numériques peuvent également être utilisées pour signer des contrats, ouvrir un compte en banque, voter, utiliser les transports en commun, envoyer des mails sécurisés… Or, FranceConnect n'est pas obligatoire et n'offre qu'un niveau de sécurité standard. Il ne pourrait donc par exemple pas servir d'élément de connexion au vote électronique, qui nécessite une authentification forte des personnes. On est donc encore loin,

---

[1] *Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ». L'association La Quadrature du Net a déposé un recours contre ce texte devant le Conseil d'État. Elle reproche à l'État de ne pas respecter le RGPD en ne laissant pas à l'utilisateur le choix de ne pas recourir au dispositif de reconnaissance faciale pour avoir accès aux services publics dématérialisés* via *AliceM. L'association appuie son action sur l'avis de la Commission nationale de l'informatique et des libertés, rendu le 18 octobre dernier, dans lequel elle estimait que* «le gouvernement ne propos[ait] pas, en l'occurrence, d'alternative à la reconnaissance faciale pour créer une identité numérique (...). Au regard de ces principes, le consentement au traitement des données biométriques ne peut être regardé comme libre et comme étant par suite susceptible de lever l'interdiction posée par l'article 9.1 du RGPD». *Elle proposait la mise en place de solutions alternatives.*

[2] *Audition de Christophe Castaner, ministre de l'intérieur, devant votre commission d'enquête le 2 septembre 2019.*

[3] *Tel que le dispose l'article 7 du décret cité ci-dessus, seront enregistrées de nombreuses données à caractère personnel (état civil, caractéristiques physiques, informations du titre d'identité, photographie et vidéo, historique des transactions associées au compte AliceM). L'article 11 précise que les données conservées sur l'équipement de l'usager seront chiffrées et inaccessibles après la suppression du compte. Les données liées à l'historique des transactions feront l'objet d'un traitement centralisé par l'Agence nationale des titres sécurisés (article 10) et seront supprimées au bout de six ans (article 12).*

comme M. Nadi Bou Hanna, directeur de la Dinsic, le souhaite, de faire de l'utilisation de FranceConnect « *un réflexe pour les Français* »[1].

Dans ce contexte, **2021/2022**[2]**, c'est-à-dire demain, doit constituer l'horizon de l'action publique dans ce domaine**. En effet, toutes les cartes d'identité seront alors renouvelées : un premier pas serait de **proposer une carte d'identité électronique**. En effet, si l'identité numérique s'incarne principalement par un identifiant unique et par un mot de passe sécurisé, le règlement eIDAS impose de recourir à un objet tiers, comme une carte d'identité électronique, pour certains services nécessitant une vérification supplémentaire. En Estonie, elle est obligatoire depuis 2002. La Belgique l'a quant à elle imposée en 2003 et a développé, depuis 2016, une application facilitant l'authentification sur *smartphone* (« *itsme* »). **Votre rapporteur ne peut que regretter le retard de la France** sur un sujet sur la table depuis les années 1970, avec pas moins de cinq projets infructueux, à l'image d'IDénum, lancée en 2010 avec La Poste.

Au regard de la **sensibilité et de la masse des données traitées**, **il est crucial que l'État se saisisse enfin de ce sujet**. Les entreprises peuvent utiliser les données transmises par les utilisateurs pour les revendre aux services de publicité ciblée, révéler des habitudes de consommation, tracer les individus… Une solution d'identification portée par l'État pourrait non seulement lui permettre de **réaffirmer sa souveraineté sur ce monopole régalien historique**, mais elle redonnerait aussi **aux citoyens la maîtrise de leurs propres données**. L'utilisation de ces données à des fins de politique publique ne devrait être possible qu'à la seule condition que les usagers y aient librement consenti.

Fournir une **carte d'identité électronique** à l'ensemble des citoyens français. Ces derniers pourraient plus facilement conduire leurs démarches administratives en ligne et bénéficieraient d'une authentification forte, sans préjudice pour leurs données personnelles. La France rejoindrait alors la grande majorité des pays européens ayant déjà développé des solutions similaires.

[1] *Audition de M. Nadi Bou Hanna, directeur interministériel du numérique et du système d'information et de communication de l'État devant votre commission, le 25 juin 2019.*

[2] *D'après l'information transmise par M. Cédric O, secrétaire d'État chargé du numérique, lors de son audition devant votre commission, le 20 juin 2019, et par M. Christophe Castaner, ministre de l'intérieur, lors de son audition devant votre commission le 2 septembre 2019.*

3. Renforcer les moyens des régulateurs à la hauteur du défi numérique plutôt que créer un unique régulateur du numérique

a) Éviter de bouleverser une architecture administrative qui fonctionne

La piste consistant à créer un régulateur unique du numérique est **régulièrement évoquée dans le débat public**. Il s'agirait ainsi d'adapter une supervision exercée par la puissance publique de façon jusqu'alors sectorielle (réseaux télécoms, contenus audiovisuels, données personnelles, contrefaçon en ligne) aux **conséquences de la convergence entre services et réseaux** provoquée par la révolution numérique[1].

Récemment encore, le ministre de l'économie et des finances, le ministre de la culture et le secrétaire d'État chargé du numérique ont confié à MM. Jean-Yves Ollier et Godefroy Beauvallet une mission sur les rapprochements éventuels entre les régulateurs du numérique. Le sujet pourrait ainsi être débattu au Parlement à l'occasion de l'examen de la prochaine loi audiovisuelle, dont le Gouvernement a annoncé la présentation à l'automne. Selon le Premier ministre, en effet : « *pour tenir compte de l'évolution de l'environnement des médias et ce qui ressemble à une "extension du domaine de la lutte", **la loi dessinera également le futur paysage de la régulation**. Il faut sans doute, à tout le moins, rapprocher le CSA et l'Hadopi, et approfondir les coopérations entre le CSA et l'Arcep* ».[2]

Le Sénat s'est lui déjà emparé de ce débat et mène depuis plusieurs années[3] **des réflexions approfondies sur le périmètre optimal de la régulation du numérique** et sur le rôle des autorités administratives indépendantes partageant une compétence en la matière. A cet égard, votre rapporteur fait pleinement sienne la position prudente dégagée au sein des commissions permanentes de notre assemblée et qui voit dans une fusion Arcep/CSA, sur le modèle britannique de l'Ofcom, « une fausse bonne solution ».

Interrogés sur ce sujet par votre commission, les présidents respectifs du CSA et de l'Arcep ont d'ailleurs émis des réserves.

---

[1] *Différents réseaux – filaire (câble, cuivre, fibre) ou hertzien - peuvent désormais transporter des services équivalents, et les protocoles informatiques peuvent faire communiquer entre eux les terminaux – télévision, PC, téléphones - comme les différentes applications.*

[2] *Discours de clôture du colloque « Médias, liberté et création » (19 juin 2019).*

[3] *« Dix ans après, la régulation à l'ère numérique » Rapport d'information n° 350 (2006-2007) de M. Bruno Retailleau, fait au nom de la commission des affaires économiques, déposé le 27 juin 2007. Ce rapport est consultable en ligne à l'adresse : https://www.senat.fr/rap/r06-350/r06-350_mono.html*

En outre, en janvier 2014 a été organisée au Sénat une « table ronde sur la régulation dans le domaine des technologies de l'information », à l'initiative du groupe d'études « Média et nouvelles technologies » de la commission de la culture, de l'éducation et de la communication, sous la présidence de Mme Catherine Morin-Desailly, et avec la participation de M. Bruno Retailleau, vice-président.

Lors de son audition, M. Roch-Olivier Maistre, président du CSA, a notamment rappelé, reprenant l'exemple de l'Ofcom, que la fusion qui l'avait vu naître s'était embourbée dans un chantier de conduite du changement administratif plutôt que de se focaliser sur les sujets de fond à traiter, faisant perdre près de quatre années à la régulation proprement dite. Votre rapporteur note en revanche que les deux autorités, Arcep et CSA, se sont dites ouvertes à un rapprochement plus approfondi de leurs compétences sur certains sujets connexes.

Votre rapporteur rejoint cette analyse et estime **préférable de ne pas bouleverser une architecture administrative qui fonctionne**.

En revanche, il **soutient l'idée d'un renforcement des compétences spécialisées dans le numérique, en particulier des capacités d'audit et de contrôle des algorithmes. Ce renforcement pourrait s'accompagner de leur mutualisation**.

b) Renforcer les moyens humains des régulateurs et approfondir leur mutualisation

Les autorités de régulation apparaissent plus que jamais **confrontées à un déficit de moyens et à une asymétrie d'information face aux grands acteurs du numérique**, au risque de les paralyser. Ce diagnostic est partagé par toutes les autorités entendues par votre commission.

Ainsi, comme sa présidente en a fait la démonstration lors de son audition devant notre commission, la **CNIL est notoirement sous-dimensionnée**. Au 31 décembre 2019, les effectifs de la CNIL étaient de **215 postes** et, malgré les 15 créations de postes consenties en 2019 pour faire face au nouveau contexte de mise en place du RGPD, votre rapporteur regrette que les effectifs de la CNIL demeurent ainsi **bien en-deçà de ceux des régulateurs européens** des autres Etats membres comparables[1].

Ce manque de moyens met gravement sous tension l'activité d'un régulateur pourtant crucial pour la préservation de notre souveraineté numérique :

- sur le traitement des **plaintes**, dont certaines concernent l'activité de géants du numérique capables de mobiliser de larges équipes de juristes chevronnés, la CNIL indique ainsi que, malgré une série de mesures tendant à soulager la charge de travail interne (partenariats sur le *spam*, montée en puissance des délégués à la protection des données, incitation au développement de mécanismes de médiation), le ratio actuel de plaintes par

[1] *À titre d'exemple, l'autorité hollandaise compte 138 agents en 2019 pour 17,12 millions d'habitants, l'autorité irlandaise 140 pour 4,84 millions d'habitants, l'autorité polonaise 250 pour 37,98 millions d'habitants, le Royaume-Uni 696 pour 66,19 millions d'habitants, l'Allemagne plus de 700 pour 82,85 millions d'habitants (l'Autorité fédérale, qui compte 253 agents, agissant en réseau avec les 16 autorités fédérées dans chacun des Länder).*

agent traitant (supérieur à 600 !) n'est pas soutenable compte tenu de la complexité juridique et technique croissante des dossiers ;

- lors de son audition, Mme Marie-Laure Denis a également donné comme exemple les possibilités trop limitées de traitement par la CNIL des **notifications des violations de données, qui est pourtant un enjeu majeur de cybersécurité** (« *nous recevons sept notifications de failles ou de violations de données par jour - sans pour autant disposer de moyens supplémentaires pour prendre en charge cette nouvelle compétence* ») ;

- alors que la France avait été parmi les pays pionniers de la protection des données il y a 40 ans, avec sa loi « Informatique et libertés » dès 1978, le faible nombre de personnes de la CNIL pouvant être mobilisées pour participer aux instances de coopération et sa taille modeste comparée à celle de ses homologues européens **remet en cause la capacité d'influence de la France et de sa conception en matière de protection des données** à caractère personnel en Europe, alors que d'autres modèles sont mis en avant (*compliance* à l'anglo-saxonne, recentrage sur une défense des seuls droits du consommateur…)

S'ajoutant à ces insuffisances quantitatives, en termes d'effectifs, le défi à relever est également qualitatif. La présidente de l'**Autorité de la concurrence** relève ainsi devant votre commission que « *les régulateurs peinent à recruter des experts dans ces secteurs, comme des* data scientists ». Elle estime, elle aussi, que « *l'État doit renforcer ses autorités de régulation, en leur octroyant plus de moyens humains et techniques* ».

À cet égard, comme le note le récent rapport d'inspection sur la politique de la concurrence à l'échelle européenne[1] à propos des services de la Commission européenne en charge de l'application du droit de la concurrence (direction générale de la concurrence, ci-après DG concurrence) : « *la* ***présence des algorithmes rend les comportements opaques et complexes à analyser*** *et (…) la taille des acteurs et l'explosion des échanges digitaux nécessitent de collecter et de traiter un nombre colossal de données : 5,2 téraoctets de données regroupant 1,7 milliard de recherches dans le cadre du dossier Google Shopping par exemple* ».

Dans ce contexte, il est **critique et indispensable à la crédibilité de leur action que les autorités de régulation disposent de compétences de pointe pour analyser les comportements des géants du numérique**. Le prochain budget annuel de l'Union Européenne prévoit une ligne de crédits spécifique visant à recruter au sein de la DG concurrence des *data scientists* et à doter la direction de moyens en adéquation avec les enjeux numériques. Le Gouvernement serait bien avisé de faire de même dans le prochain projet de loi de finances.

---

[1] *Rapport d'inspection précité, intitulé* « La politique de la concurrence et les intérêts stratégiques de l'UE ».

Un **tel recrutement serait sans doute favorisé par la mutualisation de ces experts entre différentes autorités de régulation**, qui serait par ailleurs justifiée par la similitude des problématiques d'ordre technique à résoudre, comme la compréhension d'un algorithme ou d'une grande base de données.

Plutôt que de procéder à des fusions potentiellement coûteuses et lourdes, il convient de **renforcer les moyens humains** des autorités de régulation en ciblant les recrutements sur des **profils spécialisés** dans le numérique, en particulier des capacités d'audit et de contrôle des algorithmes.

De telles ressources humaines pourraient utilement être **mutualisées** entre plusieurs autorités de régulation.

4. Mieux responsabiliser certaines plateformes en affinant le régime de responsabilité aménagée des intermédiaires techniques ?

Plusieurs réflexions sont en cours sur l'opportunité et les modalités d'**actualisation de la directive européenne de 2000 dite « commerce électronique » ou « e-commerce »**[1] face aux imperfections du régime de responsabilité atténuée qu'elle octroie à certains intermédiaires techniques.

Le régime de responsabilité aménagée et les devoirs de certains intermédiaires techniques

Transposant en droit français les dispositions de la directive 2000/31 du 8 juin 2000, dite directive « *commerce électronique* » ou « *e-commerce* », l'article 6 de la loi n° 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* prévoit un régime de responsabilité limitée pour les fournisseurs d'accès[2] et les hébergeurs de contenus[3].

S'ils ne sont pas responsables *a priori* des contenus qu'ils « stockent » et donc ne sont pas astreints à un devoir de surveillance de ces contenus, certains de ces intermédiaires techniques ont néanmoins pour obligation d'agir promptement pour retirer toute donnée dont le contenu serait manifestement illicite.

[1] *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.*

[2] *À savoir les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne.*

[3] *À savoir les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services.*

Concernant certaines infractions spécifiques, les intermédiaires techniques doivent également :

- informer promptement les autorités publiques compétentes des signalements reçus par le biais des dispositifs de signalement ; ces signalements sont traités par la plateforme « Pharos »[1] ;

- mettre en place un dispositif « *facilement accessible et visible permettant à toute personne de porter à leur connaissance* » les contenus jugés contraires à l'intérêt général ;

- rendre publics les moyens qu'ils consacrent à la lutte contre ces activités illicites.

Le Sénat a récemment pris position sur ce sujet, en adoptant à l'initiative de notre collègue Catherine Morin-Desailly une résolution européenne[2] en faveur d'une révision de la directive « e-commerce ». Cette dernière appelle à faire émerger un « troisième statut », à côté de celui des hébergeurs et des éditeurs. Il doit être défini au niveau européen, et ménager la liberté d'expression et la compétitivité des acteurs du secteur.

Votre rapporteur reconnaît également le caractère désormais daté de la directive de 2000 : l'évolution technologique a permis la création d'acteurs numériques d'un genre nouveau, rendant obsolète la dualité hébergeur/éditeur (plateformes interactives, réseaux sociaux, tri et mise en avant algorithmique de contenus) qui occupent désormais une place sociale et économique bien plus importante qu'il y a 20 ans. Ces nouveaux acteurs numériques sont aujourd'hui au centre du processus de circulation de l'information pour les citoyens, dotés d'un modèle économique propre fondé sur la gratuité, l'exploitation des données, et la diffusion toujours plus rapide de contenus sans obligations de contrôle préalable.

Interrogé par notre commission, M. Benoît Thieulin, ancien président du Conseil national du numérique, a fait part de l'évolution de sa position sur ce sujet, appelant désormais lui aussi à revoir la directive sur le commerce électronique (« *Il faut réfléchir à un nouveau statut pour les plateformes, en leur imposant un cahier des charges contraignant : aujourd'hui, les règles de droit classiques mises à part, elles assument trop peu de responsabilités*. »).

---

[1] *Cette « plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements » est placée au sein de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (Oclctic) qui relève de la sous-direction de la lutte contre la cybercriminalité (SDLC) de la direction centrale de la police judiciaire (DCPJ). La plate-forme Pharos compte une vingtaine d'enquêteurs (policiers et gendarmes) et exploite le portail www.internet-signalement.gouv.fr qui permet depuis 2009 aux internautes et aux acteurs d'internet de signaler les contenus illicites du web. Elle mène également une veille proactive sur internet pour de détecter des contenus illicites ou contribuer à la résolution d'enquêtes.*

[2] *Résolution européenne n° 31 (2018-2019) sur la responsabilisation partielle des hébergeurs de contenus numériques, devenue résolution du Sénat le 30 novembre 2018* https://www.senat.fr/dossier-legislatif/ppr17-739.html

À l'échelle de l'Union européenne, il est particulièrement significatif que, dans son programme de candidature à la présidence de la Commission européenne[1], Mme Ursula Von der Leyen ait mentionné l'adoption d'un nouveau *Digital services Act*, qui viendrait modifier la directive dite « e-commerce ».

Les premières orientations officieuses des services de la Commission européenne pour une révision de la directive sur le commerce électronique

Une note rédigée par les services de la Commission européenne et publiée par voie de presse fin juin 2019 expose qu'un nouveau régime législatif horizontal (en ce qu'il s'appliquerait à tous les services numériques) pourrait être nécessaire en vue de :

- renforcer le marché unique numérique, qui fait face à de nouvelles problématiques actuellement réglées au niveau national, faisant ainsi courir le risque de fragmentation de ce marché – c'est par exemple le cas en matière de lutte contre la haine en ligne ou en matière de régulation de l'économie collaborative ;

- actualiser les règles applicables – la distinction jurisprudentielle entre hébergeur passif ou actif ne semble pas suffisamment précise, alors que certains secteurs, comme la publicité en ligne, devraient être davantage régulés ;

- renforcer la supervision des autorités publiques, actuellement inefficace ;

- diminuer les barrières à l'entrée, par exemple en prévoyant un cadre harmonisé de « bacs à sables réglementaires », c'est-à-dire de dispositifs permettant d'innover dans des conditions réglementaires assouplies.

Parmi les sujets abordés, celui de la **responsabilité des hébergeurs** ferait l'objet d'une clarification, la notion d'acteur actif ou passif serait remplacée par celles de fonctions éditoriales, de connaissance et de degré de contrôle.

Le secrétaire d'État chargé du numérique, M. Cédric O, a cependant fait preuve d'un certain pessimisme sur le sujet. Selon lui, « *la question du tiers-statut est très intéressante, mais elle est inacceptable pour les pays nordiques. Doit-on mener le combat pendant quelques années ou se concentrer sur certains secteurs - la culture, les atteintes à la vie privée... - et réussir à s'affranchir de la dichotomie « hébergeur-éditeur » pour gagner des batailles à plus court terme ?* »[2]. Si la prudence est donc de mise sur la faisabilité d'une telle réforme européenne, votre rapporteur estime que le Gouvernement ne devrait pas s'interdire de **poursuivre la réflexion sur la création d'un statut tiers** pour certains intermédiaires techniques, notamment ceux ayant atteint une taille ou un volume d'activité importants.

[1] *Ursula von der Leyen,* A Union that strives for more, My agenda for Europe, political guidelines for the next European commission 2019-2024.

[2] *Audition par la commission de la culture, de l'éducation et de la communication du Sénat, le 24 juillet 2019.*

Il convient de **poursuivre la réflexion sur la faisabilité ainsi que les avantages et les inconvénients d'une révision du régime de responsabilité limitée des hébergeurs**.

5. Localisation des données et extraterritorialité des lois : assumer un rapport de force international

a) L'obligation de localisation géographique : une solution imparfaite

Si promouvoir, voire dans certains cas imposer, une obligation de localisation des données sur un territoire précis (en France ou en Europe) est une idée qui peut paraître intéressante au premier abord, **l'utilité réelle en termes de souveraineté numérique d'une telle démarche doit aujourd'hui être largement nuancée**.

Votre rapporteur note certes, comme plusieurs personnes auditionnées, que ces initiatives pourraient présenter **un intérêt limité dans certains cas** :

- avant tout pour **protéger certaines données particulièrement sensibles** (traitements publics souverains, données privées financières ou commerciales stratégiques) ; à ce titre, lors de son audition, Mme Claire Landais, secrétaire générale du SGDSN, ne défend le recours à un *cloud* « interne » géographiquement localisé que pour les données les plus sensibles, dans une logique de cercles concentriques aux exigences de sûreté décroissante. Votre rapporteur considère également que l'on ne saurait imposer un mode de stockage particulier aux entreprises sans leur offrir des solutions industrielles performantes et accessibles répondant à leurs besoins. De telles solutions pourraient ainsi être imposées dans le cadre plus général des régimes des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE) ;

- également pour **garantir une accessibilité renforcée**, soit du point de vue des entreprises dans une logique de gestion des risques (lorsque les données ne sont plus localisées en France ou en Europe, il est plus difficile en pratique de les contrôler et d'avoir une assurance de l'usage qui a été fait par des prestataires ou des partenaires localisés à l'étranger), soit du point de vue de la puissance publique (pour faciliter l'accès à ces données par la justice ou les régulateurs nationaux dans le cadre de l'exercice de leurs pouvoirs de contrôle sectoriel, comme l'a souligné la présidente de l'Autorité de la concurrence) ;

- et enfin, de façon générale, en stimulant la demande, pour **soutenir l'écosystème industriel** des acteurs du *Cloud* et le développement des capacités de traitement des données.

Le Sénat a ainsi pu, par le passé, soutenir des initiatives largement transpartisanes en ce sens : en 2016, lors des débats relatifs à la loi pour une

République numérique, notre assemblée avait adopté, sans hélas être suivie par l'Assemblée nationale, un amendement[1] de notre collègue Eliane Assassi et des membres du groupe communiste républicain et citoyen, avec un avis favorable de la commission des lois, visant à faire figurer dans la loi « *Informatique et libertés* » l'obligation de stockage des données personnelles des citoyens français sur le territoire européen.

De telles initiatives doivent néanmoins prendre en compte l'évolution récente du droit européen et des systèmes juridiques étrangers, et il apparaît qu'une obligation de localisation des données ne répondrait pas au défi posé par certaines législations à vocation extraterritoriales.

D'une part, s'agissant des données non personnelles, **le droit européen limite drastiquement la possibilité d'imposer des exigences de localisation.** Elles sont désormais interdites *« sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité »*[2].

D'autre part, et en tout état de cause, **les clauses de localisation des données n'offrent pas de garanties face aux nouvelles législations ou pratiques étrangères à portée extraterritoriale** (sanctions internationales, « *Cloud Act* » adopté aux Etats-Unis en mars 2018, etc.) ni contre la porosité entre certains acteurs industriels et leur Gouvernement (certains équipementiers chinois, par exemple). Ainsi, quand bien même des données seraient physiquement localisées sur le territoire français ou européen, les entités qui contrôlent les centres de données (*datacenters*) continueront, en raison de leur nationalité, à être également soumises à des régimes juridiques les obligeant à coopérer avec des puissances étrangères.

Identifier les cas où une obligation de **localisation des données sur le territoire national peut être justifiée par des motifs de sécurité publique**.

Cartographier et faire émerger des solutions pour l'hébergement et le stockage des données sensibles de ces entreprises, autour de prestataires français et européens non soumis aux législations étrangères à portée extraterritoriale.

b) Défendre nos données stratégiques contre l'extraterritorialité de lois étrangères : un rapport de force qui reste à engager

Pour préserver les données stratégiques de nos entreprises, et devant les limites du recours à la localisation géographique de celles-ci, votre

[1] https://www.senat.fr/enseance/2015-2016/535/Amdt_473.html

[2] *Article 4 du règlement européen du 14 novembre 2018 établissant un cadre applicable au libre flux des données non personnelles dans l'Union européenne. Ledit règlement prévoit par ailleurs que les États membres doivent veiller, d'ici au 30 mai 2021, à ce que toute exigence existante de localisation des données établie dans une disposition législative, réglementaire ou administrative de nature générale et qui n'est pas conforme à cette interdiction soit abrogée. L'objectif recherché est ici de favoriser la mobilité des données non personnelles dans le cadre d'un marché intérieur numérique plus intégré.*

rapporteur partage l'**approche réaliste et volontariste** du SGDSN. Devant votre commission, sa secrétaire générale, Claire Landais a estimé qu'il ne fallait pas se dérober au rapport de force juridique qui s'engageait actuellement avec certains de nos partenaires tentés par une application extraterritoriale de leur droit ; bien au contraire, **dans la perspective de conflits de normes, et pour rester crédibles en vue des négociations internationales appelées à les résoudre, il reste essentiel de pouvoir pour l'instant opposer fermement nos propres textes – européens, comme le RGPD ou nationaux, comme une « loi de blocage », éventuellement rénovée et renforcée.**

Le « *CLOUD Act* » aux Etats-Unis : Contexte d'adoption, portée et enjeux

Le « *Claryfying Lawful Overseas Use of Data Act* » (« *CLOUD Act* »[1]) a été adopté par le congrès des États-Unis d'Amérique en mars 2018 : Il vise principalement à réaffirmer le droit dont disposent les autorités américaines d'exiger des intermédiaires techniques soumis à leur juridiction la communication de toutes données stockées, même à l'étranger. Il prévoit aussi, et indépendamment, la conclusion d'accords bilatéraux spécifiques et réciproques avec les États-Unis en la matière.

Une réponse américaine à l'incertitude juridique née de l'évolution des techniques

L'évolution rapide des techniques de stockage des données – désormais distribuées et conservées de manière dynamique dans des centres de données répartis à travers le monde par des multinationales du numérique – a fragilisé l'application du régime américain d'accès aux données. Certains acteurs ayant contesté avec succès la portée extraterritoriale que les autorités entendaient donner à ces dispositions, cette question de principe devait être tranchée, courant 2018, par la Cour suprême[2]. C'est à cette incertitude que le « *Cloud Act* » est venu mettre fin, consacrant la possibilité pour les autorités américaines d'obtenir des données matériellement stockées à l'étranger.

Cette loi permet ainsi aux autorités américaines de contourner les procédures de demande d'entraide d'État à État et de s'affranchir des règles classiques de la

[1] *Inséré sous forme de « cavalier » au sein d'un vaste texte budgétaire (« Consolidated Appropriations Act, 2018 »), le «* Cloud Act *» modifie la loi sur les données des communications électroniques « Stored Communications Act » (SCA) de 1986, qui définit notamment les régimes d'accès et de protection des données de communication traitées ou stockées par certains intermédiaires techniques.*

[2] *Pour un exposé sommaire de ce contentieux, voir l'audition des représentants de Microsoft France devant la commission, et pour l'état du droit antérieur au* CLOUD Act *on pourra utilement se référer à l'étude du Pr. Théodore Christakis :* « Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques » *dans* USA v. Microsoft : Quel Impact ? Statut des données, souveraineté numérique et preuves dans les nuages *(2017).*

coopération judiciaire internationale[1] (entourée d'un plus grand formalisme, et de certaines garanties et délais).

Un très vaste champ d'application (entités concernées, infractions visées, données collectées)

Tous les fournisseurs de services de communications électroniques et les prestataires d'informatique en nuage relevant de la juridiction des États-Unis peuvent faire l'objet d'une demande de gel et de communication des données d'un de leurs utilisateurs au titre du « *Cloud Act* », et ce sans considération du fait que ces données soient localisées à l'intérieur ou à l'extérieur des Etats-Unis[2].

Comme le relève le rapport Gauvain[3], presque toutes les entreprises françaises et européennes sont ainsi potentiellement concernées par ce régime, « *compte tenu de l'état actuel du marché mondial du stockage de données numériques, dominé très largement par des acteurs américains (marché détenu à hauteur de 65% par Amazon, 15% par Microsoft et 5% par Google)* ».

Les autorités américaines présentent volontiers[4] la procédure comme limitée à la collecte de preuves pour réprimer pénalement un nombre restreint d'infractions pénales (les crimes les plus graves), et soulignent que les mandats nécessaires aux autorités de poursuite sont dans ce cas toujours soumis à l'approbation d'un magistrat indépendant, cependant :

- d'une part, la notion de « crime grave » reste floue, n'apparaît que dans la partie consacrée aux futurs accords bilatéraux, et pour limiter les seules demandes adressées aux États-Unis par les États tiers[5] ;

- d'autre part, la portée extraterritoriale consacrée par le « *Cloud Act* » a également vocation à s'appliquer à d'autres régimes d'accès aux données, hors répression pénale des crimes graves et sans production d'un mandat[6] (notamment à certains régimes de demandes des métadonnées sans intervention d'un juge ni test de « probable cause »).

Les types de données pouvant être transmis aux autorités sur ce fondement sont variées : contenus de communication, fichiers enregistrés, information, sans

---

[1] *Et notamment l'Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire conclu à Washington le 25 juin 2003.*

[2] *« A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States. » (§2713. Required preservation and disclosure of communications and records).*

[3] Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale*, juin 2019 ; M. Raphael Gauvain a été entendu par le rapporteur lors d'une audition ouverte aux membres de la commission.*

[4] *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act ; White Paper, U.S. Department of Justice (avril 2019).*

[5] *Cf. Rapport Gauvain, 1.2.4.2.2 « Les infractions visées » (p. 30).*

[6] *C'est ce que soulignent le Comité Européen de la Protection des Données et le Contrôleur européen de la protection des données, dans leur évaluation du CLOUD Act (« Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence », p. 2).*

distinguer entre données à caractère personnel des personnes physiques ni données non personnelles ou relevant de personnes morales.

Un risque pour nos données stratégiques et une contrariété avec le RGPD pour les données à caractère personnel

En organisant ainsi un accès unilatéral et facilité des autorités judiciaires américaines aux données stratégiques des personnes morales, le « *Cloud Act* » organise le contournement des traités d'entraide judiciaires et affaiblit les garanties dont pourraient normalement se prévaloir les entreprises mises en cause. Concernant les demandes d'accès à des données personnelles d'européens, la contrariété de la loi américaine avec le RGPD a été soulevée récemment par l'organe qui rassemble les CNIL européennes[1].

Alors que l'Union européenne envisage de se doter, elle aussi, d'une législation sur l'accès aux preuves électroniques[2] – incluant une dimension extraterritoriale –, votre rapporteur partage le souhait de voir aboutir des négociations avec les États-Unis en la matière, souhait exprimé tant par les organes de protection des données personnelles de l'Union que par la ministre de la Justice lors de son audition devant votre commission[3].

Ces critiques valent également à l'encontre des géants chinois du numérique, actifs en France, comme l'entreprise Huawei, régulièrement soupçonnée d'entretenir des liens étroits avec le Gouvernement chinois.

---

[1] « Nous sommes d'avis qu'actuellement, à moins qu'un mandat pris sur le fondement du Cloud Act ne soit reconnu ou rendu exécutoire sur la base d'un accord international, la licéité de tels transferts de données à caractère personnel ne saurait être établie, sans préjudice de circonstances exceptionnelles dans lesquelles un traitement de données est nécessaire afin de protéger les intérêts vitaux de la personne concernée » ("We are of the view that currently, unless a US Cloud Act warrant is recognised or made enforceable on the basis of an international agreement, the lawfulness of such transfers of personal data cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject"*), courrier sur l'impact du Cloud Act américain sur le cadre juridique européen en matière de protection des données à caractère personnel émanant du Comité Européen de la Protection des Données et du Contrôleur européen de la protection des données en réponse à une demande de la commission LIBE du Parlement Européen (10 juillet 2019).*

[2] *Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, dite « e-evidence ».*

[3] *« L'Union a décidé de s'engager dans la négociation d'un accord bilatéral sur le recueil de preuve numérique avec les États-Unis, car le Cloud Act peut mettre en échec les demandes des magistrats européens lorsqu'ils souhaitent obtenir des preuves numériques auprès des principaux fournisseurs mondiaux de communications électroniques. Cette négociation sera menée par la Commission au nom des Etats membres. Ceux-ci sont néanmoins étroitement associés et la France a tout particulièrement veillé à ce que le mandat de négociation confié à la Commission le 6 juin dernier soit le plus exigeant possible. »*

La porosité des grands acteurs chinois du numérique avec leur Gouvernement : l'exemple Huawei

L'impact incertain de la loi chinoise de 2017 sur le renseignement

La **loi chinoise sur le renseignement de 2017**[1] génère les mêmes inquiétudes que le *Cloud Act* aux États-Unis. Son article 14 dispose notamment que **les services de renseignement chinois peuvent requérir la coopération de tout citoyen chinois et de toute organisation**. Les analyses juridiques transmises par l'entreprise à votre rapporteur[2] – qui portent également sur les lois sur le contre-espionnage de 2017, antiterroriste de 2018 et sur la sécurité des réseaux informatiques de 2016 – confirment les propos tenus devant votre commission lors de l'audition de l'entreprise, à savoir que **cette loi n'est pas applicable en dehors du territoire chinois**. Pour reprendre les termes utilisés par la note transmise à votre rapporteur, « *ces dispositions n'ont pas d'effet extraterritorial, de sorte qu'elles ne s'appliquent pas aux entreprises et individus situés en dehors du territoire de la République populaire de Chine* ». La note poursuit : « *il est, de plus, important de noter que ces dispositions ne sont pas liées à un critère de nationalité* ». Elle précise qu'en conséquence, toute entreprise située en Chine sera soumise à ces lois.

Cependant, particulièrement succincte – une dizaine de pages, contre 37 pages transmises à la FCC américaine en mai dernier – elle ne précise pas expressément que les citoyens chinois et filiales d'entreprises chinoises ne sont pas soumis à ces lois[3]. Du reste, certaines études sur la loi sur le renseignement contredisent l'affirmation selon laquelle cette loi ne s'appliquerait pas aux entreprises et individus situés en dehors du territoire chinois[4].

Qui détient l'entreprise ?

Dans un article publié en avril dernier[5], deux chercheurs américains ont montré que la holding de l'entreprise est détenue à 1,14 % par son fondateur Ren Zhengfei et à 98,86% par une entité appelée « comité syndical », dont on sait peu de choses, hormis le fait qu'il est censé élire « *selon des règles de vote démocratiques* »[6] une commission représentative de 115 membres chargée d'élire à son tour le comité directeur.

---

[1] *Dont on peut trouver une traduction en anglais sur le site internet chinalawtranslate.com.*

[2] *Chen & Co. Law Firm, Note générale sur les demandes d'accès gouvernementales, 29 avril 2019.*

[3] *Financial Times,* Is Huawei compelled by Chinese law to help with espionage *?, 5 mars 2019.*

[4] *Voir, par exemple, l'article du cabinet suédois Mannheimer Swartling,* Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities*, janvier 2019. Cette étude conclut que la loi s'applique aux groupes chinois où que soient implantées les filiales et pourrait être interprétée comme s'appliquant à tout citoyen chinois, quel que soit son lieu de résidence. On peut également citer l'article du Professeur Donald Clark, The Zhong Lun* Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law*, 17 mars 2019. Cet article considère que, dans la mesure où le droit chinois s'applique à la holding de Huawei, il n'y a pas de raison que la holding ne requiert de ses filiales qu'elles lui transmettent des informations si elle y est contrainte en application du droit chinois.*

[5] *Christopher Balding et Donald Clarke,* Who owns Huawei ?*, 17 avril 2019.*

[6] *Source: présentation du groupe Huawei transmise à votre rapporteur. Ces règles ne sont cependant pas précisées.*

Ces chercheurs en tirent la conclusion selon laquelle, au vu du rôle que jouent les syndicats en Chine, Huawei pourrait être considérée comme contrôlée par l'État. Ils affirment, en revanche, qu'il est clair que Huawei n'est pas détenue par ses salariés, qui bénéficient seulement de ce qui est assimilable à un régime d'intéressement et de participation aux bénéfices, contrairement à ce que l'entreprise affirme pourtant régulièrement, en premier lieu sur son site internet, selon lequel « *Huawei est une société privée totalement détenue par ses employés* »[1].

Lors des auditions de votre commission, plusieurs **solutions juridiques ou techniques ont été esquissées pour préserver notre souveraineté malgré ces dispositions à portée extraterritoriale. Doivent être envisagées :**

- la séparation juridique de l'activité dans différentes entités **filiales étanches** en fonction de l'implantation géographique des services (c'est ainsi la solution retenue par l'entreprise française OVH pour lui permettre d'étendre ses activités aux Etats-Unis[2]) ;

- la stratégie de **mobilisation contentieuse** au cas par cas des entreprises pour contester en justice des demandes de l'administration qui ne passeraient pas par le canal de la coopération judiciaire internationale (c'est l'engagement pris notamment par les représentants de Microsoft France et Europe lors de leur audition[3]) ;

- et, surtout, le recours extensif aux **technologies de chiffrement robuste** des données dont seul le client aurait la clé et non l'intermédiaire technique. Ceci rend impossible le décryptage par les autorités locales, même en cas de coopération forcée de l'entreprise.

Néanmoins, ces solutions n'ont qu'une portée limitée : elles ont un coût et sont tributaires des moyens juridiques et techniques que les entreprises sont prêtes à déployer ou que leurs clients peuvent s'offrir.

---

[1] *Cf.* https://www.huawei.com/en/about-huawei/corporate-information. *Devant votre commission d'enquête, le directeur général de Huawei en France a confirmé, en des termes plus précis, cette affirmation :* « Huawei est une entreprise 100% privée, détenue par plus de 96 000 de ses employés et son fondateur, qui ne dispose que de 1,14% des parts de l'entreprise, selon un modèle coopératif ».

[2] *Selon M. Michel Paulin, directeur général d'OVH entendu par votre commission le 11 juillet 2019 :* « Aux États-Unis, notre filiale est régie par le droit américain. À ce titre, elle respecte scrupuleusement la loi américaine. En revanche, nous avons fait en sorte que seule cette filiale soit soumise au Cloud Act et qu'elle ne dispose d'aucun accès aux données situées à l'extérieur des États-Unis : il s'agit d'un bastion isolé. L'accès ne serait tout simplement pas possible d'un point de vue technique : de ce fait, aucun agent américain ne pourra accéder aux données situées en dehors du territoire américain. »

[3] *Selon M. Marc Mossé, directeur juridique et affaires publiques de Microsoft Europe :* « Nous protégeons les données de nos clients : premièrement en répondant aux autorités qui nous sollicitent qu'il faut demander ces données directement aux clients, deuxièmement en avertissant nos clients si nous sommes saisis d'une telle demande, et troisièmement en envisageant fortement de nous opposer à une telle demande en cas de conflit de loi précis et clair. »

Votre rapporteur trouve dès lors plus intéressante la recherche de solutions pérennes dont la responsabilité incomberait à la puissance publique. À ce titre, doivent particulièrement être saluées les analyses et préconisations que de notre collègue député Raphael Gauvain[1] a présentées au Premier ministre à l'issue de la mission qu'il lui avait confiée :

- le droit étant devenu une arme au service de la guerre économique des États-Unis contre le reste du monde, nos entreprises ne doivent pas être laissées démunies face à l'application d'une panoplie de lois à portée extraterritoriale (législation anti-corruption, sanctions économiques contre des États, lois sur le renseignement, lois permettant la collecte de données dans le cadre de procédures administratives ou judiciaires, comme le *Cloud Act* de mars 2018) ;

- la France doit y répliquer par une stratégie volontariste, qui implique notamment une **modernisation et un durcissement de la loi de 1968, dite « loi de blocage »**[2] (création d'un mécanisme obligatoire d'alerte en amont ; mise en place d'un accompagnement des entreprises ciblées par de telles mesures grâce à une administration dédiée ; augmentation des sanctions prévues en cas de violation de la loi) ;

- **une extension des principes protecteurs du RGPD aux données non personnelles des personnes morales** permettrait de protéger les entreprises françaises en sanctionnant la transmission indûe par les hébergeurs de leurs données stratégiques aux autorités judiciaires étrangères en dehors des canaux de l'entraide administrative ou judiciaire.

Renforcer la « loi de blocage » de 1968 (déclaration aux autorités françaises, accompagnement par une administration dédiée et durcissement des sanctions encourues).

Encourager la conclusion rapide **d'accords de coopération entre l'Union européenne**, ses États membres et les États-Unis dans le cadre du *Cloud Act*.

Réaffirmer **la pleine application du RGPD** et sanctionner les entreprises étrangères procédant à des transferts de données en méconnaissances de ces règles, conformément à l'avis du Comité Européen de la Protection des Données.

Réfléchir à l'opportunité **d'étendre les sanctions prévues par le RGPD aux données non personnelles stratégiques des personnes morales**, pour sanctionner les hébergeurs qui transmettraient aux autorités étrangères des données en dehors de l'entraide administrative ou judiciaire.

[1] Rapport précité.

[2] *Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.*

6. Au-delà du RGPD : passer d'un droit à la portabilité à une forme d'interopérabilité ?

a) Une première année d'application du RGPD, outil ambitieux au service des valeurs et de la souveraineté numérique européennes

Comme l'a exposé à notre commission Mme Marie-Laure Denis, présidente de la CNIL, le règlement général sur la protection des données (RGPD) a instauré **un cadre juridique ambitieux et puissant et une régulation à la mesure des enjeux de souveraineté numérique.**

Le règlement général sur la protection des données : principes et premier bilan

Le règlement (UE) 2016/679 dit **« règlement général sur la protection des données » (RGPD)** est entré en vigueur le **25 mai 2018**.

Le RGPD vise à adapter la législation relative au traitement des données à caractère personnel aux évolutions des technologies numériques en l'uniformisant au niveau européen. Il est d'application directe mais autorise aussi les États membres à procéder à certaines adaptations nationales.

Il poursuit trois **objectifs** principaux :

– renforcer les droits des personnes physiques dont les données sont utilisées ; il réaffirme les principes de base (transparence et consentement), en crée de nouveaux, mieux adaptés aux évolutions des usages numériques (« droit à l'oubli » et droit à la portabilité) et facilite leur exercice afin que les particuliers puissent s'en saisir et les faire respecter (droit au recours par mandataire, voire collectif, réparation des préjudices) ;

– responsabiliser tous les acteurs traitant des données en graduant leurs obligations en fonction des risques pour la vie privée ; il privilégie le recours à des études d'impact et à des outils de droit souple, généralise la nomination de « délégués à la protection des données » et supprime ou allège les formalités administratives préalables ;

– crédibiliser la régulation à la mesure des enjeux de souveraineté numérique ; le règlement peut recevoir une application extraterritoriale, les autorités européennes sont appelées à coopérer en cas de traitements de données transfrontaliers, et les sanctions sont enfin réellement dissuasives (jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires annuel mondial).

La loi « Informatique et libertés » de 1978 a été modifiée en juin 2018 afin de décliner ces grands principes dans l'ordre juridique français. Le **bilan au 1er octobre 2019** de la première année d'application du RGPD en France est éloquent :

- 8 395 **plaintes**[1] ont été reçues par la CNIL depuis le 1er janvier 2019, soit + 4,7% par rapport à la même période 2018 ; environ **une plainte sur cinq concerne des traitements transfrontaliers** de données ;

[1] *Sachant que 12 253 plaintes avaient été reçues par la CNIL entre le 25 mai 2018 et le 25 mai 2019, chiffre qui représentait déjà une hausse de 42 % par rapport à la même période en 2017-2018.*

- la CNIL a reçu 2 793 **notifications** de violation de données (depuis mai 2018) ; ces violations auraient concerné près de 100 millions de personnes ;

- plus de 20 800 **délégués** à la protection des données (personnes physiques ou morales) ont été désignés, pour plus de 63 000 organismes.

Son champ d'application territorial et matériel est vaste : le règlement doit être appliqué dès lors que le responsable de traitement est établi sur le territoire de l'Union européenne (« **critère de résidence** »). Mais **il a aussi vocation à s'appliquer hors de l'Union**, dès lors qu'un résident européen est visé par un traitement de données (par une offre de biens et de services, ou le suivi du comportement), y compris donc par internet (« **critère du ciblage** »). Alors que les acteurs du numérique s'intéressent au gisement de profit majeur que représente le marché européen et ses plus de 500 millions de consommateurs, ses règles protectrices trouvent ainsi à s'appliquer même à l'égard des entreprises qui ne disposent pas d'un établissement en Europe[1].

Les sanctions sont graduées et considérablement renforcées : outre les mesures correctives classiques[2], les autorités nationales ont également le pouvoir de prononcer des **amendes** atteignant, selon la catégorie de l'infraction, **10 ou 20 millions d'euros**, ou, dans le cas d'une entreprise, **de 2 % à 4 % du chiffre d'affaires annuel mondial** (le montant le plus élevé étant retenu). Le RGPD prévoit ainsi des sanctions administratives désormais dissuasives, en cas de méconnaissance de ses dispositions, à la hauteur des moyens mobilisés par les géants du numérique et de la gravité des risques que font encourir les traitements massifs de données.

Enfin, parmi les innovations juridiques introduites par le RGPD au bénéfice des particuliers dont les données personnelles font l'objet de traitement, le règlement consacre un **droit à la portabilité** des données. Son article 20 confère aux personnes concernées le droit de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement.

La consécration du droit à la portabilité constitue effectivement un instrument important de souveraineté numérique : il facilite la libre

---

[1] *Les entreprises sont en contact avec un « **guichet unique** », l'autorité de contrôle de l'État membre où se trouve leur établissement principal. Cette autorité chef de file aura la responsabilité d'organiser des contrôles, voire d'infliger des sanctions en cas de traitements transfrontaliers. La coopération est d'ailleurs renforcée entre autorités de régulation nationales et un **Comité européen de la protection des données** - CEPD - les rassemble pour veiller à l'application uniforme du droit. Le règlement étend par ailleurs explicitement aux **sous-traitants** une large partie des obligations imposées aux responsables de traitement.*

[2] *Avertissement, rappel à l'ordre, mise en demeure, limitation d'un traitement, suspension des flux de données, injonction de satisfaire aux demandes d'exercice des droits d'une personne ou de procéder à la rectification, la limitation ou l'effacement des données, retrait de certification.*

circulation des données à caractère personnel dans l'Union et stimule la concurrence entre les responsables du traitement en limitant la constitution d'écosystèmes numériques fermés et de barrières à l'entrée. Il facilite ainsi le passage d'un prestataire de services à un autre et la mise au point de nouveaux services. Enfin, il encourage l'émergence d'acteurs concurrençant les géants établis du numérique. Comme le résume la présidente de la CNIL : la portabilité « *doit permettre aux petits acteurs économiques de défier plus facilement les grands, en attirant les clients qui peuvent désormais leur apporter leurs données, diminuant ainsi le pouvoir de captation des grandes plateformes* ».

Dans sa dimension individuelle, la souveraineté numérique peut aussi être présentée comme une capacité d'**autodétermination informationnelle**[1], c'est-à-dire la possibilité pour chaque individu de « rester maître de son destin sur les réseaux » comme l'a exposé à votre commission Mme Pauline Türk.

Le RGPD entend, à cet égard, contribuer à une prise de conscience chez les citoyens-internautes de l'utilisation qui est faite de leurs données : il renforce le droit à l'information et oblige les responsables de traitements de données personnelles à une meilleure intelligibilité des explications fournies sur les finalités poursuivies et l'utilisation qu'ils en font.

Mais dans un univers numérique marqué par une **forte asymétrie entre, d'un côté, ceux qui contrôlent données et algorithmes et, de l'autre, ceux qui utilisent les plateformes**, imposer le respect de ces droits et les rendre effectifs pour les particuliers reste encore concrètement à accomplir.

Plusieurs représentants de ces grandes plateformes ont d'ailleurs reconnu que les outils développés pour rendre effective et systématique l'information présentée à leurs utilisateurs étaient récents et perfectibles. Interrogé sur ce point par le Président de notre commission, notre collègue Franck Montaugé, le représentant de *Google* a ainsi mis en avant le « tableau de bord » permettant désormais d'accéder à l'historique d'utilisation des données personnelles fournies, mais il a également reconnu que les internautes s'étaient encore peu saisis du droit à la portabilité et qu'une marge de progression était encore possible, notamment pour améliorer transparence des recommandations faites aux internautes sur la plateforme *Youtube*.

Pour favoriser la prise de conscience chez les citoyens-internautes de l'utilisation qui est faite de leurs données, il paraît souhaitable d'**encourager et de contrôler la mise en place des dispositifs techniques (tableaux de bords, envoi d'informations sur simple demande…) permettant de rendre effectifs les droits consacrés par le RGPD** en faveur des particuliers.

[1] *Pour de plus amples développement sur cette notion juridique et la revendication d'un droit en la matière, voir Les droits émergents dans le monde numérique : l'exemple du droit à l'autodétermination informationnelle (in Revue Politeia, N° 31, décembre 2017, Les métamorphoses des droits fondamentaux à l'ère du numérique, par Pauline Türk).*

La collecte de données par les acteurs du numérique repose d'ailleurs principalement sur le recours à des traceurs lors de la navigation des internautes sur le web, notamment les cookies, qui permettent de collecter des données extrêmement détaillées. Celles-ci sont fréquemment utilisées pour créer des profils détaillés à des fins de publicité ciblée, dans des conditions de transparence et de maitrise insuffisantes par l'utilisateur.

Or, ces opérations sont majoritairement réalisées par des acteurs situés en dehors de l'Union européenne, ce qui soulève des enjeux de souveraineté du fait de la nature des données collectées et des usages qui en sont faits. Une étude récente[1] a ainsi démontré que la régie publicitaire de Google collectait des données sur près de 45% des sites web du panel testé, tandis que le service d'analyse statistique du même acteur était présent sur près de 70% des sites du panel. De façon plus globale, cette même étude indique que, sur plus de 91% des sites du panel, la navigation des internautes est suivie par un acteur tiers.

Ainsi la souveraineté numérique ne peut être assurée que si ces dispositifs, particulièrement intrusifs et encadrés, notamment par la directive vie privée et communications électroniques, sont utilisés uniquement d'une manière permettant aux personnes concernées de garder la maîtrise sur leurs données.

Les utilisateurs doivent être informés de manière claire et complète sur l'impact des cookies et autres traceurs. Il s'agit d'une condition sine qua non pour recueillir leur consentement éclairé. Comme l'a rappelé récemment la Cour de justice de l'Union européenne[2], **ce consentement nécessite un acte positif clair qui implique un assentiment véritable de l'utilisateur**. Il convient donc de renverser le mécanisme actuellement à l'œuvre, qui ne garantit aucunement ce consentement véritable, afin de faire respecter la lettre de la loi européenne et nationale.

b) Aller plus loin : instaurer une obligation d'interopérabilité ?

La nécessité d'aller plus loin que le droit à la portabilité des données personnelles entre plateformes a été soutenue par plusieurs intervenants devant notre commission, qui souhaitent poursuivre et généraliser le mouvement bénéfique entamé avec le RGPD. Ils appellent de leurs vœux une

[1] *Imane Fouad, Nataliia Bielova, Arnaud Legout, and Natasa Sarafijanovic-Djukic, Tracking the Pixels: Detecting Unknown Web Trackers via Analysing Invisible Pixels.*

[2] *« le consentement (…) n'est pas valablement donné lorsque le stockage d'informations ou l'accès à des informations déjà stockées dans l'équipement terminal de l'utilisateur d'un site Internet, par l'intermédiaire de cookies, est autorisé au moyen d'une case cochée par défaut que cet utilisateur doit décocher pour refuser de donner son consentement » (affaire C-673/17, 1er octobre 2019).*

intervention du législateur qui garantirait une **obligation d'interopérabilité** à la charge des grandes plateformes du numérique[1].

On l'a vu, la portabilité permet à un utilisateur de quitter une plateforme avec une copie de ses données personnelles dans leur état au moment de la demande. Dans son principe, **l'interopérabilité garantit, elle, de poursuivre ailleurs l'activité initialement menée sur une plateforme sans perdre les contacts ni les liens sociaux établis.** Elle permettrait de communiquer d'une plateforme à une autre, sur le modèle des messageries électroniques : être abonné à un prestataire n'empêche pas de recevoir des courriels de personnes abonnées à d'autres prestataires. Concrètement, l'interopérabilité permet à quiconque de lire depuis un service A les contenus diffusés par ses contacts sur un service B, et d'y répondre comme s'il y était lui-même.

Votre rapporteur note avec intérêt que cette proposition n'émane pas seulement d'universitaires ou d'associations de défense des droits et libertés des internautes, mais qu'elle commence à être débattue au sein des instances européennes : Le rapport *Competition policy for the digital era* commandé par la commissaire européenne Mme Vestager et rendu public en avril 2019 y consacre de longs développements, distinguant interopérabilité des protocoles et interopérabilité des données. Il fait de l'interopérabilité un vecteur envisageable de promotion de la concurrence adapté, sous certaines conditions, aux spécificités d'une économie des plateformes dominée par des acteurs géants difficiles à contester en raison des forts coûts d'entrée.

En outre, selon les premières orientations officieuses des services de la Commission européenne pour une révision de la directive sur le commerce électronique, « *lorsqu'il existe des services équivalents, l'encadrement normatif devrait tenir compte de l'application émergente des règles existantes en matière de portabilité des données et explorer d'autres options permettant de faciliter les transferts de données et d'améliorer l'interopérabilité des services lorsqu'une telle interopérabilité est logique, techniquement réalisable et peut accroître le choix des consommateurs sans entraver la capacité de croissance (en particulier des petites entreprises). De telles initiatives pourraient être accompagnées d'initiatives de normalisation appropriées et d'approches de corégulation* »[2].

Dès lors, votre rapporteur comprend mal la frilosité du Gouvernement, telle qu'elle ressort des réponses écrites du secrétaire d'État au numérique, M. Cédric O, aux questions de votre rapporteur à ce sujet. Il

---

[1] *Lettre commune :* Pour l'interopérabilité des grandes plateformes en ligne *(21 mai 2019), signée par 75 organisations de défense des libertés, organisations professionnelles, hébergeurs et fournisseurs d'accès Internet associatifs.*

[2] *« Where equivalent services exist, the framework should take account of the emerging application of existing data portability rules and explore further options for facilitating data transfers and improve service interoperability where such interoperability makes sense, is technically feasible, and can increase consumer choice without hindering the ability of (in particular, smaller) companies to grow. Such initiatives could be accompanied by appropriate standardisation initiatives, and co-regulatory approaches ».*

l'encourage donc, comme il l'indique, à « *instruire correctement l'ensemble des aspects quant aux objectifs précisément poursuivis [par l'interopérabilité], à sa faisabilité technique et opérationnelle, à son coût ou à son impact sur l'innovation* », et à présenter rapidement au Parlement la position qu'il compte défendre au niveau européen.

Dresser un **bilan du droit à la portabilité** des données personnelles depuis la loi « République numérique » et le RGPD et des obstacles pouvant subsister à sa pleine application.

Étudier la faisabilité technique et opérationnelle d'une obligation d'interopérabilité (bénéfices, coûts, impact sur le consommateur et l'innovation), y compris comme mesure de régulation asymétrique imposée aux grandes plateformes systémiques, en associant les régulateurs nationaux (ADLC, CNIL) et en présentant au Parlement la position que le Gouvernement compte défendre au niveau européen.

D. RÉPONDRE AU DÉFI FISCAL LANCÉ PAR LES GRANDES ENTREPRISES DU NUMÉRIQUE : UN ENJEU DE SOUVERAINETÉ ET D'ÉQUITÉ

Après l'ordre économique et l'ordre juridique, **le pouvoir acquis par certaines entreprises du numérique**, en particulier américaines, et de plus en plus asiatiques, **remet en cause deux autres missions régaliennes de l'État**, au cœur de sa souveraineté : **lever les impôts et battre monnaie**. Pour autant, ces deux domaines pourraient aussi se révéler être de puissants instruments pour reconquérir notre souveraineté numérique, individuelle ou collective.

1. L'impôt contourné

a) Les entreprises du numérique sont régulièrement accusées de contourner les règles d'imposition nationales

Les **stratégies utilisées par les entreprises du numérique pour contourner les législations fiscales nationales** ont été très bien documentées par le rapport d'information de notre collègue Catherine Morin-Desailly sur *L'Union européenne, colonie du monde numérique ?*, déjà cité.

Si ces multinationales utilisent des méthodes « traditionnelles » pour optimiser leur imposition, elles tirent également profit des caractéristiques propres au secteur du numérique : (i) le peu d'accroches stables pour la fiscalité ; (ii) une part importante d'actifs incorporels, ce qui ne rend que plus ardue leur valorisation comptable ; (iii) la difficulté à localiser la valeur ajoutée créée dans l'économie numérique, du fait du découplage que ces entreprises peuvent facilement opérer entre lieu

d'établissement et lieu de consommation (ex. les stratégies dites du « double irlandais » ou du « sandwich néerlandais »[1]) ; (iv) la prévalence dans cette économie du modèle de l'intermédiaire, qui capte la marge au détriment des acteurs traditionnels.

Les **règles fiscales internationales** étant **largement inadaptées à la création de valeur dans l'économie numérique,** la France ne peut pleinement remplir l'une de ses missions régaliennes, celle de lever l'impôt[2]. Sa souveraineté sur les acteurs du numérique et dans le monde numérique s'en trouve donc fragilisée, d'autant plus **que ces entreprises bénéficient parfois du concours de pays partenaires**. À titre d'exemple, la Commission européenne a fini par qualifier d'aide d'État le régime fiscal spécifique accordé par l'Irlande à Apple[3].

Les États se trouvaient donc démunis face aux pratiques de ces multinationales. Le seul levier sur lequel ils pouvaient s'appuyer, et qu'ils utilisent encore, est celui de la procédure contentieuse. Google a ainsi conclu une convention judiciaire d'intérêt public[4] avec le Parquet national financier et un accord avec l'administration fiscale française. Dévoilé le 12 septembre, le montant total de ces deux accords s'élève à près d'un milliard d'euros et met fin à une procédure lancée par l'État en 2015, par le biais du dépôt d'une plainte pour « fraude fiscale aggravée et blanchiment en bande organisée de fraude fiscale aggravée ». En dépit de certains succès, le recours à la justice ne remédie pas aux causes mais aux conséquences du problème sous-jacent, celui de l'absence d'équité fiscale.

Sur ce sujet, comme sur d'autres, **le Sénat recommande depuis longtemps que la France avance au niveau national avant d'avancer au**

---

[1] *Pour une description détaillée de ces processus, voir le rapport de la mission d'expertise sur la fiscalité numérique, Pierre Collin et Nicolas Colin (2013), p. 21. Lien vers le rapport : https://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf*

[2] *Pour reprendre les termes de Bernard Stiegler, auditionné le 12 juin 2019 par le Président de votre commission d'enquête,* « l'industrie numérique menace la puissance publique de devenir incapable. N'ayant pas la capacité de percevoir l'impôt et de percevoir les taxes, elle est mise dans une situation d'incapacitation structurelle » (cf. Les actes du forum de fiscalité numérique du 14 février 2012, annexe V).

[3] *L'Irlande est accusée par la Commission européenne d'avoir octroyé pour près de 13 milliards d'euros d'avantages fiscaux à Apple entre 1991 et 2014. Ainsi, selon la Commission, Apple n'aurait payé en 2014 que 0,005 % de taxe sur ses profits réalisés en Europe. Voir la décision (UE) 2017/1283 de la Commission du 30 août 2016 concernait l'aide d'État S.38373(2014/C) (ex 2014/NN) (ex 2014/CP) octroyée par l'Irlande en faveur d'Apple.*
Lien vers la décision en français :
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32017D1283.
Lien vers la décision en anglais (la seule faisant foi) :
http://ec.europa.eu/competition/state_aid/cases/253200/253200_1851004_674_2.pdf

[4] *Pour rappel, c'est la loi n° 2018-898 du 23 octobre 2018 relative à la lutte contre la fraude qui a autorisé, par le biais de deux amendements soutenus par le Sénat, la conclusion de transactions pénales en matière de fraude fiscale et autorisé la DGFiP à conclure un accord avec les contribuables concernés. La signature de cette convention signifie la fin des poursuites et permet à Google de ne pas reconnaître sa culpabilité sur le chef d'accusation de fraude fiscale.*

niveau européen. Le Gouvernement tient compte de ces exhortations. D'abord en proposant une taxe sur les services numériques (TSN), puis en émettant l'idée d'un dispositif de « *name and shame* », qui dresserait une liste noire des plateformes numériques non collaboratives[1]. Le Gouvernement avait pourtant critiqué en 2015, devant le Sénat, tout dispositif national de type « taxe Google »[2] , en insistant sur le fait que le seul échelon pertinent était l'échelon européen. Pourtant, face au refus de quatre États membres, l'unanimité étant requise en matière fiscale, **la France n'a pu que constater l'échec des négociations au niveau de l'Union européenne**. C'est ce qui l'a conduite à agir seule, devenant le premier pays européen à instaurer une taxation spécifique sur les services numériques.

Le tableau suivant présente l'état d'avancement des projets de taxation des services numériques dans l'Union européenne.

[1] *Quatre critères seraient retenus pour établir cette liste : le paiement de la taxe sur les services numériques française si l'entreprise y est assujettie, le paiement de la TVA, la facilité avec laquelle l'administration fiscale obtient des réponses aux demandes qu'elle adresse à l'entreprise, et la transmission des revenus des utilisateurs.*

[2] *Discussion lors de la séance du 16 avril 2015 du projet de loi Croissance, activité et égalité des chances économiques. Lien vers la discussion :* http://www.senat.fr/seances/s201504/s20150416/s20150416007.html

Comparaison des projets de taxation des services numériques dans l'Union européenne

	Calendrier	Taux	Seuils	Champ
Union européenne	Projet abandonné	3 %	Chiffre d'affaires mondial supérieur à 750 millions d'euros pour l'ensemble des activités et chiffre d'affaires sur les services taxables supérieur à 50 millions d'euros au niveau de l'Union	Services de publicité ciblée, de mise à disposition d'interfaces numériques entre utilisateurs et de transmission de données sur les utilisateurs
France	Entré en vigueur pour l'année 2019	3 %	Chiffre d'affaires mondial supérieur à 750 millions d'euros et chiffre d'affaires supérieur à 25 millions d'euros en France	Services de publicité ciblée, de mise à disposition d'interfaces numériques entre utilisateurs leur permettant de fournir des biens et services ; vente de données à des fins publicitaires
Italie	Adoption dans la loi de finances pour 2019 mais pas de publication des décrets d'application	3 %	Chiffre d'affaires mondial supérieur à 750 millions d'euros pour l'ensemble des activités et chiffre d'affaires sur les services taxables supérieur à 5,5 millions d'euros en Italie	Services de publicité, d'intermédiation et de vente de données générées par les utilisateurs ; fourniture de contenus numériques, des services de communication ou des services de paiement
Espagne	La dissolution du Congrès a rendu caduc le projet de loi déposé de TSN	3 %	Chiffre d'affaires mondial supérieur à 750 millions d'euros pour l'ensemble des activités et chiffre d'affaires sur les services taxables supérieur à 25 millions d'euros en Espagne	Services de publicité, d'intermédiation et de vente de données générées par les utilisateurs ; publicité non ciblée et vente de données à d'autres fins que le ciblage publicitaire
Royaume-Uni	Envisagé dans la loi de finances 2019-2020, avant la démission de Theresa May	2 %	Chiffre d'affaires mondial supérieur à 500 millions de livres au titre des services couverts et chiffre d'affaires sur ces mêmes services supérieur à 25 millions de livres au Royaume-Uni	Services d'intermédiation en ligne et d'utilisation des données retirées de ces usages
Autriche	Constitution d'un groupe de travail en janvier 2019	5 %	Chiffre d'affaires mondial supérieur à 750 millions d'euros pour l'ensemble des activités et chiffre d'affaires sur les services taxables supérieur à 25 millions d'euros en Autriche	Services de publicité ciblée

b) La taxe française sur les services numériques : une réaction justifiée mais périlleuse

Frédéric Bastiat, économiste français du XIXe siècle, écrivait qu' « *il arrive presque toujours que,* ***lorsque la conséquence immédiate est favorable, les conséquences ultérieures sont funestes****, et* vice versa »[1]. Votre rapporteur ne peut qu'attirer l'attention du Gouvernement sur la justesse de cet avertissement. **En décidant de faire cavalier seul** sur la taxation des géants du numérique, pour répondre à un objectif qu'on ne peut lui reprocher, celui de rétablir l'équité fiscale entre les entreprises, **la France s'expose aux représailles américaines**.

Cette menace est d'ailleurs l'une des illustrations les plus frappantes des **limites de la souveraineté française** vis-à-vis des acteurs du numérique. Le 10 juillet 2019, le Président Trump a annoncé avoir confié au bureau du représentant américain pour le commerce, M. Robert Lighthizer, le soin de mener une enquête sur les répercussions de la TSN française et sur l'éventuelle discrimination subie par les entreprises américaines. Dès le 24 juin, les sénateurs américains Chuck Grassley (républicain) et Ron Wyden (démocrate) avaient envoyé au secrétaire au Trésor, Steven Mnuchin, une lettre l'enjoignant à inciter la France à faire machine arrière.

Si le ministre de l'Économie et des Finances, M. Bruno Le Maire, a rapidement réagi à ces menaces en arguant que **cette taxe relevait des prérogatives souveraines de la France** et qu'elle n'avait pas été construite pour viser exclusivement les entreprises américaines, il n'en demeure pas moins que **les risques sont grands**. Lors de leur audition devant M. Lighthizer, le 19 août 2019, les entreprises américaines du numérique ont ainsi vertement critiqué le dispositif français, condamnant une initiative qui nuit aux négociations en cours à l'OCDE, qui les discrimine et qui leur impose des coûts élevés de mise en conformité.

Votre rapporteur relève en outre que **de telles pressions sont fort peu communes entre pays alliés**. Le recours par les États-Unis à la procédure dite de la section 301 du *Trade Act* de 1974, utilisée par Washington dans son conflit qui l'oppose à Pékin sur la violation des droits de propriété intellectuelle, est en effet inédit dans l'histoire de ses relations commerciales avec la France. Outre le rehaussement des tarifs douaniers sur certaines marchandises françaises, comme le vin ou les produits de luxe, les États-Unis pourraient également **doubler les impôts appliqués aux entreprises et aux nationaux français résidant sur le sol américain**, tel que les y autorise l'article 891 du *US Code*.

[1] Ce qu'on voit et ce qu'on ne voit pas, *Frédéric Bastiat, 1850*.

La section 301 du *Trade Act* (1974)

Cet article autorise le bureau du représentant des États-Unis pour les questions commerciales internationales à prendre certaines mesures (suspension ou retrait des concessions, imposition de droits supplémentaires, autres restrictions à l'importation) en réponse aux obstacles au commerce imposés par d'autres pays. Quand les négociations visant à remédier à ces « barrières » commerciales ont en effet échoué, les États-Unis peuvent prendre toute action destinée à compenser ces pertes. Une liste de « représailles » avec les produits concernés est alors publiée.
Source : https://www.trade.gov/mas/ian/tradedisputes-enforcement/tg_ian_002100.asp

L'article 891 du *US Code*

Lorsque le Président des États-Unis estime qu'une loi étrangère discrimine les citoyens ou les entreprises des États-Unis, ou a une portée extraterritoriale à leur encontre, il peut doubler les impôts auxquels sont soumis les citoyens et les entreprises du pays concerné, par le biais d'une proclamation annuelle renouvelable. La somme totale due ne peut dépasser 80 % du revenu taxable des entités concernées.
Source : https://www.law.cornell.edu/uscode/text/26/891

Les 400 millions d'euros que la TSN est censée rapporter pour l'année 2019[1] vaudront-ils ces éventuelles représailles ?

Le G7 : la perspective d'un accord bilatéral ?

À l'issue du G7, qui s'est tenu à Biarritz du 24 au 26 août 2019, un compromis aurait été trouvé entre les États-Unis et la France sur la TSN française. Outre la perspective d'un accord international à l'OCDE au premier semestre 2020[2], il s'agirait plus concrètement d'instaurer une déduction des effets de la taxe française. Ainsi, si une entreprise paye 10 millions d'euros en 2019 au titre de la taxe française, mais qu'elle n'aurait dû en payer que 5 si la formule internationale était entrée en vigueur, les autorités fiscales françaises lui rembourseront les 5 millions d'euros d'écart, sous la forme d'un crédit d'impôt.

Cet accord a été vivement dénoncé par la *Computer & Communications Industry Association*, qui représente notamment Google, Amazon et Facebook, et qui critique toujours les effets discriminatoires de la TSN française.

[1] *Selon les chiffres de l'étude d'impact annexée au projet de loi.*

[2] *Un groupe de travail réunissant les États-Unis, la France et l'OCDE devrait être constitué pour régler les derniers points techniques sur lesquels achoppent encore les négociations internationales. Selon Pascal Saint-Amans, directeur du centre de politique et d'administration fiscales de l'OCDE, un projet d'accord devrait être présenté avant le G20 Finances, qui se tiendra à Washington le 17 octobre. Quatre points seraient encore âprement débattus : la définition du lien entre l'entreprise et le territoire dans lequel elle opère ; le niveau de taxation ; la définition des entreprises concernées ; la question d'accorder ou non un statut particulier aux entreprises purement et exclusivement digitales.*

2. Modifier nos règles d'imposition : un monopole régalien et une opportunité pour l'attractivité de notre territoire

Plusieurs personnes auditionnées par votre commission ont souligné **l'iniquité des règles d'imposition actuelles** : les grandes entreprises du numérique, spécialistes de l'optimisation fiscale, profitent des infrastructures et des formations françaises financées par l'impôt de leurs utilisateurs et clients. Une étude de la Commission européenne publiée en 2017 estimait ainsi que le différentiel d'imposition entre les multinationales du numérique et les multinationales traditionnelles était de 14 points (9,5 % contre 23,2 %)[1].

Ce constat a suscité deux types de réaction, à la finalité commune. La première est le projet européen de taxe sur les services numériques, avorté mais poursuivi à l'échelle nationale par quelques pays européens comme la France, le seul où il ait, à ce jour, officiellement abouti. La seconde est la relance des négociations internationales, dans le cadre de l'OCDE, sur la révision des règles de la fiscalité.

a) La taxe sur les services numériques : une démarche incomplète

Si elle constitue une première réponse, **la taxe sur les services numériques** (TSN), définitivement adoptée par le Parlement au mois de juillet 2019, **est incomplète**.

Elle couvre deux types de services : (i) les services d'intermédiation, qui permettent aux utilisateurs d'entrer en contact et d'interagir entre eux, notamment en vue de fournir directement des biens et des services ; (ii) la publicité ciblée et la vente de données à des fins publicitaires. Le but était d'**appréhender la valeur générée par le « travail gratuit » des utilisateurs situés en France**. De fait, ce périmètre exclut les services de mise à disposition de contenus numériques (ex. Netflix, iTunes) ou la vente en ligne pour compte propre (ce qui correspond, par exemple, à une partie non négligeable des activités d'Amazon). Cette action, au périmètre restreint, **ne répond pas non plus aux enjeux tels que la localisation des bénéfices, l'harmonisation de la réglementation des prix de transfert ou encore la lutte contre la fraude par le commerce en ligne**.

La commission des finances du Sénat a en outre alerté le Gouvernement sur les **conséquences juridiques incertaines** de cette législation nationale[2]. Trois difficultés ont ainsi été ignorées. La taxe n'a pas

---

[1] *Centre for European Economic Research (ZEW), études réalisées pour la Commission européenne, TAXUD/2013/CC/120 :* Effective tax rates in an enlarged European Union – Final report 2016 *(2017) et* The Impact of Tax - planning on Forward - looking Effective Tax Rates *(2016).*

[2] *Rapport n° 496 (2018-2019) de M. Albéric de Montgolfier du 15 mai 2019, fait au nom de la commission des finances, sur le projet de loi portant création d'une taxe sur les services numériques et modification de la trajectoire de baisse de l'impôt sur les sociétés. Lien vers le rapport : https://www.senat.fr/rap/l18-496/l18-4961.pdf*

été notifiée à la Commission européenne, son éventuelle remise en cause conduirait l'État à devoir rembourser les sommes indûment perçues. Ne concernant qu'un seul groupe français, elle pourrait être qualifiée de restriction déguisée. Enfin, la taxe pourrait être requalifiée par le juge comme relevant du champ des conventions fiscales[1].

Votre rapporteur estime que **la mise en œuvre de la TSN sera délicate et que le rendement, estimé à 400 millions d'euros, doit être envisagé avec précaution**.

Une taxe est toujours, au moins en partie, supportée par le consommateur final[2], en particulier quand les entreprises sont en position ultra-dominante, comme c'est le cas des Gafam. Malgré les dénégations de l'administration, **les coûts induits par cette tentative de l'État pour réaffirmer son monopole souverain pourraient bien être supportés par les entreprises et citoyens français**. Amazon France a ainsi annoncé, le 1er août 2019, son intention de répercuter la TSN sur les services proposés aux entreprises utilisant sa plateforme de commerce en ligne.

Le recouvrement de la taxe sera en outre complexe : il repose sur une procédure déclarative et sur la transmission de données difficiles à analyser. En l'absence de déclaration, il sera très compliqué pour l'administration de taxer d'office l'entreprise : les services devront, en cas de contentieux, exposer les données sur lesquelles ils se sont appuyés pour définir le montant de l'imposition due, ce qui pourrait rendre l'assiette de TSN retenue fragile et contestable.

Compte tenu de ces importantes limites, et prenant au mot le Gouvernement, qui n'a cessé de répéter que la taxe serait temporaire et qu'une solution internationale était toute proche d'être trouvée, **le Sénat avait insisté sur le caractère non permanent de la taxe et sur la nécessité de faire aboutir les négociations internationales, pour parvenir le plus rapidement possible à un accord**. Votre rapporteur ne peut que réitérer cette position.

b) Parvenir à un accord mondial sur la fiscalité

Il est nécessaire, comme l'a rappelé M. Henri Verdier devant votre rapporteur, « *de prendre acte du fait qu'internet a transformé la chaîne de création des valeurs* ». Cela ne suppose pas de révolutionner nos normes fiscales ou de complexifier nos règles, il faut simplement **prendre la mesure des**

---

[1] *Cela en annihilerait automatiquement les effets puisque la France ne pourrait percevoir les produits de la taxe que sur les entreprises disposant d'un établissement stable sur son territoire, conformément aux principes internationaux en vigueur.*

[2] *Les craintes d'une répercussion de la taxe sur les entreprises et particuliers résidant en France avaient été soulevées lors de la discussion par la commission des finances du projet de loi portant création de la taxe sur les services numériques et modification de la trajectoire de baisse de l'impôt sur les sociétés, le mercredi 15 mai 2019. Lien vers le compte-rendu : https://www.senat.fr/compte-rendu-commissions/20190513/fin.html#toc2*

changements induits et modifier nos principes, ce qui ne pourra se faire sans un travail constant et une présence accrue dans les fora de négociations internationales.

Votre rapporteur rappelle que le **projet initial de la Commission européenne** sur la fiscalité du numérique poursuivait un double-objectif : l'instauration à court-terme, d'une taxe européenne sur les services numériques et, à plus long terme, **l'introduction d'un nouveau critère pour qualifier un établissement stable** : celui de « **présence numérique significative** ». La numérisation de l'économie rend en effet obsolète le concept d'établissement stable, selon lequel une entreprise doit être physiquement présente sur le territoire d'un État pour ce que ce dernier puisse l'imposer. Cette révision devait également permettre de mieux appréhender le rôle joué par les données et le « travail gratuit » fourni par les utilisateurs, au bénéfice des entreprises du numérique.

Dans le cadre du **projet BEPS** (érosion de la base d'imposition et transfert de bénéfices), lancé en 2013 à Saint-Pétersbourg, l'OCDE a ouvert un cycle de travail pour adapter le système fiscal international aux stratégies des multinationales, et en particulier à celles des multinationales du numérique. D'après le programme de travail de l'OCDE, la réforme envisagée s'appuierait sur **deux piliers** : (i) **définir le lieu et la base pour le paiement de l'impôt sur les bénéfices** ; (ii) **instaurer un taux d'imposition minimal pour toutes les multinationales**.

Sur le premier pilier, les options divergent. Les États-Unis et le Royaume-Uni sont davantage favorables à une **dissociation des bénéfices entre profits dits « routiniers »,** issus d'activités traditionnelles telles que la production, la distribution, la recherche et le développement, **et profits dits « non routiniers »**, ensuite répartis entre les pays pour y définir le montant de l'imposition due. La seconde option consisterait à **fractionner le bénéfice global de la société en fonction des pays où elle opère**. L'OCDE ne renonce pas non plus à défendre une troisième option plus spécifique pour les Gafam, avec une imposition non pas fondée sur le pays de production, mais sur le pays de distribution des services.

Le projet BEPS

L'érosion de la base d'imposition et le transfert de bénéfices fait référence aux stratégies utilisées par les entreprises pour exploiter les failles et les différences entre les règles fiscales afin de faire « disparaître » des bénéfices ou de les transférer dans des pays à la fiscalité avantageuse mais dans lesquels elles n'exercent aucune activité réelle. En 2015, l'OCDE estimait que **les pertes de recettes générées par ces pratiques pourraient s'élever jusqu'à 240 milliards de dollars, soit 10 % des recettes fiscales globales**.

Le Cadre inclusif pour coordonner les mesures internationales pour lutter contre les pratiques de BEPS et améliorer les règles fiscales internationales rassemble 129 pays et juridictions.

Source : OCDE, http://www.oecd.org/fr/ctp/beps/

Enfin, **votre rapporteur regrette que le Gouvernement ne se soit pas saisi des nombreux rapports rédigés sur le sujet de la fiscalité du numérique**, qui lui auraient sans doute permis de porter des idées plus novatrices sur le plan international et conforme aux valeurs aujourd'hui défendues par l'Union européenne. Par exemple, dans leur rapport, MM. Collin et Colin défendaient l'application du principe du « pollueur-payeur » aux entreprises chargées de traiter des données personnelles, afin de les inciter à adopter des pratiques conformes à des objectifs d'intérêt général tels que la protection des libertés individuelles, de la vie privée ou l'innovation[1].

Défendre, dans les négociations internationales encadrées par l'OCDE, une nouvelle définition de l'établissement stable pour les entreprises du numérique et un principe d'imposition non plus fondé sur le lieu de production, mais sur le lieu de consommation.

c) La fiscalité, un enjeu d'attractivité

Votre rapporteur considère que **la France aurait tort de ne considérer sa prérogative souveraine que sous l'angle de la sanction**, qui viendrait punir le comportement des multinationales du numérique. La fiscalité doit également être conçue et réfléchie comme un outil d'avenir pour **maintenir la compétitivité et l'attractivité de la France**, que ce soit en facilitant l'installation des infrastructures stratégiques du numérique ou en attirant le capital financier et humain nécessaire au développement des innovations (faisant l'objet de développements ultérieurs).

[1] *Mission d'expertise sur la fiscalité de l'économie numérique, Pierre Collin et Nicolas Colin, janvier 2013.*

E. DEVENIR PROACTIF ET INNOVANT DANS LE DOMAINE MONÉTAIRE

1. Les cryptoactifs : la monnaie concurrencée ?

Les cryptoactifs[1] se définissent par leur caractère privé, totalement virtuel et par leur absence d'adossement physique ou financier. Il en existerait près de 1 600 aujourd'hui pour une capitalisation estimée à près de 270 milliards de dollars[2]. Votre rapporteur a pu constater qu'il existait une forte ambivalence sur les cryptoactifs : une **attirance forte pour les innovations proposées** mais un **souci constant de protéger les investisseurs, les consommateurs et la stabilité du système financier**.

Définir les cryptoactifs

Les actifs numériques, ou cryptoactifs, ont été pour la première fois définis au 7° bis de l'article L. 561-2 du code monétaire et financier comme « *tout instrument contenant sous forme numérique des unités de valeur non monétaire pouvant être conservées ou être transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur* ». **Cette définition, indirecte, est apparue dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme**.

Dans le cadre de la mise en place d'un **régime d'imposition des gains issus de la cession de cryptoactifs** par des particuliers, la loi de finances pour 2019 a modifié le code général des impôts. L'article 150 VH *bis* distingue ainsi deux catégories d'actifs numériques :

- « *les jetons, à l'exclusion de ceux remplissant les caractéristiques des instruments financiers (...) et des bons de caisse* ». *Les jetons sont des* « biens incorporels représentant, sous forme numérique, un ou plusieurs droits, pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien » ;

- « *toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement* ».

[1] *Votre commission d'enquête reprend ici l'appellation officielle des autorités publiques et des banques centrales, qui ne qualifient pas ces actifs de « cryptomonnaies ». Ces actifs ne remplissent en effet pas les trois fonctions dévolues à la monnaie : une unité de compte, un intermédiaire des échanges, et une réserve de valeur.*

[2] *Ce chiffre est à prendre avec précaution, du fait de la volatilité très forte des cryptoactifs. Il est tiré du rapport remis au ministère de l'économie et des finances par MM. Landau et Genais sur les cryptomonnaies (juillet 2018). Lien vers le rapport :* https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/184000433.pdf

Face à leur développement et pour répondre à leur potentiel, **la loi Pacte**[1] **encadre de manière plus explicite les intermédiaires en actifs numériques,** avec **deux volets de régulation**.

Le **premier volet est optionnel** : les intermédiaires, comme les plateformes d'échanges de cryptoactifs, pourront solliciter un agrément auprès de l'Autorité des marchés financiers (AMF), qui est un gage de fiabilité et de sérieux.

Le **second volet est contraignant**. Il prévoit un enregistrement obligatoire de toutes les plateformes de change entre cryptoactifs et monnaies conventionnelles, au titre de **la lutte contre le blanchiment d'argent**. Dans son rapport d'activité pour l'année 2018, Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins)[2] notait en effet que « *des marges de progression existent en termes de volume de déclaration chez tous les professionnels des cryptoactifs* », alors même que le nombre de déclarations a déjà plus que doublé entre 2017 et 2018 (250 contre 528)[3]. **Il reste bien sûr à voir si les pouvoirs publics disposeront des capacités nécessaires pour dresser une liste exhaustive de ces plateformes et pour les contrôler**.

Votre rapporteur ne peut qu'**enjoindre les pouvoirs publics à ne pas relâcher leurs efforts et à ne pas réduire les moyens alloués à la régulation de ces cryptoactifs**, en particulier alors que les acteurs du numérique, à l'instar de Facebook, se montrent de plus en plus intéressés par leurs potentialités (cf. *infra*).

2. Répondre au défi des cryptoactifs : la perspective d'une cryptomonnaie banque centrale

a) Les projets développés par les acteurs privés doivent inciter la puissance publique à agir plus rapidement dans ce domaine

Comme toute innovation, les cryptoactifs peuvent s'avérer, dans l'usage qui en est fait, positifs et menaçants, en particulier si l'État souverain ne s'en empare pas au bon moment et de la bonne façon. Il risque alors **de se voir concurrencé et finalement dépassé par des acteurs privés**, sur lesquels la force de sa régulation pourrait se trouver amoindrie.

Les banques centrales et autorités financières considèrent aujourd'hui que **les cryptoactifs ne constituent pas une menace pour la**

---

[1] *Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite loi Pacte.*

[2] *Tracfin est un service à compétence nationale placé sous l'autorité du ministère de l'Action et des Comptes publics chargé du renseignement financier en vue de lutter contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme.*

[3] *Rapport annuel d'activité de Tracfin* Traitement du renseignement et action contre les circuits financiers clandestins, *2018, p. 28.*
Lien vers le rapport : https://www.economie.gouv.fr/files/web_RAA_tracfin-2018.pdf

stabilité financière mondiale, en raison de leur volume limité et de leur faible acceptabilité[1]. Toutefois, les pays du G20 rappellent constamment que les États doivent, par leurs réglementations, **s'assurer que ces actifs numériques ne sont pas utilisés pour des actions de blanchiment de capitaux ou de financement du terrorisme**, étant entendu qu'ils peuvent garantir un **quasi-anonymat à leurs détenteurs**. La Banque centrale européenne (BCE) a par exemple créé en mai 2018 un groupe de travail informel pour accroître sa connaissance des enjeux soulevés par les cryptoactifs et pour en surveiller les potentiels effets négatifs[2].

Jusqu'ici, les autorités de supervision, nationales, européennes ou internationales, considéraient plutôt les cryptoactifs comme des **actifs risqués, réservés aux investisseurs les plus avertis**. La plupart des États ont ainsi adopté l'**approche dite du « bac à sable »**, en allégeant les obligations pesant sur ces acteurs pour qu'ils puissent tester leurs technologies et se lancer plus facilement sur le marché. Le régulateur est ensuite conduit à évaluer les changements induits par ces produits et, éventuellement, à renforcer les obligations à l'encontre des acteurs concernés. En outre, **tous les cryptoactifs ne portent pas l'ambition de devenir de véritables « monnaies privées »**, certains sont avant tout des actifs financiers ou des moyens de paiement et n'ont pas vocation à concurrencer les banques, mais bien à proposer un nouveau service financier.

Les États et les cryptoactifs

Plusieurs pays et banques centrales ont lancé des travaux de recherche et des projets innovants sur les cryptoactifs, avec des résultats contrastés :

- selon les dernières informations communiquées par la Banque populaire chinoise en août 2019, la Chine pourrait être le premier État à émettre sa propre cryptomonnaie, une *stablecoin* adossée au yuan. Ce projet, débuté en 2014, serait aujourd'hui entré en phase de test et viserait à progressivement remplacer l'usage de l'argent liquide, mais aussi à mieux surveiller les transactions de ses utilisateurs ;

- l'Estonie souhaitait créer sa propre crypto-devise, l'estcoin, avant que la Banque centrale européenne et les autorités bancaires nationales ne fassent part de leurs réticences ;

- au Japon, le *bitcoin* a été reconnu système de paiement officiel en avril 2017 et toutes les plateformes d'échange de cryptoactifs doivent s'enregistrer auprès de la *Japan Financial Services Agency* (JFSA) ;

[1] *Banque centrale européenne,* Crypto-assets : implications for financial stability, monetary policy and payments and market infrastructures *(Mai 2019). Lien :* https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf
[2] *Op. cit.*

- le Brésil n'a pas renoncé à son projet d'émettre une *stablecoin* adossé au real, sa monnaie nationale. Des plateformes brésiliennes devraient bientôt pouvoir le proposer ;

- la Suède étudie depuis plusieurs années la possibilité d'émettre une cryptomonnaie banque centrale, l'e-krona, qui lui permettrait par exemple de répondre à la diminution de l'utilisation de l'argent en espèces ;

- le Canada et Singapour ont conduit plusieurs expérimentations utilisant la *blockchain* pour les règlements bruts en temps réel (c'est-à-dire dans ce système, une instruction de transfert de fonds ou de titres est transmise, traitée et réglée au moment où elle est émise).

Source : Rapport d'information de l'Assemblée nationale, mission d'information relative aux monnaies virtuelles (janvier 2019). Lien : http://www.assemblee-nationale.fr/15/rap-info/i1624.asp ; Bech et Garrat (Banque des règlements internationaux), 'Central bank cryptocurrencies'. Bank of International Settlements, (septembre 2017). Lien: https://www.bis.org/publ/qtrpdf/r_qt1709f.htm ; commission d'enquête.

Dans ce contexte, **l'annonce par Facebook au mois de juin 2019 du lancement de son propre cryptoactif au début de l'année 2020, le libra, a provoqué une onde de choc**[1]. Pour reprendre les mots de Benoît Coeuré, membre du directoire de la BCE à qui le G7 a confié la direction d'un groupe de travail sur le libra : on a maintenant à faire à « ***un éléphant dans le bac à sable*** »[2]. **C'est en effet bien le pouvoir de marché de Facebook et sa puissance de frappe, fort de ses 2,4 milliards d'utilisateurs, qui a conduit l'ensemble des régulateurs nationaux et internationaux à s'inquiéter des velléités de l'entreprise**. Le ministère de l'économie et des finances a indiqué devant votre rapporteur qu'il ne permettrait « *jamais* à *une entreprise privée de se doter de cet instrument de souveraineté d'un État qu'est la monnaie* » et a ajouté, à l'OCDE le 12 septembre 2019, que « *nous ne pouvions pas autoriser le développement du libra sur le sol européen* ». Les pouvoirs publics français ont-ils réellement la capacité de s'opposer au libra ?

[1] *À noter que d'autres acteurs du numérique sont déjà présents dans le domaine des paiements, à l'image d'Apple. L'entreprise propose, depuis 2014, Apple Pay, un service qui permet de réaliser des paiements sans contact avec un iPhone ou l'Apple Watch, et vient de lancer aux États-Unis l'Apple Card, une carte de crédit en partenariat avec la Goldman Sachs.*

[2] La taxe GAFA et la cryptomonnaie libra, principaux sujets de discussion entre ministres des finances du G7, article publié dans Le Monde par Marie Charrel (17 juillet 2019). Lien vers l'article : *https://www.lemonde.fr/economie/article/2019/07/17/libra-et-la-taxe-gafa-au-menu-des-ministres-des-finances-du-g7_5490152_3234.html*

Le libra en six questions

1. Quelles sont les ambitions du libra ?

En se référant au livre blanc du libra et aux statuts de Libra Networks, l'association basée à Genève et dirigée par David Marcus, ancien dirigeant de Paypal, le champ d'intervention du libra est potentiellement très vaste. Le libra vise en effet à « *fournir des services dans les domaines de la finance et de la technologie* ». Le libra pourrait servir de moyen de paiement sur internet et sur les applications du groupe Facebook. Il pourrait également s'acheter sur des plateformes d'échange, être stocké et revendu. Il serait convertible en unités de compte officielles, contrairement au bitcoin.

2. Qui sont les partenaires de Facebook ?

Facebook compte déjà près d'une trentaine de partenaires, pour la plupart de grandes entreprises du commerce ou du paiement (Uber, Visa-Mastercard, Paypal, Kiva, Spotify et Iliad, seul partenaire français du projet pour le moment).

3. Quels sont les intérêts des parties prenantes au projet ?

Facebook a conscience des limites de son modèle, basé sur la vente de publicité personnalisée sur ses réseaux sociaux. En lançant sa propre cryptomonnaie, Facebook prendrait de vitesse ses concurrents directs et pourrait à terme développer des services financiers associés, comme l'envisagent d'ailleurs d'autres entreprises, à l'image d'Apple. Enfin, Facebook cherche à se placer aux avant-postes dans la compétition mondiale entre réseaux sociaux : en Chine, WeChat a intégré avec succès un système de paiement à son application. En Asie, mais aussi en Amérique du sud, l'essor des « **super-applications** » précède de quelques années celui que l'on observe maintenant en Occident : elles visent à compléter une offre de services publics parfois défaillants et offrent des solutions de paiement au champ très vaste (ex. les Chinois peuvent payer leur fournisseur d'électricité *via* WeChat).

Pour les partenaires de Facebook, l'intérêt est double : élargir leur clientèle, notamment dans les pays en développement, et, pour les acteurs installés du paiement, comme Visa-Mastercard ou Paypal, ne pas se laisser dépasser par les nouvelles solutions proposées par Facebook en s'y associant.

Pour les commerçants qui viendraient à accepter ce système de paiement, les commissions pourraient diminuer, les systèmes opérants sur la technologie de la *blockchain* étant réputés moins coûteux.

4. Quelle est la gouvernance de ce projet ?

Selon les premières informations communiquées, et confirmées par l'audition du représentant de Facebook en France par votre rapporteur, le 18 juillet, la structure de décision, soit une association à but non-lucratif basée en Suisse, sera collégiale. Facebook ne serait alors qu'un partenaire parmi d'autres au sein de l'association.

5. Sur quelle technologie s'appuie le libra ?

Le fonctionnement du libra s'appuiera sur la technologie de la « chaîne de blocs », ou *blockchain*, une technologie de transmission d'informations transparente et cryptée. Les nœuds de la chaîne seront opérés par les partenaires. Ainsi, contrairement au *bitcoin*, tout individu disposant des capacités de minage

nécessaires ne pourra pas lui-même ajouter un bloc à la chaîne, cette prérogative sera réservée aux membres de l'association.

6. Pourquoi le libra est-il décrit comme un *stablecoin* ?

Le libra serait une *stablecoin*. Ce cryptoactif serait adossé à un panier de devises stables (dollar, euro, yen, livre sterling). Chaque partenaire du projet a dû verser un « ticket » d'une dizaine de millions de dollars. La réserve ainsi constituée permettrait ensuite de stabiliser ce cryptoactif. La valeur du libra dépendrait des réserves investies par l'association, qui se tournerait vraisemblablement vers des actifs peu risqués, comme les titres obligataires.

Pour mesurer la capacité de résilience de nos systèmes, de nos normes et de nos autorités de supervision, face à l'irruption de ce cryptoactif d'un nouveau type, il convient de distinguer les trois applications qui pourraient en être faites :

1°) le libra serait tout d'abord **un moyen de paiement**, permettant à des particuliers de pouvoir payer ou transférer des fonds en libra. Le Gouverneur de la Banque de France[1] a reconnu devant votre commission qu'il existait des marges de progrès dans ce domaine, les paiements transfrontières étant encore soumis à des procédures lourdes et coûteuses. Pour être utilisé comme moyen de paiement, et pour que son lancement ne se traduise pas par une régression des progrès constatés dans ce domaine, **le libra devrait respecter toutes les réglementations anti-blanchiment**. La question de la **protection des données** devrait également être observée de près, les données associées aux paiements étant à la fois **très nombreuses et très sensibles.** Il semble que ce soit l'option choisie par l'association puisque, le 11 septembre 2019, l'Autorité fédérale de surveillance des marchés financiers (Finma) suisse a confirmé que Facebook avait sollicité auprès d'elle une demande d'agrément du libra en tant que système de paiement [2] **;**

2°) si l'association envisage de **proposer des services bancaires**, que ce soit des instruments de dépôt, de crédit ou d'épargne, elle ne pourra opérer dans aucun grand pays sans avoir au préalable obtenu une **licence bancaire** ;

3°) à terme, **le libra pourrait être acheté partout dans le monde**, en tant que monnaie locale en substitution de la monnaie nationale. C'est une menace particulièrement forte pour la souveraineté des pays dans lesquels le système financier n'est pas stable ou a perdu la confiance de la population (ex. Venezuela et les périodes d'hyperinflation, l'Argentine…).

Yves Mersch, membre du directoire de la BCE, a estimé qu'une intervention réglementaire était nécessaire pour statuer sur la classification du libra. Il a également appelé les citoyens européens à refuser de se laisser happer par « *les promesses séduisantes, mais perfides du chant des sirènes de*

[1] *Audition de M. François Villeroy de Galhau, Gouverneur de la Banque de France, devant votre commission d'enquête le 11 juillet 2019.*
[2] *Communiqué de presse de la FINMA disponible à l'adresse suivante : https://www.finma.ch/fr/news/2019/09/20190911-mm-stable-coins/*

Facebook »[1]. La capacité pour le libra de toucher une vaste partie de la population mondiale ne fait en effet que **renforcer les risques liés à la nature même des cryptoactifs** :

- **la protection des données**. David Marcus a assuré, devant le Sénat américain, que, « *pour le moment* », il n'y avait aucune raison de partager les données entre libra et Facebook. Cela veut-il dire que cette séparation pourra un jour être remise en cause, selon les besoins de Facebook et de ses partenaires ? Un second risque est celui de la **patrimonialisation des données** : Facebook pourrait proposer d'octroyer des libras en échange de données personnelles ;
- **la capacité de Facebook à conduire un tel projet**, après plusieurs scandales liés au détournement de ses produits au profit d'actes malveillants, y compris à l'encontre de la souveraineté des États (ex. les tentatives de manipulation des élections) ;
- **la naissance d'une superstructure**, avec l'intégration de plus en plus forte des services de Facebook avec Whatsapp et Instagram et le développement de nouveaux services financiers ;
- **la perte de souveraineté monétaire**, en particulier dans les pays en développement aux devises instables ;
- **la stabilité financière et la protection des investisseurs** ;
- **le contournement des sanctions internationales** et du **cadre normatif de lutte contre le blanchiment des capitaux et le financement du terrorisme**, l'utilisation du libra pour rémunérer les auteurs d'actes criminels (cyberattaques ou autres).

Devant votre commission, Bruno Le Maire a insisté sur trois de ces risques : le contournement des réglementations visant à lutter contre le blanchiment d'argent, le risque systémique du fait du nombre d'utilisateurs de Facebook et le risque pour la souveraineté monétaire des États[2].

Pour répondre à ces inquiétudes, **Facebook n'a eu de cesse d'expliquer qu'il ne s'agissait pour lui ni de concurrencer les États, ni de faire « cavalier seul »**. L'entreprise a affirmé qu'elle avait d'ores et déjà entamé un travail de consultation avec les régulateurs nationaux et internationaux et qu'elle comptait prendre le temps de répondre à tous les doutes et de recevoir l'approbation des autorités concernées avant de lancer le libra. Votre rapporteur considère que ce changement de méthode ne fait que refléter la sensibilité de ce nouveau projet, la fragilité de la position de Facebook et le risque qu'elle a de perdre la confiance de ses utilisateurs.

---

[1] *La Tribune,* Pour la BCE, le Libra de Facebook pourrait nuire à l'euro, *2 septembre 2019. Propos tenus lors de la conférence sur les enjeux juridiques au sein du système européen de banques centrales, le 2 septembre 2019.*

[2] *Audition de Bruno Le Maire, ministre de l'économie et des finances, devant votre commission le 10 septembre 2019.*

Votre rapporteur constate que le projet libra est porté par **Facebook, entreprise américaine**. L'audition de David Marcus devant le Sénat américain était à cet égard très éclairante : à plusieurs occasions, il a affirmé que si **Facebook ne lançait pas son projet, d'autres pays le feraient, avec des valeurs différentes**, et sur lesquels le régulateur américain aurait moins de prise. Il a insisté sur **la nécessité, pour les États–Unis, de se montrer pionnier dans ce domaine et de saisir cette opportunité pour être les premiers à définir les normes dans ce champ encore relativement inexploré de l'innovation numérique**. Les relations étroites entre l'État américain et les entreprises du numérique, à l'origine du développement des plus grandes multinationales, ne doivent pas ici être sous-estimées et sont renforcées par une réelle convergence d'intérêt. Il existe ainsi un **lien profond entre le développement d'un projet innovant et l'affirmation de la souveraineté étatique**[1].

Si votre rapporteur estime que **ce projet doit être surveillé avec la plus grande vigilance, du fait des risques qu'il représente**, il considère également qu'il faut **savoir en prendre la bonne mesure**. Tout d'abord, il n'est pas certain que le libra voit le jour, et certainement pas comme une monnaie à part entière. Ensuite, l'histoire a montré que les devises privées achoppent toujours sur leur absence d'adossement : en cas de panique financière, les épargnants et les investisseurs finissent toujours par se tourner vers la puissance publique, garante de la monnaie et de leurs dépôts. Enfin, les États n'ont aucunement l'intention d'abandonner leurs prérogatives : les impôts, les documents comptables, les prestations en argent public… tout ceci ne s'exprime que dans les monnaies légales.

Prudent, Facebook a laissé entendre, dans ses documents trimestriels transmis à la *Securities and Exchange Commission* (SEC), qu'il pourrait retarder, voire ne jamais lancer, le projet libra, devant la méfiance des régulateurs et des représentants nationaux. Pour autant, et **même si le projet libra ne devait jamais advenir, la force des réactions qu'il a suscitées et les ambitions qu'il porte doivent conduire nos autorités financières à agir plus rapidement et plus fortement dans le domaine des cryptoactifs**.

---

[1] *Ceci vaut également pour la Suisse, acteur souvent méconnu dans le domaine numérique. L'actuel président de la Confédération, M. Ueli Maurer, a depuis longtemps fait part de son intention de faire de la Suisse une « cryptonation », un projet qui se concrétiserait avec l'installation de l'association libra. Pourquoi la Suisse ? De nombreuses organisations internationales et organisations non-gouvernementales sont installées en Suisse et beaucoup travaillent sur des programmes visant à promouvoir l'accès à des services financiers et bancaires dans les pays en développement, un marché explicitement visé par le libra, qui veut devenir un recours pour les 1,7 milliard de personnes débancarisées. La Suisse présente également une fiscalité et une réglementation favorable, ainsi qu'une réserve de main d'œuvre hautement qualifiée.*

Les risques du projet libra selon Facebook

Ces risques sont de plusieurs ordres :

- la participation à l'association libra soumettrait l'entreprise à une supervision accrue des régulateurs, ce qui pourrait affecter négativement ses affaires, sa réputation et ses résultats financiers ;

- libra est basé sur une technologie relativement nouvelle, la *blockchain*, et la régulation des cryptoactifs n'est encore ni définitive, ni claire ;

- en participant à ce projet, l'entreprise serait soumise à une très grande diversité de législations et de réglementations, aux États-Unis et ailleurs, ce qui pourrait générer d'importants conflits de normes. L'application de l'ensemble de la régulation pourrait en outre retarder ou empêcher le lancement du libra et le développement d'autres produits/services, et accroître les coûts de fonctionnement de l'entreprise ;

- il n'y a aucune garantie sur l'acceptabilité du libra par le marché et ses agents.

Source : document transmis par Facebook à la SEC, disponible ici : http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/69ea7934-e26b-499f-85ca-eb67cd2a9fc1.pdf, p. 60

Le projet libra présente moins une menace pour l'État et sa souveraineté monétaire que pour le système bancaire traditionnel. Libra compte en effet tirer profit des avantages de la technologie de la *blockchain* : transfert d'argent plus rapide et moins onéreux, transactions plus fluides, registre transparent des transactions, sécurité des échanges, opportunité pour les personnes débancarisées. Le lancement de ce projet part donc d'un constat que votre rapporteur partage : comment se fait-il qu'il soit aujourd'hui devenu aussi facile de transférer des données, des documents, des photographies mais pas de l'argent à l'heure des services mondialisés ?

b) Une piste de réaction à explorer : la cryptomonnaie de banque centrale

Il est intéressant de noter que **le bitcoin**, le plus célèbre des cryptoactifs, **est apparu en 2009**, au moment où **le système financier traversait l'une des plus graves crises de son histoire**. Les promesses des cryptoactifs, notamment en termes de transparence et de décentralisation, seraient autant d'atouts dont pourraient se saisir nos banques centrales nationales et la BCE. La naissance d'une **cryptomonnaie banque centrale** (*central bank digital currency* - CBDC) pourrait ainsi soutenir les levées de fonds en jetons et le financement des innovations numériques, les investisseurs pouvant alors faire appel à cet actif garanti, sans risque de subir les incertitudes liées à la volatilité des cryptoactifs privés. Plaide également en faveur d'une CBDC la diminution de l'utilisation de l'argent liquide en France[1].

La question est donc de savoir si les entreprises et les particuliers ont besoin d'avoir accès à des services de paiement dématérialisés en

[1] *Même si son usage demeure bien plus répandu que dans les pays du nord de l'Europe, où il ne représente plus que 10 à 20 % des transactions.*

monnaie banque centrale et si la banque centrale peut offrir aux agents économiques des services fiables et sécurisés en conservant ses missions traditionnelles (superviser et s'assurer du bon fonctionnement du marché interbancaire, garantir la fluidité des paiements, fournir des liquidités aux banques commerciales). Le développement **d'une cryptomonnaie banque centrale aurait** des **coûts d'élaboration et pourrait avoir des implications inattendues** sur la stabilité financière, sur la transmission des décisions de politique monétaire à l'économie réelle, sur l'efficacité du système de paiements ou encore sur la capacité à répondre aux « paniques » bancaires[1].

En effet, **il ne s'agit pas ici de jouer aux « apprentis sorciers »**, rien ne dit que cette cryptomonnaie banque centrale devrait être immédiatement accessible à l'ensemble des acteurs économiques. Il est vrai que l'utilisation de l'argent liquide demeure importante, et que la BCE vient de lancer un système de paiement transfrontalier très performant. Votre rapporteur considère toutefois que **si nos banques centrales n'agissent pas, elles prennent une fois de plus, le risque d'être dépassées par des acteurs privés, dans un domaine où tout change très vite**. La BCE et les banques centrales nationales doivent au moins approfondir leurs connaissances sur les éventuels impacts de l'émission d'une CBDC. **Conserver une position attentiste ne leur permettra pas d'être capables de répondre rapidement à la concurrence des acteurs privés**. Force est de constater que, sur ce point, le projet libra a joué un rôle d'accélérateur.

La cryptomonnaie de banque centrale : une idée qui se diffuse en Europe

Lors de la conférence annuelle des dirigeants de banque centrale de Jackson Hole, le 23 août 2019, le gouverneur de la Banque d'Angleterre, Mark Carney, a relancé le débat autour de l'émission d'une cryptomonnaie banque centrale. Il s'est montré optimiste sur la perspective d'une « *monnaie hégémonique synthétique* », émise par un réseau de banques centrales et qui viendrait concurrencer l'influence du dollar dans le commerce international. Cette monnaie s'appuierait sur un panier de devises pouvant ensuite servir de valeurs refuges pour les pays émergents, qui disposeraient alors d'une alternative au dollar.

Le ministre de l'économie et des finances, M. Bruno Le Maire, a estimé qu'il fallait engager « *une réflexion sur une monnaie numérique publique, émise par les banques centrales, qui garantirait la sécurité totale des transactions, leur rapidité, leur simplicité et leur gratuité* ». Lors de son audition devant votre commission, il a indiqué qu'il proposerait de lancer une réflexion sur ce sujet à l'occasion de la réunion des ministres des finances du G7 à Washington en octobre prochain. Christine Lagarde, candidate à la direction de la Banque centrale européenne, a également jugé l'idée d'une *stablecoin* de banques centrales « *très intéressante* ».

Sources : Bruno Le Maire favorable à une monnaie numérique publique, *La Tribune, 06 septembre 2019 ; audition de Bruno Le Maire, ministre de l'économie et des finances, devant votre commission le 10 septembre 2019.*

[1] *Pour une présentation approfondie du sujet, voir l'article de Bech et Garrat et l'étude de la BCE sur les implications des cryptoactifs pour la stabilité financière, précédemment cités.*

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

c) Soutenir le développement d'acteurs européens des systèmes de paiement : un enjeu de souveraineté méconnu mais crucial

Dans la remise en cause de l'ordre fiscal et monétaire, **le sujet des systèmes de paiement est rarement abordé**. **Il est pourtant crucial et beaucoup moins hypothétique que le libra**. Il fait partie des « communs » dont la neutralité devrait être, selon Henri Verdier, garantie par l'État[1].

L'Inde : un pays très actif sur le front des systèmes de paiement

Lors de son audition devant la commission d'enquête, Henri Verdier, ambassadeur pour le numérique, a utilisé l'exemple de l'Inde pour illustrer son propos sur la neutralité des « communs ». Depuis la fin des années 2010, l'Inde a en effet adopté deux grandes réformes visant à la fois à donner accès à chaque citoyen à des moyens de paiement et à favoriser le développement d'acteurs nationaux :

- en 2016 : le gouvernement lance l'application *Aadhaar Payment*, qui permet à chacun de payer ses achats en utilisant son empreinte digitale. Aadhaar est un projet de l'Autorité d'identification unique de l'Inde, qui entend doter chaque citoyen d'une carte d'identité virtuelle. À noter que Morpho, filiale de Safran jusqu'en 2017, et Idemia, issue du rapprochement de Morpho et d'*Oberthur Technologies*, collaborent à ce projet en fournissant des capteurs biométriques. Toutefois, ce système est encore fragile et a déjà été victime de plusieurs cyberattaques. Il présente des risques importants pour la protection de ces données personnelles très sensibles ;

- en 2018 : la banque centrale indienne (RBI) décide que toutes les informations relatives aux paiements réalisés en Inde devront être enregistrées localement. Si elle justifie cette restriction par la nécessité de mieux superviser les transactions, d'aucun considère qu'il s'agissait surtout d'entraver la collecte et la revente de données de plus d'1,3 milliard de citoyens au profit des entreprises américaines, afin de favoriser plutôt l'émergence de *start-up* nationales.

Les géants numériques américains ont su très vite s'adapter aux nouvelles réglementations. Après avoir tenté de repousser l'entrée en vigueur de la réforme et avoir été brièvement interdites d'opération sur le territoire indien, Visa et Mastercard ont rapidement consenti aux investissements nécessaires pour localiser les données visées en Inde (sans toutefois préciser s'ils n'en gardaient pas une copie ailleurs).

[1] *Audition de M. Henri Verdier, ambassadeur pour le numérique, devant votre commission le 4 juin 2019.*

S'il est tout à fait possible de réaliser des paiements digitaux et instantanés dans tous les pays de la zone euro, les systèmes de paiement sont encore largement nationaux, sans harmonisation entre les pays de la zone euro, et **les acteurs dominants du marché des paiements transfrontières sont tous non-européens**.

Quel est l'intérêt des géants du numérique à se développer dans le domaine des systèmes de paiement, longtemps considéré comme une simple activité d'intendance ? Ce secteur est en réalité une **interface entre l'univers bancaire et le reste du monde**. Comme l'a expliqué devant votre commission le Gouverneur de la Banque de France, M. François Villeroy de Galhau[1], les entreprises du numérique, dont le modèle repose sur l'exploitation des données, peuvent collecter, par le biais des paiements, des **données précieuses et commercialisables, sans pour autant devoir se soumettre aux contraintes réglementaires fortes** qui pèsent sur les acteurs proposant de « vrais » services bancaires (dépôt, épargne, crédit…). Cette conjugaison de **faibles barrières à l'entrée et intérêts économiques élevés** explique la pénétration des acteurs du numérique, américains ou asiatiques, dans ce secteur.

C'est pour répondre à l'ensemble de ces risques que votre rapporteur **soutient les efforts en faveur d'une stratégie européenne des paiements**, permettant d'éviter que nos citoyens deviennent les consommateurs de services produits par d'autres et voient leurs données les plus personnelles et sensibles exploitées et traitées par des acteurs américains ou asiatiques. **Par le passé, les banques européennes n'avaient pas su répondre à Visa et Mastercard, il serait dommageable que l'Union européenne continue aujourd'hui à creuser son retard dans ce domaine[2]**.

Le Gouverneur de la Banque de France a alerté votre commission sur le fait que **le temps était désormais compté** : il estime que les pays européens disposent de **deux ans** pour promouvoir une initiative européenne **avant de se trouver de fait exclus de ce marché pourtant stratégique**.

La création d'une solution de paiement paneuropéenne s'appuierait sur une consolidation des schémas nationaux existants, ainsi que sur une **infrastructure existante et performante** : le **Target Instant Payment Settlement** (TIPS). Lancé par la BCE en novembre 2018, c'est une offre de règlement brut des virements instantanés. Similaire à Visa-Mastercard, il n'a pourtant pas encore réussi à convaincre toutes les banques européennes. Défendre TIPS, c'est également lutter contre la fragmentation de ce marché, où coexistent de très nombreux acteurs, des plus traditionnels aux entreprises du numérique et de la fintech. Ce système dispose en outre d'un

---

[1] *Le 8 juillet 2019.*

[2] *Paypal a par exemple lancé « Xoom » dans 32 pays européens. Ce service permet d'envoyer de l'argent à l'étranger, de transmettre des espèces récupérables rapidement dans des points de retraits locaux, de créditer le forfait téléphonique d'un proche ou encore de régler ses factures.*

avantage non-négligeable vis-à-vis de ses concurrents : la transaction est réalisée en monnaie banque centrale, ce qui veut dire qu'**il n'y a plus de risque de crédit,** risque contre lesquels les acteurs privés des systèmes de paiement doivent s'assurer, en en faisant porter la charge au consommateur.

Les systèmes de paiement : la BCE, un temps d'avance sur la Fed

La Réserve fédérale américaine (FED) semble tout juste prendre conscience du caractère stratégique des systèmes de paiement. Elle vient d'annoncer qu'elle travaillait au déploiement d'un système de paiement en temps réel d'ici 2024. Lael Brainard, membre du conseil des gouverneurs, n'a pas hésité à souligner le retard de la FED dans ce domaine, notamment vis-à-vis de l'Europe. Elle a également confié que la FED entendait ainsi réagir aux initiatives d'entreprises privées, à l'image de celle de Facebook et du libra.

Coordonner les innovations européennes afin de développer une **solution de paiement européenne**, protectrice des données personnelles et capables de répondre aux produits de plus en plus sophistiqués proposés par les entreprises américaines et chinoises.

II. COMMENT REMPORTER LE DÉFI DE LA SOUVERAINETÉ NUMÉRIQUE ?

Après avoir envisagé les scénarii permettant de répondre aux menaces pesant sur notre souveraineté dite classique, il convient d'envisager la façon dont peut s'exercer la souveraineté numérique, c'est-à-dire la capacité de l'État à agir dans le cyberespace, dans deux dimensions :

- la capacité d'exercer une souveraineté dans l'espace numérique : qui repose sur une capacité autonome d'appréciation, de décision et d'action dans le cyberespace. Ceci correspond de fait à la cyberdéfense,

- et la capacité de préserver ou restaurer la souveraineté de la France sur les outils numériques afin de pouvoir maîtriser nos réseaux, nos communications électroniques et nos données, publiques ou personnelles.

Ces actions de sauvegarde de la souveraineté numérique doivent être pilotées. À ce jour, cette évidence peine toutefois à se traduire concrètement.

A. POUR RELEVER LE DÉFI DE LA SOUVERAINETÉ NUMÉRIQUE : FÉDÉRER ET ANTICIPER

1. Créer un forum institutionnel pour remédier à une gouvernance insatisfaisante

a) Le consensus : la France et l'Union européenne à la croisée des chemins

En entamant ses travaux au mois d'avril 2019, votre commission a eu la sensation de s'être constituée au moment opportun. Ces derniers mois, la souveraineté numérique s'est en effet imposée comme un terme récurrent du débat public. Après une phase d'utopie, que d'aucuns pourraient qualifier de naïve, le développement du numérique est devenu un terrain d'affrontement mondial, avec des conséquences néfastes sur notre société et sur notre souveraineté.

En dépit d'affaires retentissantes (les révélations d'Edward Snowden, Cambridge Analytica) et des révélations d'écoutes inopinées (Alexa, Siri), le capital confiance des entreprises du numérique est resté considérable, retardant ainsi l'action des gouvernements à leur égard. L'Union européenne a longtemps atermoyé, le numérique ne devenant que très récemment l'une des grandes priorités de la Commission européenne.

La rapidité des évolutions numériques et des innovations ne peut seule disqualifier l'action publique. Le règne de la complaisance doit prendre fin et les dirigeants français et européens doivent accepter de prendre leurs responsabilités face aux défis de l'ère numérique.

Les travaux de la commission ont renforcé cette impression : de nombreux intervenants ont témoigné de cette prise de conscience, qualifiant notre époque de « tournant décisif », de croisée des chemins. Les énergies, les initiatives, les forces existent pour répondre à ce moment décisif. Reste à prendre la bonne direction, selon le bon tempo.

b) Donner l'impulsion fédératrice nécessaire

Alors que des décisions majeures doivent être prises, **votre commission se demande si le Gouvernement dispose d'une stratégie globale sur le numérique**. Elle a entendu des propositions de toute part, des kyrielles de stratégies sectorielles, des dizaines de millions d'euros débloqués sur une multitude de projets. Tout ceci est loin d'offrir une image de cohérence et de maîtrise.

C'est d'autant plus alarmant que **le numérique est un sujet par définition transversal, un constat qui ne se reflète plus dans l'organisation gouvernementale** depuis que le secrétaire d'État chargé du numérique n'est plus placé sous l'autorité du Premier ministre mais sous l'égide des ministères économiques et financiers. Les auditions de cinq membres du Gouvernement n'ont pas convaincu votre rapporteur sur leur bonne

appréhension de ces enjeux de transversalité. C'est particulièrement frappant quand il s'agit du nerf de la guerre : le financement de projets numériques ambitieux.

Le **projet ARTEMIS** (architecture de traitement et d'exploitation massive de l'information multi-sources)[1], porté par la direction générale de l'armement, est emblématique de cet état de fait. Devant votre commission, la ministre des Armées a ainsi regretté que la charge financière de ce projet (60 millions d'euros), qui pourrait bénéficier à l'ensemble des ministères, soit exclusivement portée par les armées à ce jour : « *ce n'est pas le ministère des armées seul qui pourra porter cette question, assurer le financement de solutions dont notre administration, notre État a besoin* »[2].

Votre rapporteur estime que l'action gouvernementale ne s'appuie ni sur une ligne directrice lisible, ni sur une vision partagée. Ceci pourrait être une source d'incohérences préjudiciable à la défense de notre souveraineté numérique. En fonction des ministères et des thèmes abordés, les priorités et les avis changent. Un problème de gouvernance se fait jour. Il découle en partie des contradictions que porte l'ère numérique. Comment, dans ces conditions, arbitrer entre souveraineté et libertés publiques, sécurité et défense, et présence économique effective sur un marché nécessairement mondial ?

Pour y répondre, **votre rapporteur promeut un nouveau pilotage et la fédération de tous les acteurs impliqués dans le numérique.** La loi pour une République numérique avait tenté d'aller en ce sens, sans succès.

Votre rapporteur propose aujourd'hui de transformer le Conseil national du numérique en un **Forum institutionnel de concertation, temporaire.** Celui-ci réunirait les acteurs du public et du privé, des administrations aux industries, en passant par les universitaires et les *start-up*, sans oublier les collectivités territoriales, qui jouent un rôle crucial dans l'aménagement numérique du territoire.

Ce Forum permettrait de fédérer des individus et des entités aux positions parfois radicalement opposées, afin qu'ils puissent dialoguer ensemble et être source de propositions fortes pour défendre notre souveraineté numérique. Ce Forum créerait alors une véritable culture du numérique et réunirait les personnes les plus qualifiées dans ce domaine, afin de tirer profit du trésor de compétences et de savoir-faire dont nous disposons en France, où il existe une véritable culture scientifique et technologique. C'est sur elle qu'il faut s'appuyer et sur les savoir-faire industriels de haute technologie.

---

[1] *Selon le ministère des armées, ARTEMIS, développé dans le cadre d'un partenariat d'innovation avec trois entreprises, vise à développer la future plate-forme sécurisée de big data et d'intelligence artificielle. Des déploiements pilotes auront lieu en 2020, avec une version homologuée attendue pour 2021. À plus long terme, une version sera ouverte à la communauté scientifique et industrielle.*

[2] *Audition de Florence Parly, ministre des armées, devant votre commission le 3 septembre 2019.*

Ce Forum, enfin, aurait une durée de vie limitée, de deux ans maximum, afin que le Parlement puisse ensuite s'emparer de ces sujets et des recommandations émises par ses membres. En effet, ce n'est pas en travaillant en « vase clos » que nous réussirons à définir une véritable stratégie pour affirmer notre souveraineté numérique : le Gouvernement, le Parlement, les élus locaux, les entreprises, les chercheurs, n'y parviendront pas seuls.

Transformer le Conseil national du numérique en un forum de concertation, réunissant les administrations de l'État, les collectivités territoriales, des parlementaires, des universitaires et des entreprises. Ce forum aurait une existence temporaire et la conclusion de ses travaux donnerait au Parlement et au Gouvernement l'occasion d'arbitrer sur ses principales recommandations, aiguillant ainsi sur le long terme l'action des ministères pour défendre la souveraineté numérique française.

2. Créer un moment politique récurrent au service de la souveraineté numérique nationale

Si le Forum institutionnel doit permettre de définir notre stratégie et remettre de l'ordre dans des initiatives qui apparaissent parfois trop déconnectées les unes des autres, cette stratégie devra ensuite s'incarner au niveau législatif. C'est au Parlement que revient la charge d'assurer un suivi régulier et de contrôler la mise en œuvre des priorités ainsi définies.

Votre rapporteur a conscience de **l'ampleur de la tâche et de la diversité des champs d'innovation dont la France doit se saisir pour défendre sa souveraineté numérique** et endiguer les tendances hégémoniques décrites. Pour que cela fonctionne, il faut donc un pilotage à la fois souple et de long terme : il faut des investissements inscrits dans le temps long, autour d'une **vision partagée et permanente**, mais aussi une capacité de réaction rapide pour répondre aux nouvelles innovations.

À ce titre, votre rapporteur recommande l'élaboration d'une **loi d'orientation et de suivi de la souveraineté numérique (LOSSN)**.

Cette LOSSN, triennale, s'inspire de la loi de programmation militaire (LPM), déjà éprouvée. Elle permettrait à la France de se projeter dans des secteurs dans lesquels elle peut encore défendre une place de leader européen et/ou mondial, comme le *edge computing*, une *blockchain* moins consommatrice d'énergie ou encore l'intelligence artificielle embarquée. Seraient également inclus des objectifs liés à la formation dans ces secteurs en tension. Le secrétaire d'État chargé du numérique, M. Cédric O, considère ainsi que **les difficultés de recrutement sont la première limite à l'expansion de l'écosystème des start-up et des licornes en France et en Europe**.

Elle constituerait un rendez-vous politique mobilisant les pouvoirs publics autour des enjeux stratégiques de la souveraineté numérique nationale.

Élaborer une loi d'orientation et de suivi de la souveraineté numérique (LOSSN) afin de garantir davantage de lisibilité aux entreprises, de bénéficier d'un pilotage plus rigoureux des innovations et des actions à mettre en œuvre en faveur de la souveraineté numérique française. Le suivi de l'exécution de la LOSSN par le Parlement garantirait la gestion politique de ces choix stratégiques.

B. LA CYBERDÉFENSE DOIT RESTER UNE PRIORITÉ

1. La mise en œuvre d'une cyberdéfense française : pour une autonomie française dans le cyberespace

La cyberdéfense se distingue de la lutte contre la cybercriminalité, mais aussi de la numérisation des armées et des théâtres d'opération. Elle recouvre la politique mise en place par l'État pour protéger activement des réseaux et des systèmes d'information essentiels à la vie et à la souveraineté du pays. Si les cyberattaques et les menaces sont importantes, nombreuses et constatées depuis plus d'une décennie, la mise en place de la cyberdéfense française a été progressive.

a) Des menaces avérées

Depuis la première cyberattaque visant une structure étatique qui a frappé l'Estonie en avril 2007[1], la menace s'est concrétisée et accentuée. Il ne se passe pratiquement pas une journée sans que l'on signale, quelque part dans le monde, des attaques ciblées contre les réseaux de grands organismes publics ou privés.

La France n'est pas épargnée par ce phénomène. Comme l'ont confirmé les représentants des organismes chargés de la protection des systèmes d'information, les administrations[2], les entreprises ou les

[1] *L'Estonie, voulant marquer son indépendance vis-à-vis de la Russie, avait décidé de déplacer un monument de l'Armée Rouge du centre de la capitale à Tallinn vers la banlieue. Cette décision montrant le rapprochement estonien des puissances occidentales aurait déclenché une réaction russe, qui n'a pas été officiellement prouvée. La Russie aurait loué les services de hackeurs pour accroître le nombre d'ordinateurs impliqués dans l'attaque en déni de service lancée contre l'Estonie qui a duré quelques jours.*

[2] *Sur ce sujet, voir le récent rapport d'information n° 299 (2018-2019) - 6 février 2019 de MM. Olivier Cadic et Rachel Mazuir, fait au nom de la commission des affaires étrangères, de la défense et des forces armées,* Cyberattaque contre « ARIANE » : une expérience qui doit nous servir.

opérateurs d'importance vitale (énergie, transports, santé, etc.) sont victimes chaque jour en France de plusieurs millions d'attaques informatiques.

On peut recenser trois types d'attaques :

- les exemples cités, extraits du rapport de Jean-Marie Bockel[1], sont volontairement datés pour ne pas nuire à l'action des services qui ont été entendus à huis clos par votre commission d'enquête ;

- la perturbation de sites institutionnels, à l'image du site Internet du Sénat, rendu inaccessible fin 2011 lors de la discussion de la loi sur le génocide arménien ; il s'agit de ce que les spécialistes appellent une attaque par « déni de service » : le site Internet est rendu inaccessible car il est saturé de milliers de requêtes ;

- l'attaque informatique d'envergure dont avait fait l'objet, fin 2010, le ministère de l'économie et des finances, dans le cadre de la préparation de la présidence française du G8 et du G20. Il s'agit là d'une vaste intrusion informatique à des fins d'espionnage : un logiciel espion est introduit grâce à un « cheval de Troie », qui se présente sous la forme d'une pièce jointe piégée ouvrant une « porte dérobée » ; l'attaquant peut alors surveiller et prendre, à distance et à l'insu de l'utilisateur, le contrôle de son ordinateur, par exemple pour extraire des données, lire ses messages électroniques, et même écouter ses conversations ou filmer sa victime en déclenchant lui-même le micro ou la caméra de l'ordinateur ; il peut ensuite, par rebonds successifs, prendre le contrôle d'autres ordinateurs, voire de la totalité du réseau ;

- l'espionnage d'opérateurs sensible. Il y a plusieurs années, la presse s'était fait l'écho d'une opération subie par le groupe AREVA, entreprise française du secteur nucléaire.

Les armées sont également la cible de ces cyberattaques. Entendu par votre commission d'enquête[2], le Général François Lecointre, chef d'État-Major des armées (CEMA) a indiqué que « *les armées sont la cible d'attaques informatiques particulièrement nombreuses. Ainsi, en 2018, 831 événements significatifs ont été recensés par le commandement de la cyberdéfense (Comcyber), soit une augmentation de l'ordre de 20% par rapport à 2017. Une centaine consiste en des attaques informatiques avérées, dont six sont caractéristiques de modes d'action de groupes structurés affiliés à des États. Toutes ces attaques ont été menées à des fins d'espionnage de hauts responsables du ministère ou de fonctions opérationnelles.*

En 2018, le ministère des armées a été la cible d'attaques par un mode d'action connu de nos services, que certains attribuent à Turla, groupe affilié au service fédéral de sécurité russe. Les cibles identifiées sont des membres du ministère ayant des responsabilités dans le domaine des relations internationales, ou des

[1] *Rapport n° 681 (2011-2012) sur la cyberdéfense, au nom de la commission des affaires étrangères de la défense et des forces armées.*
[2] *Audition du 25 juin 2019.*

fonctions opérationnelles d'intérêt, comme l'approvisionnement en carburant des bâtiments de la marine nationale, afin de suivre les escales de nos bâtiments. ».

b) Une lente montée en puissance de la cyberdéfense

Le Sénat s'est emparé de cette question essentielle qu'est la cyberdéfense dès 2008, avec le rapport d'information de notre collègue Roger Romani[1], puis en 2012, avec le rapport d'information de notre collègue Jean-Marie Bockel[2] intitulé « *La cyberdéfense : un enjeu mondial, une priorité nationale* ». Ces rapports constataient que, malgré une prise de conscience des enjeux, notre pays accusait un relatif retard dans la mise en œuvre d'une stratégie de cyberdéfense.

C'est sous l'impulsion du Président Barack Obama que la cybersécurité a été qualifiée de priorité stratégique aux États-Unis, mobilisant plusieurs organismes, au sein du département chargé de la sécurité intérieure ou du Pentagone, comme l'Agence de sécurité nationale (NSA) ou le Cybercommand. De 2010 à 2015, les États-Unis ont consacré 50 milliards de dollars à la cyberdéfense et plusieurs dizaines de milliers d'agents travaillaient sur ce sujet.

Le gouvernement britannique a adopté dès novembre 2011 une nouvelle stratégie, mise en œuvre par le *Government Communications Headquarters* (GCHQ), l'agence chargée du renseignement technique. Environ 700 agents s'occupaient alors des questions de cyberdéfense et malgré un contexte budgétaire tendu, un effort supplémentaire de 650 millions de livres (750 millions d'euros) a été fourni entre 2010 et 2014 pour la cyberdéfense.

En Allemagne enfin, une stratégie était élaborée dès février 2011, coordonnée par le ministère fédéral de l'Intérieur auquel est rattaché l'office fédéral de sécurité des systèmes d'information (BSI) disposant d'un budget de 80 millions d'euros et de plus de 500 agents.

En France, le Livre blanc sur la défense et la sécurité nationale de 2008 a donné une réelle impulsion à la cyberdéfense qui a abouti, en juillet 2009, à la création de l'Anssi, identifiée comme l'autorité nationale de défense des systèmes d'information Dès février 2011, l'agence a rendu publique la stratégie de la France en matière de cyberdéfense. Toutefois, avec des effectifs de 230 personnes et un budget de l'ordre de 75 millions d'euros, les moyens de l'Anssi étaient alors très loin de ceux dont disposaient les services des pays alliés.

La montée en puissance s'est faite lentement. La cyberdéfense a été érigée au rang de priorité nationale par le Livre blanc pour la défense et la sécurité nationale de 2013. Le Comcyber, unité opérationnelle, commandant de façon organique ou fonctionnelle l'ensemble des forces de cyberdéfense

---

[1] *Rapport n° 449 (2007-2008) sur la cyberdéfense, au nom de la commission des affaires étrangères de la défense et des forces armées.*

[2] *Rapport n° 681 (2011-2012) précité.*

des armées françaises a été créé en 2017. La loi de programmation pour 2013-2018 a pallié un manque important en imposant aux opérateurs d'importance vitale (OIV) de renforcer la sécurité des systèmes d'information qu'ils exploitent[1]. Le réel tournant date de la revue stratégique de cyberdéfense de 2018.

c) La revue de cyberdéfense de 2018 : un document stratégique structurant[2]

La revue stratégique de cyberdéfense a été confiée par mandat du Premier ministre en date du 21 juillet 2017[3] au Secrétariat général de la défense et de la sécurité nationale (SGDSN). Elle avait vocation à présenter une vue intégrée des efforts de l'État en matière de cyberdéfense et s'appuyait pour ce faire sur une succession de documents doctrinaux (livres blancs sur la défense et la sécurité nationale de 2008 et de 2013, stratégie nationale de sécurité numérique de 2015 et Chocs futurs, étude prospective à l'horizon 2030 passant au crible les impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité).

Selon la revue stratégique de cyberdéfense du 12 février 2018, la souveraineté numérique peut être entendue : « comme la capacité de la France d'une part, d'agir de manière souveraine dans l'espace numérique, en y conservant une capacité autonome d'appréciation, de décision et d'action, et d'autre part, de préserver les composantes les plus traditionnelles de sa souveraineté vis-à-vis des menaces nouvelles tirant partie de la numérisation croissante de la société ».

La France a donc fait le choix de conserver une autonomie de décision en matière de défense et de sécurité du cyberespace. L'atteinte de cet objectif repose sur les éléments suivants :

- une **capacité souveraine à détecter les attaques informatiques** qui affectent l'Etat et les infrastructures critiques. Ainsi, l'Anssi développe ses propres systèmes de détection pour la supervision des administrations, et des travaux ont permis de faire émerger des solutions industrielles de confiance pour la France au profit des entreprises. L'Agence a qualifié en avril 2019 les sondes de détection de deux industriels français. En outre, les capacités françaises de détection ont été significativement renforcées par la LPM 2019-2025 qui permet aux opérateurs télécoms de mettre en œuvre des dispositifs de détection au sein de leur réseau et à l'Anssi de déployer une sonde sur le réseau d'un hébergeur infecté par un attaquant. Ce mécanisme entre désormais dans une phase de mise en œuvre pratique ;

---

[1] Ces obligations s'appliquent aux systèmes d'information d'importance vitale (SIIV) désignés par les OIV et comprennent la déclaration d'incidents, la mise en œuvre d'un socle de règle de sécurité et le recours à des produits et à des prestataires de détection qualifiés.

[2] Cette partie s'appuie sur la contribution écrite du SGDSN, transmise à votre commission d'enquête suite à l'audition de la SGDSN le 23 mai 2019.

[3] Cette revue a fait l'objet de travaux interministériels associant le secteur privé, a été validée par le Président de la République en janvier 2018 puis publiée le 12 février 2018.

- une **capacité souveraine à attribuer les cyberattaques**. Le choix de développer et de maintenir une telle capacité est une orientation majeure. La maîtrise de telles capacités ne sera accessible à terme qu'à un nombre très limité de pays qui auront fait le choix stratégique de les détenir ;

- une **doctrine nationale de découragement et de réaction**, reposant notamment sur :

- une **méthode nationale d'évaluation de la gravité d'une cyberattaque**, intégrant nos normes juridiques (code pénal, code de la défense, règlement général sur la protection des données, etc.). Appelé par la Revue stratégique de cyberdéfense, un schéma de classement des cyberattaques a ainsi été préparé par l'ensemble des acteurs de la cyberdéfense et validé par le Président de la République,
- une **doctrine nationale de réponse**, fondée sur le principe que la réponse résulte d'une **décision politique** formulée au cas par cas à la lumière des critères établis par le droit international. La réponse peut se traduire par une attribution publique, par l'adoption de contre-mesures voire, dans la mesure où il n'est pas exclu qu'une cyberattaque puisse atteindre le seuil de l'agression armée, par le recours à la légitime défense au sens de l'article 51 de la Charte des Nations unies ;

- des **capacités offensives** permettant, face au risque d'agression armée, de disposer d'options de réponse de nature militaire dans le milieu cyber comme dans les autres milieux. L'arme cyber est aujourd'hui pleinement intégrée parmi les capacités opérationnelles des armées, et fait l'objet d'une doctrine qui encadre son emploi dans les opérations militaires sur les théâtres d'opération extérieurs, dans le respect du droit international ;

- enfin, la **promotion à l'international de la vision française de cybersécurité** (qui fait l'objet d'un développement ci-après).

2. Des actions probantes dans le domaine de la cybersécurité

a) Un système efficace, désormais offensif en cas d'attaque

La revue stratégique de cyberdéfense organise la gouvernance cyber de l'État autour de quatre piliers aux gouvernances spécifiques : la prévention, sous la responsabilité de l'Agence nationale de la sécurité des systèmes d'information et du Premier ministre ; le renseignement, avec la DGSE, la DGSI et les ministères de tutelle ; l'action judiciaire qui relève de la Chancellerie, et l'action militaire, conduite par le chef d'état-major des armées et le Président de la République.

Chaque pilier a une gouvernance autonome et tous se coordonnent autour d'un comité de coordination des crises cyber ou « C4 », qui articule le cycle de la cyber défense – détection, attribution, réponses, car il s'agit bien de définir les stratégies de réponse qui sont soumises et validées par les autorités politiques.

Les orientations prises par la revue de cyberdéfense sont opérationnelles selon les propos du Général François Lecointre devant votre commission : « *le CEMA dépositaire de la conduite des opérations militaires a été renforcé dans sa responsabilité de cyber défense sur le périmètre du ministère des armées, et pour la conduite des opérations numériques. Le commandement cyber a été créé il y a moins de deux ans, il me seconde dans cette double responsabilité. Le rôle stratégique, central, de la cyberdéfense militaire a été parfaitement reconnu.*

(…) les armées, investies de la responsabilité de préserver la souveraineté nationale, sont plutôt en avance. La donnée occupe depuis longtemps une place centrale ; sa protection et son utilisation ont toujours été une préoccupation. Dans ce champ comme ailleurs, l'autonomie stratégique, garante de la souveraineté, est l'objectif que nous nous fixons.

Aujourd'hui, notre organisation, qui repose sur la Dirisi et le Comcyber, est mature. Nos capacités d'action et de protection sont de très bon niveau, comme le montre notre victoire récente lors de l'exercice international Locked shields. ».

Selon les auditions menées par votre commission d'enquête, en 2018, **14 opérations de cyberdéfense** ont eu lieu en réponse à un incident de sécurité majeur menaçant directement les systèmes numériques et compromettant les opérations liées à l'activité d'une organisation d'importance vitale ou fortement sensible. La même année ont été recensés 400 incidents significatifs dont 16 majeurs.

L'État français a indiqué en janvier 2019 que sa nouvelle doctrine de cyberdéfense comprenait une dimension offensive[1]. L'armée pourra désormais **riposter** à une attaque informatique, mais aussi employer l'arme cyber sur le champ de bataille. Enfin, l'arme cyber est aujourd'hui pleinement intégrée parmi les capacités opérationnelles des armées et fait l'objet d'une doctrine qui encadre son emploi dans les opérations militaires sur les théâtres d'opération extérieurs, dans le respect du droit international.

La ministre des Armées, Florence Parly a ainsi déclaré : « *La guerre cyber a commencé et la France doit être prête à y combattre. En cas d'attaque cyber de nos forces, nous nous réservons le droit de riposter dans le respect du droit, par les moyens et au moment de notre choix. Nous nous réservons aussi, quel que soit l'assaillant, le droit de neutraliser les effets et les moyens numériques employés* » pour illustrer la doctrine de **lutte informatique offensive** (LIO).

[1] *Discours de Mme Florence Parly, ministre des armées,* Stratégie cyber des Armées, *Paris, le 18 janvier 2019.*

La LPM 2019-2025 a doté la cyberdéfense de 1,6 milliard euros et 1000 cybercombattants supplémentaires sur la période de programmation. Prévoir plus de moyens supplémentaires ne serait probablement pas efficace tant il est difficile de recruter les personnels hautement qualifiés dont les armées et les services ont besoin. D'ici 2025, la France devrait être dotée de *« 4000 cybercombattants et combattantes »*.

Enfin, l'utilisation de l'internet par les armées fait l'objet d'une attention particulière : surveillance permanente des échanges de fichiers, sécurisation des sites, anonymisation des recherches sur source ouverte. Enfin, tous, du cadre au soldat, sont sensibilisés et formés à l'hygiène numérique, dont votre rapporteur estime qu'elle devrait être généralisée au moins à toutes les administrations publiques, si ce n'est tous les acteurs économiques sensibles.

b) … objet de l'attention de votre commission d'enquête : un bilan positif de la revue stratégique de cyberdéfense

Votre commission d'enquête a souhaité dresser un **premier bilan de l'application de la revue de cyberdéfense** et a pu en cela compter sur l'entier soutien du SGDSN. Aux termes des réponses communiquées, les précisions suivantes peuvent être apportées sur l'exécution de la revue.

Les recommandations de la revue ont fait l'objet d'un plan d'action piloté par le cabinet du Premier ministre. Ont notamment été atteintes aujourd'hui, les propositions suivantes :

- l'introduction de **nouvelles structures de gouvernance** : le comité directeur de la cyberdéfense, en charge de l'organisation générale et de la gouvernance capacitaire du domaine, et le comité de pilotage de la cybersécurité, en charge d'orienter et de suivre la mise en œuvre de la stratégie nationale de cybersécurité ont été mis en place ;

- la **mise œuvre du C4** qui a d'ores et déjà permis de formaliser le premier schéma national de classement des attaques informatiques, et de coordonner les stratégies de réponse face à plusieurs menaces actives ;

- **l'implication des opérateurs télécoms dans la détection des cyberattaques** : les dispositions de la LPM 2019 2025 permettent dorénavant aux opérateurs de communications électroniques de mettre en œuvre des dispositifs de détection des attaques affectant les systèmes d'information de leurs abonnés, et à l'Anssi de déployer un dispositif de détection sur le réseau d'un hébergeur ;

- **l'extension du champ des acteurs réglementés en matière de cybersécurité** dans les domaines économiques et sociétaux, par une transposition ambitieuse de la directive européenne *Network and Information Security* (NIS) ;

- l'intégration d'une **dimension sécurité numérique dans la plateforme FranceNum** destinée à accompagner les TPE/PME dans leur

transformation numérique. Un volet dédié à la sécurité numérique (sensibilisation au risque cyber et mise en relation avec des prestataires) a été intégré fin 2018 ;

- l'établissement d'une **position française relative au contrôle à l'exportation des outils d'attaque**. Sa déclinaison concrète, et en particulier la proposition de contrôle export des armes cyber au titre des matériels de guerre, sera principalement portée par le cycle annuel de négociation de l'arrangement de Wassenaar[1].

Certaines recommandations nécessitent des travaux complémentaires que **votre rapporteur incite à poursuivre**, en particulier :

- **l'identification et la recherche de la maîtrise de l'ensemble des technologies essentielles pour notre sécurité numérique** s'est, à ce stade, pour des raisons de ressources, centrée sur le besoin prioritaire d'un *cloud* de confiance. Ce point est déterminant et plaide en faveur de l'élaboration d'une LOSSN, déjà citée, afin de programmer les actions à mener dans ce domaine, donner aux acteurs concernés une visibilité nécessaire, et permettre un suivi politique, par le Parlement, de ces objectifs déterminants pour la souveraineté numérique française ;

- les **premières ressources pédagogiques** destinées à l'enseignement secondaire sont encore en cours de construction ;

- la **résilience et la sécurité du réseau interministériel de l'État** seront encore renforcées. Des ressources supplémentaires, prévues par la LPM, devraient y être consacrées dès 2019.

3. Des orientations à soutenir : la promotion de la vision française et le développement du chiffrement

a) La promotion à l'international de la vision française de cybersécurité

La **promotion à l'international de la vision française de cybersécurité** se décompose en deux items : (i) le droit international est applicable au cyberespace, et (ii) l'attribution publique est une décision politique qui relève de la souveraineté et ne peut être faite par une structure multinationale, qu'elle soit interalliée comme l'OTAN ou autre.

La violence légitime, attaquer et défendre, est un **monopole régalien** par excellence. Face à une menace cyber qui ne cesse de croître, certains acteurs, essentiellement américains, remettent en cause le monopole des États dans l'usage de la violence légitime. Se fondant sur une interprétation discutable du droit à la légitime défense dans l'espace cyber, qui n'est pas celle de la France, ils font la promotion d'une doctrine offensive de réponse aux attaques, autorisant une riposte par les acteurs privés eux-mêmes (*hack*

[1] *Il s'agit d'un régime multilatéral de contrôle des exportations d'armements conventionnels et de biens et technologies à double usage civil et militaire.*

back) qui va au-delà de la simple protection de leurs propres systèmes d'information, autorisant par exemple des intrusions dans les systèmes adverses pour les détruire.

Les risques que voit la France à une telle légalisation de pratiques dans certains pays et à leur diffusion au niveau international sont bien réels : risque d'erreur d'attribution, d'une part, car face à la difficulté pour obtenir une identification fiable de l'origine de l'attaque – et à ce titre, une action de riposte non encadrée pourrait prendre pour cible un tiers innocent ; risque de dommage collatéral et de riposte incontrôlée, d'autre part, de nature à aggraver l'instabilité du cyberespace.

Dans ce contexte, la France a choisi de maintenir l'interdiction actuellement en vigueur de cette pratique en droit français et de prôner activement son interdiction au niveau international. Ainsi, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, rendu public par le ministre de l'Europe et des affaires étrangères le 12 novembre dernier au Forum de Paris sur la Paix, et soutenu par le Président de la République à l'occasion de son discours à l'UNESCO devant le Forum sur la gouvernance de l'Internet, a été l'occasion de réaffirmer le monopole étatique de la violence légitime. Cette initiative se décline aujourd'hui de façon opérationnelle dans différents fora, notamment à l'OCDE et à l'ONU.

La France **promeut donc à l'international** sa vision selon laquelle le droit international est applicable au cyberespace et l'attribution publique reste une décision politique qui relève de la souveraineté et ne peut donc être déléguée à une organisation internationale. Dans ce domaine, la défense de la souveraineté numérique est affirmée.

Le 9 septembre 2019, Florence Parly a annoncé la parution d'un rapport concernant l'application du droit international aux opérations dans le cyberespace en temps de paix et en temps de conflit. Ce rapport vise à :

- éclairer les travaux des Nations unies,

- confirmer l'application du droit international au cyberespace, réduire les risques d'escalade non maîtrisée[1].

b) L'enjeu de la protection des données stratégiques : quel chiffrement pour quelles données ?

En matière de protection des données et des communications de l'État, des entreprises et des citoyens, la diversité des enjeux conduit, selon les indications présentées lors des auditions de votre commission d'enquête, à décliner le niveau d'ambition de la France en différentes sphères :

[1] *Voir le communiqué de presse du ministère des armées* La France s'engage à promouvoir un cyberespace stable, fondé sur la confiance et le respect du droit international, *publié le 9 septembre 2019 sur le site www.defense.gouv.fr.*

- pour les données et communications classifiées, l'obligation de résultat, garantissant leur protection contre des attaques ciblées des adversaires les plus compétents est indiscutable. Cette ambition implique la maîtrise nationale de certaines technologies, au premier rang desquelles le chiffrement des communications. La France possède dans ce domaine une industrie de confiance, apte à fournir des équipements de très haut niveau de sécurité, agréés pour protéger les données échangées de niveau de classification Secret Défense. **Le maintien d'une industrie nationale à la pointe dans ce domaine est une absolue priorité** ;

- pour le champ plus étendu des données et communications sensibles, doivent être fixées des contraintes auxquelles se conformeront les solutions numériques utilisées par l'État et les opérateurs critiques. Il est illusoire de chercher à répondre à l'ensemble de ces besoins par des solutions purement nationales. Sans exclure fondamentalement des fournisseurs étrangers, cet objectif nécessite de disposer en France **d'un tissu industriel de confiance**, capable de produire des briques élémentaires de sécurité, mais aussi de concevoir des systèmes complexes en y intégrant des briques étrangères. Ceci implique que les **opérateurs français gardent un niveau de compétence suffisant pour concevoir les architectures de sécurité prévoyant l'insertion de telles briques** ;

- pour le champ plus large de la sécurité économique des entreprises non vitales et de la protection des usages numériques des citoyens, l'État doit préserver sa capacité d'influence des choix numériques des acteurs concernés, en identifiant des solutions de qualité sans les imposer. À cette fin, l'Anssi généralisera progressivement son dispositif de **labellisation** à l'ensemble des solutions numériques, afin d'encourager le recours aux meilleures solutions. Ce dispositif gagnera en pertinence économique grâce à son extension à l'échelon européen, permise par le *Cybersecurity Act* adopté le 12 mars 2019 par le Parlement européen[1].

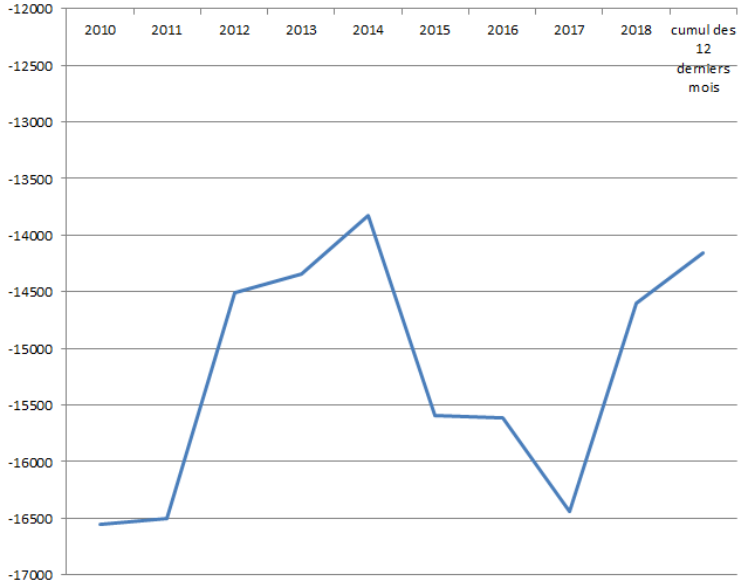
Cette déclinaison en trois sphères s'applique pleinement à la question du *cloud*. Ainsi, pour ses données classifiées, l'État a recours exclusivement à un *cloud* interne. En revanche, pour d'autres données publiques et pour les besoins des entreprises, la qualification des *clouds* par l'Anssi permettra d'identifier les offres – pas nécessairement nationales – qui apportent des garanties suffisantes vis-à-vis des risques tant techniques (risque d'attaque informatique) que juridiques (contraintes de mise à disposition des données à des autorités étrangères).

[1] *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité).*

C. FAVORISER LE DÉPLOIEMENT DES INFRASTRUCTURES NUMÉRIQUES SUR NOTRE TERRITOIRE.

Dès 2010, un rapport au Premier ministre estimait que « *l'Europe ne saurait en effet devenir la simple utilisatrice de biens et services, conçus et produits ailleurs dans le monde* »[1]. Or, comme le montrent les graphiques suivants, **la France est toujours un pays consommateur de produits et de services numériques et producteur de données captées par les grands acteurs étrangers.** Il est difficile d'ignorer l'insuccès des politiques publiques conduites jusqu'à aujourd'hui dans ce domaine.

Un pays consommateur de produits numériques – solde des échanges de produits informatiques, électroniques et optiques[2] (en millions d'euros)



Source : direction générale des douanes et des droits indirects (https://lekiosque.finances.gouv.fr/site_fr/A129/data_cvs.asp?serie=S30CI&r=1)

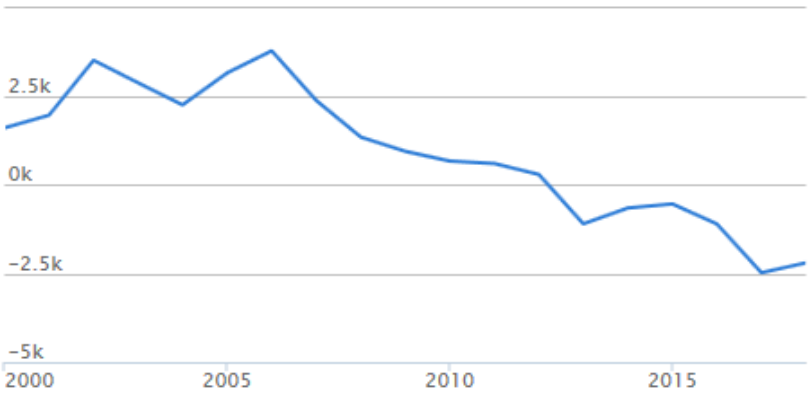
NB : selon le rapport de l'inspection générale des finances, intitulé Le soutien à l'économie numérique et à l'innovation *et publié en janvier 2012 : en 2002, le déficit sur ce point était encore à environ 5 milliards d'euros. Le décrochage observé au cours des années 2000 s'expliquerait par les nombreuses fermetures d'usines et l'érosion des parts de marché d'entreprises françaises comme Alcatel-Lucent.*

---

[1] *Jean-Michel Hubert, Perspectives pour une Europe numérique, 2010.*

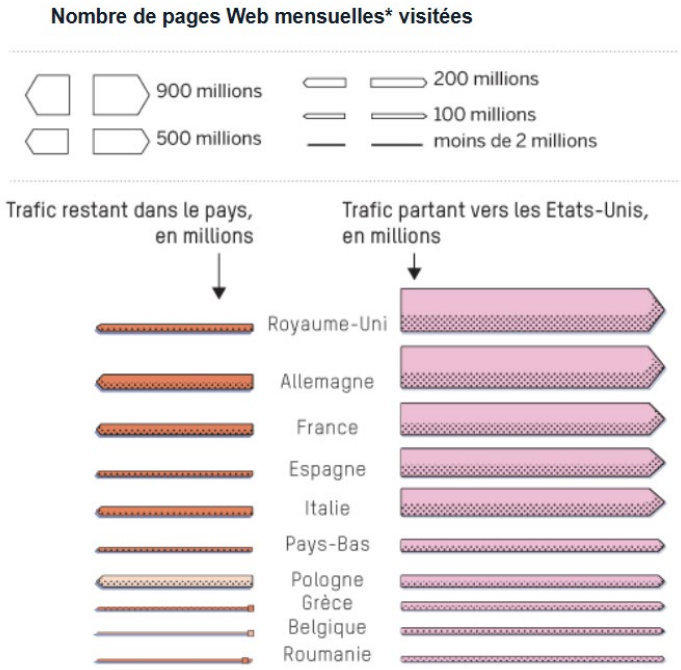
[2] *Cette catégorie de produit correspond, selon la classification des produits française, aux catégories suivantes : composants et cartes électroniques, ordinateurs et équipements périphériques, téléphones et équipements de communication, produits électroniques grand public, appareils de mesure, d'essai et de navigation, équipements électromédicaux de diagnostic et de traitement, matériels optique et photographique ; supports magnétiques et optiques. Notre balance commerciale n'est positive que sur les postes composants et cartes électroniques et appareils de mesure, d'essai et de navigation.*

Un pays consommateur de services numériques – Solde brut des transactions courantes en services de télécommunications, d'informatique et d'information (en millions d'euros)



Source : banque de France[1]

Un pays exportateur de données – La captation des données des Français et des Européens par les grands acteurs du numérique



Source : Lemonde.fr, d'après les calculs établis par la Chaire Castex de cyberstratégie (IHEDN), l'Inria et l'IFG (Université Paris-VIII)

Comme le remarquait notre collègue député Cédric Villani dans son rapport sur l'intelligence artificielle[2], « *80% des visites vers les 25 sites les plus populaires sur un mois sont captés par les grandes plateformes américaines. De ce*

[1] *http://webstat.banque-france.fr/fr/quickview.do?SERIES_KEY=302.BPM6.A.N.FR.W1.S1.S1.T.B.SI._Z._Z._Z.EUR._T._X.N.*

[2] *Cédric Villani,* Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne, *mars 2018.*

point de vue, l'Europe fait figure d'exception : tant la Russie que la Chine, pour ne citer qu'elles, parviennent à capter l'essentiel des données de leurs utilisateurs ».

À l'image de la réindustrialisation de la France, le soutien à l'émergence d'une « industrie » française du numérique permettra de rapatrier la création de valeur ajoutée dans notre pays. S'il fallait une preuve supplémentaire de cette nécessité, les mesures adoptées par le Gouvernement américain dans le cadre de la guerre commerciale qui l'oppose à la Chine démontrent l'urgence de se doter, là où cela est possible, d'une capacité autonome de production.

L'un des piliers de la souveraineté numérique est « *l'existence d'une base industrielle suffisamment solide pour permettre à l'entité politique de disposer d'un minimum d'autonomie quant aux infrastructures, aux équipements et aux logiciels qui lui permettent d'intervenir dans le cyberespace* »[1]. Devant votre commission[2], le Dinsic a estimé que « *si nous ne disposons pas d'acteurs capables de produire les infrastructures, de construire les services, de gérer la relation de premier niveau avec les usagers et de maîtriser les interfaces, nous serons probablement relégués en deuxième division en matière de souveraineté* ».

Une politique volontariste en la matière doit poursuivre trois directions, pour que la France et l'Europe retrouvent une pleine souveraineté sur l'ensemble des couches du cyberespace :

- déployer les infrastructures numériques sur notre territoire ;

- se doter d'une véritable politique industrielle identifiant les secteurs technologiques clés dans lesquels investir nos forces ;

- créer un écosystème favorable mobilisant les moyens humains et financiers pour faire émerger des champions français et européens.

Sur le premier point, comme cela a déjà pu être souligné dans le présent rapport, malgré le caractère immatériel du web et du « cyberespace », internet **garde un ancrage territorial donnant prise à la puissance publique** : le réseau dépend en effet d'**actifs physiques** stratégiques indispensables qui nécessitent des investissements considérables et relèvent, au moins pour partie, d'ordres juridiques nationaux. Mais les actifs physiques ne sont pas les seuls indispensables à l'exercice de la souveraineté numérique. Comme on l'a vu, l'importance des données rend nécessaire le fait de **disposer de gigantesques bases de données**, ne serait-ce que pour rester dans la course de l'intelligence artificielle.

Cet effort en faveur des infrastructures doit cependant être au service d'une politique nationale de souveraineté : il serait en effet

---

[1] *Didier Danet,* Quelle base industrielle et technologique pour la souveraineté numérique ?, *in Droits et souveraineté numérique en Europe, 2016.*

[2] *Audition du 25 juin 2019.*

paradoxal de financer les autoroutes sur lesquelles circuleraient des usagers qui se jouent des lois et normes locales.

1. Être attractif dans le domaine des câbles sous-marins

Les **câbles sous-marins** accueillent 99 % des communications électroniques intercontinentales. Selon le site internet de référence en la matière[1], il y a actuellement 378 câbles déployés dans le monde représentant 1,2 million de kilomètres de fibre optique.

Le fait qu'un pays **dispose de câbles sous-marins en nombre suffisant et sécurisés** est donc un élément indispensable à sa souveraineté numérique[2]. Devant votre commission, la Secrétaire générale de la défense et de la sécurité nationale, Claire Landais, a fait état des réflexions de l'État français sur le sujet : « *La protection des réseaux passe (…) par celle de nos câbles sous-marins, essentiels dans l'architecture des réseaux actuels. La problématique de la résilience se double d'un enjeu d'attractivité pour notre territoire, et nos réflexions en la matière mobilisent plusieurs départements ministériels, afin que nous soyons compétitifs* ».

Le législateur a déjà renforcé l'attractivité de notre pays pour les investissements de ce type, à travers :

- une disposition introduite dans la loi ELAN[3] à l'initiative du Sénat en vue de faciliter les procédures administratives ;

- et une autre introduite en loi de finances pour 2019[4] à l'initiative de l'Assemblée nationale en vue d'exclure explicitement les câbles sous-marins de communications électroniques du champ de la redevance d'archéologie préventive.

Il convient de **poursuivre ce chantier de la simplification administrative** pour l'atterrage des câbles sous-marins de communication électronique, par exemple en nommant un point de contact unique pour les investisseurs internationaux.

---

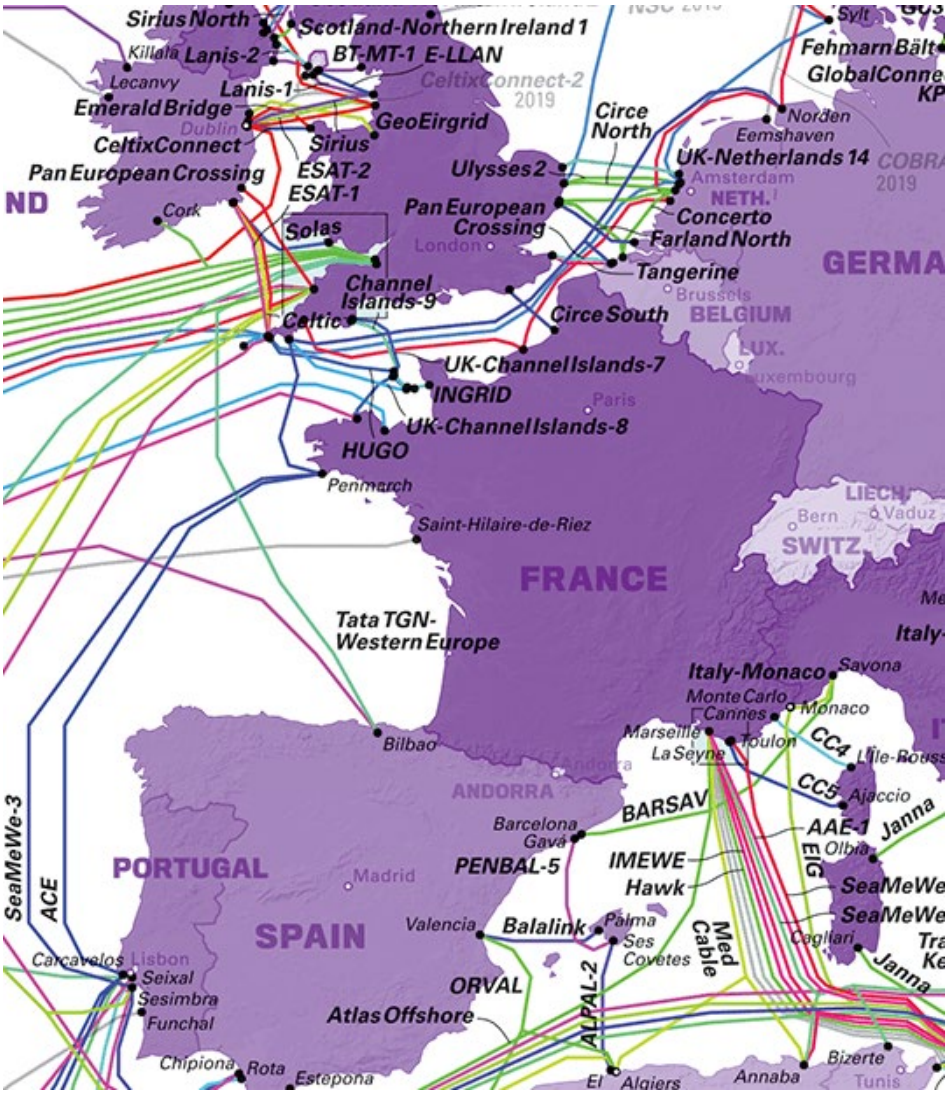
[1] *telegeography.com*

[2] *Il l'est encore plus dans un pays comme la France, dont 70 à 80 % du trafic internet transite par les câbles transatlantiques – la Chine et la Russie en sont moins dépendantes, dans la mesure où ces Etats ont développé leur propre Internet (voir l'article intitulé* Internet : les Gafa font main basse sur les câbles sous-marins *d'Elsa Bembaron publié le 27 août dernier dans Le Figaro).*

[3] *Article 224 de la loi n° 2018-1021 du 23 novembre 2018 portant évolution du logement, de l'aménagement et du numérique.*

[4] *Article 74 de la loi n° 2018-1317 du 28 décembre 2018 de finances pour 2019.*

Carte des câbles sous-marins de communications électroniques reliant la France



Source : https://submarine-cable-map-2019.telegeography.com

Dans une logique de souveraineté technologique, il est nécessaire de **s'assurer que ces infrastructures ne soient pas détenues exclusivement par des entités étrangères et ne puissent pas faire l'objet de dégradations**.

Sur le premier point, l'offensive des Gafam inquiète[1]. Jusqu'à il y a quelques années, ces câbles étaient en effet propriété de *consortia* d'entreprises principalement composés d'opérateurs de télécommunications. Ils sont désormais portés par les géants américains du numérique afin de s'assurer que les capacités des câbles sous-marins supportent le trafic généré

[1] *Voir, par exemple, l'article intitulé* Facebook, Google, Amazon... Pourquoi les géants du Net se ruent sur les câbles sous-marins *publié sur le site internet Challenges.fr le 18 juillet 2019. Les citations qui suivent de Jean-Luc Vuillemin, directeur des réseaux internationaux d'Orange, en sont issues.*

par leurs activités[1] et relient leurs centres de données. Selon Jean-Luc Vuillemin, directeur des réseaux internationaux d'Orange[2], « *les opérateurs télécoms sont concurrencés par les Gafam qui représentent 30 % de nos clients. Il y a dix ans, 5 % des câbles sous-marins étaient contrôlés par les Gafam. Aujourd'hui c'est 50 % et ce sera 95 % d'ici trois ans* ». Il estime également que « *Facebook projetterait d'investir trois milliards de dollars dans le secteur et s'appuie sur une division de 250 personnes spécialisées sur le sujet* ».

Or, « *cet appétit grandissant fait que le secteur est devenu un véritable Far West. Les câbles sous-marins sont le seul domaine de l'Internet qui n'est pas régulé. Les Gafam, comme les autres acteurs, peuvent faire ce qu'ils veulent* ». De même, un rapport rédigé par un parlementaire britannique a pu souligner que « *le droit en vigueur correspond davantage au rôle secondaire que jouaient les câbles dans les années 1970-1980 qu'à leur caractère aujourd'hui indispensable* »[3]. Il conviendrait donc de **réfléchir à une régulation internationale de ces infrastructures stratégiques**, qui permettrait aux États d'imposer certaines règles, tant pour des raisons sécuritaires qu'économiques (afin de garantir la neutralité des flux transportés).

Sur le second point, toute atteinte à un câble sous-marin pourrait avoir des effets économiques désastreux. Or, le caractère public de leur localisation les rend extrêmement vulnérables.

Il conviendrait donc d'effectuer un audit de sécurité de ces câbles et, le cas échéant, de **renforcer les exigences de sécurité qui leurs sont applicables**. Le Sénat a déjà effectué un premier pas en ce sens, en insérant dans la loi « 5G »[4] un rehaussement du montant de l'amende applicable en cas de dégradation d'un câble sous-marin, y compris des stations d'atterrage[5].

Ces câbles peuvent également faire l'objet de menaces d'ordre étatique : il est ainsi de notoriété publique que des sous-marins et des bâtiments de surface russes ont été repérés à leur proximité[6]. Julien Nocetti, chercheur à l'Institut français des relations internationales a souligné devant votre commission que « *les points d'atterrage et d'interconnexion des câbles sont un enjeu stratégique, qui permettent aux États de conduire des opérations d'espionnage, de piratage et d'intimidation. Certains pays, tels que la Russie, ne se*

---

[1] *C'est ainsi que le vice-président en charge de l'ingénierie des réseaux justifie la démarche de Facebook dans l'article publié le 18 novembre 2018 par le magazine Wired et intitulé* Google and Facebook are gobbling up the internet's subsea cables.

[2] *L'entreprise est partenaire du projet de câble transatlantique Dunant, porté par Google, qui reliera la France et les États-Unis à l'horizon 2020.*

[3] *Rishi Sunak,* Undersea Cables, Indispensable, Insecure, *2017.*

[4] *Loi n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.*

[5] *L'amende passe de 3 750 à 75 000 euros.*

[6] *Voir le rapport rédigé par un parlementaire britannique précité, qui consacre une partie entière au* « risque en provenance de Russie ».

privent pas d'exploiter la dimension physique d'Internet sous un angle stratégique. C'est un enjeu de souveraineté majeur pour l'Union européenne ».

Afin de s'assurer de la résilience des communications électroniques intercontinentales, il convient de :
- poursuivre le chantier de la **simplification** administrative pour l'atterrage des câbles sous-marins de communication électronique ;
- effectuer un **audit de sécurité** de ces câbles et, le cas échéant, renforcer les exigences de sécurité qui leurs sont applicables.
Une réflexion sur la **régulation internationale** de ces infrastructures stratégiques devrait également être menée afin de déterminer la position de la France sur le sujet.

2. Accélérer la couverture numérique du territoire

L'existence d'une « fracture numérique » **minore le potentiel de la France en matière de compétences et d'innovation**. Elle se traduit, d'une part, par l'existence de territoires privés d'un accès performant au numérique, d'autre part, par l'éloignement du numérique de certains de nos concitoyens[1] – ce que le Gouvernement a pu désigner par le terme « d'illectronisme » – et de nos entreprises[2]. Force est de constater que, malgré une amélioration, **la couverture numérique est toujours insuffisante, tant sur le fixe que sur le mobile**.

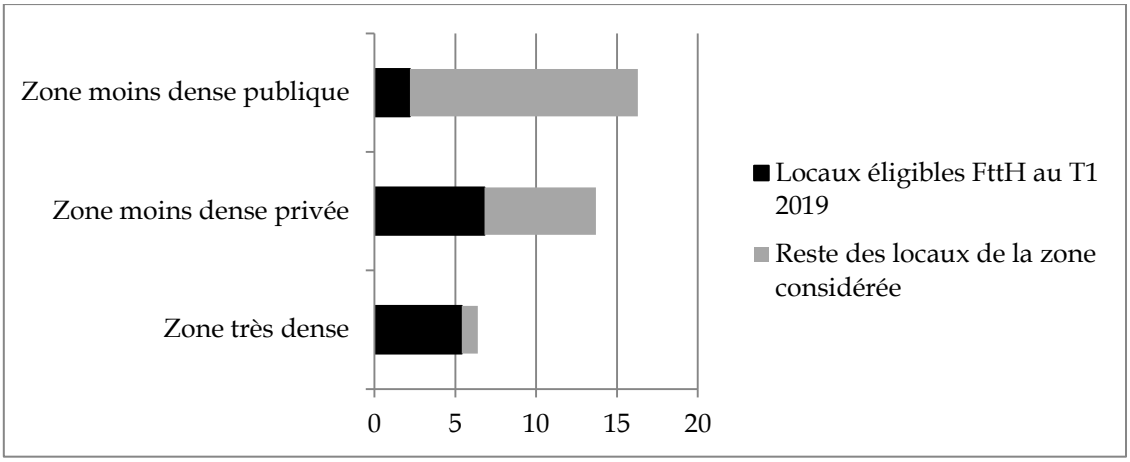
Selon le *digital economy and society index* (Desi) de la Commission européenne, en 2018, la France était **dernière en Europe en termes de couverture en très haut débit fixe**. Pourtant, dès 2010, notre pays s'est doté d'un plan de financement des infrastructures fixes dans les zones les moins denses de notre territoire, rebaptisé en 2013 « plan France très haut débit ». Celui-ci ambitionne de connecter la totalité de la population au très haut débit[3] en 2022.

En 2018, seuls 58 % des locaux disposaient d'une couverture en très haut débit. De plus, comme le montre le graphique ci-dessous, la couverture en fibre optique jusqu'à l'abonné (FttH) de l'ensemble des locaux du territoire est loin d'être réalisée. Même si cela n'est pas l'objectif initial du plan, la Commission européenne[4] a fixé, pour 2025, l'objectif d'une couverture totale des locaux à 100 mégabits par seconde pouvant évoluer

[1] *Sur ce point, le manque d'ambition du plan national pour un numérique inclusif a pu être souligné par Anne-Catherine Loisier, dans son avis budgétaire n° 148 (2018-2019) relatif à la mission Economie inscrite au projet de loi de finances pour 2019.*
[2] *Voir, sur ce point, le rapport d'information n° 635 (2018-2019) déjà cité de Mme Pascale Gruny, fait au nom de la Délégation aux entreprises du Sénat et intitulé* « Accompagnement de la transition numérique des PME : comment la France peut-elle rattraper son retard ? ».
[3] *À savoir 30 mégabits par secondes, ce qui peut être atteint par la montée en débit sur cuivre, sur câble coaxial ou – solution la plus puissante – par la fibre optique jusqu'à l'abonné.*
[4] *Commission européenne, Communication,* Connectivité pour un marché unique numérique compétitif – Vers une société européenne du gigabit, *14 septembre 2016.*

vers le gigabit – ce que la seule la fibre jusqu'à l'abonné est capable de faire. Se conformer à cet objectif **nécessitera de dégager des moyens supplémentaires**, alors que le guichet France très haut débit est actuellement fermé.

Déploiements du FttH au deuxième trimestre 2018 comparé au nombre total de locaux par zone



Sources : commission, d'après les données publiées par l'Arcep (Observatoire haut et très haut débit, déploiements au T1 2019).

Le Gouvernement doit enfin publier sa stratégie d'investissement dans les réseaux en fibre optique jusqu'en 2025. L'objectif européen de la société du gigabit nécessitera de débloquer des fonds supplémentaires.

De même, en matière de couverture mobile 4G, la France était **18e en Europe en 2018**. Le « *New Deal* » **mobile** conclu en janvier 2018 et rendu opposable aux opérateurs dans les licences en juillet 2018 doit permettre d'améliorer la situation. Selon la presse, **le régulateur a récemment accentué la pression sur les opérateurs pour qu'ils respectent leurs engagements**[1].

Les enseignements des erreurs passées semblent avoir été tirés. Le projet de cahier des charges mis en consultation par l'Arcep pour l'attribution des premières fréquences **5G** insiste ainsi sur l'aménagement numérique du territoire, en prévoyant que le quart des 12 000 sites 5G à déployer d'ici à 2025 seront situés en zone rurale. L'indice Desi de la commission européenne classe d'ailleurs la France à la cinquième position de son indicateur de préparation à la 5G[2].

S'agissant de ces infrastructures terrestres, il convient, à nouveau, de souligner un paradoxe : elles sont **financées par des capitaux français** – publics et privés –, elles sont accessibles à tous, **mais assurent en premier**

[1] *Les Echos,* Couverture des campagnes en 4G : l'Arcep tape du poing sur la table*, 30 juillet 2019.*

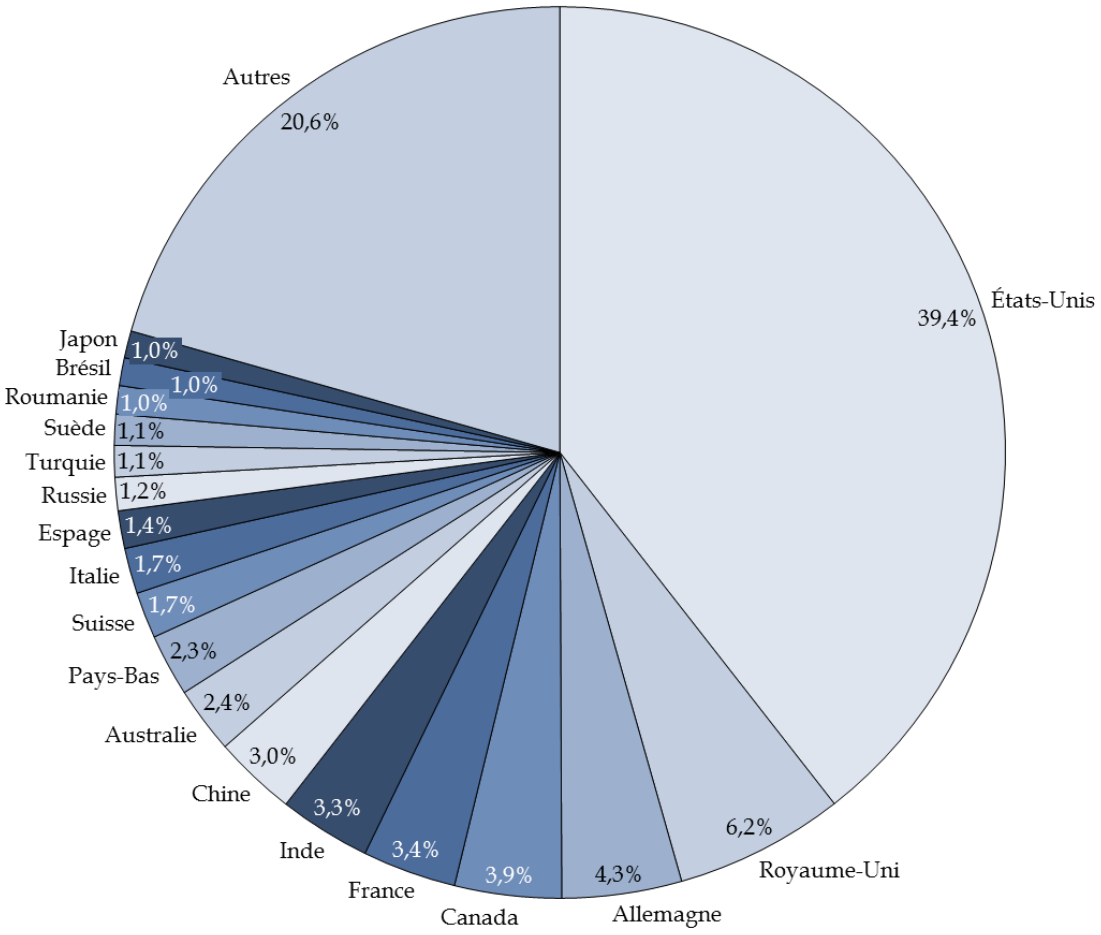
[2] *Basé sur le spectre assigné par rapport au total du spectre harmonisé au niveau européen pour la 5G.*

lieu le développement des Gafam[1], premiers utilisateurs de ces autoroutes de l'information, qui ne souhaitent pas être soumis au statut d'opérateur de communications électroniques.

3. Accroître l'attractivité de la France pour l'implantation des centres de données

On estime que **40 % des capacités d'hébergement de données sont aujourd'hui situées aux États-Unis**. **Notre pays est également moins bien doté que l'Allemagne et le Royaume-Uni.**

Localisation des *datacenters* dans le monde



Source : commission d'enquête, d'après les données de datacentersmap.com

Disposer d'une capacité suffisante d'hébergement et de traitement de données est l'une des conditions de notre souveraineté numérique. Lors

[1] *Selon le baromètre de l'interconnexion de l'Arcep, 53% du trafic vers les clients des principaux fournisseurs d'accès à internet en France provient de quatre fournisseurs : Netflix, Google, Akamai (société américaine spécialisée dans la mise à disposition de serveurs de cache pour les entreprises) et Facebook.*

de l'inauguration d'un centre de données en février dernier, le ministre de l'Économie et des Finances expliquait que « *si nous n'avons pas sur notre sol un nombre suffisant de datacenters pour héberger les données des algorithmes qui sont nécessaires au développement du véhicule autonome, les données de nos automobiles et donc la sécurité, et même la circulation de ces véhicules autonomes seront stockées dans d'autres zones géographiques et soumises au régime juridique local. C'est donc un risque industriel direct, mais aussi un risque de sécurité direct* ».

Les centres de données font donc partie des **infrastructures stratégiques du numérique** : ce sont des « forteresses » industrielles et technologiques chargées de stocker, traiter et transférer des données numériques. Le premier *datacenter* a été créé aux États-Unis en 1946, dans les laboratoires de l'armée américaine. Aujourd'hui, les Gafam ont fait le choix, pour maîtriser la gestion de leurs services et les données de leurs utilisateurs, de développer leurs propres centres de données, et non de recourir à un prestataire extérieur. .

Les centres de données : un composé technologique

Un *datacenter* nécessite un nombre conséquent d'équipements. Si les serveurs informatiques constituent le cœur du dispositif, puisqu'ils traitent la donnée, d'autres installations sont nécessaires à son bon fonctionnement :

- des installations de contrôle pour suivre les performances du centre ;

- des installations de refroidissement pour éviter que la chaleur générée par les serveurs endommage la structure ;

- des installations de sécurité pour protéger les *datacenters* (radars, systèmes de reconnaissance facile ou biométrique…).

Source : audition de Mme Clara Lahiani devant votre rapporteur, le 11 juillet 2019

Plusieurs États ont choisi de modifier leur fiscalité afin d'attirer ces infrastructures. Les centres de données sont en effet un **actif valorisé et valorisant pour un territoire qui en retire** des **bénéfices économiques** (emploi, construction, entretien), des recettes fiscales, une attraction des investissements et des talents[1]. Ils sont également, et surtout, une **infrastructure stratégique**, qui participe de la souveraineté d'un État et de ses citoyens en garantissant la protection juridique des données, la corrélation entre le nombre et/ou la surface des *datacenters* et la puissance de l'industrie du numérique, la maîtrise des services, la sécurisation des infrastructures. Enfin, de par leur nature même, les données peuvent être hébergées en tout lieu et le centre opéré à distance : **sans incitation fiscale, il serait donc plus difficile d'attirer ces infrastructures en France**.

La France peine à prendre la mesure des enjeux de cette compétition internationale. En 2018, la Norvège annonçait par exemple son

[1] *Ainsi, l'université technologique de Lulea [Suède] située à proximité du* datacenter *de Facebook a connu une hausse du taux de candidature en filière ingénieur de 100 %.*

objectif de devenir « une nation à *datacenters* ». Pour être attractif, la plupart des États engagés dans cette course, des États-Unis à la Thaïlande, en passant par les pays de l'espace économique européen, agissent sur **la fiscalité énergétique ; la consommation en électricité pouvant représenter 30% à 50 % des coûts d'exploitation d'un centre**. La Norvège a également introduit une exonération de taxe foncière pour les équipements de production et les équipements d'installation des sites industriels, ce qui revient indirectement à sortir du champ de la taxe foncière une majorité des équipements des *datacenters.*

Les choix effectués par les États relèvent de leurs prérogatives souveraines et illustrent les valeurs et priorités qu'ils souhaitent porter. Ils reflètent aussi la marge de manœuvre dont ils disposent. La fiscalité des centres de données peut donc agir, comme l'a rappelé Mme Clara Lahiani devant votre rapporteur, comme « *un* ***véritable révélateur de souveraineté*** ». Ce choix s'illustre aussi dans la conditionnalité des incitations fiscales : un minimum d'investissements ou d'emplois pour les États américains ; une consommation énergétique réduite ou « verte » dans certains pays européens comme la Suède ou le Royaume-Uni.

En France, la première incitation fiscale en faveur des datacenters a été inscrite en loi de finances pour 2019[1]. Les « centres de stockage de données numériques » pourront bénéficier d'un **taux réduit de taxe intérieure sur la consommation finale d'électricité** (TICFE), sous condition d'un seuil minimal de consommation dépendant de la valeur ajoutée. Trois éléments ont soutenu l'adoption de cette nouvelle disposition : rendre la France plus attractive dans le contexte du Brexit ; attirer les investissements déclenchés par l'entrée en vigueur du *Cloud Act* ; et participer au plan « Transformer notre industrie par le numérique ».

Le dispositif français d'incitation fiscale à l'installation des *datacenters*

Article 266 quinquies C du code des douanes :

Le tarif de la taxe applicable à l'électricité consommée par un centre de stockage de données numériques exploité par une entreprise est, pour la fraction des quantités annuelles excédant un gigawattheure et lorsque la consommation totale d'électricité de ce centre est égale ou supérieure à un kilowattheure par euro de valeur ajoutée, fixé à 12 € par mégawattheure.

Un centre de stockage de données numériques s'entend d'une infrastructure immobilière consacrée au stockage physique, au traitement, au transport et à la diffusion de données numériques, dont l'accès est sécurisé, et comprenant des dispositifs spécifiques et dédiés de contrôle de son environnement thermique, de la qualité de son air, d'alimentation en énergie et de prévention des incendies.

[1] *Modification de l'article 266 quinquies C du code des douanes par la loi n° 2018-1317 du 28 décembre 2018 de finances pour 2019 (article 69).*

La définition française du *datacenter* (infrastructure immobilière consacrée au traitement des données numériques et protégées) ne prend en compte ni le type de données traitées, ni les services associés. De même, l'incitation fiscale s'adresse autant aux *datacenters* « internalisés » (lorsque le centre ne pourvoit qu'aux besoins d'un client unique) qu' « externalisés » (lorsque le centre offre de l'espace de stockage à plusieurs clients, particuliers ou entreprises).

Source code des douanes

Le dispositif fiscal français ne cible pas les *datacenters* en fonction de leurs bénéfices économiques mais de leur consommation énergétique. Le seuil retenu, d'au moins un gigawattheure, s'adresse aux plus grandes infrastructures. Votre rapporteur considère qu'**il serait judicieux d'abaisser ce seuil au profit de plus petites structures.**

Plusieurs auditions ont souligné les enjeux environnementaux posés par l'intense consommation énergétique de ces infrastructures. Votre rapporteur considère que ces deux enjeux ne sont pas incompatibles, au contraire. Le bénéfice de la réduction de la TICFE pourrait par exemple être modulé en fonction de l'origine de l'électricité (en prévoyant par exemple un bonus en faveur de l'électricité « verte »).

Votre rapporteur **recommande de poursuivre les efforts à destination des infrastructures du numérique**, afin que la France puisse bénéficier, sur son territoire, d'équipements propres à défendre sa souveraineté et sa puissance numériques. Ces efforts pourraient également être portés au niveau européen, alors que plusieurs pays de l'Union cherchent à attirer des *datacenters* sur leur territoire *via* différents dispositifs : réduction de la TVA, assouplissement du régime des aides d'État pour les structures hébergeant des données…

Enfin, comme l'a recommandé à votre rapporteur Mme Clara Lahiani, et à l'image de ce qu'a produit la Norvège en 2018 pour faire connaître sa stratégie en ce domaine[1], il pourrait être intéressant (et profitable) que **la France publie un rapport, en français et en anglais, sur les *datacenters*. Ce rapport présenterait les mesures fiscales et non fiscales** incitatives mises en place et envisagées, **il offrirait une visibilité aux acteurs du secteur** et il constituerait un **premier élément dans ce que l'on pourrait appeler la stratégie « marketing » de la France comme future nation à *datacenters***.

[1] *Ce rapport, écrit en plusieurs langues, présente toutes les mesures prises et envisagées pour faire de la Norvège une nation à* datacenters *et inscrire cette stratégie dans des objectifs plus larges de politiques publiques : maximiser la création de valeur ; mettre en œuvre une nouvelle politique énergétique et fiscale ; faciliter la production d'énergies renouvelables ; faciliter l'acquisition et la location de terrain par les* datacenters *; faciliter l'installation de la fibre optique.*
Lien vers le rapport :
https://www.regjeringen.no/globalassets/departementene/nfd/dokumenter/strategier/strategi-nfd-eng-nett-uu.pdf

Accroître les incitations fiscales à destination des *datacenters* et élargir les critères de qualification à la réduction de la taxe intérieure sur la consommation finale d'électricité.

Publier un rapport sur la stratégie française en matière de *datacenters* et l'inscrire dans un champ plus large touchant autant à l'attractivité du territoire qu'à la politique énergétique.

4. Favoriser la constitution de bases de données massives

Comme le rappelait notre collègue député Cédric Villani[1] « *ce n'est qu'au prix d'un plus grand accès et d'une meilleure circulation (des) données, pour en faire bénéficier les pouvoirs publics, mais aussi les acteurs économiques plus petits et la recherche publique, qu'il sera possible de rééquilibrer les rapports de force* » avec les Gafam. Ces bases de données massives peuvent s'assimiler à une **infrastructure essentielle**[2], c'est-à-dire à un intrant indispensable à l'entrée d'un acteur sur un marché. Il apparaît donc nécessaire de réfléchir aux moyens de constituer des bases de données dont les acteurs économiques français et européens pourraient bénéficier. Trois leviers apparaissent complémentaires : l'ouverture de certaines données, l'imposition d'un droit d'accès régulé aux données et l'incitation au partage de données.

La politique européenne du « *free flow of data* » traite du volet relatif à la circulation des données non personnelles : les États membres ne peuvent en limiter la circulation au sein de l'Union européenne, sauf motif de sécurité publique[3].

---

[1] *Cédric Villani,* Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne, *mars 2018.*

[2] *Voir, sur ce point, les développements figurant dans le rapport de l'administrateur général des données :* La donnée comme infrastructure essentielle, rapport au Premier ministre sur la donnée dans les administrations, *2016-2017 :* « Il faut aujourd'hui considérer les données comme l'une de ces infrastructures essentielles et critiques. Essentielles car, dans une économie de l'information, l'accès à la donnée de référence fiable et à jour est la condition du développement des services numériques. Critiques car il faudra s'assurer que la fourniture de ces données ne puisse être interrompue, qu'il s'agisse de défaillances involontaires ou d'actes malveillants ». *On peut également consulter le rapport de l'OCDE intitulé* Data-driven innovation : big data for growth and well-being, *2015. Enfin, dans une récente réponse à un référé de la Cour des comptes, le Premier ministre faisait siens les propos de l'administrateur général des données :* « je considère que la donnée doit désormais être vue comme une infrastructure essentielle et critique du fonctionnement de l'économie et de l'État. La maîtrise de la production de la donnée, de son utilisation et de sa valorisation relève d'enjeux que l'on peut qualifier de souverains. Dans une économie de l'information, l'accès à une donnée de référence fiable et à jour est, en effet, le fondement et la condition du développement des services numériques » *(réponse en date du 4 mars 2019 au référé de la Cour des comptes sur la valorisation des données de l'IGN, de Météo France et du Cerema : l'enjeu de l'ouverture des données publiques).*

[3] *Règlement 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.*

La politique française de la donnée non personnelle repose, depuis plusieurs années, sur le principe d'ouverture des données (ou *open data*) en vue de favoriser la création de nouveaux services à valeur ajoutée reposant sur la réutilisation des données.

La loi pour une République numérique[1] a défini un **principe d'ouverture des données publiques et de certaines données privées**[2]. Cet édifice est amené à être complété par la révision de la directive dite « PSI »[3].

S'agissant des données privées, la France privilégie, depuis la publication en 2015 du rapport sur les données d'intérêt général[4], une approche sectorielle et des modalités diverses par domaines d'activité : c'est le cas dans le secteur énergétique[5], dans les transports[6], dans le secteur bancaire[7] ou encore, dans le secteur de la santé.

[1] *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.*

[2] *Données indispensables à l'exécution d'un contrat de concession, données essentielles d'une subvention. Elle permet également à l'Insee d'avoir accès à des données d'acteurs privés à des fins exclusives d'établissement de statistiques.*

[3] *Directive UE 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.*

[4] *Laurent Cytermann, Claudine Duchesne (Conseil général de l'économie, de l'industrie, de l'énergie et des technologies) et Laurent Vachey (Inspection générale des finances), , Rapport relatif aux données d'intérêt général, septembre 2015.*

[5] *Ouverture des données détaillées de consommation et de production issues des systèmes de comptage d'énergie des gestionnaires de réseaux publics de distribution et de transport d'électricité et de gaz (articles L. 111-73-1 et 111-77-1 du code de l'énergie).*

[6] *Le projet de loi d'orientation des mobilités en cours d'examen au Parlement contient plusieurs dispositions ayant pour objectif d'organiser un accès, sous le contrôle de l'Autorité de régulation des activités ferroviaires et routières, à certaines données : ouverture des données nécessaires à l'information du voyageur (articles 9 et 10), accès à la billettique des services de transport (article 11), accès aux données des véhicules (article 13).*

[7] *Au niveau européen, la deuxième directive sur les services de paiement (dite « DSP 2 ») oblige les banques à collaborer avec les agrégateurs de données sur les comptes en leur donnant accès aux informations des clients pour lesquels ils tiennent des comptes de paiement – autrement dit, elle oblige au partage de données entre les banques et les* « fintech » *(partage généralement désigné par les termes* « open banking »*). Ce dispositif résulte de l'article 67 de la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE et règlement délégué n° 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.*

Le Health Data Hub ou plateforme des données de santé

Lors de la remise du rapport Villani précité, le Président de la République a indiqué que la santé serait un des secteurs prioritaires pour le développement de l'intelligence artificielle. Il a, en conséquence, annoncé la création d'un *Health Data Hub* et l'élargissement du système national de données de santé (SNDS), initiatives entérinées dans la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

L'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé a créé un système national des données de santé (SNDS) sous la responsabilité de la Caisse nationale de l'assurance maladie des travailleurs salariés. Il rassemble les données de l'Assurance Maladie, des hôpitaux, des causes médicales de décès, les données relatives au handicap et un échantillon de données en provenance des organismes d'Assurance Maladie complémentaire. La loi santé de 2019 y insère les données cliniques, de nature qualitative, renseignées par le professionnel de santé à l'occasion d'une consultation ou d'un suivi.

La plateforme des données de santé, constituée sous forme de groupement d'intérêt public, est notamment chargée de réunir, organiser et mettre à disposition les données du SNDS et de promouvoir l'innovation dans leur utilisation. Selon la communication institutionnelle du Gouvernement, cette initiative doit « *permettre de faire de la France un leader dans l'utilisation des données de santé, au service du bien commun, dans le respect du droit des patients et en totale transparence avec la société civile* »[1].

Un appel à projets visant à sélectionner les premières initiatives innovantes en matière d'exploitation des données de santé et qui présentent un intérêt public a abouti à la sélection de dix lauréats en avril 2019.

Cependant, l'ouverture des données se heurte à plusieurs limites[2] – le groupement français de l'industrie de l'information n'hésite pas à la qualifier de « *déni inconscient de souveraineté* »[3]. D'abord, elle est souvent considérée comme profitant avant tout aux géants du numérique, qui seuls disposent de l'expertise pour se lancer rapidement dans l'exploitation de ces données. De plus, là où ceux-ci devaient auparavant payer pour obtenir ces données, elles sont désormais mises – le plus souvent – gratuitement à leur disposition. Cependant, les tenants de l'ouverture des données soulignent que, à défaut d'*open data*, de petites entreprises innovantes ne disposeront jamais des moyens nécessaires à l'achat de ces données. Autrement dit, mieux vaut permettre un accès large aux données afin que tout le monde parte sur la même ligne de départ, plutôt que de maintenir une situation dans laquelle seuls les géants du numérique ont accès à ces données.

---

[1] *Voir, sur les données de santé, le rapport sur l'intelligence artificielle et les données de santé de MM. Gérard Longuet, sénateur et Cédric Villani, député, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, publié le 21 mars 2019.*

[2] *L'inspection générale des finances a été missionnée par le Premier ministre pour établir un bilan de la politique d'ouverture des données publiques.*

[3] *Source : contribution écrite transmise à votre rapporteur.*

Lors des auditions de votre commission d'enquête, le Dinsic a indiqué que les critiques relatives à l'ouverture des données étaient prises en compte. Pour les données publiques, la priorité est donc la circulation de la donnée au sein de l'Etat. L'Institut national de l'information géographique et forestière a également souligné – tout en précisant que cette évolution était positive – le changement de modèle économique que l'ouverture des données lui imposait.

Quoi qu'il en soit, toute ouverture de données privées ne devrait s'envisager que :

- s'il existe un motif d'intérêt général ;

- si cette ouverture ne porte pas une atteinte disproportionnée à la liberté d'entreprendre ;

- et si ses modalités sont précisément encadrées – à travers un régulateur ou une administration dédiée, la puissance publique étant amenée à jouer le rôle de tiers de confiance dans la gestion de l'ouverture des données.

En effet, le degré d'ouverture imposé à ces données doit prendre en compte un ensemble de facteurs, notamment l'impact économique, financier et concurrentiel sur les entreprises concernées.

En matière d'**ouverture des données**, il convient donc de **retenir une approche au cas par cas afin de s'assurer de la proportionnalité du dispositif aux fins poursuivies.**

Lorsque la détention de bases de données constitue une importante barrière à l'entrée, un **droit d'accès** aux données pourrait être organisé, sous le contrôle d'un régulateur qui serait chargé d'en examiner les modalités (selon les bases applicables à la régulation des infrastructures : accès dans des conditions transparentes, non discriminatoires et raisonnables), afin de favoriser la concurrence et l'innovation.

Cette hypothèse a été évoquée par la présidente de l'Autorité de la concurrence : « *nous pourrions ainsi, par exemple, organiser un droit d'accès – pas forcément gratuit – aux données détenues par un moteur de recherche qui permettrait à un nouvel acteur de disposer des moyens pour se développer. Cela peut s'organiser par le droit de la concurrence ou par une régulation ciblée sur l'accès aux données* ». Un tel droit d'accès pourrait également être envisagé au bénéfice des autorités publiques pour la conduite de leurs politiques, comme cela est envisagé en matière de mobilité dans le cadre du projet de loi d'orientation des mobilités.

Mettre en place un **droit d'accès aux données** dans certaines hypothèses et sous le contrôle d'un régulateur afin de favoriser la concurrence et l'innovation ainsi que la bonne mise en œuvre des politiques publiques.

Enfin, si « *le premier acte de la « bataille de l'IA » portait sur les données à caractère personnel, cette bataille a été remportée par les grandes plateformes. Le second acte va porter sur les données sectorielles : c'est sur celles-ci que la France et l'Europe peuvent se différencier* »[1]. L'enjeu est donc que la France et l'Europe parviennent à faire émerger des champions autour des données professionnelles et industrielles.

C'est pourquoi il convient d'inciter les acteurs privés à mutualiser leurs données, pour créer des « communs de la donnée », l'État pouvant ici aussi être amené à jouer le rôle de tiers de confiance. Un appel à manifestation d'intérêt (AMI) a été ouvert de septembre à décembre 2018. Cet AMI visait à évaluer l'intérêt, les besoins et les initiatives des acteurs privés et publics en vue d'un futur appel à projets soutenant des initiatives de mutualisation de données. Environ 80 réponses ont été reçues, témoignant de l'intérêt des acteurs économiques pour une telle initiative. L'appel à projets a été lancé le 25 juillet dernier. Cette initiative est bienvenue.

Inciter au partage et à la mutualisation de données privées sectorielles afin de favoriser le développement de l'IA en France.

D. SE DONNER LES MOYENS DE LA SOUVERAINETÉ NUMÉRIQUE À TRAVERS UNE VÉRITABLE POLITIQUE INDUSTRIELLE[2] SOUTENANT LE DÉVELOPPEMENT DES TECHNOLOGIES CLÉS.

Dès 2015, le Sénat a plaidé, dans une résolution européenne adoptée à l'initiative de notre collègue Catherine Morin-Desailly, pour « *une véritable politique industrielle en faveur du numérique dans l'Union européenne* »[3].

Plusieurs personnes auditionnées par votre commission rejoignent cette recommandation, à l'image de Benoît Thieulin, selon qui « *il est grand*

---

[1] *Rapport de Cédric Villani précité.*

[2] *La politique industrielle est ici entendue dans un sens englobant, qui prend en compte les limites de la définition classique de l'industrie. Comme le remarquait le Conseil d'analyse économique en 2014,* « l'industrie change de nature et ne fait plus qu'une avec les services ». *Selon les experts du Conseil,* « c'est la production de masse, la réalisation d'économies d'échelle, les gains de productivité et l'application du progrès technique » *qui définissent désormais l'industrie. Et les auteurs de s'interroger :* « Apple, Google, Microsoft, IBM, Verizon, Facebook, Oracle, Amazon sont-elles des entreprises industrielles, ou des entreprises de services ? » *(Conseil d'analyse économique,* Pas d'industrie, pas d'avenir ?, *juin 2014).*

[3] *Résolution européenne pour une stratégie européenne du numérique globale, offensive et ambitieuse, 30 juin 2015. Elle plaidait pour la constitution d'une telle politique* « grâce à un pilotage stratégique et une plus grande cohérence entre la politique de concurrence de l'Union et sa politique industrielle, en assouplissant le régime des aides d'État, en mobilisant le fonds européen d'investissement stratégique du plan Juncker, en encourageant le développement du capital-risque dans l'Union, en promouvant l'adoption de normes communes en matière industrielle dans l'objectif de faciliter le développement et la croissance des entreprises innovantes du numérique et de soutenir des projets industriels d'envergure européenne - traitement des données de masse, services sécurisés mais ouverts d'informatique en nuage ».

temps de se doter d'une véritable politique industrielle. Le plan Juncker allait dans la bonne direction, il était d'assez grande ampleur, mais il ne faisait pour ainsi dire pas de choix stratégiques. On peut tout à fait accepter que la raquette numérique ait des trous – encore faut-il, néanmoins, qu'il y ait une raquette ! Je pense, évidemment, au cloud. (…) Je pense également à la 5G. (…) Nous voyons aujourd'hui l'importance géopolitique stratégique de Galileo, qui, malgré des débuts difficiles, a été un succès. Je pense, enfin, à l'operating system ». De même, pour Thierry Breton, « *l'Europe doit (…) lancer (…) une véritable politique industrielle* ».

Votre rapporteur salue le fait que le secrétaire d'État chargé du numérique juge prioritaire de « *faire émerger des champions* » – à travers une politique transversale d'écosystème, et reconnaisse que « *l'Europe et la France ne peuvent pas se permettre d'être absentes d'un certain nombre de technologiques critiques – intelligence artificielle, calcul quantique, blockchain, semi-conducteurs…* ». De même, le ministre de l'économie et des finances a-t-il estimé devant votre commission que « *sans maîtrise de ces ruptures technologiques, il n'y a plus de souveraineté politique* ».

Il apparaît urgent de **mener une revue précise** de nos avantages et de nos faiblesses dans l'économie numérique, à l'image de ce qui avait pu être fait il y a maintenant sept ans par l'Inspection générale des finances[1]. Celle-ci pourrait être effectuée sous l'égide du Forum institutionnel.

L'identification des technologies clés et l'évaluation du positionnement des filières françaises sur ces technologies pourraient permettre :

- d'orienter les priorités d'investissement ;

- d'identifier les briques technologiques menacées, par exemple en raison de la fragilité financière de certaines entreprises, ou de leur dépendance vis-à-vis de fournisseurs étrangers critiques.

L'intervention publique directe et verticale doit être assumée. Afin de ne pas éparpiller les moyens, il convient cependant de retenir une approche graduée. En somme, tout en évitant de créer des solutions *ex nihilo*, il convient de capitaliser sur nos succès existants et de miser, d'une part, sur des solutions qui se différencient, d'autre part, sur les solutions d'avenir.

[1] *Inspection générale des finances, rapport précité sur le soutien à l'économie numérique et à l'innovation, janvier 2012.*

1. Sécuriser les approvisionnements et les solutions utilisées par les secteurs sensibles plutôt que créer *ex nihilo* des solutions déjà dominées par des acteurs prépondérants.

a) Les difficultés techniques et financières de créer des solutions ex nihilo *sur des marchés déjà dominés.*

Afin de rattraper le retard français et européen dans le développement de certaines solutions structurantes pour l'internet actuel, plusieurs personnes auditionnées ont défendu la nécessité, pour l'État, d'impulser la création de solutions venant concurrencer celles proposées par les Gafam.

C'est en particulier le cas du **système d'exploitation** (ou « OS », pour *operating system*) **dit « souverain »** – qu'on pourrait également appeler domestique, car il n'est considéré comme tel que parce qu'il serait développé par des acteurs français ou européens. Ainsi selon Pauline Türk, professeur de droit public à l'université Côte d'Azur : « *il est nécessaire de développer un système d'exploitation et un moteur de recherche européens* », de même, selon Benoît Thieulin : « *il est indispensable de forger un operating system européen. Procéder sans cet outil, cela revient à faire la guerre sans chars ni fusils* ». Un rapport sénatorial s'était d'ailleurs prononcé en faveur d'une telle solution au niveau européen en 2014[1].

En revanche, d'autres personnes auditionnées ont estimé qu'il ne serait pas raisonnable, pour l'État, de se lancer dans un tel programme industriel. Le secrétaire d'État chargé du numérique Cédric O a ainsi renvoyé la responsabilité de la création d'un tel système d'exploitation au privé[2] : « *nous aurons un OS européen le jour où un acteur privé européen sera capable d'un investissement comparable à celui réalisé par Google, Microsoft ou Apple. (…) n'oublions pas que c'est l'usager qui tranche : inutile de mobiliser autant de fonds si nos concitoyens préfèrent in fine utiliser celui des concurrents privés américains...* ». De même, Jean-Gabriel Ganascia, président du comité d'éthique du CNRS, a alerté sur le fait qu'un tel système « *serait peu utilisé* » et a souligné que le rapport de la Cerna[3] sur la souveraineté à l'ère du numérique rappelle, de façon générale, « *les difficultés qu'il y aurait à revendiquer ces solutions techniques comme étant la solution au problème posé par la souveraineté numérique* ».

---

[1] *Rapport précité de Catherine Morin-Desailly,* L'Europe au secours de l'Internet ?, *dont la proposition n° 37 était ainsi libellée* « favoriser le développement d'un système d'exploitation sur mobile européen constituant une alternative crédible aux principaux systèmes d'exploitation actuellement existants ».

[2] *À cet égard, l'entreprise Tecwec estime qu'elle propose un tel système d'exploitation pouvant être qualifié de « souverain » (AcidOS). Elle fait cependant face à d'importantes difficultés de financement.*

[3] *Commission d'Éthique sur 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 », *Jean-Gabriel Ganascia, Éric Germain, Claude Kirchner, octobre 2018.*

Des critiques à propos d'un tel projet avaient déjà émergé suite à l'adoption de l'amendement relatif à l'étude de faisabilité de la création d'un commissariat à la souveraineté numérique adopté dans le cadre de l'examen de la loi pour une République numérique[1]. Le rapport étudiant la possibilité de créer un tel commissariat considère que « *hormis le cas particulier de la Chine, peu d'acteurs peuvent espérer s'imposer sur un terrain qui est déjà occupé* » et estime « *illusoire de vouloir développer un OS souverain au-delà de la sphère strictement régalienne* ». Des journalistes avaient estimé le coût de développement d'un tel système d'exploitation entre 831 millions et 1,04 milliard d'euros[2]. Enfin, le directeur général de l'Agence nationale de sécurité des systèmes d'information avait également estimé que développer un nouveau système *ex nihilo* relevait du non-sens d'un point de vue technique.

Votre rapporteur rejoint ces analyses : **il apparaît déraisonnable que l'État impulse le développement d'une solution en ne partant de rien.** Un tel programme serait trop coûteux, et risquerait de ne pas trouver son marché face à l'avance prise par le duopole constitué par Google et Apple.

On peut ainsi rappeler l'échec du projet de *cloud* souverain lancé au début des années 2010. Dans le cadre du programme d'investissements d'avenir, l'État a investi dans deux projets rivaux de « *cloud* souverain » : Cloudwatt, d'Orange et Thalès, et Numergy, de SFR et Bull – en choisissant de ne pas inclure OVH, acteur pourtant déjà très développé du *cloud*. Il s'agissait, selon la ministre déléguée à l'Économie numérique alors en poste, de « *restaurer la souveraineté numérique de la France* »[3] en mettant à l'abri des règlementations étrangères les données de l'État et des entreprises. Le projet lancé en 2010 a été poursuivi par les Gouvernements successifs jusqu'à son échec en 2016, faute d'adhésion du marché. Selon la presse, l'État aurait perdu 56 millions d'euros[4]. Fin juillet dernier, Orange a annoncé officiellement la fermeture de Cloudwatt au 1er février 2020.

Du reste, on peut relever que même Microsoft a échoué à développer un système d'exploitation susceptible de concurrencer le duopole constitué sur ce secteur.

Enfin, il est intéressant de constater que M. Pierre Bellanger[5], qui prônait, dans son ouvrage sur la souveraineté numérique, la réalisation d'un système d'exploitation souverain, semble avoir changé d'avis sur ce point.

---

[1] *Voir notamment l'article de Valentine Martin,* La République numérique en débat au Parlement : le projet de commissariat à la souveraineté numérique, *in La souveraineté numérique, le concept, les enjeux, sous la direction de Christian Valar et Pauline Türk.*

[2] *Numerama,* Développer un OS souverain made in France, combien cela coûte ? - *20 janvier 2016.*

[3] *La Tribune,* « Cloud » à la française : Fleur Pellerin justifie les deux projets concurrents », *2 octobre 2012.*

[4] *L'Express,* Le cloud à la française en plein orage, *15 juin 2016.*

[5] *Auteur de l'ouvrage ayant contribué à populariser le concept de « souveraineté numérique » intitulé La souveraineté numérique, publié en 2014.*

En effet, il a plutôt plaidé, devant votre commission, en faveur d'un encadrement des systèmes d'exploitation par des règles qui nous sont propres. Chiffrement des données et règles constitueraient les deux briques d'une « *nationalisation des données, c'est-à-dire la création d'un bien commun souverain protégé par une frontière et administré par une règle commune imposée aux acteurs entrants* ».

Ainsi, comme l'a écrit l'actuelle présidente de la Commission européenne, « *il est peut-être trop tard pour reproduire des géants du numérique, mais il n'est pas trop tard pour atteindre la souveraineté technologique dans certains secteurs technologiques critiques* »[1].

b) Sécuriser les approvisionnements et les solutions utilisées par les secteurs sensibles

Face aux difficultés de créer des solutions *ex nihilo*, il convient néanmoins de **développer des solutions technologiques pour les activités relevant directement de notre souveraineté**, à savoir les ministères les plus régaliens de l'État et, éventuellement, les opérateurs d'importance vitale au sens du code de la défense.

Sur ce point, on peut citer l'exemple du système d'exploitation **Clip OS** développé pour l'État et aujourd'hui ouvert aux secteurs sensibles. Basé sur un noyau Linux[2] et capable de gérer des informations de plusieurs niveaux de sensibilité, Clip OS est à présent disponible en *open source* dans le cadre d'un projet de développement collaboratif. L'exemple de l'application **Tchap** est également intéressant. Selon les termes du Dinsic : « *une messagerie instantanée garantissant que les données échangées entre agents publics, cabinets ministériels ou parlementaires ne se baladent pas aux quatre coins du monde nous a semblé indispensable* ».

Sur les secteurs industriels dans lesquels nous ne disposons d'aucune capacité de production, il convient de s'assurer de notre **sécurité d'approvisionnement**. On peut citer l'exemple de l'actuelle dépendance de la France et de l'Europe envers les États-Unis et certains pays d'Asie (Taïwan, Corée du sud) pour la conception et la **fonderie de composants numériques avancés**. Selon la direction générale des entreprises, à court et moyen terme, l'acquisition d'une capacité de fonderie avancée en Europe serait aujourd'hui trop coûteuse – dépassant les 10 milliards d'euros – et ne serait pas rentable face aux perspectives de marché des producteurs européens. Il convient donc, à ces échéances, de s'assurer d'une diversité de fournisseurs. Des réflexions sont engagées au niveau européen, sous l'égide

---

[1] *Ursula von der Leyen,* A Union that strives for more, My agenda for Europe*, political guidelines for the next European commission 2019-2024. Le 10 septembre dernier, la nouvelle présidente de la Commission a estimé que l'Europe doit* «tirer le meilleur parti de l'intelligence artificielle et des mégadonnées, (…) améliorer la cybersécurité et (…) lutter âprement pour (sa) souveraineté technologique».

[2] *C'est-à-dire un logiciel libre, en open service.*

de la Commission notamment, pour identifier des axes de limitation de cette dépendance.

Enfin, il convient de **s'assurer de la sécurité des solutions commercialisées sur notre sol par les entreprises étrangères**. C'est notamment le choix opéré par la France sur les équipements des réseaux 5G.

La sécurisation des réseaux mobiles de cinquième génération

La cinquième génération de standards de télécommunications mobiles, appelée « 5G »[1] promet un changement d'échelle dans les capacités des réseaux (débits multipliés par dix, temps de latence divisé par dix, plus grande flexibilité du réseau, plus grande efficacité énergétique…). On en attend également d'importantes retombées économiques (250 milliards d'euros par an en 2025 pour les opérateurs[2]), mais surtout le développement de nouveaux usages particulièrement critiques pour la vie économique d'un pays : « usine du futur », véhicule connecté, internet des objets, téléchirurgie, ville connectée…

Comme cela a pu être décrit dans le rapport de Catherine Procaccia[3], une véritable « course » à la 5G est donc engagée dans le monde entier. Le Gouvernement entend y prendre part grâce à la mise en œuvre de sa feuille de route « 5G ». Mais la criticité des usages nécessite également de rehausser le niveau d'exigence en termes de sécurité de ces réseaux : c'est l'objet de la loi n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.

La France est ainsi l'un des premiers pays à avoir officialisé sa position sur le sujet : elle a fait le choix de ne pas interdire tel ou tel équipementier, malgré les pressions exercées par le Gouvernement américain sur ses alliés en cas d'autorisation de déploiement d'équipements de la marque Huawei[4]. La loi met ainsi en place un régime d'autorisation préalable à l'exploitation de certains équipements considérés comme « à risque » et listés par arrêté du Premier ministre[5]. Cette autorisation est octroyée par le Premier ministre, après instruction du Secrétariat général de la défense et de la sécurité nationale et de l'Agence nationale de la sécurité des systèmes d'information. Tout prestataire des opérateurs

[1] *Sur la technologie 5G, voir notamment le Rapport de MM. Pierre Henriet, député et Gérard Longuet, sénateur, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, publié le 11 décembre 2018 et intitulé « Perspectives technologiques ouvertes par la 5G ».*

[2] *https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-service-revenue/*

[3] *Catherine Procaccia, rapport n° 579 (2018-2019), au nom de la commission des affaires économiques sur la proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, 19 juin 2019.*

[4] *Voir, par exemple, s'agissant de l'Allemagne : https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827.*

[5] *Jusqu'ici, la sécurité des réseaux télécoms était assurée par l'autorisation préalable à l'installation d'équipements prévue à l'article 226-3 du code pénal, déjà instruit par l'Agence national de sécurité des systèmes d'information. Mais ce régime était insuffisant, car la sécurité des réseaux 5G devra s'apprécier au-delà de la sécurité des équipements en eux-mêmes : il s'agit de s'assurer de la sécurité des modalités de déploiement et d'exploitation de ces équipements (opérations de configuration et de supervision du réseau, recours à la sous-traitance…).*

sous influence étrangère sera soumis à une forme de surveillance renforcée, car c'est un indice que le Premier ministre devra prendre en compte pour autoriser ou non l'exploitation d'un équipement par un opérateur.

En mars dernier, la Commission européenne a publié des recommandations[1] visant à s'assurer qu'il n'y aura pas de « maillon faible » sur le territoire européen : cette année, à une phase d'évaluation des risques, devra succéder une phase d'élaboration d'une « boîte à outils » susceptibles de faciliter la mise en œuvre de mesures nationales. Cette démarche pourrait éventuellement aboutir, entre autres, à un **dispositif commun de certification des équipements 5G**.

Votre rapporteur se satisfait de cette approche pragmatique, qui permettra à l'État de s'assurer de la sécurité des réseaux 5G et, ainsi, de garantir, sur ce point, la **souveraineté de ces infrastructures**.

2. Assumer le soutien direct au développement des technologies et outils dont la France doit avoir la maîtrise technique.

La France et l'Europe doivent assumer une stratégie de soutien direct à la recherche et aux entreprises du numérique selon la logique suivante :

- bâtir à partir de l'existant pour conquérir de nouveaux marchés ;

- sur les marchés déjà dominés par les géants du numérique, n'envisager de soutenir une solution concurrentielle que si elle repose sur une stratégie de différenciation ;

- investir dans les marchés d'avenir.

Cette stratégie pourrait être définie dans le cadre du forum institutionnel temporaire du numérique et de la loi d'orientation et de suivi de la souveraineté numérique, ce qui permettrait d'associer l'ensemble des forces vives du numérique. Il serait en effet trop risqué de faire reposer sur un ministre l'identification des technologies d'avenir ou, pour reprendre les termes du ministre de l'Economie et des Finances, des technologies de rupture[2].

a) Préserver et soutenir la base économique existante

Le rapport de l'inspection générale des finances publié en janvier 2012 et relatif au soutien à l'économie numérique et à l'innovation a dressé une typologie du cœur de l'économie numérique, qui représentait 5,2 % du PIB et 3,7 % de l'emploi en 2011. Si la France dispose de certains atouts dans

[1] *Commission européenne, recommandations, Cybersecurity of 5G Networks, 26 mars 2019.*

[2] *Bruno Le Maire a d'ailleurs souligné, lors de son audition devant votre commission d'enquête :* « Je ne déciderai pas personnellement quelles sont les technologies de rupture pertinentes, je n'en sais rien, mais nous avons en France les ingénieurs, les chercheurs, les industriels qui, eux, le savent ».

les technologies de base et les infrastructures[1], les services de télécommunications, les applications et les services informatiques, elle est, en revanche, plus faible sur l'économie du net.

S'agissant des technologies de base et des infrastructures, la France dispose d'une base industrielle d'excellence qu'il convient de préserver et de développer.

C'est particulièrement le cas des **câbles** terrestres de fibre optique, marché sur lequel les entreprises Acome, Nexans et Prysmian sont soit françaises soit implantées en France[2]. S'agissant des câbles sous-marins Alcatel Submarine Networks, filiale de Nokia depuis le rachat d'Alcatel-Lucent en 2015, dispose à la fois de capacités de production en France concernant tant les câbles que les terminaux optiques, et de navires permettant d'assurer la pose et la maintenance des câbles (Orange Marine est également un acteur majeur de ce dernier secteur d'activité), en particulier en matière de terminaux optiques. Pour votre rapporteur, **il est crucial de préserver ces compétences en France.**

En matière de **composants électroniques**[3], le franco-italien ST Microelectronics, Gemalto et sa maison-mère Thales ou encore la filiale du CEA Soitec disposent toujours de capacités avancées de production[4]. La poursuite du soutien à ce secteur à travers les plans « Nano » successifs[5] est primordiale. Comme le rappelait une annexe du rapport d'inspection sur le soutien à l'économie numérique et à l'innovation publié en janvier 2012, « *les composants sont au centre de l'économie numérique dont ils assurent le moteur et la mémoire et sont intégrés à la plupart des équipements professionnels et grand public* ». Dans sa contribution écrite, le Cigref a estimé que « *en matière de souveraineté technologique, l'un des domaines prioritaires, et bien souvent ignoré, concerne l'industrie du silicium, des processeurs et des composants* », considérant que les Etats-Unis, comme la Chine, la Russie ou Israël travaillent eux aussi à maintenir ou à obtenir leur autonomie stratégique en la matière. ST Microelectronics a également précisé, dans sa contribution écrite, que la Chine annoncé un investissement de 150 milliards de dollars pour soutenir son industrie des composants électroniques. Il est donc primordial de poursuivre le soutien public à ce secteur.

---

[1] Production et installation de fibre optique, équipements de télécommunications, électronique grand public, composants électroniques, matériel informatique.

[2] La balance commerciale de la fibre optique est positive depuis de nombreuses années. En revanche, en 2018, un déficit a été constaté. Il conviendra d'être vigilant à l'avenir.

[3] Il convient de noter que la balance commerciale de ce secteur est positive.

[4] Au niveau européen, sont très présents le néerlandais NXP, qui entretient un volume important d'activités de R&D en France, et l'allemand Infineon.

[5] Plan « Nano Innov » en 2009, puis Nano 2012, Nano 2017 et Nano 2022.

En matière de **supercalculateurs**[1], Atos est le seul industriel européen encore en mesure de les concevoir et de les fabriquer. Il fournit notamment le calculateur du CEA pour le programme de dissuasion.

Une résolution européenne adoptée par le Sénat à l'initiative de la commission des affaires européennes[2] rappelle en quoi ce secteur est déterminant pour la souveraineté numérique de la France et de l'Europe, notamment dans la mesure où « *la majorité des composants sont étrangers, à l'image des processeurs pour lesquels les entreprises américaines sont en quasi situation de monopole* »[3], et qu'il convient de soutenir l'initiative EuroHPC lancée par l'Union européenne. Devant votre commission, Thierry Breton estimait également que les processeurs utilisés par les supercalculateurs d'Atos « *sont essentiellement américains, taïwanais et sud-coréens. L'industrie européenne, avec STmicroelectronics, existe, mais nous sommes très loin de réaliser les processeurs spécifiques aux supercalculateurs. La Commission a fini par débloquer 250 millions d'euros dans le cadre d'un programme de développement d'un processeur purement européen, dont Atos est le chef de file. Bien qu'insuffisant, c'est un début. Pour être efficaces et pour faire face à la concurrence internationale, ces financements doivent être plutôt concentrés sur un petit nombre d'acteurs* ». Il convient de s'assurer de la réussite de ce programme, essentiel à l'indépendance technologique de l'Europe.

Le programme EuroHPC[4]

L'Union européenne a mis en place, fin 2018, l'entreprise commune européenne pour le calcul à haute performance (EuroHPC). Cette structure a pour objectif de mettre en commun les ressources de 25 pays européens en vue de :

- l'achat, dès 2019, de deux calculateurs pré-exaflopiques, le niveau le plus avancé actuellement, pour les mettre à disposition des chercheurs et des entreprises ;

- lancer un programme de recherche et d'innovation dans le calcul à haute performance pour développer un écosystème européen intégré couvrant toute la chaîne de valeur scientifique et industrielle, et notamment « *le matériel informatique, les logiciels, les applications, les services, l'ingénierie, le savoir-faire et les compétences* ».

La structure est dotée d'un budget d'un milliard d'euros, provenant à parts égales du budget de l'Union européenne et des États membres participants. Des partenaires privés apporteront des ressources complémentaires à hauteur de

[1] *Un supercalculateur est un très grand ordinateur, réunissant plusieurs dizaines de milliers de processeurs, capable de réaliser un très grand nombre d'opérations de calcul ou de traitement de données simultanées.*

[2] *Sénat, Résolution européenne n° 144 (2018-2019) sur le calcul à haute performance, 20 juillet 2019.*

[3] *Atos est positionné sur l'intégration système et les couches logicielles basses et applicatives (40% de la valeur). Les composants élémentaires tels que les processeurs (40% de la valeur) de calcul et les mémoires (30% de la valeur, mais considérés comme des commodités) sont approvisionnés à l'étranger.*

[4] *L'acronyme HPC désigne le calcul à haute performance ou intensif (en anglais* High Performing Computing*).*

400 millions d'euros. Sur le long terme, la Commission envisage d'investir 2,7 milliards d'euros.

Dans le cadre de cette structure, ***l'European processor initiative*** (EPI) a été lancée en décembre 2018 en vue d'amener sur le marché un processeur basse consommation et de s'assurer que les compétences essentielles pour la création d'un composant haut de gamme restent en Europe. L'initiative regroupe 26 partenaires publics et privés et sera dotée d'environ 120 à 130 millions d'euros de budget. Mais aucun financement n'est prévu pour le prototypage et la mise en fabrication du microprocesseur. La société Sipearl a donc été créée par les principaux cadres de l'EPI en vue de réunir ces financements. L'EPI a attiré l'attention de votre rapporteur sur les difficultés qu'elle rencontre à obtenir ces financements (estimés à 100 millions d'euros) et sur la nécessité que les bailleurs de fonds publics y participent. **Votre rapporteur déplore que les grands fabricants européens de microprocesseurs n'aient pas souhaité participer à cette initiative, de sorte que, même si la propriété intellectuelle restera européenne, la fabrication sera taïwanaise (société TSMC).**

Sources : Commission européenne, communiqué de presse, 28 septembre 2018 et contribution écrite de l'European processor initiative.

Dans les secteurs du logiciel, de la programmation, du conseil et des services informatiques, la France dispose également d'entreprises très performantes, qu'il s'agisse de l'édition de **logiciels** (Dassault systèmes), du **conseil** en activités informatiques (Capgemini), des activités de **cybersécurité** (Atos, Orange, Thales), ou du jeu vidéo (Ubisoft).

Même si, l'Europe et la France n'en sont pas leaders, il convient de souligner la réussite de certains acteurs de l' « **économie du net** », tels que vente-privée.com, Criteo, Blablacar, le groupe Webedia ou leboncoin.fr. Ces réussites doivent être valorisées et soutenues, notamment dans leur internationalisation.

Tous ces pôles d'excellence doivent être encouragés afin de ne pas reproduire les difficultés connues par le secteur des équipements de télécommunications européens durant les années 2000[1].

Enfin, dans un objectif de préservation de notre base économique, il convient de saluer l'adoption du décret du 29 novembre 2018 relatif aux investissements étrangers soumis à autorisation préalable[2] qui intègre au dispositif de **contrôle des investissements étrangers** en France de nombreux pans du numérique, tels que la cybersécurité et, dans certaines conditions, les semi-conducteurs ou encore l'intelligence artificielle. Comme on le verra ci-dessous, il convient cependant de ne pas systématiquement, et dans tous

[1] *Voir, sur ce sujet, le chapitre intitulé* Télécoms et TIC : la sortie de route *de l'ouvrage d'Elie Cohen et de Pierre-André Buigues, intitulé* Le décrochage industriel*, publié en 2014. Les auteurs débutent en soulignant qu'il aura fallu «* trente ans pour que l'Europe et la France passent d'un co-leadership mondial dans les équipements de télécommunications au duo des survivants *» (aujourd'hui Nokia et Ericsson).*

[2] *Décret n° 2018-1057 du 29 novembre 2018.*

les secteurs du numérique, assimiler financement par des fonds étrangers et perte de nos actifs stratégiques.

b) Cloud et intelligence artificielle : une stratégie basée sur la différenciation

Reproduire des technologies existantes dans un domaine où les américains bénéficient d'une position dominante ne semble à ce jour possible qu'en adoptant une stratégie de différenciation dans l'offre proposée, soit par une innovation, soit par une technologie de rupture, pour établir un avantage concurrentiel.

Cela revient notamment à **encourager les solutions conformes aux valeurs européennes, c'est-à-dire respectueuses de la vie privée** des utilisateurs, qui intègrent un principe de « *privacy by design* », autrement dit, un respect de la vie privée dès la conception.

Cette stratégie est retenue par plusieurs acteurs français tels que :

- le moteur de recherche Qwant, qui tente de se frayer une place sur ce marché à travers un modèle protecteur de la vie privée des utilisateurs, et qui bénéficie du soutien financier de la Caisse des dépôts et consignations (CDC) ;

- la place de marché Dawex, qui se différencie des courtiers en données (*data brokers*) en garantissant le respect des réglementations en vigueur selon le territoire de production et d'exploitation des données, et dont le projet de bourse mondiale des données est soutenu par la CDC ;

- Whaller, plateforme de réseaux sociaux et collaboratifs sécurisés.

À ce jour, le Gouvernement semble concentrer ses efforts sur deux secteurs en particulier : ceux du *cloud* et de l'intelligence artificielle.

(1) Le « *cloud* de confiance » : une initiative bienvenue mais qui tarde à se concrétiser.

Le marché mondial du *cloud* est dominé par quatre acteurs américains : Amazon Web Services (AWS), Microsoft, Google et IBM, à l'exception de la Chine où les entreprises chinoises (Baidu, Alibaba, Tencent, Huawei) dominent chacune des segments de marché du *cloud*. La France comprend plusieurs champions sur les couches infrastructure (*IaaS* ou *Infrastructure as a service*)[1] du *cloud* (OVH, Atos, Orange Business Services ou encore Outscale), qui s'appuient sur un marché national en forte expansion pour attaquer le marché international.

Selon la direction générale des entreprises, si la France est compétitive sur le marché du IaaS malgré la forte croissance des parts de marché des acteurs américains, le marché des services applicatifs (*SaaS* ou

[1] *Il s'agit de la mise à disposition d'une ressource matérielle virtualisée (services de calcul, de stockage et de réseau), gérée et administrée par un fournisseur.*

Software as a service)[1] est quant à lui dominé par les américains, reléguant les champions français Cegid et Oodrive aux cinquième et neuvième places mondiales.

Pour y remédier, la direction générale des entreprises pilote des travaux visant à faciliter **l'émergence d'un marché de confiance** du *cloud*, c'est-à-dire à proposer aux entreprises ainsi qu'à la puissance publique des offres diversifiées, performantes et sécurisées. Ces travaux ont **vocation à promouvoir les offres *cloud* européennes se différenciant par leur niveau de confiance**. Contrairement au projet de « cloud souverain » déjà évoqué, l'initiative vise, dans un marché qui a aujourd'hui atteint une bonne maturité, à s'appuyer sur des fournisseurs et des offres déjà exposés au marché, si nécessaire en ajustant ces offres pour répondre au besoin. Dans sa contribution écrite, le Cigref, en tant que représentant d'entreprises utilisatrices de solutions numériques, a souligné la pertinence d'une mutualisation de leurs besoins de *cloud* de confiance avec ceux de l'Etat, estimant que cela permettra de disposer d'une masse critique suffisante pour garantir la pertinence d'une offre européenne. Il estime d'ailleurs qu'une telle mutualisation pourrait être envisagée pour des besoins logiciels, comme les suites collaboratives.

Cette approche viendrait prolonger la labellisation des solutions *cloud* mises en œuvre depuis 2014.

La labellisation des solutions *cloud* par l'Anssi

En 2014, un rapport de notre collègue Catherine Morin-Desailly appelait à « *définir une classe de services labellisés « Secure cloud », faisant l'objet de cahiers des charges stricts et protecteurs, et à promouvoir un acteur européen compétent pour émettre des certificats de sécurité correspondants* »[2], solution qui avait également été proposée par Octave Klaba et Thierry Breton dans le cadre des 34 plans de « reconquête industrielle » lancés Arnaud Montebourg en 2013.

En 2014, l'Anssi a testé en conditions réelles les exigences fixées dans la première version du référentiel, alors baptisé *Secure Cloud*. En décembre 2016, le référentiel *SecNumCloud* a été officiellement lancé. Il a été modifié en 2018 afin de prendre en compte le RGPD. Il conjugue des exigences relatives au prestataire de service d'informatique en nuage, à son personnel ainsi qu'à la localisation des données client au sein de l'Union européenne – échelle territoriale de référence – et au droit applicable à ces données.

Par ailleurs, il convient de noter que la doctrine d'utilisation de l'informatique en nuage par l'Etat a été formalisée par une circulaire du Premier ministre en date du 8 novembre 2018. Elle distingue trois cercles selon la sensibilité des informations : le *cloud* interne à l'Etat, le *cloud* dédié – c'est-à-dire fourni par un prestataire mais personnalité, et le *cloud* externe, composé d'offres génériques.

[1] *Il s'agit de la mise à disposition de logiciels en ligne prêts à l'usage après un simple paramétrage.*
[2] *Rapport précité, intitulé « L'Europe au secours de l'Internet ».*

L'objectif du Gouvernement est désormais de « *disposer de premières propositions de mise en place d'un cloud sécurisé (…) d'ici la fin de l'année 2019* »[1], depuis rebaptisé « *cloud national stratégique* »… L'initiative du Gouvernement paraît toutefois **difficilement lisible** et tarde à se mettre en place.

Lors de son audition par votre commission, l'entreprise OVH a souligné la **nécessité de renforcer la transparence sur le marché du *cloud*** : tout appel d'offre – public ou privé – devrait comporter une clause sur la localisation des données stockées et sur le droit qui leur est applicable, ce qui n'est pas le cas aujourd'hui.

Par ailleurs, votre rapporteur souligne la **nécessité d'anticiper** le changement majeur à venir pour le stockage des données informatiques, à savoir le **passage de 80 % des données stockées dans le *cloud* à 80 % des données stockées en *edge computing***, ou « informatique en périphérie » en raison du développement exponentiel des objets connectés (tels que les montres, les enceintes et les assistants connectés ou encore les véhicules autonomes, etc...). L'État **doit dès maintenant se doter d'une stratégie claire** sur ce sujet.

Qu'est-ce que le *edge computing* ?

Ce terme désigne une architecture de technologie d'information distribuée qui se caractérise par une puissance de traitement décentralisée. Le *edge computing* permet de traiter des données de façon directe par le périphérique qui les produit (ou par un ordinateur local). Il n'est, dès lors, plus nécessaire de transmettre les données à un centre de données distant afin de pouvoir les traiter.

Par rapport au *cloud computing*, cela revêt trois principaux avantages provenant justement de l'absence de transmission du point d'émission des données au point de stockage et de traitement : une réduction du temps de latence du traitement de l'information, un meilleur niveau de sécurité et une réduction des coûts. Sur le premier point, Thierry Breton donnait, devant votre commission d'enquête, l'exemple du véhicule autonome et rappelait qu'Atos se positionne déjà sur ce segment de marché.

Source : www.journaldunet.fr

(2) L'intelligence artificielle : l'émergence trop lente d'une stratégie nationale.

La stratégie française en intelligence artificielle correspond également à une forme de différenciation fondée sur le volet éthique.

Elle met cependant beaucoup trop de temps à se mettre en place. Annoncée en mars 2018, son volet « recherche » n'a été défini qu'en novembre et son volet économique… en juillet 2019 ! Il est donc permis de

[1] *Bruno Le Maire, ministre de l'économie et des finances, discours d'inauguration du 8e datacenter d'Equinix en février 2019.*

penser, au regard de la rapidité de l'innovation en la matière, que ces **délais sont bien trop longs**.

De plus, comme le remarquaient les rapporteurs de la commission des finances et de la commission des affaires économiques sur le projet de loi de finances pour 2019, les **moyens financiers alloués apparaissent limités** au regard de ceux dégagés par les États-Unis et la Chine. Devant votre commission, le secrétaire d'État en charge du numérique rappelait ainsi que « *les grandes entreprises américaines investissent chaque année 30 à 40 milliards d'euros, tout comme les entreprises et l'État chinois, selon les chiffres de 2016. Le montant investi par l'Europe dans son ensemble ne s'élève lui qu'à 4 ou 5 milliards d'euros* ».

La stratégie nationale en intelligence artificielle

L'initiative France IA a permis, dès début 2017, de faire le point sur la situation de la France en matière d'intelligence artificielle (IA). Le Président de la République issu des élections de mai 2017 a néanmoins souhaité poursuivre la réflexion. C'est pourquoi il a confié en septembre 2017 à notre collègue député Cédric Villani une mission sur la stratégie française et européenne en intelligence artificielle. Le rapport intitulé *Donner du sens à l'intelligence artificielle : pour une stratégie nationale et européenne* a été publié le 29 mars 2018, à l'occasion de la conférence intitulée *AI for humanity*.

Le même jour, le Président de la République annonçait la stratégie nationale pour l'intelligence artificielle, avec pour ambition de mobiliser **1,5 milliard d'euros en cinq ans** et tenant quatre grands axes :

- conforter, en France et en Europe, l'écosystème de recherche en IA ;

- engager une politique d'ouverture des données ;

- adapter le cadre réglementaire et financier, national et européen ;

- définir les enjeux éthiques et politiques de l'IA.

Un coordinateur national rattaché à la direction interministérielle des systèmes d'information et de communication (Dinsic) est chargé de lancer et de superviser la mise en œuvre du plan d'action dans toutes ses composantes.

La stratégie nationale de recherche en intelligence artificielle a été présentée par le Gouvernement le 28 novembre 2018[1].

Elle sera financée par l'État à hauteur de 665 millions d'euros entre 2018 et 2022. Elle se déploie en six axes :

- déployer un programme national pour l'IA piloté par l'Inria, qui s'appuiera notamment sur le réseau des instituts interdisciplinaires d'intelligence artificielle (instituts 3IA) ;

- lancer un programme d'attractivité et de soutien aux talents (création de 40 chaires à partir de 2019 ; doublement du nombre de docteurs formés en intelligence artificielle) ;

[1] *Stratégie nationale de recherche en IA, dossier de presse, 28 novembre 2018.*

- dynamiser la recherche en IA à l'Agence nationale de la recherche (ANR), en fléchant 100 millions d'euros jusqu'en 2022 au sein des financements mobilisables par l'Agence ;

- renforcer les moyens de calcul (installation d'un nouveau supercalculateur sur le plateau de Saclay, accès au calcul facilité pour l'ensemble de la communauté de recherche) ;

- renforcer la recherche partenariale (65 millions d'euros seront investis par l'État d'ici 2022 pour porter le volume total des projets à au moins 130 millions d'euros) ;

- renforcer les coopérations bilatérales, européennes et internationales (renforcement de la collaboration franco-allemande, soutien à une stratégie ambitieuse de l'Europe en IA).

Le volet économique de la stratégie nationale de recherche en intelligence artificielle a été présenté par le Gouvernement le 3 juillet 2019[1].

Elle se décline en trois axes :

- faire émerger des champions de l'IA français, notamment dans les secteurs clefs tels que l'environnement, la santé et la sécurité, à travers des Challenges IA (5 millions d'euros) et les grands défis financés par le Fonds pour l'innovation et l'industrie (100 millions d'euros au total) – diagnostics médicaux, transparence et auditabilité des systèmes autonomes à base d'intelligence artificielle, automatisation de la cyber-sécurité ;

- stimuler la demande *via* le soutien de la diffusion de l'IA dans tous les secteurs et sur tout le territoire : 250 millions d'euros ont été mobilisés au travers du Programme d'Investissements d'Avenir (PIA) pour financer des projets structurants dédiés à l'IA ; la direction générale des entreprises, en concertation avec les acteurs institutionnels et économiques français, accompagne la démarche de normalisation en matière d'IA ;

- poser les bases d'une véritable économie de la donnée, *via* l'appel à projets destiné à cofinancer des initiatives de mutualisation de données et le *Health Data Hub* déjà évoqués.

Au niveau européen, la Commission européenne a publié le 25 avril 2018 une communication intitulée *L'intelligence artificielle pour l'Europe*. Le Sénat a approuvé cette communication et a appelé à la **création d'un « *projet important d'intérêt européen commun* » (Piiec)[2] pour l'intelligence artificielle**, sur le modèle du plan Nano 2022 en nanoélectronique[3]. Cette

[1] *L'intelligence artificielle au service des entreprises, Stratégie nationale pour l'intelligence artificielle : présentation du volet économique, dossier de presse, 3 juillet 2019.*

[2] *Ces projets importants d'intérêt européen commun (Piiec) permettent aux États membres de soutenir des projets transnationaux d'importance stratégique et donc de passer outre l'interdiction des aides d'Etat : le Traité sur le fonctionnement de l'Union européenne (TFUE) prévoit ainsi au point 3 de son article 107 que de tels projets peuvent faire l'objet d'aides financières de plusieurs États membres sous certaines conditions. Le rapport d'information sur la proposition de résolution européenne en rappelle les modalités de fonctionnement.*

[3] *Sénat, Résolution européenne sur les investissements dans l'intelligence artificielle en Europe, 8 mars 2019.*

recommandation est toujours d'actualité. Devant votre commission, le ministre de l'Économie et des Finances a confirmé travailler sur ce sujet avec son homologue allemand en vue de formuler des propositions dans les mois qui viennent. Votre rapporteur s'en réjouit et souligne la **nécessité d'aller vite sur ce sujet**.

La maîtrise de l'intelligence artificielle et son développement sont cruciaux pour l'ensemble des secteurs d'activité. C'est, par exemple, le cas du secteur automobile qui devra maîtriser cette technologie pour tirer profit de l'évolution du marché vers le véhicule autonome. En 2017, un rapport d'inspection sur le véhicule autonome[1] constatait que « *la France n'a pas encore atteint, dans plusieurs domaines, un niveau de préparation suffisant* ». C'est pourquoi une stratégie nationale dédiée au véhicule autonome a été publiée en mai 2018 sous l'égide d'Anne-Marie Idrac, Haute responsable pour la stratégie de développement du véhicule autonome.

c) Développer les technologies d'avenir : ordinateur quantique et blockchain

Une stratégie industrielle se doit également d'investir dans les secteurs d'avenir où, pour l'instant, aucun acteur n'est durablement établi.

Le Gouvernement a semble-t-il déjà identifié deux technologies clés : la *blockchain* et, à plus long terme, des technologies quantiques.

(1) La *blockchain,* un outil d'avenir pour défendre notre souveraineté ?

Qu'est-ce que la *blockchain* ?

La *blockchain* est un avatar de la technologie des registres distribués. Un registre distribué est une base de données qui enregistre l'ensemble des transactions, sans possibilité de masquer la moindre altération intervenue *a posteriori*. Le registre est tenu sur un réseau constitué de « nœuds », il est donc décentralisé. Cette décentralisation offre davantage de transparence et rend caduc le recours aux services intermédiaires. Le réseau est distribué dans le sens où chaque participant actif, chaque nœud dispose de sa propre copie de la base de données et peut la consulter, voire la modifier en résolvant un problème cryptographique. Il ajoute alors « un bloc » et cette modification est visible par l'ensemble des participants. Certaines *blockchains*, dites « privées », restreignent cette capacité de modification à un nombre limité de participants.

Voir également la note scientifique de l'Office parlementaire d'évaluation des choix scientifiques et technologiques intitulée Comprendre les blockchains. *Disponible à l'adresse suivante :* http://www.senat.fr/rap/r18-418/r18-4181.pdf

Le développement de la *blockchain* pourrait répondre à plusieurs des remises en cause de la souveraineté, qu'elle soit collective, individuelle ou étatique, identifiées par votre commission.

[1] *Conseil général de l'environnement et du développement durable (Cgedd) et Inspection générale de l'administration (IGA),* L'automatisation des véhicules*, février 2017.*

L'observatoire-forum de l'Union européenne sur les *blockchains*[1] travaille par exemple sur **l'identité numérique**, un prérequis essentiel pour achever le marché unique numérique. Un objectif de long terme du règlement eIDAS est de permettre aux personnes morales et physiques de pouvoir **s'identifier en ne révélant que les données nécessaires à l'authentification**[2]. Le règlement couvre aussi les prérequis pour la **fiabilisation des signatures électroniques et des documents électroniques**.

Ces trois éléments sont particulièrement propices au développement d'une *blockchain* et à la tenue d'un registre décentralisé. Le forum promeut en effet une approche dite ***self-sovereign identity*** (SSI) : les usagers peuvent gérer leurs identités numériques et les utiliser selon leurs besoins. L'État garde ses prérogatives souveraines puisqu'il peut fournir une « identité officielle » et des informations qui sont à la fois gérées par la personne concernée et qui apportent des garanties aux tiers. Si nous sommes encore loin de disposer des technologies sous-jacentes nécessaires, votre rapporteur considère que **la France et l'Europe doivent anticiper ces futurs développements**, tant pour ne pas laisser des entreprises privées les développer et les maîtriser, sans pouvoir les réguler, que pour ne pas, là-aussi, prendre du retard sur d'autres États.

De nouvelles propositions de services, basés sur la blockchain, apparaissent en effet constamment. C'est le cas par exemple de l'expérimentation conduite par les douanes françaises et Michelin, pour enregistrer des informations de suivi de manière infalsifiable. Les Douanes en ont tiré un premier bilan positif.

Le partenariat entre les douanes françaises et Michelin

Les douanes françaises, en partenariat avec Michelin, ont expérimenté un outil de suivi des écritures liées au régime particulier du perfectionnement actif[3]. Le prototype a été développé par Sopra Steria, dont le siège social se situe à Annecy. Il permet d'enregistrer, en continu et de manière infalsifiable, les événements issus des procédés logistiques et industriels (arrivée des marchandises et placement sous le régime, mouvements, transformations, sortie des marchandises, etc.). L'ensemble de ces données est partagé en temps réel avec les acteurs pertinents. Si le premier bilan est

[1] *Cet observatoire a été créé par la Commission européenne sur proposition du député européen Jakob Von Weizsäcker. Son but est de favoriser le développement de la technologie de la blockchain dans tous les secteurs de l'économie et de faire dialoguer autorités nationales et européennes, acteurs privés et chercheurs.*

[2] *Par exemple : une personne pourrait prouver qu'elle a l'âge de voter sans avoir besoin de transmettre sa date de naissance.*

[3] *Le perfectionnement actif est un régime particulier de droit communautaire destiné à favoriser l'activité économique des entreprises de l'Union européenne qui transforment des marchandises de pays tiers avant de les réexporter ou de les mettre à la consommation. Source : http://www.douane.gouv.fr/articles/a10864-regime-particulier-le-perfectionnement-actif*

positif, il conviendrait d'aller plus loin pour profiter pleinement de la valeur ajoutée d'un tel outil, par exemple en le connectant au système d'information d'un opérateur pour obtenir une plus grande traçabilité des marchandises et des transactions.

Source : douanes.gouv.fr

La *blockchain* ouvre également des perspectives en termes de financement de l'innovation, une difficulté sur laquelle achoppent nombre de start-up françaises ou européennes (cf. *infra*). Le financement par le biais de levées de fonds en jeton permettrait de contourner à la fois les contraintes en matière d'investissement et les réticences de certains établissements bancaires. C'est pour cette raison que **la loi Pacte a décidé, de manière inédite au niveau mondial, d'encadrer les levées de fonds en jetons** (ICO pour initial coin offering) : l'AMF pourra octroyer un visa optionnel aux entreprises souhaitant réaliser une telle opération. Les premiers visas devraient être attribués au mois de septembre 2019 et apporteront une **garantie aux investisseurs**, qui pourraient être **plus enclins à financer des projets innovants dans le domaine du numérique**[1].

Qu'est-ce qu'une levée de fonds en actifs numériques ?

Les *initial coin offerings* (ICO) ou levées de fonds en actifs numériques, ou encore levées de fonds en jeton, sont définies par l'Autorité des marchés financiers comme *« des opérations de levées de fonds effectuées à travers une technologie de registre distribué qui donnent lieu à une émission de jetons (« tokens »), ceux-ci pouvant ensuite, selon les cas, être utilisés pour obtenir des produits ou services, échangés sur une plateforme (marché secondaire) et/ou rapporter un profit ».*

Concrètement, un entrepreneur développe une *blockchain* dédiée à un nouveau projet (ex. jeu vidéo en temps réel, services de *clouding*…) pour laquelle il émet des jetons. Il vend ensuite ces jetons auprès d'investisseurs, qui paient en cryptoactifs (ex. bitcoin, ether) ou en monnaie légale. La transaction est le plus souvent opérée sur la *blockchain Ethereum*, qui sécurise les échanges. Les jetons confèrent des droits aux investisseurs, ces droits pouvant être de différente nature : dividendes futurs, droit de vote, droit à un service… Une fois que le porteur du projet a collecté les cryptoactifs, il peut les convertir en monnaie légale par le biais d'une plateforme de change et financer son activité.

Source : rapport fait au nom de la commission spéciale sur le projet de loi relatif à la croissance et la transformation des entreprise (lien : http://www.senat.fr/rap/l18-254-1/l18-254-11.pdf)

Pour attirer ces investissements, il faut un **écosystème favorable**. **Le champion européen des levées de fonds sur la *blockchain* était la petite ville de Zoug en Suisse**, dont les entreprises ont levé davantage de fonds

[1] *C'est d'autant plus important que d'après une étude de Satis, reprise dans un rapport de la Banque centrale européenne sur les conséquentes des cryptoactifs pour la stabilité financière et la politique monétaire, 80 % des projets appelant à des fonds* via *une ICO sont frauduleux.*

par ce biais-là que toute l'Europe continentale[1]. Surnommée *« Crypto Valley »*, la ville de Zoug a su bâtir un écosystème favorable à l'installation de ces entreprises : cadre de régulation fixé dès 2015 par l'autorité suisse des marchés financiers, portail unique pour les nouveaux arrivants, fiscalité avantageuse pour les jeunes entreprises, développement des usages des cryptoactifs, y compris pour les achats quotidiens…[2]

Enfin, comme l'a rappelé devant votre rapporteur la directrice de la division « Fintech, innovation et compétitivité » de l'AMF, Mme Domitille Dessertine, **la *blockchain* offre des perspectives à l'ensemble des secteurs de l'économie** : établissement de *smart contract*, gouvernance plus transparente et décentralisée des entreprises, diminution des coûts de transaction, appui au transfert d'un certain nombre de biens et de services (œuvres d'art, droits d'auteur, espace de stockage informatique, données personnelles etc.). C'est pour cela que la *blockchain* est un outil devenu si important aujourd'hui dans le monde numérique.

La stratégie du Gouvernement : la blockchain au secours de l'industrie

Le ministère de l'économie et des finances vient ainsi de lancer, sous l'égide de la Direction générale des entreprises, un groupe de travail, réunissant des acteurs du public (administratifs, Bpifrance, Caisse des dépôts), du privé (représentants de filières et d'associations professionnelles, comme La Chaintech ou le Cercle du Coin), des universitaires (CEA, Inria, Dauphine) et des régulateurs (AMF, ACPR) afin d'encourager l'industrie à développer des projets axés sur la *blockchain*. Les secteurs prioritaires seraient la construction (ex. émission de certificat de prestations), l'agro-alimentaire (ex. traçabilité des denrées) ou encore l'énergie (ex. certification de production d'énergie solaire).

Source : La Tribune, Bercy lance sa task force Blockchain pour pousser l'adoption dans l'industrie*, 26 juillet 2019.*

Le ministre de l'économie et des finances explique qu'**instaurer un environnement favorable aux entrepreneurs de la *blockchain* est un moyen de lutter contre *« la situation monopolistique de certains géants du numérique »*.** Votre rapporteur partage cette analyse et souhaiterait maintenant que les actes du Gouvernement soient à la hauteur de cet objectif ambitieux[3].

---

[1] Comment la Suisse veut devenir la « crypto-nation », *article publié dans les Échos par Raphaël Bloch le 21 février 2019. Lien vers l'article* : https://www.lesechos.fr/finance-marches/marches-financiers/bienvenue-dans-la-crypto-valley-992953

[2] *La France n'a elle-même que récemment adapté le dispositif fiscal relatif aux cryptoactifs. La loi de finances pour 2019 impose une déclaration annuelle, et non plus mensuelle, des plus-values. Elle abaisse le taux d'imposition de 36,2 % à 30 % et exonère les transactions de crypto à crypto pour les particuliers.*

[3] *L'Allemagne a publié le 18 septembre 2019 une stratégie détaillée pour tirer au mieux parti de la technologie de la* blockchain *et pour rester un leader mondial dans ce domaine.*

(2) Entrer dans la course des technologies quantiques.

Selon la direction générale des entreprises, les technologies quantiques sont susceptibles, par leur usage, de révolutionner des pans entiers de l'industrie et de la défense, de la médecine moléculaire au stockage de CO2 en passant par la cryptanalyse, la prospection et la navigation sans GPS, conférant ainsi aux acteurs qui les maîtrisent un avantage stratégique.

Parmi celles-ci, l'informatique quantique permettra théoriquement de résoudre des problèmes tellement complexes que même les supercalculateurs les plus performants n'auraient jamais pu les traiter[1].

Comme le rappelait Thierry Breton devant votre commission, le groupe qu'il préside se positionne sur ce secteur, à travers la commercialisation d'un premier simulateur quantique.

L'Union européenne a annoncé investir un milliard d'euros sur dix ans dans ce domaine. Il conviendrait **que la France se dote d'une stratégie dédiée au développement de ces technologies**. Sur un champ encore peu mature comme le quantique et ses applications diverses, nous avons une fenêtre d'opportunité. Une telle stratégie pourrait s'avérer d'autant plus urgente que Google a diffusé, le 20 septembre dernier, semble-t-il par erreur, une étude dans laquelle ses chercheurs affirment avoir construit un processeur quantique capable de mener un certain type d'opération en trois minutes et vingt secondes, là où il faudrait plus de 10 000 ans au plus avancé des supercalculateurs actuels[2].

Les ministères de l'Economie, des Armées et de la Recherche ont missionné, en avril dernier, notre collègue députée Paula Forteza, Jean-Paul Herteman (ancien dirigeant de Safran) et Iordanis Kerenidis (directeur de recherche au CNRS) pour mener des réflexions sur une stratégie nationale permettant à la France de capitaliser sur l'excellence de sa recherche afin de devenir un champion industriel des technologies quantiques.

---

[1] *Pour une vulgarisation de l'informatique quantique, voir Olivier Ezratty,* Comprendre l'informatique quantique*, novembre 2018.*

[2] *Il convient cependant de noter que de nombreux points amènent à relativiser la portée de cette annonce. Par exemple, Olivier Ezratty, auteur d'un ouvrage disponible en ligne sur la technologie quantique, considère que ce type de communication permettra surtout de relancer les investissements dans le domaine (20minutes.fr, Google: La firme atteint la « suprématie quantique » mais ce n'est qu'un début, 25 septembre 2019).*

Le programme européen Quantum Technology

Le programme européen Quantum Technology est l'un des trois « fleurons » (ou *Flagship*) lancés par l'Union européenne dans le cadre de sa politique de soutien à la recherche « Horizon 2020 » (les deux autres portent sur le graphène et les neurosciences). Le chantier a débuté en 2016 avec la parution d'un manifeste (« *Quantum Manifesto* ») signé par plus de 3 000 acteurs du domaine, dont 156 entreprises européennes et 20 institutions de recherche.

L'objectif est de « *consolider et étendre les forces scientifiques européennes dans ce domaine de recherche et [de] démarrer une industrie compétitive dans ce secteur* », c'est-à-dire d'accélérer le passage depuis les laboratoires vers différents marchés.

Quatre principaux secteurs ont été identifiés : calcul (ordinateur quantique), communication (leur sécurité notamment), simulation et métrologie.

En octobre 2018, 20 premiers projets ont été sélectionnés, qui seront financés sur trois ans à hauteur de 132 millions d'euros.

Source : Le Monde, Technologies quantiques : l'Europe accélère*, 29 octobre 2018.*

3. Mobiliser tous les leviers de la politique industrielle

Tous les outils de la politique industrielle doivent être mobilisés tant pour soutenir ces secteurs (politique industrielle dite « verticale ») que pour créer des écosystèmes favorables pour les acteurs privés (politique industrielle dite « horizontale » qui sera traitée au E de la présente partie). Le soutien public de la France et de l'Europe aux entreprises est essentiel dans un contexte où nos partenaires commerciaux, au premier rang desquels les États-Unis et la Chine, ne jouent pas ou plus le jeu de la concurrence libre et non faussée.

Les outils d'une politique industrielle verticale sont nombreux, des subventions (en particulier en amont du développement d'un produit) aux marchés publics en passant par les prises de participation au capital… Votre rapporteur souhaite insister sur trois points en particulier, qui avaient déjà été mis en exergue par notre collègue Catherine Morin-Desailly dans ses rapports sur l'Europe au secours de l'Internet et sur l'Europe, colonie du monde numérique.

1° Il convient de **modifier la philosophie de la politique de concurrence européenne**, afin d'éviter qu'elle ne porte préjudice à des initiatives industrielles françaises ou européennes de niveau mondial[1]. Plusieurs personnes auditionnées ont en effet souligné l'attention disproportionnée apportée, par les autorités européennes, à la concurrence et au bénéfice à court terme du consommateur, **au détriment de la constitution**

[1] *Devant votre commission d'enquête, le ministre de l'économie et des finances a ainsi regretté la décision par laquelle la Commission européenne s'est opposée à la fusion d'Alstom et de Siemens, privant l'Europe de la possibilité de se doter du leader mondial de la signalisation ferroviaire.*

de champions européens du numérique. Ainsi notamment de Thierry Breton : « *au nom de principes concurrentiels qui n'ont plus de sens aujourd'hui et qui relèvent d'une politique de marché tournée vers le consommateur, on a interdit la création de champions industriels européens ! L'Europe doit, à l'inverse, favoriser les rapprochements des grands groupes européens afin de mobiliser des investissements dans des secteurs particulièrement voraces en capitaux et garantir l'émergence d'une politique industrielle sur laquelle doit désormais s'aligner la politique de la concurrence* ».

Devant votre commission, le ministre de l'Economie et des Finances a notamment plaidé pour que le Conseil européen ou le Conseil de l'Union européenne puisse s'opposer à une décision de la Commission européenne dans ses fonctions d'autorité européenne de la concurrence, comme le Gouvernement peut le faire au niveau national en France et en Allemagne. Votre rapporteur rejoint cette préconisation. C'est dans cette même logique que le ministre estime qu'il convient de permettre un contrôle *ex post* des concentrations plutôt qu'un contrôle *ex ante*, afin de n'empêcher une concentration que si les effets anti-concurrentiels sont avérés.

En somme, tout en étant plus strict d'un côté pour prendre en compte les acquisitions « prédatrices », il convient **d'amender la politique des concentrations pour permettre la constitution de champions nationaux et européens**, à l'heure où les marchés sont mondiaux.

2° Selon un récent rapport d'inspection précité[1], il convient d'améliorer le **régime des aides d'État, singularité européenne** qui, en l'état actuel, complique et rallonge la procédure d'octroi des soutiens publics par rapport aux pratiques constatées dans les pays tiers. Il convient donc, comme le propose le rapport, de raccourcir les délais d'examen de ces aides, de mieux prendre en compte les aides d'État versées par des pays tiers et de développer les projets importants d'intérêt européen commun (Piiec).

Améliorer le régime des aides d'État afin de rapprocher l'Europe des standards internationaux en matière de soutien public à la recherche et à l'activité économique.

3° Le **levier de l'achat public** est essentiel pour promouvoir les entreprises françaises et européennes. Comme l'ont souligné devant votre commission les représentants de la licorne française du *cloud* OVH, « *choisir un acteur américain ou chinois est lourd de conséquences tant au niveau de la protection des données que pour l'ensemble de l'écosystème de la filière numérique* », rappelant que, « *si la préférence nationale est une notion absente de notre droit, c'est une réalité concrète dans les autres États* ».

[1] *Rapport d'inspection précité, intitulé* « La politique de la concurrence et les intérêts stratégiques de l'UE ».

Le **levier de l'achat public devrait être systématiquement utilisé pour encourager les entreprises françaises et européennes**, comme cela se fait partout dans le monde.

Les administrations publiques pourraient également engager une réflexion sur le recours au logiciel libre[1] en vue de s'assurer de maîtriser leurs données et de mieux conduire, potentiellement à moindre coût, les politiques publiques dont elles ont la charge.

En effet, l'État, ses administrations et ses services publics, produisent, recueillent, gèrent et diffusent des données numériques en quantité toujours croissante. Elles concernent les individus, les équipements, les territoires, les résultats des recherches, les décisions administratives ou judiciaires, les éléments de procédure, etc. Dans sa gestion courante de ces informations, s'agissant des données personnelles, il a l'obligation d'en garantir la confidentialité. Ainsi, quand les administrations utilisent des logiciels achetés à des entreprises privées, elles doivent s'assurer de la sécurité de l'accès à ces informations et de l'impossibilité pour le fournisseur de les recueillir et de les exploiter.

Lors des auditions menées par notre commission d'enquête, il ne nous est pas apparu formellement que l'État, dans ses politiques d'achats de matériels et de logiciels informatiques, avait une doctrine générale pour intégrer dans ses appels d'offre cette dimension essentielle de la sécurité des données. Pour s'assurer du respect d'un cahier des charges qui intégrerait cette exigence, il lui faudrait **se doter de moyens d'analyse des solutions proposées dont la plupart des ministères semblent dépourvus**. Plusieurs de nos interlocuteurs ont souligné que la **lisibilité totale des codes sources** des programmes informatiques pouvait être une des conditions essentielles de la souveraineté de l'État sur ses moyens numériques.

Deux conceptions opposées du recours au logiciel libre par les administrations

Les auditions de votre commission ont permis de souligner les conceptions divergentes quant à la question de savoir si les administrations devraient recourir de préférence au logiciel libre, qui permettent la lisibilité des codes sources.

Le Dinsic de l'État a ainsi fait part de sa vision particulièrement nuancée, résumée par la phrase suivante : « *Chaque fois que l'usage est bon, le logiciel libre a sa place*. » Cette conception repose sur le constat de l'inadaptation aux besoins de certaines solutions

[1] *Selon les propos tenus par le représentant de l'association April lors de son audition par votre commission le 8 juillet dernier, « Est qualifié de « logiciel libre » le logiciel qui permet d'assurer quatre libertés fondamentales : la liberté d'utilisation sans restriction d'usage, le droit d'étudier ce logiciel et de le modifier pour qu'il réponde à nos besoins - y compris en en corrigeant les erreurs -, le droit de redistribuer le logiciel et le droit d'en partager les versions modifiées. (…) L'oeuvre fondatrice du logiciel libre, Code is Law, a été écrite par le professeur Lawrence Lessig en 1999 ».*

libres déjà utilisées par l'État, qui a pu conduire les agents à recourir à des solutions propriétaires en ligne, et donc peu sécurisées. Par ailleurs, il a considéré que le coût complet (en prenant en compte les coûts de maintenance) des logiciels libres « *n'est pas si éloigné de celui des logiciels propriétaires* ». De même, M. Bruno Sportisse, président-directeur général de l'Inria considère-t-il que « sur *ce sujet, il ne faut pas avoir de dogme dans un sens comme dans l'autre.* » Enfin, la ministre des Armées a également souligné les enjeux du recours au logiciel libre pour son ministère : « *nous devons sans cesse ménager l'interopérabilité de nos forces. Nos alliés fonctionnent à partir de codes sources qui proviennent de la même entreprise, ce qui constitue une difficulté et ralentit le développement du recours aux logiciels libres.* »

A l'inverse, les associations La Quadrature du Net et April[1] ont plaidé vigoureusement en faveur du logiciel libre, tant pour les administrations que pour les individus, notamment parce que l'utilisateur, qui a accès au code source, peut en comprendre le fonctionnement et le modifier, ce qui est de nature à préserver sa liberté et à nourrir sa confiance dans la solution numérique. L'association April lutte ainsi pour éviter ou mettre fin aux partenariats conclus par les administrations de l'État avec les géants américains du numérique, comme le ministère de l'Éducation nationale, le ministère de la Justice ou celui de la Défense. Elle plaide également pour que l'État encourage le logiciel libre, par exemple au moyen d'appels d'offres, ou en soutenant les contributions des agents publics.

Le Conseil national du numérique avait également pris position en faveur du logiciel libre[2] en recommandant de leur donner la priorité dans la commande publique, pour trois raisons : le logiciel libre permet aux administrations de mieux adapter leurs services publics en développant des solutions qui leurs sont propres tout en étant interopérables, et de mieux les maîtriser, en permettant un audit et la correction en continu des failles de sécurité ; enfin, le logiciel libre serait globalement moins cher.

Pour répondre à cette exigence, mais aussi afin de réaliser, autant que possible, des **économies** d'acquisition, de gestion, de maintenance et de formation, plusieurs administrations ont fait le choix de **développer leurs propres solutions informatiques, à partir de logiciels dont les codes sources sont publics**. C'est, par exemple, le cas de la Gendarmerie qui, depuis 2009, a équipé les 80 000 postes informatiques de ses services de solutions informatiques libres qui lui ont permis de regagner son indépendance et sa souveraineté vis-à-vis des éditeurs privés. Il serait très utile de réaliser rapidement le bilan de cette expérience unique et d'évaluer les possibilités de son extension à d'autres ministères.

À tout le moins, il est **urgent d'engager rapidement une réflexion au niveau interministériel sur ce sujet**. L'idée, présentée devant notre commission, selon laquelle le choix d'acquisition de logiciels par les ministères serait, *in fine*, dicté par le confort d'utilisation des agents n'est pas recevable.

[1] *Association pour la promotion et la recherche en informatique libre.*

[2] *Conseil national du numérique, Donner priorité aux logiciels libres dans la commande publique, 2016*

4. Renforcer la place des acteurs français et européens dans les organismes de normalisation et de gouvernance d'internet.

Les équipements actifs et les protocoles utilisés pour la communication des données ou leur chiffrement répondent à des **normes techniques négociées** au sein d'instances internationales, comme l'Internet engineering task force (IETF) ou le World Wide Web consortium (W3C)[1]. Le nombre important des organismes de normalisation du numérique (quelques centaines dans le monde) et leur diversité thématique font que l'influence française dans ces *fora* ou *consortia* est assez variable.

Le Sénat a plusieurs fois souligné qu'il était important que les acteurs européens renforcent leur présence au sein des organismes internationaux de normalisation de l'internet. Cette préoccupation se retrouve, par exemple, dans la résolution du Sénat sur la régulation des objets connectés et le développement de l'internet des objets en Europe[2]. Ce constat rejoint celui de notre collègue Elisabeth Lamure, dans son rapport sur la normalisation[3], selon lequel les acteurs nationaux de la normalisation « *se livrent à une véritable course pour être à même de proposer avant d'autres l'ouverture de travaux dans les organismes européens ou internationaux de normalisation dans certains domaines* ». Au-delà du web, la question est d'autant plus cruciale aujourd'hui pour l'intelligence artificielle[4].

La France a la chance d'héberger sur son territoire l'Institut européen de normalisation des télécommunications (ETSI), acteur de premier plan mondial dans la normalisation des télécommunications et du numérique, reconnu par la Commission européenne comme l'un des trois organismes européens de normalisation. Cet acteur, majoritaire au sein du 3GPP, le consortium international établissant notamment les normes pour la 5G, et disposant d'une forte influence pour les normes de communications de machine à machine et de l'Internet des objets à travers son projet OneM2M, accueille plus de 100 acteurs français sur environ 900 membres au total.

---

[1] *Créé par Tim Berners-Lee, l'un des inventeurs du Web, en 1994, le W3C compte plus de 400 entreprises membres.*

[2] *Résolution européenne n° 106 (2017-2018), initiée par notre collègue Catherine Morin-Desailly et adoptée le 22 mai 2018, qui* « demande que les acteurs européens renforcent leur présence dans les enceintes internationales d'élaboration des normes et des standards de sécurité en matière numérique, et particulièrement l'internet des objets ».

[3] *Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général, Rapport d'information n° 627 (2016-2017) de Mme Élisabeth Lamure, fait au nom de la commission des affaires économiques, 12 juillet 2017.*

[4] *Voir notamment l'article de presse suivant : korii.slate.fr,* La course pour la domination mondiale de l'intelligence artificielle est lancée, *juillet 2019.*

La politique de la France en matière de normalisation dans le domaine du numérique

Selon la réponse écrite adressée à votre rapporteur par la direction générale des entreprises, dans le cadre de la stratégie pour un marché unique numérique, la France :

- promeut une ambition forte de l'Union européenne en matière de normalisation, la définition de priorités stratégiques européennes en matière de normalisation (5G, cybersécurité, Internet des objets…) ;

- soutient la mobilisation des acteurs français et européens dans le processus de normalisation notamment à travers différents appels à projets du programme-cadre de recherche et d'innovation de l'UE Horizon 2020 (PME, universitaires et chercheurs peuvent désormais bénéficier de financements européens pour participer aux travaux de normalisation) ;

- défend l'ancrage européen de l'ETSI afin qu'il puisse être un lieu de développement de spécification techniques en relais à des initiatives politiques de l'UE et en application de ses réglementations dans le domaine des radiocommunications ou de la sécurité, tout en veillant à son ouverture vers le monde, les normes dans le numérique ayant vocation à être mondiales ;

- a fait des propositions à la Commission européenne allant dans le sens d'une préservation de l'intérêt européen au sein de la gouvernance de la politique européenne de normalisation des technologies de l'information et de la communication face à l'entrisme de grandes entreprises non européennes.

Le renforcement de l'influence française passe également par la valorisation et la promotion des positions de l'UE dans les discussions internationales liées à la normalisation des technologies de l'information et de la communication ainsi que par la mise en place d'une stratégie de promotion des normes européennes à l'international.

Il semble que l'État n'ait pourtant pas encore pleinement pris la mesure de l'enjeu : estimant que l'intérêt de l'organisation était dorénavant limité, Orange a quitté le W3C[1], sans que l'État ne s'en émeuve ! Votre rapporteur accueille donc favorablement le souhait formulé par le ministre de l'Economie et des Finances devant votre commission de « *rénover la stratégie française de normalisation* ».

Il convient de **renforcer l'effort en faveur de la mobilisation des acteurs français et européens du numérique dans les organismes de normalisation**.

Par ailleurs, il convient de **poursuivre l'effort de multilatéralisation de l'Icann** afin de tendre vers une gouvernance mondiale de l'Internet.

La réforme de l'Icann en 2016 a permis des progrès indéniables tels qu'une meilleure redevabilité des instances décisionnelles auprès de la

[1] *L'Express, Orange quitte le W3C, le consortium qui fixe les règles du Web mondial, 10 avril 2019.*

communauté, des mécanismes de recours plus aboutis contre les décisions du conseil d'administration et, surtout, la fin du lien contractuel direct qui existait entre l'administration américaine et l'organisation.

La situation actuelle ne semble cependant pas favorable à la poursuite de l'amélioration de la gouvernance de l'organisme : la plupart des acteurs non-gouvernementaux (secteur privé, communauté technique) ainsi qu'un certain nombre de gouvernements, dont les États-Unis mais aussi une bonne partie des pays européens, privilégient désormais le *statu quo*.

Les recommandations du rapport de notre collègue Catherine Morin-Desailly intitulé « *L'Europe au secours de l'Internet* » et de la résolution européenne du Sénat « *sur la nécessaire réforme de la gouvernance de l'internet* »[1] à propos de la réforme de l'Icann sont donc toujours d'actualité. Votre rapporteur invite en conséquence le Gouvernement à les étudier à nouveau avec attention.

Selon la contribution transmise à votre rapporteur par l'Association française pour le nommage internet en coopération (Afnic), la priorité n'est cependant plus aujourd'hui à la relance d'une réforme de l'Icann, mais plutôt **l'identification des sujets prioritaires** sur lesquels l'Icann a un pouvoir, et sur lesquels les acteurs français pourraient l'amener à évoluer. Elle estime également nécessaire de maintenir un lien constant entre les autorités et les acteurs majeurs français, d'une part, et les Français membres du personnel de l'Icann, d'autre part. Enfin, elle propose la mise en place d'une bourse pour les volontaires français (associatifs, académiques, retraités…) s'impliquant dans des groupes de travail ayant un impact potentiel sur les acteurs français, évaluant le besoin financier à quelques dizaines de milliers d'euros par an dans un premier temps.

E. POUR COMBLER NOTRE RETARD, LA NÉCESSITÉ DE MOBILISER LE CAPITAL FINANCIER ET HUMAIN

Il ne peut y avoir de combat en faveur de la souveraineté numérique française sans mobiliser les armes nécessaires. Votre rapporteur insiste sur la **nécessité d'adopter une approche plus offensive**, y compris pour **davantage mobiliser les capitaux financiers et humains**. Sans ces capitaux, la France ne pourra disposer des acteurs lui permettant d'être souveraine.

La commission a pu constater que des progrès avaient été réalisés dans ce domaine et que certaines annonces du Gouvernement allaient dans le bon sens, à l'image du lancement du Fonds pour l'innovation et l'industrie le 15 janvier 2018, dont un tiers des revenus sera consacré au financement de startups *deep tech*, portant des technologies de pointe, plus risquées, avec des retours sur investissement plus longs. Ce fonds devrait être doté de

[1] *Sénat, résolution européenne n° 27 (2014-2015) sur la nécessaire réforme de la gouvernance de l'internet, 25 novembre 2014.*

10 milliards d'euros à partir de cessions d'actifs et d'apports en titres et devrait générer 250 millions d'euros par an. Ces *start-up* de la *deep tech* bénéficient en outre des financements du fonds *French Tech Seed*[1], financé par le programme d'investissement d'avenir 3 (PIA 3)[2].

Toutefois, de nombreux progrès restent encore à accomplir.

Ainsi, pour rester au premier rang de l'innovation numérique, il convient de favoriser et de financer l'émergence de pépites technologiques et de licornes[3] nationales.

1. Améliorer les dispositifs du capital-risque et du crédit d'impôt recherche

Sur le financement des pépites technologiques, votre commission a souhaité approfondir **deux constats fréquemment avancés pour expliquer le retard français** : (1) les *start-up* françaises se heurteraient à **un plafond de verre** qui les empêcherait de croître et qui les conduirait à exporter leurs idées, talents et fonds, notamment aux États-Unis ; (2) les *start-up* et entreprises innovantes françaises seraient **fréquemment rachetées par des fonds américains ou asiatiques**, ce qui nuirait à la souveraineté française.

Si votre rapporteur ne nie pas ces constats, les auditions menées lui permettent de les nuancer. Un optimisme raisonnable est possible.

a) Un manque de profondeur du capital-risque en France ?

Ce plafond de verre trouverait son origine dans un marché du **capital-risque** moins profond en France que dans d'autres pays.

Le financement par le capital-risque

Ce modèle de financement a été conçu et diffusé aux États-Unis par le Français Georges Doriot au milieu du XXe siècle. Il s'adapte parfaitement aux exigences de l'économie du numérique où le rythme de l'innovation industrielle impose des investissements considérables sur une période de temps courte. Dans ce modèle, les entreprises connaissent une croissance spectaculaire et peuvent dépasser en quelques années la capitalisation boursière d'entreprises parfois établies depuis plusieurs décennies. Grâce au capital-risque, des *start-up* peuvent compenser leur

[1] *Ce fonds, doté de 400 millions d'euros, est opéré par Bpifrance et a vocation à soutenir les startups technologiques en phase de post-maturation.*

[2] *D'après les réponses du ministère de l'économie et des finances au questionnaire transmis par votre commission, les actions en faveur des entreprises de la* deep tech *devraient se renforcer. En effet, l'intervention de Bpifrance sur certains segments très compétitifs, comme le numérique, vient de plus en plus évincer celle des acteurs privés, d'où une réflexion sur une évolution de la doctrine d'intervention de l'organisme.*

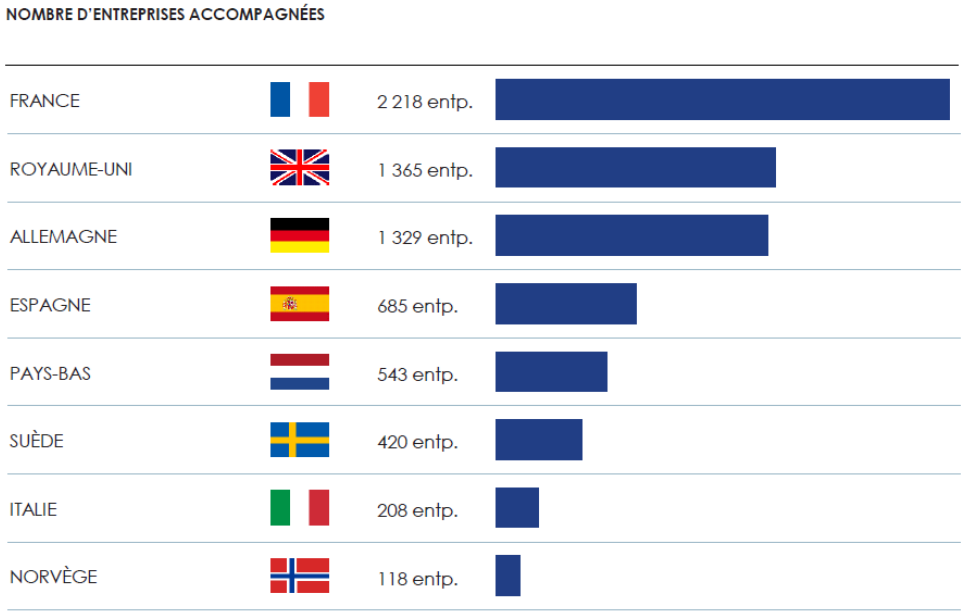
[3] *Ce terme est utilisé pour désigner les start-up non cotées et valorisées à plus d'un milliard de dollars.*

petite taille par la mobilisation rapide et massive de ressources nécessaires à l'innovation de rupture.

Source : Mission d'expertise sur la fiscalité de l'économie numérique. Lien : https://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf

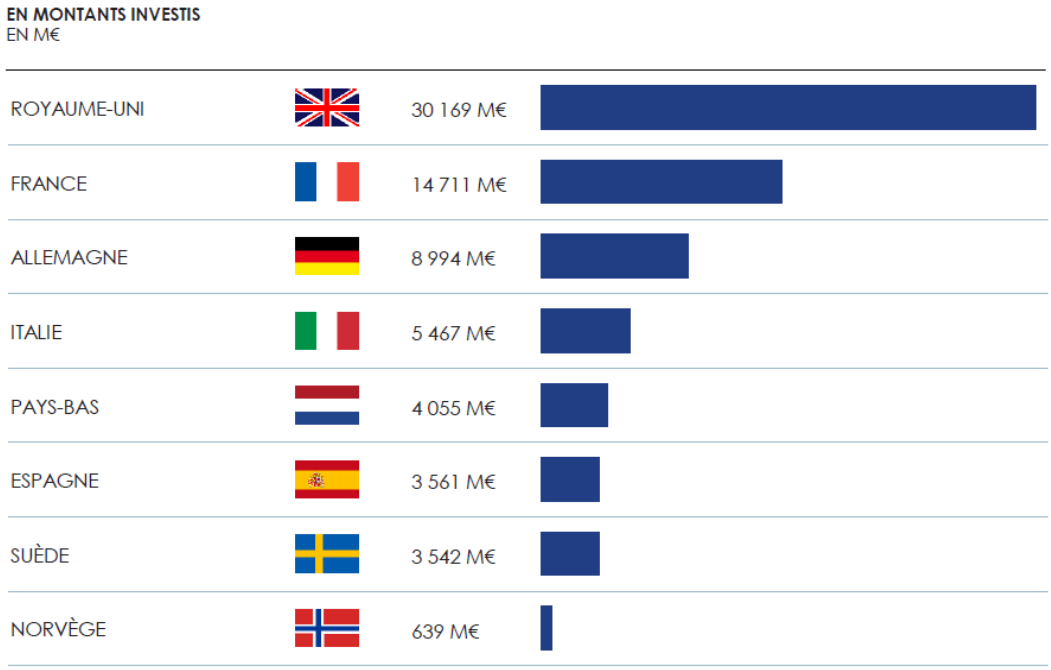
Que nous disent les chiffres ? En 2018, d'après les chiffres communiqués par France Invest à votre commission, les acteurs français du capital-investissement ont levé 18,7 milliards d'euros (+13,3 % par rapport à 2017) et accompagné 2 218 entreprises (+3,6 % par rapport à 2017).

En termes d'entreprises accompagnées, la France est le premier pays européen



Source : France Invest

Toutefois, en termes de montants investis, la France se situe encore loin du Royaume-Uni



Source : France Invest

Ces données montrent que les *start-up* et entreprises britanniques, si elles sont moins nombreuses à bénéficier des fonds investis par le biais du capital risque, obtiennent toutefois davantage de ressources lorsqu'elles sont choisies par un fonds de capital-investissement. Le constat est le même pour le capital-innovation : la France occupe la **première place pour le nombre d'entreprises accompagnées** (877 en France, contre 779 en Allemagne et 702 au Royaume-Uni) mais la **seconde pour les montants investis** (1,62 milliard d'euros en France, contre 2,04 au Royaume-Uni et 1,31 en Allemagne).

Parmi ce capital-innovation, **l'informatique et le numérique occupe la première place des secteurs bénéficiaires en France**, que ce soit en termes de montant (836 millions d'euros, soit 51,6 %) ou d'entreprises (374, soit 42,6 %). En outre, selon une récente étude d'eFront[1], la proportion de fonds dépassant la barre des 8 % de rendement, gage de plus-value pour les dirigeants, est sensiblement la même en Europe (29 %) qu'aux États-Unis (28 %), premier marché mondial pour le capital-risque. La situation est légèrement moins favorable si on ne tient compte que des **levées de fonds réalisées au profit des *start-up*** : la France se situe là en **troisième position**

[1] *Étude commandée par les Échos et portant sur 288 sociétés d'investissement du capital-risque dans l'Union européenne et sur 182 sociétés américaines. Lien de l'article : https://www.lesechos.fr/finance-marches/ma/capital-risque-seul-un-tiers-des-fonds-performent-vraiment-en-europe-1038712*

(15 % du montant total levé), derrière le Royaume-Uni (31 %) et l'Allemagne (19 %)[1].

Ces chiffres montrent que **la situation française n'est pas en décrochage par rapport à celle de ses principaux partenaires européens, exception faite du Royaume-Uni.** Cependant, à l'échelle internationale, la situation française et européenne est moins enviable. En 2018, les levées de fonds des *start-up* européennes n'ont représenté que 10 % de ce financement mondial, contre 53 % pour les États-Unis et 27 % pour la Chine[2]. Philippe Tibi ajoute que, parmi les **392 licornes** recensées au mois de juillet 2019, 182 sont américaines, 94 chinoises et 45 européennes (dont seulement **cinq françaises**).

De l'avis partagé de Bpifrance et de France Invest, auditionnés conjointement par votre commission, il ne faut pas nier les progrès accomplis. La France se situant ainsi aux **toutes premières places mondiales pour la phase d'amorçage**, elle doit maintenant **muscler ses dispositifs en phase de développement**. Ce constat est partagé par le ministre de l'économie et des finances : « *nous sommes bons pour créer des* start-up, *nous sommes bons sur la recherche, notamment fondamentale et sur l'innovation mais nous n'avons pas les moyens de les faire grandir* »[3].

Pour cela, **les fonds français doivent atteindre une taille critique pour attirer les plus grands fonds étrangers**, à la recherche de gros tickets, et **pour permettre aux entreprises qu'ils soutiennent de changer de dimension**. La Dinsic partage ce constat puisque son directeur estime qu'il y a moins un problème de capitaux qu'un problème à trouver des porteurs de projets nécessitant des tickets à plusieurs centaines de millions d'euros, sans lesquels on ne peut créer de géants du numérique.

Il existe en outre de **nombreux dispositifs de financement de l'innovation et de soutien aux entreprises innovantes**. Depuis 2011, et au 31 décembre 2018, le fonds *Ambition numérique* de Bpifrance a par exemple investi dans 43 start-up, pour un montant de 205 millions d'euros. Sont choisis des **secteurs indispensables au développement de l'économie numérique** (logiciels, objets connectés, intelligence artificielle…). Le fonds intervient à hauteur de 1 à 10 millions d'euros, dans des sociétés ayant

---

[1] *Ces chiffres ne proviennent pas de France Invest mais du rapport* Financer la quatrième révolution industrielle. Lever le verrou du financement des entreprises technologiques, *rapport remis au ministère de l'économie et des finances par Philippe Tibi, avec la collaboration de Philippe Englebert (juillet 2019), p. 16. Les auteurs s'appuient sur le baromètre trimestriel de EY sur le capital-risque.*

[2] *Rapport Tibi, p. 13.*

[3] *Audition de Bruno Le Maire, ministre de l'économie et des finances devant votre commission le 10 septembre 2019.*

dépassé la phase d'amorçage. Autre point de comparaison, l'effort de recherche français se maintient aux premières places mondiales[1].

Les explications des difficultés que peuvent rencontrer les start-up pour se financer se trouvent donc ailleurs. Premièrement, ces **cadres** de financement, qu'ils soient nationaux ou européens, sont, en termes de **maturité**, **très fragmentés** : ils interviennent soit très en amont, au niveau de la recherche académique, soit très en aval, par exemple au sein des pôles de compétitivité. **Il n'existe pas de cadre englobant** permettant, pour un même projet, de mener les recherches en amont, de conduire les produits à maturité et d'enfin aider à leur commercialisation. Pour répondre aux initiatives des géants du numérique, mais aussi des États-Unis et de la Chine, notamment sur le quantique ou sur l'intelligence artificielle embarquée, la France et l'Union européenne auraient **tout bénéfice à développer un tel cadre**.

Votre rapporteur admet qu'**il n'est pas envisageable, au moins à court et moyen terme, de vouloir rivaliser avec le Royaume-Uni, et encore moins avec les États-Unis**. C'est une position de bon sens, qui part d'abord d'un constat simple : le marché des capitaux à risque est structurellement plus étroit en Europe qu'aux États-Unis, le risque vieillesse y étant notamment géré différemment.

Votre rapporteur insiste toutefois sur **deux lacunes dans le financement privé des start-up en France** : au début de la chaîne, avec un **nombre plus faible de business angels** que chez nos partenaires européens ; en fin de chaîne, avec une **difficulté du capital-croissance à répondre aux besoins de financement des entreprises innovantes**. Or, ceci est un **handicap majeur à la défense de notre souveraineté numérique** puisque, « *dans la compétition internationale entre start-up innovantes, le montant des levées de fonds est un déterminant fondamental de la capacité à réussir le processus d'innovation : portage d'un projet technologique jusqu'à la phase d'industrialisation ou vitesse d'acquisition de parts de marché dans un projet numérique d'innovation d'usage* »[2].

L'économiste français Philippe Tibi a récemment remis un rapport sur les **moyens d'aider les jeunes entreprises françaises innovantes à lever des fonds et à réussir leur entrée en bourse**. Le constat du rapport est sans appel : en France, la seule société technologique de moins de 25 ans présente

---

[1] *Selon les données de l'OCDE, qui retient l'indicateur de la dépense intérieure de recherche et de développement, la France se situait au cinquième rang mondial, deuxième pays de l'Union européenne derrière l'Allemagne. Ces chiffres sont à retrouver dans le* Rapport sur les politiques nationales de recherche et de formations supérieures (p.169), *annexé au projet de loi de finances pour 2019.*

[2] Rapport sur les aides à l'innovation, MM. Lewiner, Stephan, Distinguin et Dubertret (mars 2018), p. 16.
http://www.igf.finances.gouv.fr/files/live/sites/igf/files/contributed/IGF%20internet/2.RapportsPublics/2018/rapport-innovation.pdf
C'est un constat également partagé par MM. Colin et Collin dans leur rapport sur la fiscalité du numérique.

au CAC 40 est Dassault Systèmes, tandis que les entreprises du secteur technologique représentent environ un tiers de l'indice S&P500 (États-Unis). Dassault Systèmes est également la seule entreprise présente dans le top 100 des entreprises numériques cotées de Forbes (49 sont américaines, 14 chinoises). Pourtant, la France dispose de nombreux atouts : sa recherche de haut niveau, ses ingénieurs reconnus pour la qualité de leur formation, un niveau d'investissement en R&D correct, l'accès à un marché européen de 500 millions de citoyens. **Le facteur clé est donc celui du financement**. Deux pistes sont proposées dans le rapport Tibi :

1°) **répondre aux manques de financement en *late stage***, c'est-à-dire les levées supérieures à 30-40 millions d'euros (et 100 millions d'euros pour atteindre le statut de licorne). Le rapport recommande de créer 10 fonds *late stage* gérant au moins un milliard d'euros chacun.

Votre rapporteur est plutôt **sceptique sur la façon dont le rapport propose d'atteindre ces volumes** : par « *un travail de conviction* ». Cela fait écho aux propos du secrétaire d'État chargé du numérique, Monsieur Cédric O, devant la commission d'enquête : « *nous pouvons agir à législation constante* », pour déplacer des millions d'euros vers ces entreprises innovantes. Une question demeure : comment ? Une première piste est esquissée avec **la mise en place d'un label** *French Tech Investissement*, à l'image de ce qui existe aujourd'hui avec les fonds labellisés « investissement socialement responsable », qui parviennent à collecter entre 1,5 et 2 milliards d'euros par an, en s'appuyant notamment sur l'épargne salariale**. Lever de tels fonds permettrait ensuite aux startups de pouvoir être introduites en bourse, un passage obligé** pour Philippe Tibi, pour qui « *tous les leaders technologiques mondiaux aujourd'hui, notamment américains et chinois, ont été accompagnés par des fonds de capital-risque jusqu'à maturité, puis se sont introduits en Bourse* »[1].

2°) **Susciter la demande des actionnaires pour les titres des *start-up* ou autres entreprises innovantes**. Le rapport préconise ici l'émergence de fonds *global tech*, tels qu'il en existe au Nasdaq. Ces fonds sont gérés par des experts des nouvelles technologies et des modèles économiques portés par ces entreprises innovantes.

L'émergence de ces fonds nécessite donc tant des moyens financiers que des compétences humaines. L'objectif est ambitieux : lancer cinq à dix fonds de dix milliards d'euros au total d'ici trois ans. Le financement reposerait ici plus largement sur les investisseurs institutionnels (huit milliards d'euros) avec, à nouveau, un travail de conviction, mené cette fois-ci auprès des particuliers, pour faire de la French Tech une nouvelle catégorie d'investissements installée et reconnue.

---

[1] Bourse : les pistes pour faire de Paris la capitale européenne de la Tech, *Les Échos, 19 juillet 2019. Lien : https://www.lesechos.fr/finance-marches/marches-financiers/bourse-les-pistes-pour-faire-de-paris-la-capitale-europeenne-de-la-tech-1039096*

Votre rapporteur rappelle que **diriger l'épargne des Français vers l'investissement productif**, ici les entreprises du numérique, **n'est pas un objectif nouveau**. Les dispositifs adoptés par les gouvernements successifs se sont pourtant montrés décevants, à l'image du dispositif PEA-PME, jugé trop complexe, de la suppression de l'ISF PME ou de la réforme de la fiscalité du capital[1]. Aujourd'hui, les valeurs technologiques représentent 7 % des encours des fonds français d'assurance-vie… mais 19 % des indices boursiers mondiaux[2].

Pour encourager le développement de *business angels*, votre rapporteur soutient une proposition du rapport de MM. Jacques Lewiner, directeur scientifique honoraire de l'ESPCI, doyen de l'Innovation et de l'Entrepreneuriat de PSL Université Paris, Ronan Stephan, directeur scientifique de Plastic Omnium, Stéphane Distinguin, président de Fabernovel et Julien Dubertret, inspecteur général des finances, sur les aides à l'innovation : **augmenter le taux et les plafonds annuels de versement du dispositif de défiscalisation IR-PME**[3]. Ce taux est actuellement de 25 %, un niveau moins incitatif que celui proposé dans d'autres pays. Cela répondrait en plus à la baisse de la collecte constatée par France Invest et Bpifrance du fait de la disparition du dispositif ISF-PME.

Cette recommandation a été reprise par le rapport d'information relatif à l'accompagnement du cycle de vie des entreprises, publié en 2018 au nom de la délégation aux entreprises du Sénat[4], qui constatait que la France manquait d'un outil adapté au capital-risque, et notamment d'une dépense fiscale avantageuse pour ces acteurs. Le manque de fonds privés sur ce segment, et notamment de fonds capables de lever des tickets supérieurs à plusieurs dizaines de millions d'euros, conduit en effet les entreprises innovantes et les *start-up* à dépendre fortement du soutien public, et notamment de Bpifrance.

Votre rapporteur souligne enfin que **les dispositifs d'incitation à l'innovation sont tellement divers qu'il serait judicieux de créer un point d'entrée unique pour toutes les entreprises**. Bruno Le Maire a lui-même reconnu qu'il fallait rationaliser ces dispositifs : « *il existe trop de canaux de financement, ce qui nuit à leur efficacité* »[5]. La création de ce portail

---

[1] *Dans les réponses transmises au questionnaire adressé par votre commission, le ministère de l'Economie et des Finances estime qu'il est encore trop tôt pour évaluer les impacts, positifs ou négatifs, de la réforme de l'ISF et de la fiscalité du capital. France Stratégie, chargé de conduire une évaluation de la réforme de la fiscalité du capital, devrait rendre ses premières conclusions cet automne. La commission des finances du Sénat publiera également, au mois d'octobre 2019, un rapport sur l'impact de la réforme de la fiscalité du capital.*

[2] *Rapport Tibi, p. 6.*

[3] Les aides à l'innovation*, rapport n° 2017-M-075-01 de MM. Lewiner, Stephan, Distinguin et Dubertret remis en mars 2018.*

[4] *Lien vers le rapport : https://www.senat.fr/rap/r17-405/r17-4051.pdf*

[5] *Audition de Bruno Le Maire, ministre de l'économie et des finances, devant votre commission le 10 septembre 2019.*

bénéficierait d'autant plus aux start-up et aux PME, qui n'ont pas toujours les moyens humains pour effectuer ce long travail de recherche.

Étudier la possibilité et les impacts éventuels d'un élargissement de la dépense fiscale IR-PME, en y incluant éventuellement une composition « numérique ».

Créer un portail unique pour que toutes les entreprises puissent avoir davantage de visibilité sur les soutiens à l'innovation numérique en France.

b) Le crédit d'impôt recherche : un dispositif favorable à clarifier

Le crédit d'impôt recherche (CIR) demeure très apprécié des entreprises pour financer leurs efforts en R&D. Une première évaluation de cette dépense fiscale, la deuxième du budget de l'État (6 milliards d'euros) a conclu que les entreprises bénéficiaires avaient globalement accru leurs dépenses en R&D, même si les études économétriques diffèrent sur son ampleur (entre 0,9 et 1,5)[1].

Le crédit d'impôt recherche

Instauré en France en 1983, le CIR a pour objectif principal d'inciter les entreprises à accroître leurs dépenses de R&D en réduisant le coût de ces activités, par le biais d'une dépense fiscale. Depuis 2008, le dispositif repose uniquement sur le volume des dépenses. Le crédit d'impôt s'impute ensuite sur l'impôt sur les sociétés à hauteur des taux suivants : 30 % pour les dépenses inférieures à 100 millions d'euros et 5 % au-delà.

La quasi-totalité des membres de l'OCDE ont un dispositif fiscal similaire, la France étant parmi les pays les plus généreux.

Votre rapporteur estime toutefois que **le CIR devrait être mieux adapté au secteur du numérique**. Les innovations dans le domaine numérique reposent moins sur des innovations technologiques que sur des innovations d'usage, en s'appuyant sur la proposition de services. Or, les critères d'éligibilité du CIR devraient être clarifiés pour que les jeunes entreprises du numérique sachent très précisément si elles peuvent en bénéficier et à quelle hauteur. Comment les critères de création de connaissances s'appliquent-ils à la création d'un algorithme, aux itérations, au développement d'un logiciel ? Cette simplification des règles bénéficierait également aux entreprises en phase d'amorçage, qui ici non plus, ne disposent pas toujours des ressources humaines suffisantes pour conduire et comprendre les démarches lourdes permettant de bénéficier de ce crédit d'impôt.

[1] *Avis de la commission nationale d'évaluation des politiques d'innovation sur l'impact du crédit d'impôt recherche, mars 2019.*
Lien : https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-cnepi-avis-impact-cir-06032019-final-web.pdf

Clarifier les conditions d'octroi du crédit d'impôt recherche pour les entreprises du secteur numérique.

c) Sur le rachat des pépites technologiques et le financement de l'innovation en France

Il existe sur ce sujet **des divergences d'opinion assez fortes** entre ceux qui considèrent que la très grande majorité des pépites technologiques françaises et européennes sont rachetées et intégrées par des grands groupes extra-européens, et ceux qui défendent le contraire et font preuve d'un certain optimisme. Votre rapporteur estime qu'**il y là matière à progrès, sans tomber dans un discours alarmiste** sur un quelconque « exode » des entrepreneurs et des brevets. À cet égard, votre rapporteur considère positivement l'initiative prise par le ministère de l'économie et des finances, à travers le service de l'information stratégique et de la sécurité économiques (SISSE), pour protéger les *start-up* structurantes de rachats en trouvant des entreprises nationales capables d'acheter leurs technologies, afin qu'elles demeurent dans le giron français. Le service veut tirer profit du *big data* et de l'intelligence artificielle pour détecter les menaces sur les intérêts économiques français.

Les grandes entreprises du numérique, que ce soit Facebook, Google ou encore Cisco, **ont largement investi en France**, par le biais de laboratoires d'innovation, du financement de programmes de formation ou encore par l'intermédiaire de programmes de soutien de *start-up*. **Votre rapporteur n'a pas la naïveté de croire que ces investissements sont désintéressés, toutefois, ils soutiennent aussi un écosystème qui peine parfois à trouver les fonds nécessaires à sa croissance**. C'est d'ailleurs une stratégie encouragée par les pouvoirs publics, qui considèrent que le développement de ces *start-up* constitue un enjeu national.

Il serait ainsi **préjudiciable d'opposer automatiquement fonds « étrangers » et souveraineté française**, d'autant plus que cela serait se méprendre sur les stratégies de ces acteurs, notamment américains. Au rachat, les entreprises installées sur le marché du numérique préfèrent parfois la collaboration avec les *start-up*. Cette stratégie dite du « donnant-donnant » fonctionne ainsi : en échange d'un accompagnement commercial, les entreprises accèdent à des produits et des solutions de point. À titre d'exemple, Microsoft a accompagné l'essor de Criteo ou de Talentsoft et se concentre, dans le cadre de son partenariat avec Station F, sur l'intelligence artificielle.

En outre, considérer que les entreprises, notamment américaines, optent pour des stratégies exclusivement prédatrices serait oublier que les dirigeants de *start-up* ou d'entreprises innovantes ont leurs propres intérêts. Derrière les entrepreneurs, il y a des fonds et des stratégies d'investissement qui ont besoin d'accroître leur rentabilité et de retirer les bénéfices de leurs investissements.

Bpifrance et France Invest, qui regroupe les acteurs français du capital-risque, l'ont d'ailleurs souligné devant votre commission : **il ne faut pas confondre financement par des fonds étrangers et perte de nos actifs, matériels ou immatériels**. L'exemple d'Israël est à cet égard frappant : pour développer ses innovations et ses entreprises, Israël incite les fonds étrangers à investir par le biais de fonds nationaux, afin qu'ils respectent la réglementation nationale et que les intérêts économiques et souverains israéliens ne soient pas menacés[1]. En outre, selon Bpifrance, seule une part minoritaire des entreprises de la tech française est effectivement rachetée par des acteurs américains. Ce qui donne cette impression de rachat massif, c'est simplement le fait qu'ils se concentrent sur les acquisitions d'entreprises en pleine croissance, avec une valorisation beaucoup plus forte.

Cela doit donc nous inciter à **améliorer nos outils de repérage et la défense des *start-up* les plus prometteuses**. C'est ce qu'a admis M. Le Maire devant votre commission : il ne faut pas que « *nous financions des start-up pour qu'elles deviennent des champions américains plus tard* », alors même que nous disposons de nouveaux moyens pour lutter contre ces pillages (cf. supra).

Ainsi, pour reprendre les termes de Christian Harbulot, directeur de l'École de guerre économique, « ***une politique de puissance n'est pas l'addition des nationalités inscrites sur les cartes d'identité des actionnaires*** »[2].

d) Recruter et fidéliser les talents

« ***La prise en compte de sujets techniques complexes*** *(mécanismes économiques, contraintes juridiques, circuits financiers, évolutions technologiques et scientifiques…)* ***impose par ailleurs d'adapter en permanence le recrutement et les formations*** *pour garantir la compréhension des enjeux, la pertinence de l'orientation des capteurs et la qualité de l'analyse dans la production des services* »[3]. Ce constat, posé pour les services de renseignement, vaut pour l'ensemble des administrations de l'État. Comme l'a rappelé la ministre des armées, Mme Florence Parly, devant votre commission, le « *sujet des ressources humaines est sans aucun doute l'un des plus difficiles* » quand il s'agit de défendre notre souveraineté numérique[4]. Pour résumer, **sans personnes qualifiées, pas de souveraineté numérique**. Or, les autorités indépendantes

---

[1] *Pour un panorama des mesures israéliennes en faveur de l'attractivité économique, voir cette note du service économique de l'Ambassade de France en Israël :* https://www.tresor.economie.gouv.fr/Articles/3e7c9641-70e6-42f2-8a7a-ebb9d11bda55/files/afd681f1-167a-45d0-afe1-80e35c544a7a

[2] *Audition de M. Christian Harbulot, directeur de l'école de guerre économique, devant votre commission d'enquête le 23 mai 2019.*

[3] *Coordination nationale du renseignement et de la lutte contre le terrorisme,* La stratégie nationale du renseignement *(juillet 2019), p. 11. Lien du rapport :* http://www.sgdsn.gouv.fr/uploads/2019/07/20190703-cnrlt-np-strategie-nationale-renseignement.pdf

[4] *Audition de Mme Florence Parly, ministre des armées, devant votre commission le 3 septembre 2019.*

et les administrations publiques ont de plus en plus de mal à recruter des experts du numérique, des informaticiens, des mathématiciens ou des ingénieurs. Dans ce contexte, comment concurrencer les rémunérations attractives proposées par ces entreprises ? **Comment conserver une réserve de talents « en interne » ?**

S'il peut sembler difficile de se battre contre des entreprises offrant des **rémunérations au moins trois à quatre fois supérieures** à celles du service public, les auditions menées par votre commission ont montré que cette bataille était loin d'être perdue.

Les administrations disposent certes de **marges de manœuvre limitées sur les rémunérations** : pas de négociation libre (ex. faire une contre-offre à une proposition du secteur privé) ; pas de dispositif semblable à la participation ou à l'intéressement ; pas d'avantages en nature liés aux fonctions… mais elles doivent **jouer sur les éléments qu'elles peuvent maîtriser** : la progression de la carrière, la souplesse des conditions de travail et du cadre, la création de grands projets d'avenir, etc.

Il semble en outre que **le sens de l'action publique**, la fierté de travailler sur des **projets d'intérêt national** et d'avenir pour notre souveraineté et pour la France demeurent un **facteur d'attractivité pour les jeunes talents et les professionnels plus expérimentés.** Les organismes peuvent également adopter des **solutions plus originales** pour retenir leurs talents : le CEA propose par exemple à ses personnels de **créer leurs propres *start-up***, en mettant à leur disposition un système d'incubation et la possibilité de nouer des partenariats industriels.

La loi Pacte comprend ainsi des dispositions visant à **encourager les chercheurs à davantage de mobilité vers le secteur privé**, en leur permettant notamment de participer plus facilement à la conduite d'un projet en entreprises ou de créer leurs propres entreprises. Ces nouvelles dispositions répondent à un constat : **ce dispositif de passerelle n'a été que très peu utilisé**, seules 51 requêtes pour travailler au sein d'une entreprise et 231 requêtes de création d'entreprises ayant été examinées par la commission de déontologie depuis 2000. Les procédures sont donc assouplies : autorisation donnée par l'établissement qui emploie le chercheur ; possibilité pour le chercheur de conserver une part de son entreprise après réintégration dans un organisme public ; possibilité de consacrer jusqu'à 50 % du temps de travail à l'entreprise.

Une partie des fonds du PIA 3 est également consacrée à la **formation des chercheurs à l'entrepreneuriat** en soutenant des programmes de formation et en octroyant des aides publiques aux lauréats de concours d'innovation, afin qu'ils puissent plus rapidement lancer leurs produits sur le marché.

Pour autant, **ces facteurs d'optimisme sont fragiles et, sans effort supplémentaire de la part de l'État,** votre rapporteur estime que **le secteur public pourrait rapidement perdre sa force d'attraction**.

Il y a là également un **enjeu civique** : notre système d'enseignement supérieur, l'un des meilleurs au monde, est financé par de l'impôt. Comment faire en sorte que les élèves qui y sont formés n'aillent pas directement travailler pour les géants du numérique, spécialistes de l'optimisation fiscale ? Au moins **en créant des débouchés attractifs** pour capter ces talents, par l'intermédiaire de grands projets d'innovation européens ou français, et **en ayant conscience des stratégies employées par les géants du numérique**. Ces derniers nouent par exemple des partenariats avec les écoles pour accueillir d'importants contingents de stagiaires au sein de leurs entités : c'est pour eux une manière de repérer les talents les plus prometteurs et de fidéliser cette main d'œuvre, en leur promettant un recrutement après le diplôme.

Faute de disposer des compétences en interne, **le recours à des contractuels est de plus en plus fréquent** pour ces métiers hautement qualifiés et spécialisés. Jusqu'à présent, deux conditions devaient être satisfaites pour recruter un contractuel, pour un contrat à durée déterminée de trois ans renouvelable : (a) lorsqu'il n'existait pas de corps de fonctionnaires susceptibles d'assurer les fonctions correspondantes ; (b) lorsque la nature des fonctions ou les besoins des services le justifiait pour les emplois de catégorie A.

Avec l'objectif de **rendre plus attractifs les postes de contractuels**, la circulaire du Premier ministre du 21 mars 2017 **facilite le recours au CDI**, lorsque cela s'avère être un **facteur de motivation** suffisant et que l'employeur public a démontré l'employabilité à long terme du profil recherché. Toutefois, **c'est loin d'être suffisant** : pour des personnels très qualifiés et des profils aussi recherchés, le CDI n'est pas nécessairement le premier critère d'entrée. Le directeur de la Dinsic, M. Nadi Bou Hanna, a bien conscience de ces enjeux : « *si l'État n'est pas capable d'attirer les meilleurs talents, il n'y aura pas de souveraineté.* ***Il faut changer les pratiques managériales****, fluidifier la circulation de l'information, associer les agents à la décision à travers des solutions numériques. Il s'agit d'un* ***changement de paradigme managérial*** ».

La **loi du 6 août 2019 pour la transformation de la fonction publique**[1] a assoupli ces conditions :

- il est maintenant **possible de recruter des contractuels** « *lorsqu'il s'agit de fonctions nécessitant des* ***compétences techniques spécialisées ou nouvelles*** » ;

[1] *Loi n° 2019-828 du 6 août 2019 de transformation de la fonction publique.*

- la loi introduit un **contrat de mission**, inspiré du contrat de chantier : pour mener à bien un projet, les administrations de l'État et établissements publics peuvent recruter un agent par un CDD, dont l'échéance est la réalisation du projet. À l'initiative du Sénat, la durée minimale de ce contrat a été fixée à un an et sa durée maximale à six ans.

Une fois l'étape du recrutement franchie, une autre difficulté se dresse devant le secteur public : la fidélisation des personnels, en particulier dans les secteurs en tension ou pour les spécialités rares. Plusieurs personnes auditionnées par votre commission d'enquête ont témoigné de la compétition existant dans ce domaine : les Gafam « chassent » et recrutent les personnels qui les intéressent avec des conditions de rémunération, mais aussi de travail (ex. moyens alloués à chaque projet) bien plus attractives. En première lecture de l'examen du projet de loi pour la transformation de la Fonction publique, le Sénat avait adopté un amendement, proposé par notre collègue Catherine Morin-Desailly, visant à faire de la protection de la souveraineté nationale un critère explicite d'évaluation et d'autorisation de la mobilité des responsables publics vers et depuis le privé. Il n'a cependant pas été retenu à l'issue de la commission mixte paritaire. S'il est vrai que l'exercice de fonctions au cœur des entreprises du numérique peut permettre de mieux les connaître, pour mieux les réguler, se pose toujours la question des intérêts ensuite défendus par les personnes concernées.

Votre rapporteur note que le Gouvernement, sous l'égide du secrétaire d'État chargé du numérique, Monsieur Cédric O, a lancé un groupe de travail chargé de proposer des solutions concrètes pour répondre à ces problèmes de recrutement, y compris pour les entreprises. L'enjeu est primordial et nécessite d'agir rapidement, en commençant par les rémunérations offertes à ces profils qualifiés et très demandés.

Enfin, il convient de souligner que ces difficultés de recrutement se trouvent accentuées par l'absence de mixité dans le secteur du numérique. La ministre des armées a ainsi exprimé son intérêt pour la démarche « les Combattantes@Numérique », lancée en septembre 2018, et qui « *vise à encourager les femmes à s'approprier les compétences du numérique et à les attirer dans [ces] industries* »[1]. En effet, selon les chiffres publiés par le Syntec Numérique lors de sa conférence semestrielle de juin 2018, les femmes ne représentent que 27,5 % des effectifs de ce secteur. La situation est encore plus préoccupante dans le domaine de la cybersécurité où, d'après une étude commandée par Kaspersky Lab en 2017, ce taux n'est que de 11,5 %. Dans un marché aussi concurrentiel, le manque de diversité pourrait pénaliser le développement et la compétitivité des acteurs publics et privés. Les administrations et les entreprises du digital se privent ainsi d'un vivier de talents et de profils de haut niveau pour piloter la transformation numérique.

[1] *Audition de Florence Parly, ministre des armées, devant votre commission le 03 septembre 2019.*

2. Maintenir l'excellence de nos formations et renforcer les liens entre la recherche publique et le secteur privé

a) La formation initiale : un atout à conserver

S'il est donc bien un point qui a fait l'unanimité auprès des personnes auditionnées par votre commission d'enquête, c'est l'**excellence des formations françaises**, que ce soit en mathématiques, en informatique ou pour les cycles d'ingénieurs, qui constituent un **vivier considérable de personnels très qualifiés pour les grandes entreprises du numérique**, en France et à l'étranger[1]. La France dispose en outre du second ratio le plus élevé de l'Union européenne de diplômés en sciences ou en ingénierie rapportés à la population totale. Ces deux facteurs expliquent sans doute l'étendue des **partenariats entre les grandes entreprises du numérique et l'enseignement supérieur français**. La collaboration de Microsoft et de l'Inria (institut national de recherché dédié aux sciences du numérique) date par exemple de 2006 ; Cisco et Polytechnique ont créé en 2014 une chaire *Internet of Everything* ; Google travaille avec l'ENS et Polytechnique ; Palantir Technologies France intervient dans le cadre d'un enseignement dédié au *big data* et à la gouvernance à Sciences Po.

Il est frappant de constater que les pouvoirs publics risquent, là-encore, d'être dépassé par les initiatives des entreprises du numérique. Celles-ci ne se contentent plus de nouer des partenariats avec les formations existantes, elles développent également leurs propres structures pour répondre à leurs besoins actuels et futurs. Ainsi, d'ici 2021, Microsoft compte ouvrir une vingtaine d'écoles sur l'intelligence artificielle, avec des partenaires comme Orange ou Capgemini. Google organise également des ateliers numériques, en lien avec les acteurs locaux (collectivités territoriales, chambres de commerce et d'industrie, association, etc.), et à destination des entreprises, des salariés et des demandeurs d'emplois.

Alors que la présidente de la Commission européenne a fait part de son attention de tripler le budget Erasmus + et que le numérique est devenu l'une des priorités de son programme de travail, votre rapporteur considère qu'il y a là une fenêtre d'opportunité à exploiter. L'**élargissement d'Erasmus + pourrait être tant qualitatif,** avec une action particulière à destination des formations numériques, **que quantitatif**, en incluant plus largement l'apprentissage et les salariés dont les postes sont soumis, avec le numérique, à de fortes transformations.

Soutenir le triplement du programme Erasmus +, en insistant plus particulièrement sur les formations au numérique.

[1] *Ce satisfecit ne doit pas conduire à sous-estimer les difficultés que connaît le secteur de la formation. Il n'a pas échappé à votre commission que les filières d'ingénieur ne parviennent pas toutes à recruter autant d'étudiants qu'elles offrent de places.*

b) Les liens entre la recherche publique et le secteur privé : des progrès louables mais insuffisants

Bpifrance, plutôt optimiste sur les outils de financement français, estime que les deux prochaines étapes indispensables au développement d'un écosystème favorable aux *start-up* et aux entreprises du numérique seront (i) de **faire davantage travailler ensemble la recherche et l'industrie** ; (ii) d'accompagner la transformation du système de production par l'innovation en encourageant les partenariats entre start-up et entreprises traditionnelles.

Malgré les efforts répétés des gouvernements successifs pour accroître la porosité entre les mondes académique et industriel, votre rapporteur est forcé de constater l'échec de cette politique publique. Combler ce fossé est pourtant un enjeu essentiel si la France souhaite développer des innovations de rupture et contrôler des technologies qui lui permettront de préserver sa souveraineté numérique.

La faiblesse des liens entre la recherche et les entreprises n'est pas un « mal européen » : en Allemagne, ces chaînes verticales se mettent en place beaucoup plus rapidement. En France, le processus semble davantage « artisanal » et s'appuie le plus souvent sur des relations historiques et de confiance entre un centre de recherche et une entreprise.

Le label Carnot : un mécanisme inspiré de l'Allemagne

Le label Carnot, créé en 2006, est un label d'excellence décerné par le ministère de l'enseignement supérieur et de la recherche et de l'innovation à des établissements de recherche en France à l'issue d'appels à candidatures. Il entend favoriser la recherche partenariale, c'est-à-dire la conduite de travaux de recherche menés par des laboratoires publics en partenariat avec des acteurs socio-économiques, notamment avec des entreprises. Les instituts Carnot favorisent le rapprochement des acteurs de la recherche publique et du monde socio-économique, afin d'accélérer le passage de la recherche à l'innovation et d'accroître le transfert de technologies vers les acteurs économiques.

Le dispositif Carnot s'inspire du modèle des instituts Fraunhofer allemands. Les établissements labellisés, Instituts Carnot, reçoivent des financements (en provenance de l'ANR), calculés en fonction du volume des recettes tirées des contrats de recherche avec leurs partenaires, notamment les entreprises.

Les 38 instituts regroupent près de 30 000 professionnels de la recherche (en équivalent temps pleins). Ils représentent un budget de recherche consolidé de 2,2 milliards d'euros et autour de 450 millions d'euros de contrats de recherche financés par les entreprises, soit 50% de la R&D publique par les entreprises (9 600 contrats de recherche par an passés avec plus de 4000 PME et ETI).

Source : ministère de l'enseignement supérieur, de la recherche et de l'innovation

Notre recherche académique est unanimement reconnue pour sa très haute qualité : pour autant, il nous est **difficile de transformer celle-ci en**

produits pour nos industries et en réussite économique nationale. Cette faiblesse française est depuis longtemps identifiée par la Commission européenne[1] : il nous faut **intensifier les liaisons entre recherche académique, centres de recherche appliquée, *start-up* et entreprises**. Ces dernières avaient fait état, en 2015, de plusieurs de leurs griefs à l'encontre des dispositifs français[2] : manque de visibilité, trop grande complexité des dispositifs, existence d'une multitude de guichets, manque de réactivité de certains acteurs publics, méconnaissance des besoins des entreprises, activités de recherche menées dans des champs scientifiques trop étroits, communication et gestion des projets inadaptés, tarifs parfois trop élevés et opaques, mobilité humaine entre le privé et le public en R&D très faible.

Face à ces constats, sans revenir sur le haut degré d'exigence de recrutement pour les responsables des structures visant à favoriser la recherche partenariale, votre rapporteur soutient **deux propositions pour améliorer la gouvernance de l'innovation et des liens entre les établissements publics de recherche et les entreprises**[3] : une **meilleure implication des entreprises au sein des établissements publics de recherche**, pour mieux prendre en compte leurs attentes et donc faciliter les projets de collaboration, par exemple à travers un comité d'orientation ; et la **création d'un interlocuteur unique pour les entreprises au sein de chaque établissement**, et d'un portail internet pour tout ce qui concerne les interactions entre entreprises et recherche publique.

Le Royaume-Uni a également mis en place un dispositif qui semble **satisfaire les petites et moyennes entreprises britanniques** : les ***innovation vouchers***, qui permettent aux PME de consulter un établissement public de recherche pour un projet innovant et de bénéficier de petites subventions (inférieures à 5 000 £), à la suite d'une procédure simple et soumise à un contrôle léger (localisation au Royaume-Uni, un seul coupon par PME). **Cette aide pourrait être reproduite en France pour les *start-up* du numérique**. Elle a l'avantage de s'appliquer à l'échelle d'un projet. En effet, certains financements incitatifs français demandent des montants minimums et des durées d'engagement élevés, ce qui ne correspond pas toujours à des projets d'ampleur limitée visant une mise en production ou une mise sur le marché rapide, comme c'est parfois le cas dans le domaine du numérique.

---

[1] *Pour la référence la plus récente, voir le rapport 2019 de la Commission européenne sur la France (lien : https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-france_en.pdf)*

[2] Les relations entre les entreprises et la recherche publique : lever des obstacles à l'innovation en France, *rapport remis à la Ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche et au Ministre de l'économie, de l'industrie et du numérique en octobre 2015.*

[3] *Ces propositions sont reprises du rapport mentionné ci-dessus.*

Accroître la visibilité des dispositifs de soutien aux partenariats recherche publique – entreprise privée en créant un point de contact unique.

Accroître la place des entreprises au sein des établissements publics de recherche, afin qu'elles puissent mieux y faire part de leurs besoins.

Réfléchir à la mise en place d'un système de « coupons d'innovation » pour les TPE-PME, à l'image du dispositif aujourd'hui en place au Royaume-Uni.

c) Une attention particulière à porter aux doctorants

Il peut sembler surprenant, lorsqu'on parle de souveraineté française, de voir l'importance des **efforts fournis par certaines entreprises étrangères pour soutenir les programmes de formation et de recherche**. Ainsi, ils accompagnent la formation aux métiers et usages du numérique de plusieurs centaines de milliers de personnes, et ce à tous les âges de formation. Là-encore, les entreprises, y compris étrangères, en retirent un bénéfice certain. L'un des trois jeunes doctorants titulaires d'un double-diplôme de Polytechnique et de Télécom Paris, une formation accompagnée par Cisco, a décidé de rejoindre la société.

Un dispositif très apprécié des entreprises est celui des **doctorants Cifre** (Conventions industrielles de formation par la recherche). Lancé au milieu des années 1980, il vise lui aussi à développer la recherche partenariale publique-privée : le projet est défini par l'entreprise, l'établissement public encadre le partenariat, l'entreprise recrute le doctorant en CDI ou en CDD, une partie de sa rémunération est assurée par l'ANR. **Ce cadre pourrait être étendu aux chercheurs post-doctorat et assoupli** (ex. la durée de trois ans est parfois trop longue au regard de la stratégie de l'entreprise).

Au-delà de nos frontières, votre rapporteur s'est montré sensible aux arguments développés par Bernard Stiegler, ancien membre du Conseil national du numérique et philosophe, pour **la défense d'un grand projet européen**, ou a minima franco-allemand, **mobilisant sur cinq ans 500 doctorants dans tous les domaines bouleversés par la révolution numérique**. La politique de soutien aux entreprises doit s'accompagner d'une politique de recherche technologique de haut niveau, pour prévenir la fuite de nos chercheurs et de nos innovations.

3. Défendre notre souveraineté nationale, s'appuyer sur l'échelon européen

La modernisation du régime des aides d'État de l'Union européenne a encouragé le financement de **projets importants d'intérêt européen commun** (Piiec déjà cités), un levier majeur pour donner aux États membres et à l'Union les moyens de défendre leur souveraineté dans la compétition numérique internationale. C'est dans ce cadre que quatre pays européens,

dont la France, ont notamment accordé 1,75 milliard d'euros à un projet dans le domaine de la microélectronique[1].

Selon un rapport remis au Gouvernement en avril 2019[2], **la coordination des Piiec par la Commission européenne pourrait être améliorée**. En effet, si l'examen de ces projets relève avant tout de la direction générale de la concurrence (DG COMP), chacune des autres directions générales ait amené à jouer un rôle clé en identifiant les secteurs pouvant faire l'objet d'un Piiec. Ce rôle devrait être davantage formalisé. Enfin, votre rapporteur, s'il ne peut que se satisfaire que de tels projets soient menés à l'échelle européenne, appelle également à un assouplissement des cadres de développements technologiques communs. **Il soutient ainsi les propositions du rapport précité**, qui appelle à **encourager des formes de collaborations temporaires ou la constitution de consortium d'entreprises européennes, qui pourraient répondre à des appels d'offres en commun**.

Votre rapporteur insiste enfin sur la nécessité de reconnaitre que **la France ne pourra jamais disposer seule de la force de frappe des États-Unis ou de la Chine**. Pour autant, il ne s'agit pas de considérer qu'elle ne pourra rien faire pour défendre sa souveraineté numérique face à ces acteurs étrangers ultra-dominants. **L'effet de levier ne sera obtenu que par la coopération européenne**, que ce soit pour soulever les volumes d'investissement nécessaires, pour développer une recherche universitaire ambitieuse ou pour définir une stratégie d'innovation de long terme. La coopération européenne, **c'est à la fois l'Union européenne** et **la construction de partenariats directement entre pays européens**.

Pour conclure, si votre rapporteur ne veut pas tomber dans l'alarmisme, il appelle pourtant le Gouvernement à écouter avec attention cet avertissement du rapport Tibi : « *notre pays peut continuer de jouer les premiers rôles dans cette nouvelle révolution* », pour nous un enjeu de puissance et de prospérité, mais « ***la leçon de ces quarante dernières années est que le succès n'est pas garanti*** »[3].

Pour défendre notre souveraineté numérique, il faut agir rapidement dans tous les champs où elle trouve aujourd'hui fragilisée, contournée et concurrencée. Tel est l'objectif des principales recommandations de votre commission d'enquête.

---

[1] *La commission européenne a en effet approuvé le 18 décembre 2018 le projet défendu par la France, l'Allemagne, l'Italie et le Royaume-Uni. La Commission estimait alors que cet apport public permettrait de lever six milliards d'euros complémentaires de la part d'investisseurs privés. Lien : https://europa.eu/rapid/press-release_IP-18-6862_en.htm Pour la France, il s'agit du programme Nano 2022 précité.*

[2] *Rapport d'inspection précité, intitulé* « La politique de la concurrence et les intérêts stratégiques de l'Union européenne ».

[3] *Rapport Tibi, p. 14.*

EXAMEN EN COMMISSION

M. Franck Montaugé, président. – Les travaux de notre commission d'enquête, entamés le 10 avril 2019, s'achèvent. Nous avons auditionné une soixantaine de personnes d'horizons différents et pris chacun conscience des bouleversements entraînés par la révolution numérique sur notre modèle social comme sur notre souveraineté. Je tiens à vous remercier pour votre implication et votre participation assidue, au terme d'un programme de travail chargé, à la hauteur des enjeux que nous devions relever.

Le mois dernier, la réunion du Bureau a permis de discuter des orientations du rapport, dont il nous appartient, si nous l'adoptons, d'autoriser la publication. Notre commission d'enquête obéit à un certain formalisme et le secret de nos travaux demeure protégé par des sanctions disciplinaires et pénales. Vous disposez, pour la présente réunion, d'exemplaires nominatifs du projet de rapport. En outre, l'autorisation de publication du rapport que nous serons amenés à donner ne sera effective que si aucune demande de constitution du Sénat en comité secret n'est formulée dans un délai de vingt-quatre heures suivant son dépôt. Notre rapport ne pourra donc être publié avant l'expiration de ce délai. Enfin, tout élément n'ayant pas été rendu public par notre commission restera soumis à la règle du secret pendant une durée maximale de trente ans, particulièrement s'agissant des auditions réalisées à huis clos.

M. Gérard Longuet, rapporteur. – Je dois, en toute modestie, reconnaître, à titre liminaire, que je connaissais mal le sujet de la souveraineté numérique, bien que le Sénat ait mené d'importants travaux sur ce thème – je pense notamment à ceux qui ont été réalisés à l'initiative de notre collègue Catherine Morin-Desailly. La création de notre commission d'enquête répond à une demande du groupe Les Républicains et s'inscrit dans le sentiment qu'un monde nouveau échappe au politique.

Notre réflexion se fonde sur un triple diagnostic. D'abord, la technologie numérique est vivante et le restera. Ensuite, la vitalité technologique et scientifique se double d'une créativité économique. J'ai notamment été impressionné, lors des auditions, par les possibilités de création de valeur en faisant apparaître de nouveaux besoins, de nouvelles possibilités et d'autres formes de relations entre clients et producteurs. Une telle créativité n'a aucune raison de cesser – voyez la commercialisation grandissante des données et le développement de la technologie des *blockchains*, laquelle repose sur l'adhésion de millions d'utilisateurs qui en espèrent un profit. Enfin, l'utilisation de l'outil numérique dans le cadre des conflits, qu'ils soient politiques ou armés, apparaît cruciale. À l'instar de la théorie française de la dissuasion nucléaire, il permet de gommer des dissymétries spectaculaires. Des pays de puissance et de philosophie politique différentes – les États-Unis et leurs Google, Apple, Facebook,

Amazon et Microsoft (Gafam), la Chine et son État centralisé et totalitaire, la Russie et son opinion publique peu exigeante, Israël ou la Corée du Nord – usent mêmement de l'arme numérique. Certes, la technologie demande des investissements colossaux, mais elle se diffuse ensuite aisément au-delà des seuls cercles du pouvoir. Le système, vivant, exige un croisement permanent des informations.

La souveraineté de l'État peut être définie comme le fait d'adopter des lois organisant les relations entre les citoyens. Aussi la dynamique numérique peut-elle perturber notre système social. Pensez à la pollution des élections présidentielles américaines ou au contrôle social mis en place par la Chine où 400 millions de caméras doivent permettre l'identification faciale des Chinois par une intelligence artificielle et le jugement du comportement qu'ils adoptent dans la rue. La science-fiction devient réalité ! Imaginez qu'une personnalité telle que Greta Thunberg devienne présidente de la Commission européenne : nous pourrions disposer chacun d'un crédit d'émissions carbone qui, une fois épuisé, nous interdirait de voyager. Si l'outil numérique le permet, certains souhaiteront l'utiliser… Comme élus, nous devons défendre la démocratie, fondée sur le suffrage universel et la liberté d'expression, et lutter contre la marchandisation des informations.

S'agissant de la souveraineté économique, il paraît insoutenable pour l'autorité de l'État que les grands acteurs ne s'acquittent pas de leurs impôts. Pour sa crédibilité comme vis-à-vis des citoyens, l'État doit retrouver sa souveraineté fiscale. Le fondement de l'économie de marché réside dans l'application sans discrimination des règles de marché. Or, quelle peut être la réalité d'un marché numérique dans lequel quelques entreprises s'arrogent un monopole ? *Quid*, en outre, des rapports entre monnaies et crypto-monnaies ?

Les liens entre souveraineté numérique et ordre public offrent des perspectives aussi vastes que fragiles. En effet, avec les technologies numériques, le faible dispose de moyens considérables. Il devient donc difficile, y compris pour les puissants, de se protéger. La France commence à se forger une culture sécuritaire : bien qu'incomplète, la prise de conscience existe. Notre système de défense repose sur un système complexe de réseaux d'information, de transport, de commandement et d'exécution. Les offensives numériques existent, notamment à l'encontre des entreprises, comme Saint-Gobain en fut victime en Ukraine, mais il demeure difficile de leur attribuer une paternité et, partant, de riposter efficacement. Pourtant, les systèmes strictement défensifs paraissent insuffisants. Une telle évolution représente une interrogation réelle pour la souveraineté d'un État.

M. Jérôme Bascher. – La lecture du rapport ne permet pas de saisir immédiatement les raisons qui ont poussé à l'adoption d'un tel plan – souveraineté politique, économique et de défense – au lieu de celui, plus classique, consistant à étudier les domaines dans lesquels l'État n'apparaît pas suffisamment souverain – les infrastructures ou les logiciels par

exemple –, les solutions pour y remédier. Votre choix aurait, me semble-t-il, mérité davantage d'explications.

M. Gérard Longuet, rapporteur. – Nous avons préféré retenir, comme fil rouge, les agressions, par le numérique, à la souveraineté française. Il ne s'agissait pas d'adopter une position de repli sino-russe consistant à rétablir l'autorité de l'État en contrôlant les relations entre les citoyens et le reste du monde, mais à montrer comment le système numérique remet en cause, dans une douceur trompeuse, les logiques collectives acceptées par l'ordre juridique établi. Le caractère agressif du numérique ne semble pas caractérisé comme lors du franchissement des Ardennes par l'armée allemande, mais il n'en apparaît pas moins réel. L'accord Blum-Byrnes de 1946 signant la fin des quotas de films américains en France ou l'affranchissement de Netflix des règles de diffusion imposées par la chronologie des médias ressortent, à mon sens, d'une forme d'agression. Nous subissons, à cause du numérique, une perte d'indépendance s'agissant de notre mode de vie, un marché économique déséquilibré par le monopole de quelques acteurs incontournables et des offensives égalitaristes à paternité inconnue qui déstabilisent notre système de défense. J'ai donc préféré fonder notre rapport sur la perte de citoyenneté plutôt que sur le contrôle étatique.

Mme Catherine Morin-Desailly. – Je vous remercie pour votre passionnant travail. J'ai également étudié le sujet de la souveraineté numérique, notamment en 2014 dans le cadre de la mission commune d'information relative au nouveau rôle et à la nouvelle stratégie pour l'Union européenne dans la gouvernance de l'Internet. Je retrouve dans le présent rapport les thèmes que nous avions alors évoqués. Le diagnostic demeure sensiblement identique et Internet est hélas ! devenu, comme nous le prévoyions, un lieu mondial d'affrontements. Certes, quelques recommandations ont été suivies d'effets et plusieurs avancées, quoique modestes, doivent être saluées – l'adoption du Règlement général sur la protection des données (RGPD), de la directive européenne sur le droit d'auteur et les droits voisins et, dans une moindre mesure, de mesures fiscales –, mais, en matière de droit de la concurrence, les progrès demeurent nuls.

Je rejoins les propositions de notre rapporteur et partage son parti pris : nous ne devons pas nous situer sur la défensive. D'ailleurs, quand la France et l'Allemagne se montrent offensives, elles sont écoutées et, souvent, suivies. Le sujet de la souveraineté numérique a, pour la première fois, été abordé lors de la dernière campagne présidentielle, puis a fait l'objet de débats lors des élections européennes du mois de juin 2019. Pour autant, aucune solution n'a encore été proposée pour exister face aux Gafam et à la Chine. En matière numérique, les perspectives de progrès paraissent aussi immenses que les craintes qu'elles suscitent en matière économique, politique et culturelle. Nous avons, hélas, souvent tendance à nous résigner !

Trop de fonctionnaires rejoignent le secteur privé, notamment les géants de l'Internet. La prise de conscience demeure en-deçà des menaces que font planer les nouvelles technologies et nos dirigeants restent passifs face aux défis politiques, industriels et économiques que représentent les Gafam, dont la puissance bat en brèche toute tentative de récupération de notre souveraineté.

Nous devons réguler le système numérique ! Le créateur d'Internet, Tim Berners-Lee, comme l'un des fondateurs de Facebook, Chris Hughes, estime que la régulation constitue un impératif de la survie d'un Internet durable. En sursis, il porte, en effet, en lui la critique de son propre modèle, celui que Shoshana Zuboff, professeure à Harvard, appelle le « capitalisme de surveillance » dans lequel rien n'est gratuit et tout concourt au renforcement des monopoles constitués. Ce n'est pas sans raison que, au temps de l'affaire Snowden, la *National Security Agency* (NSA) a écouté des fonctionnaires européens chargés de la concurrence ni que les élections américaines font l'objet de soupçons de manipulation. Ne soyons pas naïfs ! Nous devons nous montrer offensifs et anticiper la nouvelle génération de technologies.

Ces entreprises profitent de la disparité de nos régimes fiscaux.

Le rachat de nos start-up par des acteurs étrangers réjouit souvent ; on le voit comme un succès, mais il représente aussi une perte de souveraineté. Le partenariat entre l'État américain et Cisco, le choix de Palantir pour équiper nos services de renseignement, ou encore le financement par Google de notre école du numérique sont autant de signaux inquiétants. Il faut donc mener une politique volontariste d'investissement dans les écosystèmes numériques. L'État doit orienter les marchés vers les PME innovantes et aider les entreprises à développer des outils cryptographiques, notamment dans les domaines de la banque, de l'assurance et de la santé.

Les exemptions fiscales et les contrats publics, notamment dans le domaine militaire, peuvent être des outils puissants, que les États-Unis emploient d'ailleurs avec succès.

L'exemple allemand montre, quant à lui, que certaines mesures peuvent être prises à coût zéro : les autorités de ce pays imposent aux entreprises étrangères, notamment américaines, la création de *data centers* sur le territoire national allemand. C'est d'autant plus important que l'administration Trump a cessé d'octroyer une quelconque protection juridique aux citoyens étrangers en la matière. Il faut en somme user de tous les instruments à la disposition de l'État pour reconquérir notre souveraineté dans le domaine numérique.

Mme Sylvie Robert. – Je partage les propos de Mme Morin-Desailly. Le rapport qui nous est aujourd'hui présenté est extrêmement pédagogique. Il a la vertu de pointer et d'expliquer à nouveau certains défis auxquels nous

devons répondre. J'espère que le suivi des diverses préconisations sera fait ; un comité de vigilance pourrait être utile. La mobilisation doit être collective, aux différents niveaux de l'État, des collectivités, et sur le plan international. Des dispositions législatives importantes ont été prises, mais il faut maintenir la pression.

M. Rachel Mazuir. – J'ai retenu de la présentation de M. le rapporteur plusieurs points essentiels. Il fallait bien s'intéresser à la formation, à la recherche, et à la politique industrielle.

En évoquant la remise en cause de la liberté de nos concitoyens, M. le rapporteur s'est presque excusé de faire de la philosophie, mais cela me paraît bien être le point essentiel. En Chine, on compte déjà une caméra de surveillance pour trois habitants et leur nombre ne cesse d'augmenter ; ce n'est pas anodin. L'État de Californie a, pour sa part, interdit l'installation de caméras à reconnaissance faciale. On met le doigt sur quelque chose de très important : la liberté telle qu'on la conçoit en France et en Europe est complètement remise en cause. Les applications de nos téléphones portables sont dangereuses, en particulier les applications relatives à la santé : si l'on vous pirate, on saura exactement tout ce que vous faites dans la journée, et même la nuit. On entre dans un monde complètement différent de celui que nous avons connu.

Il faut nous donner les moyens de contrecarrer cette dérive folle, ce mouvement vers une société où les hommes seront menacés par le transhumanisme. Certains appellent de leurs vœux « l'homme augmenté » ; c'est nous renvoyer à une condition de sous-hommes. Quelle société voulons-nous ? Le numérique est une bombe, la souveraineté nous a échappé. Je n'ai pas de réponses, mais j'ai des inquiétudes. Alors, allons-y, reconquérons notre souveraineté, faisons des propositions ! Celles que contient ce rapport sont déjà importantes.

M. Gérard Longuet, rapporteur. – Je trouve cet échange passionnant. Nous ne sommes pas nécessairement parvenus à la présentation la plus parfaite possible du problème, mais je pense que vos préoccupations sont largement reprises dans le rapport.

Monsieur Mazuir, je juge, moi aussi, crucial le travail que nous menons sur ce modèle de société qui nous est imposé contre notre volonté. La souveraineté a longtemps été simplement le fait de protéger un territoire. Elle s'est ensuite élargie à divers phénomènes économiques. On a pris conscience de l'importance, par exemple, de la balance commerciale pour une nation : il s'agit de l'expression d'une aptitude à être aussi utile aux autres qu'ils nous le sont ; c'est donc, pour un pays, une liberté. Or, à présent, nous sommes confrontés à un système où, par suite d'un défaut de souveraineté, nous subissons une irruption dans la vie quotidienne qui change complètement les comportements de chacun, et ce sans qu'il y ait eu de débat, sans que la décision collective ait eu prise.

Madame Robert, je suis d'accord : il sera important d'assurer un suivi de ces recommandations. J'ai posé sur ce point des questions sur le Conseil national du numérique, où ne siège plus désormais qu'un seul sénateur. Cela pose le problème du rôle du Parlement par rapport au Gouvernement et à la société civile. Je suis profondément parlementaire. Il faudrait un forum de la souveraineté numérique, qui obligerait ceux qui sont aujourd'hui seuls à parler publiquement de ce sujet, notamment les entrepreneurs, à rencontrer des hommes et femmes politiques qui, contrairement aux représentants de l'exécutif, n'ont pas la responsabilité de l'immédiat, mais le devoir et le goût de la chose publique et de la réflexion, ce qui manque trop souvent à ces entrepreneurs.

Quand Bruno Le Maire tient de beaux discours sur les technologies de rupture, il est dans le rôle de l'exécutif : il existe médiatiquement, sans avoir à donner un contenu précis à ses propos ni à suivre dans le temps leur application. La nature de l'opinion publique contemporaine est telle qu'on oublie vite les discours tenus dans le frissonnement de l'immédiat.

Le Parlement, du fait du caractère collectif du débat, est mieux capable d'embrasser la totalité du sujet. Certes, une formule pourra aussi le séduire, mais il saura en général aller au-delà. Cela recouvre également la préoccupation de Mme Catherine Morin-Desailly. La loi triennale qu'elle suggère constituerait un rendez-vous ; en la préparant, on remettrait le Parlement dans la boucle.

M. Franck Montaugé, président. – Je vous propose à présent d'examiner les cinq propositions de rédaction qui ont été déposées sur le rapport.

M. Jérôme Bascher. – Ma proposition n° 1 vise simplement à préciser quelles banques centrales pourraient contribuer à l'élaboration d'une cryptomonnaie publique.

M. Gérard Longuet, rapporteur. **–** J'y suis favorable. Les cryptomonnaies déracinées qui existent depuis plusieurs années constituent une remise en cause de la responsabilité publique d'émission de la monnaie, responsabilité qui protège les citoyens. Je n'ai pas la passion de l'État, mais il est un meilleur garant de la valeur d'une monnaie que des acteurs inconnus et incontrôlables. On sent d'ailleurs que les banques centrales souhaitent aller dans cette direction.

La proposition n° 1 est adoptée.

M. Franck Montaugé, président. – Ma proposition n° 2 a pour objet l'application du Règlement général sur la protection des données. Le RGPD a constitué un progrès important, mais l'utilisateur *lambda* doit pouvoir accéder plus facilement à un exposé de ses droits, de manière à prendre conscience de l'utilisation qui est faite de ses données. Techniquement, cela peut être accompli par des tableaux de bord accessibles sur simple demande.

Ce n'est qu'un vœu, cela ne va pas encore très loin, mais cela me paraît tout de même utile.

M. Gérard Longuet, rapporteur. – J'y suis favorable. On pourrait confier une mission d'examen de cette question à l'une des autorités, lesquelles, à défaut de fusionner, devraient mieux coopérer ensemble. Elle pourrait procéder au moins par sondages, en examinant certains des règlements proposés par les plus grands acteurs du secteur. J'ai essayé l'autre jour de consulter les conditions d'usage du Wi-Fi de la SNCF : c'était incompréhensible, même pour moi, qui ne suis pas le plus incompétent des usagers. Les grandes entreprises n'aiment pas être prises la main dans le sac d'une turpitude ; les exposer ainsi à des sondages critiques pourrait être utile. Il faudra y réfléchir ; là encore, le forum institutionnel du numérique que nous recommandons de créer pourrait s'emparer de cette question.

Mme Sylvie Robert. – Ma proposition n° 3 s'apparente à la précédente. Elle a pour objet les *cookies*, des traceurs qui servent à profiler les utilisateurs. La notion de consentement n'est pas claire. L'utilisateur doit être réellement informé et donner son accord par un acte positif ; il s'agit sur ce point de renverser le mécanisme actuel. Cela rejoint le combat mené par la Commission nationale de l'informatique et des libertés (CNIL).

M. Jérôme Bascher. – Je ne vois pas comment cela marcherait. Les sites Internet donnent déjà un choix à l'utilisateur : accepter ou non les conditions d'usage et la collecte des données.

Mme Sylvie Robert. – Il faut renverser le mécanisme. Aujourd'hui, on accepte par défaut.

M. Gérard Longuet, rapporteur. – La jurisprudence impose bien d'interpréter le RGPD de la sorte.

Les propositions n^os^ 2 et 3 sont adoptées.

M. Pierre Ouzoulias. – À l'origine de notre proposition n° 4, il y a un constat : à l'évidence, l'État gère une masse croissante de données ; certaines lui appartiennent, mais d'autres non. Il doit une certaine sécurité aux utilisateurs dont il gère les données. Or nos auditions ont montré l'absence, chez les plus hauts responsables, d'une prise de conscience forte et clairement structurée de l'usage que font les administrations de ces données. Il y a comme un irénisme de la commande publique en matière de logiciels : les administrations se soucient très peu de la confidentialité des données quand elles utilisent des logiciels tiers.

L'objet de cette proposition est donc de demander au Gouvernement de mettre en place une doctrine sur ce sujet. Certaines expériences sont probantes. Ainsi, la gendarmerie nationale a installé sur 80 000 postes un nouveau logiciel qui lui a permis d'économiser 2 à 3 millions d'euros, de résoudre bien des problèmes de formation et de maintenance, et ainsi de faire repartir de nombreux gendarmes sur le terrain. Le logiciel libre est l'une

des solutions, même si ce n'est pas toujours la seule. J'ai été surpris et effrayé du discours tenu devant nous par un représentant de l'administration, selon qui le choix des logiciels dépend avant tout de leur ergonomie pour le fonctionnaire qui les utilisera : c'est une conception assez catastrophique !

M. Gérard Longuet, rapporteur. – Je suis très favorable à cette proposition, car le sujet a été assez mal traité par le Parlement jusqu'à présent. J'en veux pour illustration la loi pour une République numérique. Son article 16 dispose : « Les administrations veillent à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information. Elles encouragent l'utilisation des logiciels libres et des formats ouverts lors du développement, de l'achat ou de l'utilisation, de tout ou partie, de ces systèmes d'information. » Le verbe ici employé, « encourager », n'appartient pas au droit et n'a aucune force juridique. C'est un problème que nous rencontrons trop souvent dans les textes législatifs actuels. On n'encourage pas un condamné à mort à avoir la tête tranchée ! Cela me conforte dans l'idée qu'un débat permanent est nécessaire sur ces sujets.

M. Christophe-André Frassa. – J'étais le rapporteur de cette loi et je sais bien pourquoi on y a fait figurer le terme « encourager ». C'est la quadrature du Net qui l'avait voulu ! Le gouvernement d'alors, et, en particulier, Mme Lemaire, était tout feu tout flammes en faveur du logiciel libre, mais ils n'avaient pas le début du commencement d'une rédaction à proposer. À défaut d'être normatif, on a été vague. Des pans entiers du sujet du numérique ont été ignorés par ce gouvernement ; il nous a fallu débroussailler, puisque l'exécutif était incapable de prévoir et d'anticiper. Certes, il faut aller plus loin, mais on ne peut imposer de favoriser le logiciel libre, dans la mesure où il est parfois impossible d'y avoir recours du fait d'un manque de techniciens.

M. Gérard Longuet, rapporteur. – C'est tout à fait compréhensible, il ne faut pas jeter la pierre. On ne peut pas pour autant se contenter de la formule actuelle ; c'est pourquoi nous devons remettre le sujet à l'ordre du jour.

M. Pierre Ouzoulias. – Il s'agit de demander au Gouvernement de fournir aux ministères, aux diverses administrations, l'expertise qu'ils n'ont pas. L'Éducation nationale en particulier est aujourd'hui incapable de développer des solutions internes. Il faut mutualiser les compétences de manière interministérielle.

La proposition n° 4 est adoptée.

Mme Martine Filleul. – Ma proposition n° 5 vise à nous inviter à une plus grande vigilance en faveur de la mixité femmes-hommes dans le secteur du numérique. On compte seulement 27 % de femmes dans le secteur du numérique ; elles ne sont que 11 % dans la cybersécurité. Cela représente une déperdition importante de talents et donc un danger pour l'avenir : le monde qui est en train de se mettre en place risque d'être un monde

d'hommes pour les hommes ! On cite souvent le cas d'un algorithme conçu par un géant du commerce en ligne pour trier les *curriculum vitae* ; il s'est avéré qu'il traitait de manière préférentielle ceux des hommes. En République, il nous faut être vigilants sur l'égalité.

M. Gérard Longuet, rapporteur. –Je suis tout à fait favorable à cette idée. Je suis plus nuancé quant à la place des femmes au sein de l'armée, mais c'est une position très personnelle.

La proposition n° 5 est adoptée à l'unanimité.

M. Franck Montaugé, président. – Il nous revient maintenant d'adopter le rapport ainsi rédigé et d'autoriser sa publication ainsi que celle des documents annexés – il s'agit notamment du compte rendu de la présente réunion, et des auditions publiques figurant au tome II.

La commission adopte à l'unanimité le rapport ainsi modifié, ainsi que les annexes, et en autorise la publication.

M. Franck Montaugé, président. – Enfin, comme c'est l'usage, je vous propose, mes chers collègues, d'autoriser le secrétariat à procéder aux modifications de forme nécessaires à la publication du rapport.

Il en est ainsi décidé.

La réunion est close à 19 h 55.

LISTE DES PERSONNES ENTENDUES PAR LA COMMISSION

16 mai 2019

M. Pierre BELLANGER, président-directeur-général de Skyrock.

23 mai 2019

Mme Claire LANDAIS, secrétaire générale du Secrétariat général de la défense et de la sécurité nationale (SGDSN), **MM. Julien BARNU**, conseiller pour les questions industrielles et numériques et **Gwenaël JEZEQUEL**, conseiller pour les relations internationales.

MM. Nicolas MAZZUCHI, chargé de recherche à la Fondation pour la recherche stratégique, **Julien NOCETTI**, chercheur à l'Institut français des relations internationales et **Christian HARBULOT**, directeur de l'École de guerre économique.

M. Benoît THIEULIN, ancien président du Conseil national du numérique, rapporteur de l'avis « Pour une politique de souveraineté européenne du numérique » adopté par le Conseil économique, social et environnemental.

M. Bernard BENHAMOU, secrétaire général de l'institut de la souveraineté numérique.

28 mai 2019

M. Thierry BRETON, président-directeur général d'ATOS.

4 juin 2019

M. Henri VERDIER, ambassadeur du numérique.

Mmes Pauline TÜRK, professeur de droit public à l'université Côte d'Azur et **Annie BLANDIN**, professeur à l'IMT Atlantique, membre du Conseil national du numérique.

MM. Jean-Gabriel GANASCIA, président du comité d'éthique du CNRS, **Éric GERMAIN**, chargé de mission « éthique des nouvelles technologies, fait religieux et question sociétale » à la direction générale des relations internationales et de la stratégie du ministère des armées, et **Claude KIRCHNER**, directeur de recherche émérite à l'Institut national de recherche dédié aux sciences du numérique.

12 juin 2019

MM. Thomas COURBE, directeur général des entreprises et commissaire à l'information stratégique et à la sécurité économique, et **Mathieu WEILL**, chef du service de l'économie numérique à la direction générale des entreprises (DGE).

Mme Claire MATHIEU, directrice de recherche au CNRS.

M. Éric LÉANDRI, président et cofondateur de Qwant.

20 juin 2019

M. Cédric O, secrétaire d'Etat auprès du ministre de l'Economie et des Finances et du ministre de l'Action et des Comptes publics, chargé du Numérique.

25 juin 2019

M. Nadi BOU HANNA, directeur interministériel du numérique et du système d'information et de communication de l'État au ministère de l'action et des comptes publics.

Général François LECOINTRE, chef d'État-Major des armées (CEMA), **général de division Olivier Bonnet de PAILLERETS**, commandant cyber de l'état-major des armées et **général de brigade Jean-Jacques PELLERIN**, chef de la division de l'état-major des armées, en charge du numérique et de la cohérence des programmes interarmées.

2 juillet 2019

M. Jean-François FERLET, directeur à la direction du renseignement militaire (DRM) (à huis clos).

M. Nicolas LERNER, directeur général de la sécurité intérieure (DGSI) (à huis clos).

M. Eric BUCQUET, Directeur de la direction du renseignement et de la sécurité de la défense (DRSD) (à huis clos).

9 juillet 2019

Me Alexis FITZJEAN O COBHTHAIGH, avocat, **M. Axel SIMON** (La Quadrature du Net), **M. Étienne GONNU**, chargé affaires publiques (April - Promouvoir et défendre le logiciel libre) et **Me Olivier ITEANU**, avocat (ISOC France).

10 juillet 2019

M. Daniel BURSAUX, directeur général de l'Institut national de l'information géographique et forestière (IGN), **MM. Sylvain LATARGET**, directeur général adjoint, et **Claude PÉNICAND**, délégué à la stratégie de l'établissement.

Mme Marie-Laure DENIS, présidente de la CNIL, **MM. Gwendal LE GRAND**, secrétaire général adjoint, et **Mathias MOULIN**, Directeur de la Direction de la protection des droits et des sanctions.

Mme Isabelle de SILVA, présidente de l'Autorité de la concurrence, **M. Roch-Olivier MAISTRE**, président du CSA et **M. Sébastien SORIANO**, président de l'Arcep.

11 juillet 2019

M. Guillaume POUPARD, directeur général de l'ANSSI (à huis clos).

M. Michel PAULIN, directeur général d'OVH.

M. François VILLEROY DE GALHAU, Gouverneur de la Banque de France.

17 juillet 2019

MM. Laurent GIOVACHINI, pour le « Comité souveraineté et sécurité des entreprises françaises » du Medef et le Syntec numérique et **Christian NIBOUREL**, du Medef.

M. Loïc RIVIÈRE, Délégué général de Tech in France.

M. Benoît TABAKA, secrétaire général adjoint de Google France.

18 juillet 2019

M. Anton'Maria BATTESTI, responsable des affaires publiques de Facebook.

MM. Marc MOSSÉ, directeur juridique et affaires publiques de Microsoft Europe et **Mathieu COULAUD**, directeur juridique de Microsoft France.

MM. Laurent DEGRÉ, Directeur général, **Guillaume DE SAINT-MARC**, Directeur de l'innovation, **Jean-Charles GRIVIAUD**, Responsable cybersécurité, **Bruno BERNARD**, Directeur des affaires publiques, **Mme Pascale SEROT**, de CISCO France.

MM. Weiliang SHI, directeur général, **Benjamin HECKER**, directeur juridique et de la protection des données, et **Gwenaël ROUILLEC**, directeur de la cybersécurité, de Huawei France.

2 septembre 2019

M. Christophe CASTANER, ministre de l'intérieur.

M. Bruno SPORTISSE, Président-directeur général de l'INRIA.

3 septembre 2019

Mme Nicole BELLOUBET, garde des sceaux, ministre de la justice.

Mme Florence PARLY, ministre des armées.

MM. Julien GROUES, directeur général et **Stephan HADINGER**, directeur technique pour Amazon Web services.

MM. Michel COULOMB, responsable des ventes, région sud incl. France, **Daniel MATRAY**, responsable App Store Europe, et **Erik NEUENSCHWANDER**, responsable vie privée des utilisateurs, d'Apple.

10 septembre 2019

M. Bruno LE MAIRE, ministre de l'économie et des finances.

LISTE DES PERSONNES ENTENDUES PAR LE PRÉSIDENT ET LE RAPPORTEUR

12 juin 2019

M. Bernard STIEGLER, philosophe et spécialiste des transformations de la société à l'ère numérique.

2 juillet 2019

MM. Frédéric POTIER, Serge ABITEBOUL et **Benoît LOUTREL**, membres de la mission « Régulation des réseaux sociaux - Expérimentation Facebook ».

M. Patrick PAILLOUX, directeur technique de la DGSE.

8 juillet 2019

M. Michel DEVERDET, secrétaire général d'Enedis.

M. Arnaud VIEUX, directeur général délégué de Tecwec Systems.

9 juillet 2019

M. Jean-Yves Le GALL, président du centre national d'études spatiales.

M. Raphaël GAUVAIN, député, chargé de mission sur la protection contre les législations de portée extraterritoriale.

M. Guillaume de MALZAC, président de AR 24.

10 juillet 2019

Mme Domitille DESSERTINE, directrice de la division « Fintech, Innovation et Compétitivité » à l'Autorité des marchés financiers, **M. Vincent LORPHELIN**, entrepreneur, coprésident de l'Institut de l'Iconomie et **M. Alexandre STACHTCHENKO**, cofondateur de Blockchain Partner, président de la Chaintech.

11 juillet 2019

M. Tariq KRIM, entrepreneur, fondateur de Netvibes et de Jolicloud.

Mme Clara LAHIANI, chercheur, fiscaliste internationale chez Kerin, **Mme France VASSAUX D'AZÉMAR DE FABRÈGUES**, directrice générale adjointe de France Invest et **M. Paul-François FOURNIER**, directeur exécutif de Bpifrance en charge de l'innovation.

17 juillet 2019

M. Hugues FOULON, directeur de la stratégie et des activités de cyber-sécurité d'Orange, **M. Laurentino LAVEZZI**, directeur des affaires publiques d'Orange et **Mme Claire CHALVIDANT**, directrice des affaires institutionnelles d'Orange.

M. Philippe PIRON, président d'Alcatel submarine networks.

18 juillet 2019

M. Jean-René LEQUEPEYS, directeur des programmes & directeur adjoint du CEA-Leti.

M. Laurent VACHEY, **Mme Claudine DUCHESNE** et **M. Laurent CYTERMANN**, auteurs du rapport sur les données d'intérêt général.

DÉPLACEMENT À BRUXELLES LES 17 ET 18 JUIN 2019

LUNDI 17 JUIN

Contrôleur Européen de la Protection des Données (CEPD / EDPS)
- Entretien avec M. Wojciech Wiewiórowski, contrôleur adjoint

Représentation permanente de la France auprès de l'UE
Entretien avec :
- M. Guillaume Drano, conseiller fiscalité
- M. Mickael Bazin, conseiller industrie, télécommunications et société de l'information
- M. Pascal Rogard, conseiller numérique, télécommunications et postes

Cabinet de M. Julian King, commissaire à la sécurité
- Entretien avec Mme Severine Wernert, conseillère terrorisme, cyber-espace, crime organisé, cooperation policière
- et M. Ulrik Trolle Smed, conseiller cyber-sécurité, justice criminelle, autonomie stratégique

Cabinet de Mme Věra Jourová, commissaire justice, consommateurs et parité
- Entretien avec M. Wojtek Talko, conseiller protection des données, régulation de la protection des données et aspects internationaux de la protection des données

Service européen d'action extérieure (SEAE)
- Entretien avec M. Wiktor Staniecki, chef d'unité cyber-sécurité à la direction politique de sécurité et de défense

MARDI 18 JUIN

DG for Communications Networks, Content and Technology
- Entretien avec M. Roberto Viola, directeur général

DG Stabilité financière, services financiers et Union des marchés de capitaux
- Entretien M. Olivier Guersent, directeur général

Coordination européenne pour la lutte contre le terrorisme
- Entretien avec M. Emmanuel Saliot, conseiller de M. Gilles de Kerchove, coordinateur de la lutte contre le terrorisme, auteur d'un rapport sur les risques de la 5G pour la lutte contre le terrorisme

ANNEXE 1 : LES GAFAM OU LE PAROXYSME DE LA PUISSANCE ÉCONOMIQUE FACE À L'ÉTAT

a) Les Gafam ont atteint une ampleur systémique

Les Gafam déploient leurs activités à travers le monde. Leur taille sans précédent peut se vérifier à leur **nombre d'utilisateurs, leur capitalisation boursière, leur chiffre d'affaires et leur part mondiale de marché.** Ainsi, Facebook revendique près de deux milliards et demi d'utilisateurs. La quasi-totalité des systèmes d'exploitation des téléphones intelligents sont équipés par Google ou Apple, et la quasi-totalité des systèmes d'exploitation des ordinateurs personnels par Microsoft ou Apple. Ces quelques acteurs économiques sont devenus incontournables pour se rendre sur internet – à travers les systèmes d'exploitation des terminaux – comme pour s'y mouvoir – pour effectuer une recherche, interagir avec ses amis, y faire ses achats… De même une entreprise souhaitant développer son activité sur les téléphones intelligents est contrainte de passer par les magasins d'application d'Apple et de Google.

La **valorisation boursière** cumulée des Gafam dépasse 4 000 milliards de dollars, soit **plus de deux fois celle de la totalité du CAC 40**.

Les Gafam sont, depuis plusieurs années maintenant, les premières capitalisations boursières mondiales. Avant la crise de 2008, seule Microsoft était déjà dans le peloton de tête de la valorisation boursière. La crise économique a joué un rôle accélérateur de la concentration du marché numérique : on a pu parler alors d'un « hold-up d'internet » par les entreprises de la tech devenues systémiques après la crise économique, édictant leurs règles, très éloignées des objectifs des fondateurs du World Wide Web.

Aujourd'hui, **sept des dix premières capitalisations boursières mondiales sont issues du secteur numérique. L'ascension des acteurs chinois** du numérique est remarquable : Alibaba (l'Amazon chinois) et Tencent (conglomérat de services en ligne, qui détient notamment l'application WeChat, comparable à la fois à Facebook, Skype, WhatsApp, Paypal et Instagram) étaient valorisées au 1er juillet dernier respectivement 438 et 430 milliards de dollars, soit les septième et huitième capitalisations mondiales.

Les **chiffres d'affaires des Gafam sont comparables aux ressources fiscales françaises**[1]. Ainsi, les revenus d'Amazon en 2017 équivalaient au produit de la taxe sur la valeur ajoutée en France – qui est la première recette

[1] *Comparables mais pas équivalents : près de 650 milliards de dollars en 2017 pour un peu plus de 650 milliards d'euros la même année.*

fiscale de l'État[1]. Ceux d'Apple s'approchaient du tiers de la totalité des recettes fiscales de l'État français[2].

L'ampleur systémique des Gafam leur permet d'optimiser leur positionnement sur les marchés mondiaux. Quel que soit le secteur, **leur objectif semble être le contrôle des marchés**, depuis la vente de livres à la location de logements de tourisme, en passant par le service de transport avec chauffeur aujourd'hui, sans chauffeur demain avec les véhicules autonomes.

b) Ils développent des services en concurrence avec les missions régaliennes de l'État

Dans une logique « solutionniste » d'inspiration libertarienne récusant les tutelles étatiques, les grands acteurs du numérique proposent d'assumer à la place des États un certain nombre de prérogatives qui relevaient de leur souveraineté classique comme, par exemple :

- **battre monnaie**, avec le libra de Facebook ;

- établir une **cartographie** et donc, *in fine*, un cadastre[3], avec Google Maps ;

- attribuer puis vérifier les **identités** – comme, par exemple, avec le service Facebook Connect et le développement de solutions de reconnaissance faciale ;

- concourir à la **sécurité intérieure** – avec le Facebook Safety Check ;

- concourir à l'exercice de la **justice**, à travers le projet de « cour suprême » de Facebook[4].

La secrétaire générale de la défense et de la sécurité nationale a également souligné la remise en cause du monopole de la **violence** légitime : « *Face à une menace cyber qui ne cesse de croître, certains acteurs, essentiellement étatsuniens, remettent en cause le monopole des États dans l'usage de la violence légitime. Se fondant sur une interprétation discutable du droit à la légitime défense*

---

[1] *Près de 178 milliards de dollars pour 152,4 milliards d'euros.*

[2] *Près de 230 milliards de dollars pour 217 milliards d'euros.*

[3] *Celui-ci fait d'ailleurs régulièrement l'objet de polémiques en cas de situation géopolitique délicate : l'entreprise fait ainsi prévaloir l'interprétation de l'État dans lequel l'utilisateur se trouve pour afficher les résultats, plutôt que ceux du droit international. C'est ainsi que Google Maps affiche une frontière en pointillés entre l'Ukraine et la Crimée lorsque l'on se connecte en dehors de Russie, mais que la frontière est pleine lorsque l'utilisateur se connecte en Russie. Voir, par exemple, L'Obs, Google Maps, des frontières à la carte pour ne froisser personne, 6 juin 2015. Devant votre commission d'enquête, le directeur général de l'IGN rappelait :* « On se souvient encore, en 2014, de la complaisance de Google vis-à-vis des régimes russe et ukrainien lors de la crise de Crimée : selon le pays dans lequel on se connectait, les frontières n'étaient pas tout à fait les mêmes. On peut également citer la question du Tibet vue par les Chinois ou encore celle du Sahara occidental vue par le Maroc ».

[4] *Lors de son audition, Jean-Gabriel Ganascia a également souligné que les grands acteurs du numérique* « peuvent aussi se développer dans le domaine de la justice, avec l'idée de justice prédictive ».

dans l'espace cyber, qui n'est pas la nôtre, ils font la promotion d'une doctrine offensive de réponse aux attaques, autorisant une riposte par les acteurs privés eux-mêmes (« hack back ») qui va au-delà de la simple protection de leurs propres systèmes d'information, autorisant par exemple des intrusions dans les systèmes adverses pour les détruire. »

Annie Blandin a même estimé devant votre commission que ces entreprises développent une nouvelle composante de la souveraineté, « *qui consiste à produire ou à utiliser des données, et à maîtriser l'accès à l'information* ».

Pour de nombreux cas – la cartographie, l'identité numérique et demain peut-être la monnaie – on constate ainsi une **forme de concurrence, dont l'usager est l'arbitre**, entre les services étatiques et ceux redoutablement performants, ergonomiques, et apparemment gratuits proposés par ces « entreprises souveraines ».

c) Ils font preuve d'un rapport ambigu aux législations nationales

(1) Ces acteurs établis à l'étranger sont des spécialistes de l'optimisation juridique et fiscale

De nombreux pans du droit ne sont pas tout à fait adaptés à l'économie numérique, ce qui permet aux grands acteurs, dotés d'importants moyens juridiques, de tirer profit de tous les interstices qui leurs sont favorables. Ils choisissent également de s'implanter dans les États dans lesquels un droit plus souple est en vigueur. Ils sont en quelques sortes les spécialistes du paradis juridique et fiscal. Devant votre commission, Pierre Bellanger a considéré que « *machines, réseaux, programmes, services ne répondent pas de nos lois* ».

Ainsi, comme l'a noté le rapport de la mission sur la régulation des réseaux sociaux[1], le **principe du pays d'origine applicable au niveau européen** confie le rôle de régulateur au seul État membre dans lequel le service a établi son siège social. En conséquence, le pays accueillant le siège social de l'entreprise concernée ne lutte pas contre les pratiques dommageables à l'extérieur de son territoire et les États les subissant sont impuissants à y remédier.

(2) Réciproquement, ils créent leurs propres normes…

Du fait de leur caractère transnational, les **conditions générales d'utilisation** (CGU) de ces géants de la « tech » créent un droit applicable à leurs services qui, par une inversion de la hiérarchie des normes, se retrouve au-dessus de celui des États. Annie Blandin considère que les CGU « *se présentent comme de véritables lois de l'internet* »[2].

---

[1] *Mission « Régulation des réseaux sociaux – Expérimentation Facebook », Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne, mai 2019.*
[2] *Article précité.*

Or, ces « lois » sont des **vecteurs de valeurs qui ne sont pas forcément les nôtres**. Comme le relevait Pierre Bellanger dans son ouvrage sur la Souveraineté numérique, la nudité ou la violence sont traitées selon des référentiels culturels américains et non européens. Pendant longtemps, certains acteurs comme Facebook ont d'ailleurs maintenu des **clauses** attributives de compétence **illégales** en ce qu'elles octroyaient aux tribunaux américains la compétence pour trancher un litige.

On constate, par ailleurs, qu'**invoquer une violation de ces conditions d'utilisation est parfois plus efficace qu'attendre le traitement d'une plainte par les autorités locales**. La presse avait ainsi relayé l'étonnement du directeur général des douanes et des droits indirects sur la promptitude de Facebook à censurer le partage de « L'origine du monde » de Gustave Courbet, jugé non-conforme à ses règles d'utilisation[1], au regard du manque de diligence de la firme à retirer des annonces pour des ventes de produit de contrebande[2].

Comme l'a rappelé Pierre Bellanger devant votre commission d'enquête, parfois, l'État ne parvient pas à faire appliquer sa volonté : « *à l'été 2016, quelques dizaines de Français ont été mis à mort sur une messagerie chiffrée. L'État français a tenté de faire interdire ce service, de faire retirer la liste, mais les plateformes ont refusé de fermer l'application. L'État s'est trouvé démuni face à la mise en danger de ses citoyens* ».

Autre exemple : le 25 septembre dernier, Google a annoncé sa volonté de ne pas appliquer la loi sur les droits voisins des agences de presse et des éditeurs de presse[3] votée en France à l'unanimité des deux assemblées en application d'une directive européenne[4].

En somme, on rappellera les termes utilisés par Pauline Türk, qui résumait la situation devant votre commission de la façon suivante : « *Les multinationales américaines (…) disposent de facto du pouvoir d'imposer des règles. Elles bénéficient d'une suprématie grâce à leur position dominante sur le marché, et sont les véritables pouvoirs souverains dans le cyberespace. Qui fixe les conditions générales d'utilisation ? Qui est en situation de monopole pour la fourniture de services devenus indispensables ? Qui a le pouvoir de se faire obéir ? Qui peut décider de supprimer des contenus, de censurer un tableau, de fermer le profil d'un*

---

[1] *Lors de son audition par votre commission, le représentant de l'entreprise Facebook a cependant confirmé qu'il est désormais possible de publier une telle image sur le réseau social :* « Je tiens à le réaffirmer devant vous. Ce tableau est autorisé, et de manière générale, la peinture de nu est autorisée. (…) il y a eu une erreur de modération sur ce tableau. ».

[2] *La lettre A, Après le fisc, les douanes aussi s'intéressent aux fraudeurs sur Facebook, 22 novembre 2018.*

[3] *Loi n° 2019-775 du 24 juillet 2019 tendant à créer un droit voisin au profit des agences de presse et des éditeurs de presse.*

[4] *Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE.*

Voir, sur ce sujet, le communiqué de presse de la commission de la culture, de l'éducation et de la communication du Sénat, en date du 26 septembre dernier.

utilisateur – cela équivaut à une mort sociale, notamment pour la jeune génération – , de vendre des données personnelles, de ne pas rendre des données stockées sur un cloud ? Ce sont toujours les mêmes : Google, Amazon, Facebook, Apple, etc ».

(3) …et entendent influencer la décision publique

Dotés d'importants moyens financiers, ils entendent **peser sur la prise de décision publique** comme aux États-Unis, en Europe. Lors des débats sur la directive dite « droits d'auteur »[1], imposant aux géants du numérique de verser de tels droits aux créateurs de contenus diffusés sur des plateformes numériques telles que Google Actualité ou encore YouTube, le lobbying fut particulièrement intense et agressif. Lors de son audition, Benoît Thieulin a ainsi affirmé : « *Par leur activisme contre la directive sur le droit d'auteur, les plateformes m'ont profondément choqué : elles ont utilisé leur propre force de frappe à des fins de propagande. Il s'agit là d'un véritable problème démocratique* ».

Ce phénomène va croissant. Entre 2011 et 2017, les dépenses de lobbying de Google auprès des instances de l'Union européenne sont passées d'un à six millions d'euros[2].

[1] *Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE.*

[2] *Source : registre de transparence de la Commission européenne. Il convient de noter que ce registre n'est pas exhaustif car il ne couvre qu'environ 300 fonctionnaires sur les 30 000 de la Commission européenne.*

ANNEXE 2 : SYNTHÈSE DES RAPPORTS DE L'OPECST

1. Souveraineté numérique et sécurité numérique

⇨ ***Le risque numérique : en prendre conscience pour mieux le maîtriser ?***

Rapport n° 721 (2012-2013), MM. Bruno Sido, sénateur et Jean-Yves Le Déaut, député

Face au risque numérique, **deux grands domaines d'action** étaient identifiés par le rapport :

(i) **Favoriser l'émergence d'acteurs européens**, y compris pour la collecte et le stockage des données. Le rapport soulignait également que **les exemples asiatiques pourraient inspirer les Européens**, puisqu'ils proposent leurs propres services de l'Internet ;

(ii) **Se protéger contre des technologies qui pourraient nuire à la sécurité des États**. Ainsi, il était proposé d'interdire à l'échelle européenne le développement d'équipements de cœur de réseau d'origine chinoise et présentant un risque pour la sécurité nationale. Il s'agissait là « d'un **enjeu de souveraineté nationale, voire de souveraineté européenne partagée** ». Était enfin envisagée, à terme, et en parallèle de l'Europe de l'aéronautique ou du spatial, la création d'une **Europe des industries de la cybersécurité**. La cybersécurité fait en effet partie, selon le capitaine de vaisseau Alexis Latty, du **premier cercle de souveraineté**.

⇨ ***Sécurité numérique et risques : enjeux et chances pour les entreprises***

Rapport n° 271 (2014-2015), Mme Anne-Yvonne Le Dain, députée, et M. Bruno Sido, sénateur

L'omniprésence du numérique, au-delà de ses potentialités, présente aussi un risque pour les entreprises. Devant l'ampleur possible des dommages des attaques, **les États doivent protéger leurs infrastructures critiques et leurs opérateurs d'importance vitale ; c'est une condition de souveraineté numérique**. La sécurité du numérique mêle le militaire et le civil, le professionnel et le personnel.

Le rapport recommande d'**assurer les conditions de l'autonomie numérique pour préserver la souveraineté française**. En effet, les règles relatives à la mise en place d'Internet sont d'abord le fait de certaines sociétés commerciales et de leur État d'origine. **Ce n'est pas le droit qui**

prévaut, mais les rapports de force entre États et entre acteurs privés. En outre, la complexité du numérique freine parfois les efforts des entreprises pour en assurer la sécurité. Les comportements humains, même accidentels, sont à l'origine d'importantes failles et, in fine, d'attaques, ce qui justifie de meilleurs campagnes de sensibilisation et d'information sur la sécurité du numérique. Enfin, le rapport recommande de ne pas intégrer le numérique dans les accords de libre-échange conclus par l'Union européenne tant que des **garanties** ne s'imposeront pas **pour la protection des données personnelles et la gouvernance d'Internet.**

⇨ ***Les zones à régime restrictif (ZRR) dans le cadre de la protection du potentiel scientifique et technique de la Nation***

Rapport n° 402 (2018-2019), MM. Cédric Villani, député, et Gérard Longuet, sénateur

Le dispositif des ZRR est au cœur du régime de protection du potentiel scientifique et technique, régi par le secrétariat général de la défense et de la sécurité nationale (SGDSN). Au sein des établissements de recherche, privés ou publics, **les ZRR protègent l'accès, physique ou virtuel**, aux savoirs et aux technologies sensibles. Ce dispositif, qui vise à protéger la sécurité de la France mais aussi de ses entreprises, est **critiqué par une partie de la communauté scientifique pour les lourdeurs qu'il occasionne** (délai d'autorisation des candidats, communication entre chercheurs, coopération avec une entreprise étrangère…). Pour autant, l'Anssi estime que des **menaces informatiques graves pèsent sur la recherche**.

Pour concilier ces deux impératifs de sécurité et de flexibilité, l'OPESCT suggère d'adapter le dispositif des ZRR en y introduisant une gradation en fonction des risques ; de protéger des projets sensibles et non des secteurs au sens large ; de développer une culture de sécurité pour tous les acteurs impliqués, en diminuant la part des mesures contraignantes.

2. <u>Souveraineté numérique et évolutions technologiques</u>

⇨ ***Pour une intelligence artificielle maîtrisée, utile et démystifiée***

Rapport n° 464 (2016-2017), M. Claude de Ganay, député, et Mme Dominique Gillot, sénatrice

L'intelligence artificielle renvoie à de nombreuses technologies reposant sur l'utilisation d'algorithmes. **Parmi les enjeux soulevés par ces technologies**, le rapport pointait **la place prépondérante de la recherche**

privée, dominée par les entreprises américaines et, bientôt, chinoises ; la place de la France et de l'Europe dans cette compétition mondiale ; le passage à une économie dominée par des plateformes ou, encore les biais et problèmes posés par les données.

Outre le développement de compétences, par la formation ou à l'école, le rapport préconisait de **soutenir la constitution de champions européens en intelligence artificielle**, tout en soutenant les PME spécialisées, notamment les start-up. En effet, **la domination de la recherche privée, mais aussi des grandes entreprises « plateformistes »**, touche « aux **problématiques de souveraineté et d'indépendance nationale** », alors que « **la colonisation numérique américaine est une réalité incontestable** » et que des acteurs comme la Chine ou d'autres pays émergents (Inde) s'imposent de plus en plus dans ce domaine.

⇨ ***Les enjeux technologiques des blockchains (chaînes de blocs)***

Rapport n° 584 (2017-2018), MM. Valéria Faure-Muntian, Claude de Ganay, députés, et Ronan Le Gleut, sénateur

Les **blockchains** sont des **technologies de stockage et de transmission d'informations**, utilisant des **réseaux décentralisés** pair à pair, **sans organe central de contrôle**, et **sécurisés grâce à la cryptographie**. Ce sont les **technologies sous-jacentes aux cryptomonnaies**, comme le bitcoin, mais elles ont aussi **d'autres applications** (ex. services d'attestation et de certification pour l'état civil, le cadastre, les contrats de type notarié, la protection de la propriété intellectuelle). Les transactions effectuées par les utilisateurs sont regroupés en bloc et **chaque bloc est validé par des « mineurs »**. Ces mineurs se sont parfois organisés en groupement, pour mutualiser leurs ressources informatiques et énergétiques.

Toutefois, **quatre groupements, dont trois chinois, assurent aujourd'hui 60% de la puissance de calcul nécessaire à la blockchain du bitcoin** et le risque est qu'ils utilisent cette position dominante contre l'intérêt des autres utilisateurs. Enfin, les blockchains doivent aussi **répondre à un enjeu environnemental et énergétique**, alors que les activités de minage sont très intensives en électricité (24TWh/an pour le seul bitcoin).

⇨ ***Les perspectives technologiques ouvertes par la 5G***

Rapport n° 188 (2018-2019), MM. Pierre Henriet, député, et Gérard Longuet, sénateur

La cinquième génération de standards de téléphonie mobile (« 5G ») est annoncée comme une **innovation de rupture**. Allant plus loin qu'une

simple augmentation des débits, **elle aura des impacts autant techniques qu'économiques et sociétaux** (ex. les usages liés à l'internet des objets). Ces avancées devraient permettre de **couvrir des besoins spécifiques dans des secteurs critiques tels que l'énergie** (production, stockage ou transport de l'énergie), la santé (télémédecine) ou les transports (réactivité des véhicules autonomes).

Le déploiement de la 5G implique cependant de répondre à plusieurs questions, dont certaines ont trait à la **souveraineté numérique de la France** : **attribution des fréquences** (choix des opérateurs) ; coopération européenne ou mondiale ; **sécurisation des réseaux** (la 5G sera totalement virtualisée, tout pourra donc se localiser dans un *cloud*, dans n'importe quel pays).

3. Souveraineté numérique et santé

⇨ ***Le numérique au service de la santé***

Rapport n° 465 (2014-2015), M. Gérard Bapt, député, Mme Catherine Procaccia, sénateur

Les domaines concernés par la révolution numérique dans le secteur de la santé sont nombreux : la télémédecine, la prévention, le décloisonnement entre la ville et l'hôpital, le suivi d'une maladie chronique à distance, les dossiers médicaux électroniques, les applications de santé sur téléphone portable, la domotique et le maintien à domicile. Le numérique apparait alors comme un **élément de solution aux difficultés rencontrées par notre système de soins**.

Toutefois, le numérique soulève aussi plusieurs problèmes, concernant notamment **la sécurité et la confidentialité des informations des patients**.

⇨ ***L'intelligence artificielle et les données de santé***

Rapport n° 401 (2018-2019), MM. Cédric Villani, député, et Gérard Longuet, sénateur

La mise en œuvre de la stratégie nationale pour l'intelligence artificielle dans le domaine de la santé passe par **la collecte des données, leur organisation et la régulation de leurs modalités d'accès et d'utilisation**. De leurs auditions, les membres de l'OPESCT retiennent que notre système de santé aurait tort de ne pas s'ouvrir à l'intelligence artificielle, au numérique et au pilotage par les données**. Le second risque**

serait de se voir développer des algorithmes étrangers, privés, et donc non régis par les règles françaises (cadre éthique, protection des données). Enfin, les auditions et débats de l'OPESCT avaient montré que **l'articulation entre les acteurs privés et la puissance publique était délicate**, puisqu'il s'agissait tant d'encourager l'innovation privée que de garder le contrôle d'un processus impliquant des millions de données personnelles.

ANNEXE 3 : RAPPORT ÉTUDIANT LA POSSIBILITÉ DE CRÉER UN COMMISSARIAT À LA SOUVERAINETÉ NUMÉRIQUE

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES

TELEDOC 792
BATIMENT NECKER
120, RUE DE BERCY
75572 PARIS CEDEX 12

N° 2016/27/CGE/SG

Mars 2017

RAPPORT ÉTUDIANT LA POSSIBILITÉ DE CRÉER UN COMMISSARIAT À LA SOUVERAINETÉ NUMÉRIQUE

Rapport à

Monsieur le Ministre de l'Économie et des finances

établi par

Jean CUEUGNIET
Ingénieur général des Mines

Philippe LOUVIAU
Ingénieur général des Mines

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

SOMMAIRE

SYNTHESE

Adopté à l'initiative du Parlement, l'article 29 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique prévoit que « *Le Gouvernement remet au Parlement, dans un délai de trois mois à compter de la promulgation de la présente loi, un rapport sur la possibilité de créer un Commissariat à la souveraineté numérique rattaché aux services du Premier ministre, dont les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège. Ce rapport précise les moyens et l'organisation nécessaires au fonctionnement du Commissariat à la souveraineté numérique*. »

L'audition de la plupart des acteurs concernés par ce sujet, notamment les parlementaires à l'origine de l'amendement confirme le constat relevé dans l'exposé des motifs sur le fait que la France et l'Europe sont en retard dans le domaine stratégique et en forte croissance du numérique. La maîtrise du Cyberespace est le nouvel enjeu du 21e siècle, et le domaine de l'Internet, créé par les USA est aujourd'hui dominé par les entreprises américaines (les GAFAM, et autres Uber ou AirBnB…), et le sera peut-être aussi demain par la Chine, dès lors qu'elle a réussi à faire émerger, sur son territoire national protégé, des géants capables d'envahir le monde.

La plupart des secteurs sont touchés par cette suprématie étrangère, que ce soit au niveau des matériels (routeurs et équipements de Télécom, ordinateurs, mobiles…), des logiciels et systèmes d'exploitation (Windows, MS Office, Android…) et des acteurs du Web précités. Le système conduit à un transfert massif des données et de la valeur ajoutée vers ces nouveaux acteurs.
Cette situation pose un problème de souveraineté à la fois parce que les informations stratégiques de l'Etat sont gérées par des systèmes sur lesquels nous n'avons qu'une maîtrise partielle, et aussi parce que les acteurs économiques français sont de plus en plus dépendants des acteurs étrangers auxquels ils concèdent une part non négligeable de la valeur ajoutée : les « Store » prennent 30 % de commission sur les applications qu'ils hébergent.

A quelques exceptions près, la sphère étatique réussit néanmoins à protéger ses informations stratégiques, grâce aux actions que les directions en charge du sujet ont pu prendre : Création de la DINSIC[1] et du RIE[2], obligations de sécurité faites aux Organismes d'importance vitale via la Loi de Programmation Militaire, stockage sur le territoire français des données de l'Etat et des collectivités locales. Le problème se situe plutôt au niveau de l'économie en général et de la dépendance accrue aux plateformes du web et aux systèmes de type Cloud. Malgré quelques avancées comme le Règlement général de protection des données, et des procédures en cours au niveau de l'UE contre quelques géants du web, le domaine de la fiscalité et du partage de la valeur ajoutée reste un problème majeur, de même que l'incapacité de la France et de l'Europe à faire émerger des acteurs de taille internationale. En effet, le numérique a un très fort effet de réseau et les start-ups françaises ne réussissent que rarement à atteindre la taille critique nécessaire.

[1] DINSIC : Direction interministérielle du numérique et du système d'information et de communication de l'Etat

[2] RIE : Réseau Interministériel de l'Etat

L'opportunité d'un Commissariat à la souveraineté numérique, tel que prévu dans l'exposé des motifs de la loi et donc axé sur la sphère étatique ne semble pas s'imposer car les directions en place, pour beaucoup au niveau des services du Premier ministre (SGDSN, DINSIC, SGMAP), ont la capacité de mettre en œuvre une politique de souveraineté dès lors qu'il y a une volonté politique en écho. C'est cette volonté politique qui doit primer, pour imposer par exemple l'usage de logiciels libres à l'Education nationale ou soutenir l'industrie des composants cryptologiques, plutôt que la création d'un Commissariat.

Sur le second volet, relatif à la transformation numérique de l'économie, la mobilisation est absolument nécessaire pour redresser nos positions dans le domaine du numérique. La bataille n'est pas perdue dans ce milieu bouillonnant d'innovations où des acteurs se créent régulièrement et où les positions ne sont jamais acquises. La mission a listé quelques actions possibles dont plusieurs nécessitent une action au niveau européen, soit parce que la fiscalité nécessite un accord européen, soit parce qu'il convient de faire naître un marché européen homogène mais protégé, de telle sorte que nos start-ups puissent bénéficier d'emblée d'un marché d'un demi-milliard de personnes. Le fait de pouvoir privilégier l'achat local (via un Small Business Act) est aussi à négocier à Bruxelles. Une implication plus forte dans le capital risque est enfin souhaitable pour permettre aux jeunes pousses d'atteindre la taille critique sur ces marchés.

Parallèlement, différentes possibilités d'organisation nouvelle pour une structure de type commissariat destinée à impulser ces actions ont été examinées, notamment :

- Secrétariat d'Etat au Ministère de l'économie et des finances,
- Commissariat général d'une douzaine de personnes rattaché au Premier ministre,
- Mission globale confiée à une direction actuelle chargée d'impulser les autres directions,
- Grande direction chez le Premier ministre regroupant des services existants…

L'organisation proposée serait celle d'un Commissariat général à la transformation numérique placé auprès du Premier ministre et du ministre chargé du numérique, doté d'une douzaine de personnes et ayant le pouvoir d'orienter les budgets vers les directions concernées.

Néanmoins nombre de facteurs de réussite de la transformation numérique (fiscalité, levée de barrières réglementaires intra-européennes sur les données, politique d'achat, politique industrielle…) passent par le niveau européen qui peut permettre de disposer d'un marché pionnier suffisant.

*
* *

TABLE DES RECOMMANDATIONS

Avertissement : l'ordre dans lequel sont récapitulées ci-dessous les recommandations du rapport ne correspond pas à une hiérarchisation de leur importance mais simplement à leur ordre d'apparition au fil des constats et analyses du rapport.

1 CONTEXTE : LA SOUVERAINETE ET SA DECLINAISON DANS LE MONDE NUMERIQUE

1.1 La souveraineté au sens usuel

Dans son titre premier, la Constitution du 4 octobre 1958 traite de la souveraineté notamment dans les termes suivants :

- Son principe est : gouvernement du peuple, par le peuple et pour le peuple (article 2) ;
- La souveraineté nationale appartient au peuple qui l'exerce par ses représentants et par la voie du référendum (article 3) ;
- Les partis et groupements politiques … doivent respecter les principes de la souveraineté nationale et de la démocratie (article 4).

En outre :

- L'article 55 stipule que « *Les traités ou accords régulièrement ratifiés ou approuvés ont, dès leur publication, une autorité supérieure à celle des lois, sous réserve, pour chaque accord ou traité, de son application par l'autre partie* » ;
- L'article 88-1 stipule que « *La République participe à l'Union européenne constituée d'États qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007* ».

Les compétences d'un Etat peuvent se décomposer en :

a) Les fonctions régaliennes traditionnelles :

Dans presque tous les États, la souveraineté s'exerce au minimum dans les domaines suivants :

- la loi (définition de normes juridiques) ;
- la justice ;
- la sécurité extérieure : la diplomatie (prévention) et la défense nationale (armée en cas de conflit) ;
- la sécurité intérieure : la police ;
- les finances : le pouvoir de battre monnaie, la collecte des impôts et le contrôle des marchés financiers.

Pour conforter certaines de ces fonctions régaliennes, la plupart des États ont développé une politique en matière d'intelligence économique.

b) À ces domaines traditionnels de compétences se sont ajoutés (liste non exhaustive) :

- l'enseignement ;
- la santé ;
- le développement économique ;
- les politiques sociales : le logement, la sécurité sociale, la cohésion sociale ;
- l'environnement : la prévention des risques industriels, les catastrophes naturelles…
- la culture : c'est un point sensible pour la France qui défend le principe de l'exception culturelle.

En droit français, la Constitution distingue les transferts de compétences par l'État français à l'Union européenne des transferts de souveraineté. Les premiers sont autorisés car ils consistent en un transfert qui est réversible, tandis que les seconds sont inconstitutionnels, car définitifs. Le *Brexit* – en cours de déclenchement – permettra de mieux évaluer le prix à payer pour la réversibilité de ce transfert de compétences.

Les limites à la souveraineté issues des organisations internationales :

Les organisations internationales finissent par développer leurs propres compétences et se détacher de la volonté propre de certains de leurs États-membres, soit par des règles de majorité, soit par des transferts de compétence.

Au-delà de la simple concertation intergouvernementale, elles peuvent comporter des pouvoirs supranationaux, reconnus notamment par des traités, qui s'imposent aux institutions des pays membres de ces organisations.

C'est notamment le cas de l'Union Européenne qui, notamment par le vote à la majorité qualifiée de certaines décisions, peut contraindre les États-membres.

En effet, l'Union Européenne :
- exerce des compétences exclusives notamment pour ce qui concerne les règles de concurrence intracommunautaire, l'union économique et monétaire (*point qui constitue un transfert de compétences par rapport aux fonctions régaliennes traditionnelles*), la conclusion de certains accords commerciaux internationaux…
- exerce des compétences partagées avec les Etats-membres notamment pour ce qui concerne la politique agricole, énergétique, environnementale, régionale, sociale, de recherche et d'innovation, des transports…

Par ailleurs, quatre libertés fondamentales s'appliquent dans l'Union Européenne : la libre circulation des marchandises, des services, des capitaux et des personnes.

1.2 Les bouleversements liés au numérique

L'impact de l'informatique, puis des technologies numériques sur la société remonte au début des années 1970 avec une première accélération lors de l'émergence d'internet dans les années 1990 et une deuxième accélération dans le courant de la dernière décennie grâce à la capacité à développer des modèles d'informatique distribuée, mobile, hautement communicante et personnalisée. La révolution numérique en cours a augmenté les capacités d'agir, de communiquer, de produire tant au niveau individuel qu'industriel, commercial et sociétal. Cependant, elle a induit des risques importants dont le grand public et les milieux politiques ont pris pleinement conscience avec les révélations d'Edward Snowden (*mise sur la place publique à l'été 2013 des détails des programmes américains de surveillance de masse*).

Cette révolution numérique remet en cause de nombreuses fonctions régaliennes :
- en l'absence de frontières bien délimitées, quelle est la loi applicable ?

- la faculté de battre monnaie (*ex. du bitcoin*) ;
- la fiscalité appliquée, eu égard à l'effacement des frontières dans le monde numérique ;
- l'enseignement, avec le développement des MOOC (*Massive Open Online Courses*) ;
- le logement, avec le développement dans d'Airbnb au cœur de grandes métropoles…

Indépendamment de la cybercriminalité (*terrorisme, criminalité organisée, pédopornographie…*), le nombre des attaques informatiques augmente de façon très importante dans tous les pays vis-à-vis :

- des services de l'Etat ou d'infrastructures vitales (*que ce soit pour accéder à des informations sensibles ou bien pour paralyser un service, une activité*) ;
- des entreprises (*vol de fichiers-client, espionnage industriel, attaque visant à bloquer le site internet, « fraude au président »…*)
- des particuliers (*détournement des identifiants pour accéder à toutes sortes d'espaces-client, usurpation d'identité…*).

Certaines attaques informatiques – concernant chacune des trois catégories ci-dessus – visent la destruction pure et simple des données stockées ou bien leur chiffrement, les rendant inaccessibles si l'on ne paye pas une rançon (« *logiciel malveillant de type ransomware* »).

Dans la sphère économique, le numérique a révolutionné l'accès à l'information et bousculé les positions acquises dans plusieurs secteurs en moins de dix ans. Ce mouvement de transformation va se poursuivre et atteindre une part croissante de la production des biens et des services en soumettant les organisations existantes à une forte pression.

Par ailleurs, la protection des données personnelles a mis en évidence les conflits juridiques entre les Etats-Unis et l'Union Européenne :

- invalidation le 6 octobre 2015 par la Cour de Justice de l'Union Européenne (CJUE) de la norme juridique américaine « Safe Harbor » ;
- adoption le 27 avril 2016 par le Parlement Européen et le Conseil de l'Union Européenne du nouveau règlement général sur la protection des données, qui entrera en application à compter du 25 mai 2018.

1.3 La souveraineté numérique

Face aux bouleversements liés au numérique, la souveraineté au sens usuel du terme perd progressivement de sa substance du fait de l'absence de frontières bien délimitées. Ce constat est valable tant pour les fonctions régaliennes traditionnelles (*lois applicables, fiscalité des plates-formes numériques…*) que pour d'autres domaines de compétences (*par ex. le transport avec Uber*).

La souveraineté numérique peut couvrir (ou dépendre de) plusieurs aspects :

- les outils techniques : composants électroniques, systèmes d'exploitation, les infrastructures de réseau et de stockage des données…
- les compétences en matière de conception de ces outils, de cryptographie, d'analyse des données (*data science*), d'intelligence artificielle…
- la mise à disposition des citoyens français d'une identité numérique permettant d'effectuer des démarches administratives ou des transactions électroniques avec plus de facilité et un socle minimal de sécurité ;
- la capacité à se protéger des attaques informatiques, à assurer la protection des données personnelles ainsi qu'industrielles et commerciales ;
- les dispositions d'ordre législatif ou réglementaire et la capacité de les faire appliquer ;
- la faculté, dans une optique offensive, de conduire une guerre électronique (*cf. annonce du 12 décembre 2016 concernant la mise en place d'un commandement des opérations cyber, le Cybercom, placé sous la responsabilité directe du chef d'état-major des a*rmées) ; ce point ne sera pas développé plus avant dans le présent rapport.

Certains pays, tels que la Chine ou la Russie, sont allés beaucoup plus loin en termes de souveraineté numérique en voulant par exemple contrôler les contenus auxquels la population peut accéder. Nous examinerons plus loin ces particularités.

L'autre facette des bouleversements liés au numérique concerne la sphère économique dès lors que la révolution numérique en cours modifie en profondeur l'économie traditionnelle. En effet, les coûts de traitement des données et de communication de celles-ci sont si faibles qu'ils favorisent l'émergence de monopoles de fait (*ce qui soulève un autre problème en matière de droit de la concurrence, compétence régalienne relevant plutôt du niveau européen*). Dans l'industrie numérique, la valeur ajoutée provient de plus en plus des données.

De ce fait, la souveraineté numérique ne peut plus être séparée de la souveraineté économique, tant la révolution numérique en cours bouleverse l'économie traditionnelle.

Dans la suite de ce rapport, sera examiné dans quelle mesure « *Nous ne sommes pas collectivement maîtres sur nos réseaux, nous sommes subordonnés, soumis, dépendants, à la merci de la volonté d'autrui. Les règles imposées et les traitements subis sont décidés ailleurs et nous privent des droits les plus élémentaires, puisque notre droit national n'y est pas reconnu et que le droit de ceux qui nous dominent ne nous est pas appliqué* » ainsi que Pierre BELLANGER nous alerte dans son ouvrage « La souveraineté numérique ».

2 DE NOMBREUX DOMAINES RELEVENT DIRECTEMENT DE LA SOUVERAINETE NUMERIQUE

Le présent chapitre examine les différents domaines relevant de la souveraineté numérique.

2.1 Les composants

Lorsqu'un acteur industriel commercialise un produit dépendant d'un (ou plusieurs) composant(s) électronique(s), il doit au minimum maîtriser la conception et le design de ce(s) composant(s) sachant qu'il y a plusieurs fondeurs ayant des usines dans l'Union européenne : Infineon (ancienne division de Siemens), NXP (ancienne division de Philips) racheté fin 2016 par l'américain Qualcomm et STMicroelectronics, ce dernier disposant d'un site de production à Crolles dans l'Isère.

Compte tenu des règles américaines ITAR (pour *International Traffic in Arms Regulations*) qui peuvent bloquer l'exportation d'un équipement contenant un composant classifié ITAR, il est souhaitable – d'un point de vue souveraineté nationale – de pouvoir s'appuyer des composants électroniques conçus et fabriqués en France.

2.2 Les systèmes d'exploitation (OS)

Dans le domaine des micro-ordinateurs, le principal système d'exploitation est Windows (de Microsoft), sachant que Mac OS – qui équipe les micro-ordinateurs d'Apple – est un cas minoritaire positionné sur le segment haut de gamme du marché grand public des micro-ordinateurs.

Dans le cas des serveurs informatiques, le principal système d'exploitation est Linux – logiciel libre – dont la conception est plus adaptée aux besoins des informaticiens qui en sont les principaux utilisateurs.

Dans le cas des smartphones, les deux principaux systèmes d'exploitation sont Android (de Google) et iOS d'Apple, lui aussi utilisé par des appareils haut de gamme tels que l'iPhone, l'iPod et l'iPad. A titre d'exemple, Samsung qui avait développé son propre OS a désormais adopté Android.

Afin de disposer d'un OS sécurisé pour smartphones, l'ANSSI a travaillé au développement et au déploiement de SecDroid. SecDroid a été développé sur la base de l'Android Open Source Project et a pour objectif de disposer d'une solution de mobilité sécurisée intégrable sur des smartphone du commerce. A ce jour, la solution est utilisée au sein du SGDSN et de l'ANSSI (plus de 500 terminaux), du ministère de la justice (environ 1000 terminaux), de la préfecture de police de Paris (quelques dizaines de terminaux) et au ministère de l'intérieur à travers le projet Neogend/ Neopol. Ce dernier projet offre aux gendarmes et aux policiers la possibilité d'avoir accès sur le terrain en toute sécurité à de très nombreuses applications métier leur permettant ainsi de gagner en efficacité et d'améliorer leur action. 10000 terminaux sont actuellement déployés et la cible pour 2017 est de 70000 terminaux. Le développement d'une solution sécurisé pour smartphones de la sphère régalienne a mobilisé une dizaine d'ETP à l'ANSSI et chez les ministères utilisateurs de la solution.

Les équipes techniques de l'ANSSI ont élaboré, pour des administrations ayant un haut besoin de sécurité, un système d'exploitation sécurisé dénommé CLIP OS. Cet OS basé sur Linux intègre un ensemble de mécanismes de sécurité qui lui confèrent un très haut niveau de résistance aux codes malveillants et lui permettent d'assurer la protection d'informations sensibles. Il fournit par ailleurs des mécanismes de cloisonnement qui rendent possible le traitement simultané, sur le même poste informatique, d'informations publiques d'une part et sensibles d'autre part, au sein de deux environnements logiciels totalement isolés, dans l'objectif d'éliminer les risques de fuite des informations sensibles sur le réseau public. A ce stade, CLIP a fait l'objet de plusieurs déploiements de taille limitée (quelques centaines d'utilisateurs) au sein de l'administration depuis 2009. Comme le modèle économique peine aujourd'hui à se mettre en place, du fait de la faiblesse des volumes de déploiement envisagés, ce constat a conduit l'ANSSI à étendre le périmètre de déploiement de CLIP, initialement très restrictif, en incluant notamment les OIV (cf. § 2.7), pour lesquels il pourrait fournir une solution adaptée à certains besoins de sécurité récurrents, en particulier en matière de télé-administration sécurisée. Plusieurs expérimentations ont été montées avec différents OIV afin de valider l'adaptation de CLIP à ces besoins, mais aucun déploiement dans cette sphère n'a à ce jour été lancé. En revanche, il n'est pas envisagé de transformer CLIP en OS générique.

2.3 Les principales catégories de logiciels et d'applications informatiques

Les logiciels de base pour la micro-informatique sont : le traitement de texte (Word de Microsoft ou LibreOffice Writer), le tableur (Excel de Microsoft ou LibreOffice Calc), le logiciel de présentation (PowerPoint de Microsoft ou LibreOffice Impress) et le logiciel de publication assistée par ordinateur (Publisher de Microsoft ou LibreOffice Draw). Par ailleurs, il existe un logiciel de dessin assisté par ordinateur (Photoshop d'Adobe) conçu pour le traitement et la retouche de photographies, présent dans un cercle plus restreint d'utilisateurs.

Les applications de base pour le web sont : une messagerie électronique (Outlook de Microsoft ou Gmail de Google), un moteur de recherche (Google de Google ou Bing de Microsoft ou encore DuckDuckGo ou Qwant plus respectueux de la vie privée), un navigateur (Internet Explorer de Microsoft, Google Chrome, Mozilla Firefox…), un réseau social (Facebook ou Twitter ou bien LinkedIn dans le monde professionnel), un site de vente en ligne (Amazon ou eBay), un service de paiement en ligne (par ex. PayPal). On pourrait compléter cette liste par les messageries instantanées (WhatsApp, Facebook Messenger…) et bien d'autres logiciels.

La montée en puissance des smartphones a vu se développer un nouveau type d'application : la plate-forme de téléchargement d'applications en ligne telle que App Store d'Apple, Google Play ou Windows Phone Store. Ces « stores » sont parfois le seul moyen d'installer des applications sur des smartphones, générant ainsi des revenus s'apparentant à une véritable rente (*par ex. Apple se réserve 30 % du montant des ventes pour toutes les applications payantes installées sur l'App Store… alors que les risques ont été pris par les développeurs de ces applications à qui Apple a mis à*

disposition le kit de développement SDK). Ces « stores » posent clairement un problème de concurrence qui pourrait être qualifié d'abus de position dominante.

2.4 Les infrastructures de réseau

Internet est le réseau informatique mondial accessible au public. C'est un réseau de réseaux, sans centre névralgique, composé de millions de réseaux aussi bien publics que privés, universitaires, commerciaux ou gouvernementaux.

Le développement des usages du web s'appuie sur ce réseau mondial et suppose à la fois des moyens de transmission performants et des routeurs de plus en plus intelligents.

Pour ce qui concerne les moyens de transmission, le Gouvernement a lancé au printemps 2013 le Plan France Très Haut débit qui vise à couvrir l'intégralité du territoire en très haut débit d'ici 2022. Celui-ci repose principalement sur la fibre optique et, pour les zones les moins denses, sur divers moyens de type hertzien (*boucle locale radio, satellite…*). Même si les montants financiers ou les délais de mise en œuvre peuvent être revus à la hausse, ce plan permet de renforcer la compétitivité de l'économie française.

La diversité des moyens de transmission et des besoins en matière de réseau privé virtuel (VPN) suppose des routeurs de plus en plus intelligents. Les routeurs actuels jouent pour les données un rôle analogue à celui des commutateurs téléphoniques pour la voix. Le marché des routeurs est dominé par l'américain Cisco, suivi d'un autre américain Juniper Networks et des acteurs tels qu'Alcatel-Lucent-Nokia et le chinois Huawei. De tels équipements peuvent contenir une porte dérobée (backdoor) permettant d'obtenir les droits administrateurs, l'accès à la configuration de l'équipement et de déchiffrer les connexions VPN, ce qui pose un réel problème de souveraineté numérique. A titre d'exemple, une vulnérabilité a été découverte dans Juniper ScreenOS ; elle permettait à un attaquant de provoquer un contournement de la politique sécurité. Plusieurs failles de sécurité, critiques au niveau du système ScreenOS, ont été identifiées à la suite d'un audit de code interne réalisé (en 2015) par Juniper ; de plus, le mot de passe de la porte dérobée avait été identifié et publié sur Internet (*source : Bulletin d'alerte de l'ANSSI du 11 avril 2016*).

2.5 Les infrastructures de stockage des données

La croissance très forte des données produites a conduit de nombreuses entreprises à externaliser la fonction de stockage des données chez des sous-traitants, créant ainsi le « cloud ». Sur le marché mondial du cloud, les principaux acteurs sont : Amazon Web Services loin devant Microsoft Azure et Google Cloud Platform.

Le fait de recourir à des prestataires étrangers est loin d'être anodin**.** Les autorités d'un pays étranger (*le plus souvent les Etats Unis, au vu de la nationalité des principaux prestataires de Cloud*) peuvent accéder facilement à des données stockées dans des serveurs situés sur le territoire américain mais aussi en dehors de ce territoire en prétextant de la nationalité du prestataire.

Dès lors, les entreprises françaises et européennes doivent être particulièrement vigilantes face à la confidentialité des données qu'elles comptent externaliser.

Ce constat avait conduit le Gouvernement à lancer en 2009 le projet d'un cloud souverain qui a conduit à subventionner deux offres (Cloudwatt et Numergy) qui ont connu un succès mitigé. Par ailleurs, un opérateur français OVH, créé en 1999, est devenu le leader européen du Cloud sans avoir bénéficié de subventions.

En 2014, l'ANSSI avait testé en conditions réelles la pertinence des exigences fixées dans la première version du référentiel, alors baptisé « Secure Cloud ». Le référentiel a alors été mis à jour pour prendre en compte le retour d'expérience. Désormais, le référentiel, rebaptisé « SecNumCloud » en décembre 2016, a évolué vers deux niveaux d'exigences : Essentiel (*un incident de sécurité aurait une conséquence limitée pour le client*) et Avancé (*un incident de sécurité aurait une conséquence importante pour le client, voire pourrait mettre en péril sa pérennité*).

2.6 La mise à disposition d'une identité numérique en France

Afin de permettre aux citoyens français de faire leurs démarches administratives en ligne, le SGMAP a développé le service « FranceConnect » qui permet de disposer d'une identité numérique obtenue auprès d'un des trois fournisseurs d'identité (CNAMTS, DGFiP et La Poste). Après une expérimentation au 2nd semestre 2015, le service est officiellement ouvert depuis le 1er janvier 2016 ; début avril 2017, un peu plus de 620.000 personnes utilisent le service « FranceConnect ».

Il convient de rappeler que le règlement européen n° 910/2014 « eIDAS » (*electronic IDentification And trust Services*) adopté le 23 juillet 2014 a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur européen. Ce règlement prévoit trois niveaux de garantie des schémas d'identification électronique : faible, substantiel et élevé. Au niveau français, le rôle d'organe de contrôle pour les services de confiance est assuré par l'ANSSI. Le service « FranceConnect », tel que développé par la DINSIC, correspond dans sa version actuelle au niveau de garantie faible, validé par l'ANSSI. A échéance de septembre 2018 est prévue une reconnaissance mutuelle obligatoire des identités électroniques par tous les Etats membres.

2.7 La capacité à se protéger des attaques informatiques

Face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs, l'ANSSI a pour mission d'accompagner les opérateurs d'importance vitale (OIV) dans la sécurisation de leurs systèmes d'information d'importance vitale (SIIV). En effet, l'article 22 de la loi de programmation militaire (loi n° 2013-1168 du 18 décembre 2013) impose aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent.

L'Etat identifie comme Opérateurs d'Importance Vitale, les organisations publiques ou privées pour lesquelles une défaillance de certaines de leurs activités, suite à un acte de malveillance, sabotage ou

terrorisme, pourrait compromettre le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, ou mettre en cause gravement la santé ou la vie de la population.

A partir du 1er juillet 2016, l'entrée en vigueur d'une première série d'arrêtés a marqué la mise en place effective de ce dispositif pour certains secteurs d'activité. Les autres arrêtés ont été progressivement publiés au Journal Officiel dans le courant du 2nd semestre 2016.

Dans le prolongement des travaux ci-dessus, le Parlement européen et le Conseil de l'Union européenne (UE) ont adopté le 6 juillet 2016 la directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation « directive NIS » (Network and Information Security). Elle prévoit en effet le renforcement des capacités nationales de cybersécurité et établit un cadre formel de coopération entre Etats membres.

2.8 Les plates-formes numériques et leurs conséquences

Les coûts de traitement des données et de communication de celles-ci sont si faibles qu'ils favorisent l'émergence de monopoles de fait. La forme la plus classique est celle des sites de vente en ligne avec des taux de commission supérieurs ou égaux à 5 % ; autour de son site de vente en ligne, eBay a racheté et développé un moyen de paiement en ligne (PayPal).

Dans le domaine de la réservation de chambres d'hôtel en ligne, un duopole s'est constitué à partir de la création en 1996 de start-ups, l'une américaine (Expedia), l'autre néerlandaise (Booking) qui avaient identifié une niche inoccupée dans le marché du voyage en ligne. Au fil des années, ces deux sites ont pu augmenter progressivement leur taux de commission jusqu'à atteindre 25 % (*répercuté sur l'hôtel*) car ils rendent un service apprécié par les utilisateurs et sont désormais un intermédiaire incontournable entre les voyageurs et les hôtels. En outre, ces sites appliquent des clauses abusives (*cf. Décision n° 15-D-06 de l'Autorité de la concurrence du 21 avril 2015 sur les pratiques dans le secteur de la réservation hôtelière en ligne*) vis-à-vis d'hôtels qui ne font pas partie d'un groupe puissant et disposant d'une forte notoriété.

Dans le domaine de la location touristique de logements de particuliers, Airbnb s'est imposé dans les grandes métropoles. Si un logement français est une résidence secondaire, la location saisonnière est alors considérée comme un usage commercial de logement et le propriétaire doit enregistrer un changement d'usage à sa mairie lorsque la ville dépasse les 200.000 habitants. A Paris, 60.000 logements sont proposés sur le site Airbnb ; louer une petite surface à des touristes est 2,6 fois plus rentable dans la capitale que de la louer à l'année ; la proportion des logements loués de façon saisonnière à des touristes représente 7 % des logements dans les quatre premiers arrondissements de la capitale. Dans un autre domaine, c'est Uber qui a bousculé une profession réglementée – les taxis – qui, d'une certaine façon, ne s'était pas adaptée aux attentes des clients ; en outre, on peut considérer qu'Uber est en infraction avec la protection sociale des chauffeurs affiliés. Le point commun à ces deux exemples est la difficulté pour la puissance publique d'encadrer ces phénomènes : plusieurs modifications législatives et réglementaires ont été nécessaires sans pour autant avoir la certitude que les dérives aient été totalement enrayées.

Dans l'industrie numérique, la valeur ajoutée provient de plus en plus des données. Le business model des plates-formes numériques repose largement sur les données fournies par les utilisateurs sans que ceux-ci en aient mesuré toutes les implications lorsqu'ils ont cliqué pour accepter les conditions générales d'utilisation, au demeurant très longues et peu lisibles pour un profane. Ce phénomène sera encore amplifié avec la prolifération des capteurs de toutes sortes (objets connectés) qui font qu'une plate-forme comme Google peut détecter par ex. plus rapidement que les réseaux sanitaires classiques une épidémie telle que la grippe. Certains acteurs s'accordent pour dire que la masse des données collectées et leur traitement (Big Data) permettent connaître de façon de plus en plus détaillée les comportements des individus, ce qui pourrait ouvrir des perspectives assez inquiétantes ; pour les données collectées dans l'Union Européenne et traitées aux Etats-Unis, la différence d'approche entre ces deux entités (cf. § 2.9) constitue un défi pour « les droits et les libertés individuels et collectifs que la République protège ».

Sur un plan économique, des plates-formes de téléchargement d'applications en ligne telle que App Store ou Google Play prélèvent une commission de 30 % sur les ventes réalisées par les applications affiliées. Le point commun à beaucoup de plates-formes numériques est la captation d'une forte part de la valeur ajoutée, l'érosion des bases fiscales en France sans pour autant qu'il y ait un surplus de recettes fiscales aux Etats-Unis compte tenu des pratiques agressives de celles-ci en matière d'optimisation fiscale. De ce point de vue, celles-ci se comportent comme des entités supranationales.

2.9 La protection des données personnelles

Compte tenu des traitements de masse appliqués aux données fournies (plutôt) passivement par les utilisateurs des plates-formes numériques, la protection des données personnelles est un enjeu de tout premier ordre.

Concernant la protection des données personnelles, deux approches sensiblement différentes s'affrontent : la vision américaine et la vision européenne.

La directive européenne 95/46/CE, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données stipule que « Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel… destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si… le pays tiers en question assure un niveau de protection adéquat ».

Afin de faire la passerelle entre ces deux approches de respect de la vie privée et de permettre aux entreprises américaines de se conformer à la Directive européenne, le département du Commerce des États-Unis, en concertation avec la Commission européenne, a instauré un cadre juridique dénommé « Safe Harbor » (sphère de sécurité). Dans sa Décision n° 2000/520/CE du 26 juillet 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité », la Commission a considéré que les "principes de la 'sphère de sécurité' relatifs à la protection de la vie privée" appliqués conformément aux orientations fournies par les "questions souvent posées"

publiées le 21 juillet 2000 par le ministère du commerce des États-Unis d'Amérique assurent un niveau adéquat de protection des données à caractère personnel transférées depuis la Communauté vers des organisations établies aux États-Unis compte tenu des (différents) documents émis par le ministère du commerce des États-Unis.

Dans ce cadre, un citoyen autrichien a déposé une plainte auprès de l'autorité irlandaise de contrôle, considérant qu'au vu des révélations faites en 2013 par M. Edward Snowden au sujet des activités des services de renseignement des États-Unis (*en particulier la NSA*), le droit et les pratiques des États-Unis n'offrent pas de protection suffisante contre la surveillance, par les autorités publiques, des données transférées vers ce pays. La CJUE a été saisie d'un renvoi préjudiciel aux fins de l'examen de la validité de la décision n° 2000/520/CE. À cet égard, la Cour a rappelé que la Commission était tenue de constater que les États-Unis assuraient effectivement, en raison de leur législation interne ou de leurs engagements internationaux, un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive lue à la lumière de la Charte des droits fondamentaux de l'Union européenne. La Cour a relevé que ce cadre est uniquement applicable aux entreprises américaines qui y souscrivent, sans que les autorités publiques des États-Unis y soient elles-mêmes soumises. De ce fait, la décision de la Commission du 26 juillet 2000 a été invalidée et, par conséquent, le cadre juridique « Safe Harbor » également.

Suite à l'invalidation du cadre juridique « Safe Harbor », un accord a été négocié entre 2015 et 2016 entre l'Union européenne et les États-Unis d'Amérique dans le domaine du droit de la protection des données personnelles, qui a conduit au nouveau cadre juridique « Privacy Shield » (bouclier de protection des données). Comme le G29, Groupe de travail Article 29 sur la protection des données, a rendu un avis le 13 avril 2016, indiquant que le « Privacy Shield » offre d'importantes améliorations par rapport aux décisions du « Safe Harbor », mais que trois points majeurs de préoccupation ayant trait à la suppression des données, à la collecte de quantités massives de données, et à la clarification sur les pouvoirs et l'indépendance du médiateur demeurent, une invalidation du nouveau cadre juridique « Privacy Shield » ne saurait être exclue. En termes de souveraineté numérique, qu'elle soit française ou européenne, confier le contrôle d'un accord UE-USA à un médiateur américain ne peut que rendre perplexe.

Dans le même temps, le Parlement européen et la Commission européenne ont adopté le 27 avril le Règlement 2016/679 communément appelé Règlement Général sur la Protection des Données (RGPD) applicable à partir du 25 mai 2018. Ce Règlement constitue une avancée majeure en termes de protection des données personnelles… sous réserve qu'un traité international n'adopte pas des dispositions contraires. C'est la raison pour laquelle il conviendra d'être très vigilant dans les négociations « TTIP » où les États-Unis mettent en avant la notion de « free flow of data » transatlantique.

2.10 L'intelligence économique

Afin d'assurer la protection et la promotion du patrimoine matériel et immatériel de l'économie française, le décret n° 2016-66 du 29 janvier 2016 a créé un service de l'information stratégique et de la sécurité économiques. Ce service est dirigé par le Commissaire à l'information stratégique et à la

sécurité économiques, associé à la définition et à la mise en œuvre de la défense de la souveraineté numérique.

Face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs, le présent rapport se focalisera sur la défense du patrimoine immatériel. Les attaques qui paralysent ou détruisent un système d'information ou encore modifient le contenu d'un site internet, sont bien évidemment détectées ; en revanche, celles qui visent à récupérer des informations sensibles ne le sont pas forcément.

Le développement de l'internet a entraîné la connexion de (presque) tous les acteurs et de leurs systèmes d'information, sur la base de protocoles normalisés et d'outils numériques – provenant pour une large majorité d'un très petit nombre de fournisseurs – largement répandus, ce qui peut faciliter les attaques en masse, à moins qu'on ait pris la précaution de cloisonner les services visibles depuis l'internet du reste du système d'information.

Face à cet état de fait, il est impératif que tous les acteurs intègrent davantage ce risque et appliquent des mesures de bonne pratique afin de le réduire. C'est globalement le cas dans la sphère régalienne et chez les OIV qui recouvrent les acteurs les plus importants de la sphère économique. C'est moins vrai chez les ETI et les PME, et encore moins chez les TPE et les particuliers.

Courant janvier 2017, l'ANSSI a mis à jour son Guide d'hygiène informatique destiné à renforcer la sécurité d'un système d'information en s'appuyant sur 42 mesures. Au-delà de la nécessaire sensibilisation aux enjeux de sécurité informatique et aux risques de vol de données, il convient de promouvoir les produits qualifiés par l'ANSSI, notamment les outils de chiffrement d'une messagerie ou d'un disque dur : c'est l'un des moyens d'éviter des vols de données.

Par ailleurs, l'arrivée des plates-formes de cours en ligne ouverts et massifs (MOOC) dans le domaine de la formation professionnelle fait émerger une nouvelle menace au travers des informations que le cadre d'une entreprise fournit de façon consciente (*ses coordonnées et son positionnement dans l'entreprise*) et inconsciente (*via les cours suivis et toutes les données enregistrées par la plate-forme à cette occasion*).

2.11 Des start-ups qui ont du mal à prospérer

L'écosystème français et européen est favorable à l'innovation en ce sens qu'autant de start-ups naissent en Europe qu'aux Etats-Unis ou qu'en Asie. Il existe en France un certain nombre de dispositifs favorisant l'innovation : le crédit d'impôt innovation, le statut des jeunes entreprises innovantes, les aides provenant de BPI France (*entrée au capital, subventions…*), la *French Tech*… Selon le baromètre 2016 EY – France Digitale relatif à « La performance économique et sociale des start-ups numériques en France », leur chiffre d'affaires ne cesse de croître de manière considérable (de 3 Mds€ à 4,2 Mds€ entre 2014 et 2015, soit + 39 %).

Si beaucoup de start-ups naissent en Europe, elles se développent moins vite qu'aux Etats-Unis ou qu'en Asie. De ce fait, l'Europe ne comptait en 2015 que 15 licornes (*start-ups valorisées à plus d'un*

milliard de dollars) dont 3 françaises (BlaBlaCar, Criteo et Vente-privee.com) contre 90 aux Etats-Unis et 31 en Asie.

Le financement reste l'une des priorités clefs pour les start-ups numériques en France : l'accès aux financements est le facteur le plus critique pour leur développement (*capital-risque aux premières étapes de leur développement*). Le capital-risque fait intervenir des fonds d'investissement publics ou privés spécialisés, ainsi que des « business angels ». Le poids du capital-risque en France ne représente que 0,1 % du PIB (*contre 0,4 % aux Etats-Unis et en Chine ou bien 0,2 % au Royaume-Uni*). Cette différence peut s'expliquer en partie par l'absence de fonds de pension en France.

L'écosystème du financement du capital-risque en France conserve d'importantes marges de progression si l'on compare aux volumes mobilisés par des pays de même niveau de développement. Si la France veut rattraper le retard qui est le sien dans la révolution numérique, elle devrait se fixer comme objectif de quadrupler le montant des financements du capital-risque, ce qui ne signifierait jamais que passer de 2 Mds€ à 8 Mds€. Ce montant est très faible comparé au patrimoine des ménages français (*10.334 Mds€ fin 2014 selon l'INSEE, dont 4.625 Mds€ d'actifs financiers et plus particulièrement 1.246 Mds€ d'actions et 1.694 Mds€ d'assurance-vie*). Pourtant, la France est le pays qui a le plus de difficultés à financer l'innovation et la croissance des entreprises.

La première réponse a consisté à développer le soutien public via BPI France. Cependant, la France se caractérise par la part importante des fonds publics dans le financement du capital-risque (*plus du quart des fonds levés*) et la taille relativement faible des fonds d'investissement spécialisés (*dix fois moins que les plus grands fonds américains*). Cette situation pèse sur la vitesse de développement des start-ups numériques en France. Aussi, l'enjeu pour la France est double : augmenter significativement les montants globaux investis dans les start-ups numériques et favoriser l'émergence de fonds d'investissement spécialisés de taille plus importante.

Concernant les actifs financiers représentant le stock le plus élevé, la LFR 2013 a prévu la création des contrats d'assurance vie euro-croissance et vie-génération. Par la suite, la loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques a ouvert la voie au lancement du premier contrat d'assurance vie en « capital investissement ». Désormais, les assureurs-vie pourront proposer des unités de compte correspondant à des parts de fonds de capital-investissement, c'est-à-dire en parts de fonds qui investissement en titres non cotés de PME. Il conviendra d'évaluer l'efficacité dans le temps de ces nouveaux dispositifs.

2.12 Comment dépasser certaines contraintes supposées de l'Internet

La première idée reçue largement partagée est que l'internet est un réseau sans frontières. Or, la Chine a montré qu'un pays – certes peuplé de près d'1,4 milliard d'habitants – pouvait développer un écosystème fermé depuis la fin des années 90 avec notamment :

- Huawei dont le métier historique est la fourniture de réseaux de télécommunication aux opérateurs ; depuis, cette entreprise s'est développée dans les solutions numériques (chiffre d'affaires 2015 : 60 milliards de dollars) telles que les terminaux mobiles ou le cloud ;
- Baidu moteur de recherche chinois, mieux adapté au mandarin mais permettant aussi de filtrer les recherches non autorisées en Chine ; depuis, Baidu s'est diversifié dans les objets connectés,

l'intelligence artificielle, les véhicules autonomes… (chiffre d'affaires année 2015 : 10 milliards de dollars) ;
- Alibaba site de vente en ligne ; depuis, Alibaba dans le paiement en ligne (Alipay) et le cloud ; (chiffre d'affaires année fiscale 2016 : 11 milliards de dollars) ;
- Tencent avec des applications de messagerie instantanée QQ (*deuxième communauté virtuelle la plus importante au monde derrière Facebook*) et WeChat.

Même si ces entreprises se sont d'abord développées pour des raisons politiques – clairement non transposables dans le monde occidental, elles sont désormais parties à la conquête du monde sur la base de fonds levés sur le Nasdaq.

La deuxième idée reçue largement diffusée est que l'Europe n'aurait pas les moyens pour stocker au sein de l'Union Européenne toutes les données qui y sont générées. Au contraire , il ressort des travaux du rapport conjoint CGE – IGF sur « Accord plurilatéral sur le commerce des services et partenariat transatlantique pour le commerce et l'investissement : enjeux numériques des négociations » d'avril 2016, que l'UE dispose d'une capacité de stockage suffisante sur son territoire pour assurer l'hébergement et le traitement des données à caractère personnel des citoyens européens circulant actuellement en vue de leur traitement aux États-Unis.

La troisième idée reçue est qu'hors des GAFAM il n'y aurait point de salut. D'une part, il existe des marchés de niche pour des produits spécifiques. D'autre part, il est possible d'adopter des solutions alternatives mais il faut que le droit à la portabilité des données personnelles (article 20 du RGPD) s'applique effectivement et, par ailleurs, ça signifie notamment pour les réseaux sociaux qu'on se coupe du reste de la communauté.

2.13 Logiciels libres vs. Logiciels propriétaires

Comme cela a été développé aux § 2.2 et 2.3, il existe pour pratiquement tous les types de logiciels des versions libres et des versions propriétaires. Pourquoi dans certains cas, les logiciels libres s'imposent et dans d'autres ce sont les logiciels propriétaires qui le font ?

Les logiciels propriétaires, facturés aux utilisateurs, ne peuvent se vendre que s'ils répondent aux attentes de ces derniers notamment pour ce qui concerne la simplicité d'usage et l'ergonomie. Si les éditeurs de ces logiciels adoptent un positionnement tarifaire raisonnable, les utilisateurs ont peu de raisons d'opter pour une autre solution étant donnés les coûts induits par une migration vers un autre logiciel, qu'il soit libre ou propriétaire : formation des utilisateurs, mise à niveau des applications informatiques interfacées à ces logiciels…

Les logiciels libres, gratuits pour ce qui concerne leur mise à disposition, sont généralement plus complets (*grâce aux améliorations apportées par la communauté des utilisateurs*) mais pèchent parfois sur l'ergonomie pour l'utilisateur final. Suivant la catégorie d'utilisateurs, le logiciel libre peut être en position de force (*cas de Linux pour les serveurs informatiques où les utilisateurs sont les administrateurs-système*) ou bien cantonné à des domaines très spécifiques (*cas d'OpenStreetMap qui ne peut lutter contre l'ergonomie orientée grand public d'un produit d'apparence gratuit qu'est Google Maps*).

Ceci dit, deux exemples de migration d'un ensemble de logiciels propriétaires vers un ensemble de logiciels libres peuvent être cités qui montrent qu'il n'y a pas de réponse unique :
- l'Assemblée nationale qui, fin 2006, avait décidé de travailler pour la législature suivante (2007-12) avec des logiciels libres, a décidé, à l'été 2012, de revenir à des logiciels propriétaires au moins pour ce qui concerne la suite Office ;
- la Gendarmerie nationale qui a migré il y a quelques années vers un ensemble de logiciels libres ; dans ce cas, la formation des utilisateurs et la conduite du changement ont été à la hauteur si bien qu'à ce jour, cette migration ne semble pas poser de problème.

Aussi, le choix entre logiciels libres et logiciels propriétaires ne semble pas relever d'un choix technique mais plutôt d'un choix politique : quel objectif veut-on atteindre avec les logiciels libres ou avec les logiciels propriétaires ? Prenons le cas de la formation dans l'enseignement secondaire ou supérieur : veut-on former de simples utilisateurs des outils numériques ou bien former au monde numérique de demain ? Selon la réponse, on choisira des logiciels propriétaires ou bien des logiciels libres.

2.14 Concentrer ses efforts sur les compétitions futures

La maxime « The winner takes all » s'applique y compris entre membres du GAFAM : par exemple, Microsoft a voulu lancer son propre moteur de recherche « Bing » afin de mieux concurrencer la suprématie du géant Google, numéro 1 absolu du secteur. Huit ans après son lancement, Bing est parvenu à capturer 20 % du marché des recherches aux Etats-Unis mais Google conserve une domination écrasante de ce marché en Europe.

Si Microsoft, avec ses moyens financiers, n'a pas réussi à concurrencer une offre préexistante d'un autre poids lourd de l'internet, cela signifie qu'hormis le cas particulier de la Chine, peu d'acteurs peuvent espérer s'imposer sur un terrain qui est déjà occupé. Pour cette raison et aussi pour ne pas ignorer les craintes liées à la protection des données personnelles, il paraît illusoire de vouloir développer un OS souverain au-delà de la sphère strictement régalienne.

Il est donc préférable soit de prospecter les marchés vierges où un besoin n'est pas satisfait par une plate-forme numérique, soit de concentrer ses efforts sur la prochaine génération technologique.

La défense de notre souveraineté numérique doit s'appuyer sur une stratégie industrielle de développement des technologies numériques.

3 CES NOUVEAUX DOMAINES SOULEVENT PLUSIEURS ENJEUX ESSENTIELS

3.1 Les données et leur traitement

La société numérique se caractérise par une production massive de données de toutes sortes et par la capacité de les interconnecter et de faire communiquer les personnes, les objets et les différentes organisations. Ces données sont en quelque sorte la matière première de la société de l'information. Elles représentent un enjeu économique stratégique.

Ces données viennent de partout et de tout le monde. Chaque individu crée des données, soit de façon passive, à travers son identité numérique ou la dématérialisation d'actes administratifs, soit de façon active, par exemple en participant à des réseaux sociaux.
Les entreprises, les banques, les institutions à travers leurs activités de production, de gestion, d'interaction avec les clients, en produisent beaucoup. De plus en plus de données sont également produites par des systèmes dits embarqués qui, à travers différents capteurs, interagissent et recueillent des informations liées à leur environnement.

La numérisation croissante accompagnée d'une meilleure exploitation des données contribue donc au développement de produits et de services innovants. La donnée seule est cependant rarement source de valeur, elle en acquiert par la mise en relation avec une multitude d'autres. La valeur provient essentiellement de l'exploitation massive de données par des opérateurs capables de les recueillir, de les agréger et de les analyser. De fait, nous sommes entrés dans l'ère du *big data*, mais aussi dans celle des algorithmes qui en assurent le traitement automatisé.

La collecte croissante de données couplée aux capacités de traitement, capables d'apprentissage automatique (*machine learning*), peut permettre d'offrir des services de plus en plus personnalisés, mais aussi de faciliter des traitements discriminatoires (*par ex. dans le domaine de l'assurance*).

3.2 La transformation numérique de l'économie

Le numérique pose un défi aux entreprises traditionnelles, en transformant radicalement tous les secteurs de l'économie, et en imposant de profondes mutations sur leur fonctionnement même. A titre d'exemple, il convient de se rappeler que Sony, qui disposait d'une position prépondérante sur le marché de la musique tant par la maîtrise des technologies que par son catalogue d'œuvres musicales, s'est fait complètement déborder par Apple en l'espace de quelques années.

Ce qui s'est produit dans un domaine d'activité au niveau mondial peut se reproduire dans tous les secteurs d'activité au niveau français. Tous les secteurs sont concernés par la transformation numérique, à plus ou moins brève échéance. Il convient de prendre conscience, au travers de quelques exemples, des enjeux qui se posent du fait de l'émergence d'un modèle disruptif et d'alerter sur les risques qui pèsent sur notre économie.

Les secteurs déjà touchés par la transformation numérique (cf. § 2.8) ont été les sites de vente en ligne (Amazon, eBay…), l'hébergement d'abord pour ce qui concerne la réservation de chambres d'hôtel (Booking ou Expedia), puis la location touristique de logements de particuliers (Airbnb), le transport de personnes (les VTC et surtout Uber). Face à ces nouveaux acteurs, le premier réflexe des acteurs traditionnels a été la dénonciation d'une concurrence déloyale de la part d'entreprises ne répondant pas aux mêmes obligations fiscales et juridiques. L'Etat a été appelé à la rescousse par les acteurs traditionnels et a procédé à plusieurs modifications législatives et réglementaires, sans pour autant enrayer l'essor de ces innovations portées par des acteurs du numérique qui répondent à une demande des consommateurs ou qui s'engouffrent dans l'espace laissé par les acteurs traditionnels.

Les fractures provoquées par Airbnb ou Uber dans leur secteur pourraient se reproduire dans d'autres où des rigidités, notamment réglementaires, freinent les innovations, comme les secteurs de l'éducation, de la santé, de la banque ou de l'assurance.

L'arrivée des plateformes de cours en ligne ouverts et massifs (MOOC) offrent de nouvelles perspectives au monde universitaire et entrent également en concurrence avec la formation professionnelle traditionnelle. Coursera, entreprise américaine, a lancé début 2012 des cours conçus pour être suivis en ligne potentiellement par des dizaines de milliers d'étudiants partout dans le monde. A l'été 2012, Coursera a noué des partenariats avec des universités principalement américaines, puis en 2013 avec quelques grandes écoles françaises. Le modèle économique de Coursera repose selon toute vraisemblance sur la collecte de données fournies par les étudiants inscrits dans les cours proposés, ce qui pose des questions par rapport à la réutilisation des données collectées. En janvier 2014 ont débuté les MOOC de France Université Numérique (FUN) gratuits et ouverts à tous.

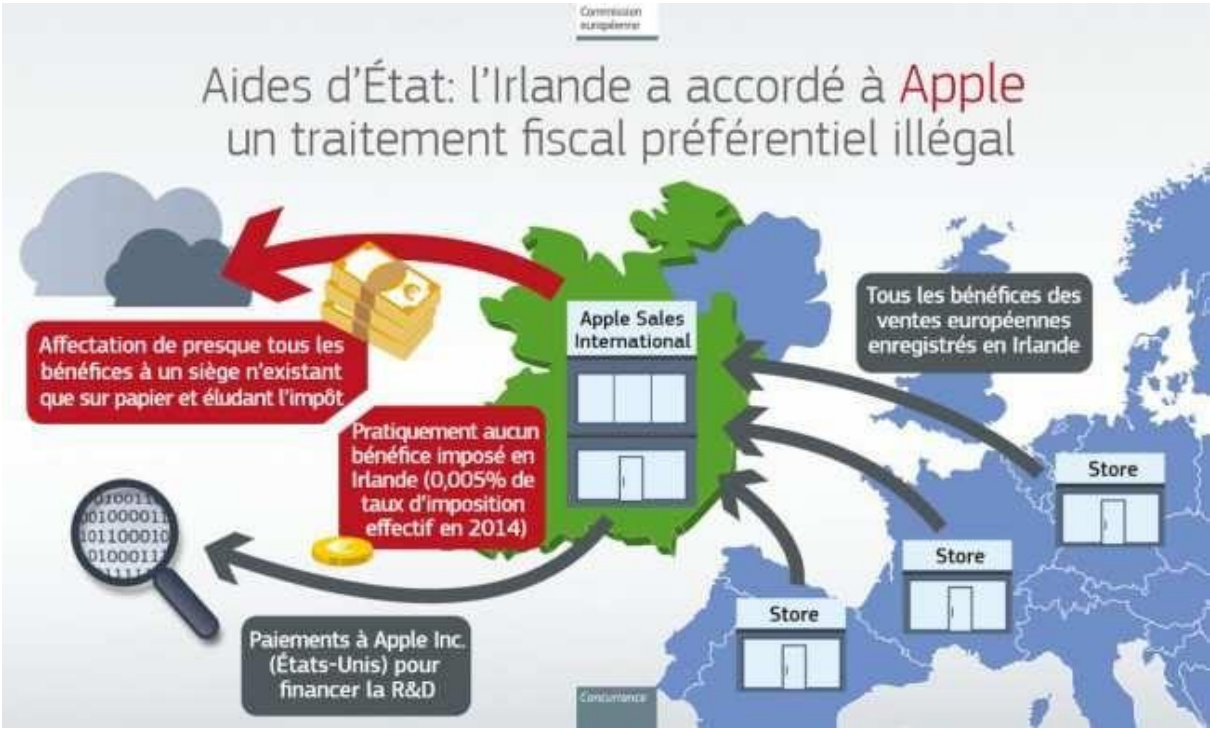
La santé est l'un des secteurs dont on attend le plus d'évolutions générées par le numérique, notamment grâce aux objets connectés et au diagnostic à distance. Le développement de la santé connectée permettrait de relever plusieurs défis en matière de santé publique : une réponse (*partielle*) aux déserts médicaux, la prise en charge avec maintien à domicile des pathologies ne nécessitant pas une hospitalisation ou un placement dans un établissement de type EHPAD, et le traitement des pathologies chroniques (*détectées, via des objets connectés, par des algorithmes analysant des données collectées en masse*). Ces évolutions, qui permettraient de préserver la qualité du système de santé existant, posent la question de l'accès aux données médicales. Dans le domaine des objets connectés de santé, la France avait vu la création en 2008 d'une start-up numérique Withings. Malgré des levées de fonds notamment auprès de BPI France, Withings a été rachetée en 2016 par Nokia.

3.3 La régulation des plates-formes numériques

Du moteur de recherche jusqu'à la plate-forme mettant en relation une offre de service et un client, le numérique conduit au développement d'intermédiaires qui se positionnent comme acteurs à l'échelle mondiale.

Comme l'a si bien décrit Jean TIROLE dans son livre « Economie du bien commun » dans le chapitre « Quand le digital modifie la chaîne de valeur » qui se concentre sur les stratégies des entreprises dans les marchés numériques et les défis pour la régulation de ces marchés, au centre de l'analyse se trouvent les plates-formes bifaces qui permettent aux différents côtés du marché de se rencontrer et d'interagir. Leur importance économique est substantielle et croissante. Aujourd'hui, trois des cinq plus grosses entreprises mondiales sont des plates-formes bifaces : Google, Apple, Microsoft. Par exemple, pour un moteur de recherche, les consommateurs ne voient que la face « prix bas » tandis que les annonceurs ne voient que la face « prix élevés » : en effet, la quasi-totalité du chiffre d'affaires du moteur de recherche Google vient de la publicité.

Aujourd'hui, l'intermédiation est souvent centralisée au sein de plates-formes qui captent une partie significative de la valeur ajoutée. Cette valeur ajoutée transite par un pays de l'Union Européenne à fiscalité avantageuse, puis va alimenter un trésor de guerre localisé dans des filiales offshore : en effet, les GAFAM n'ont pas intérêt à rapatrier leur trésorerie aux Etats-Unis sous peine de payer des impôts du même ordre qu'en France. A titre d'exemple, Apple est à la tête d'une trésorerie de 246 Mds$ dont la majeure partie se situe en dehors des États-Unis pour des raisons désormais bien connues d'optimisation fiscale.
Concernant les pays de l'Union Européenne à fiscalité avantageuse, la Commission Européenne a demandé fin août 2016 à Apple de rembourser 13 Mds€ à l'Irlande du fait que les accords passés entre Apple et l'Irlande étaient illégaux, car considérés comme une aide d'Etat abusive.



Au-delà du traitement européen de la fiscalité appliquée aux GAFA, deux questions se posent :

- Les trésors de guerre accumulés par les GAFA leur permettent de racheter des start-ups numériques (*sur la base de valorisations très élevées*) tuant ainsi dans l'œuf toute velléité de concurrence ;
- Le bon niveau pour définir les bases de la fiscalité du numérique semble être l'OCDE afin de lutter collectivement contre l'érosion des base fiscales.

Par ailleurs, la position dominante de ces plates-formes numériques constitue-t-elle un abus ? Comme le souligne Jean TIROLE, « Les régulateurs devraient donc s'abstenir d'appliquer mécaniquement des principes classiques du droit de la concurrence là où ils ne s'appliquent tout simplement pas. L'élaboration de nouvelles lignes directrices du droit de la concurrence adaptées aux spécificités des marchés bifaces requiert plutôt de considérer les deux faces du marché ensemble ».

Ceci dit, il convient de revenir sur la façon dont la Commission Européenne a traité le cas de Google : dans un premier temps, le Commissaire à la concurrence Joaquin ALMUNIA a cherché entre 2010 et fin 2014 à négocier des changements de pratiques sous formes d'engagements ; peu après son arrivée comme Commissaire à la concurrence, Margrethe VESTAGER a ouvert en avril 2015 une procédure d'abus de position dominante à l'encontre Google portant sur le lien entre Android et Google Sérac, puis communiqué en avril les premiers griefs de la Commission, suivis en juillet 2016 de griefs complémentaires concernant Google Shopping et Ad Sense. Cette procédure devrait déboucher, en toute logique, sur une sanction dans le courant de l'année 2017. Le droit de la concurrence semble donc applicable aux plates-formes numériques à condition de mettre en œuvre les bons outils.

3.4 Les enjeux de souveraineté économique

La transformation numérique de l'économie est engagée. Aujourd'hui, elle est menée par les entreprises dominantes, majoritairement américaines, qui imposent leurs règles. Quand on lit la lettre du *Deputy USTR Robert Holleyman* adressée à *l'USTR Froman* du 13 janvier 2017 à laquelle est jointe la stratégie des États-Unis dans ce domaine (document « *The Digital Two Dozen* »), il est clair que cette volonté ne va pas disparaître avec les changements dans l'administration américaine : « *The United States is committed to transforming the rules of international trade to promote the free flow of goods, services, and data across a free and open Internet* ».

Le mouvement de transformation numérique va se poursuivre et atteindre une part croissante de la production des biens et des services, y compris les services publics, en exerçant son potentiel d'optimisation et de transformation des organisations. La révolution numérique n'en est qu'à ses débuts !

Si l'innovation vient principalement des start-ups numériques, pour autant, toutes les entreprises, petites ou grandes, sont concernées par la transformation numérique. Mais ces dernières accusent un retard certain, qui se ressent dans la compétitivité globale de notre économie. Le numérique pose en effet un défi aux entreprises traditionnelles, petites, moyennes et grandes, en transformant radicalement tous les secteurs de l'économie, et en imposant de profondes mutations sur leur fonctionnement même. Or, si les PME françaises n'adaptent pas leur modèle économique, elles seront confrontées à un fort risque de perte de compétitivité, l'écosystème numérique restera à la traîne de celui de la Silicon Valley et la majeure partie du tissu économique des PME périclitera. Les PME en sont conscientes, mais elles sont nombreuses à ne pas se croire concernées par le numérique ou à ne pas juger comme prioritaire l'investissement dans les technologies numériques.

Pour tirer tout le parti de la révolution numérique, pour en être les acteurs plutôt que la subir, il ne faut pas l'attendre, il faut la provoquer. Sans un accent fort mis sur l'acquisition des compétences, en formation initiale ou continue, la France demeurera un pays consommateur de produits et de services numériques, producteur de données captées par les GAFA et non un pays créateur de valeur ajoutée. Si la valeur ajoutée n'est plus en France, cela se traduira par une érosion des bases fiscales.

3.5 Un cadre plus favorable pour la transformation numérique

Pour que ce retard ne se transforme pas en handicap, face aussi aux inquiétudes légitimes que suscite la révolution numérique, il importe de définir des objectifs collectifs, de fixer des principes, d'offrir un cadre propice aux innovations et d'accompagner les transformations. **Dans ce contexte, un engagement fort des pouvoirs publics apparaît plus que jamais nécessaire**.

Le pays possède des atouts (infrastructures, ingénieurs, pénétration des usages dans la population). **Dans un monde en perpétuelle évolution, le premier enjeu est celui de la formation, initiale et tout au long de la vie**. Selon le ministère du travail américain, 65 % des écoliers d'aujourd'hui pratiqueront, une fois diplômés, c'est-à-dire dans une vingtaine d'années, des métiers qui n'ont même pas encore été inventés. La question de l'adaptation des compétences revêt une importance cruciale, afin de répondre aux enjeux de conversion numérique et de formation des jeunes générations. Il conviendra de même d'élargir le champ des activités reconnues par la formation professionnelle aux supports numériques, en particulier les MOOC.

Le deuxième enjeu concerne le financement de l'économie numérique. Au départ, les entrepreneurs sollicitent leurs proches puis des business angels dans la phase d'amorçage. Enfin, interviennent les acteurs du capital-investissement. En France la phase d'amorçage est bien couverte grâce à des financements publics et privés. Mais la France souffre d'une lacune dans la phase de développement. Les investisseurs sont trop peu nombreux et la structuration des fonds repose encore trop souvent sur des fonds publics nationaux voire européens. Si la France veut rattraper le retard qui est le sien dans la révolution numérique, elle devrait se fixer comme objectif de quadrupler le montant des financements du capital-risque.

La multiplicité des cadres réglementaires dans l'ensemble de l'Union européenne et leur rigidité peuvent également être un frein. BlaBlaCar – qui est une des trois licornes françaises – a indiqué être confrontée pour son développement européen à 24 langues (*sujet hors du champ de ce rappo*rt) mais surtout à 28 réglementations différentes. A la différence des Etats-Unis, où une start-up numérique se positionne dès sa création sur un marché intérieur de plus de 320 millions d'habitants, une start-up européenne voit son développement ralenti par la persistance d'un cadre légal fragmenté en Europe. En effet, la Commission européenne a identifié plus de 50 mesures nationales faisant obstacle à la circulation des données au sein de l'Union européenne. Malgré l'objectif affiché dans le RGPD « *Pour que le marché intérieur fonctionne correctement, il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques* », les restrictions juridiques ou administratives se multiplient en Europe, notamment sous la forme d'exigences en matière de localisation des données nationales. **Le troisième enjeu est donc la libre circulation des données dans l'Union Européenne**.

Si, comme l'indique la Commission européenne, le RGPD ne s'applique pas aux données à caractère non personnel lorsqu'il s'agit de données industrielles ou générées automatiquement, alors il faudra soit recourir à une initiative législative sur la levée des obligations de stockage local de données (*point de vue du Conseil National du Numéri*que), soit poser clairement le principe d'une liberté de circulation des données en Europe (*position du Syntec Numérique*) qui viendrait s'ajouter à la libre circulation des personnes, des biens, des services et des capitaux. Cette libre circulation des données devrait s'accompagner de standards élevés en matière de sécurité informatique et de garanties strictes en matière de stockage des données. Au besoin, une attention particulière doit être apportée à la libre circulation des données comptables et fiscales qui pourrait nécessiter un renforcement de la coopération entre les différentes autorités de supervision.

De façon plus générale, l'Union Européenne fait face à un paradoxe : alors que le numérique est un vecteur de facilitation des échanges, la mise en place du marché unique numérique se heurte encore à la fragmentation des marchés et à la persistance d'obstacles nationaux empêchant l'émergence d'un marché intégré. En effet, un espace européen fragmenté freine le développement d'acteurs émergents, la capacité à s'adresser directement à un marché de 500 millions d'européens ; ce sont avant tout les PME et les start-ups numériques qui font les frais d'un marché économique fragmenté, n'ayant pas les moyens de dupliquer leurs efforts dans chacun des 28 Etats-membres. Or, comme l'ont souligné Nicolas COLIN et Henri VERDIER dans L'âge de la multitude, « L'Union Européenne a tous les moyens pour trouver son propre chemin : un niveau élevé d'éducation… de nombreuses infrastructures de grande qualité… des capitaux abondants, des grands groupes, des entrepreneurs. Il ne lui manque que la bonne stratégie et les dirigeants capables de la porter ». Comme le numérique abat les frontières, l'échelon le plus pertinent est donc celui de l'Union européenne. **Le quatrième enjeu est donc l'instauration du Digital Single Market.** Annoncé dans le cadre de la stratégie de la Commission européenne dès mai 2015, il tarde à se concrétiser. En l'absence d'un cadre juridique harmonisé et stable, le risque est l'apparition de réglementations nationales et/ou de la définition de certaines notions variant d'un pays à l'autre. Comme ni la France, ni un autre Etat-membre ne peut légiférer uniquement pour son propre pays, il est indispensable d'adopter au plus vite une approche d'emblée européenne sur toutes les questions relatives au numérique et que chaque pays, au premier rang desquels la France, joue un rôle moteur à Bruxelles afin faire effectivement émerger le marché unique numérique.

4 DES MESURES DEJA PRISES POUR RENFORCER LA SOUVERAINETE NUMERIQUE

4.1 Les mesures déjà prises en termes de sécurité

Un certain nombre de mesures ont déjà été prises à la fois en termes d'organisation et en termes réglementaires. La plupart de ces mesures sont plutôt orientées vers les aspects de défense et de sécurité des données de la sphère étatique :

- Dans le cadre de la LPM (Loi de programmation militaire) et de la directive NIS (Network and information security du 6 Juillet 2016), les OIV (Organismes d'importance vitale) sont tenus de mettre en place un certain nombre de règles (déclaration des incidents) et de matériels (sondes) afin de s'assurer que les informations sensibles de ces organismes ne sont pas divulguées. Le SGDSN est l'entité pilote pour ces actions.
  Toujours sous l'impulsion du SGDSN, et en complément de la réglementation sur le classifié de défense, une instruction interministérielle récente (IGI 901, janvier 2015) édicte des règles pour la manipulation des informations sensibles Diffusion restreinte. Les audits de sécurité des administrations effectués par l'ANSSI vont dans le même sens.
- L'ANSSI a développé et utilise un système d'exploitation sécurisé (CLIP) basé sur des logiciels libres. Elle a également acheté une licence globale au sein de l'administration pour un outil de sécurisation du poste de travail (Prim'X). Ce dernier est à ce stade insuffisamment utilisé par les services.
- La création du RIE (Réseau interministériel de l'Etat) permet de conserver dans une sphère de confiance les informations des administrations. Dans le cadre du RGS (Règlement général de sécurité), les échanges des administrations avec les citoyens sont sécurisés.
- La création d'un Commissaire à l'information stratégique et à la sécurité économiques (décret 2016-66 du 29 janvier 2016) est tout à fait dans la ligne visant à la souveraineté numérique. Il est très impliqué dans les décisions visant à s'opposer à des rachats stratégiques par des sociétés étrangères.

4.2 La modernisation numérique de l'Etat

La création du SGMAP et de la DINSIC ont permis d'accélérer la transformation numérique de l'Etat :

- Les différentes administrations ont mis en place ces dernières années un grand nombre de télé-procédures dématérialisant les démarches des entreprises et des citoyens.

- Par ailleurs, l'État plate-forme vise l'émergence de nouveaux services publics numériques pour les usagers grâce à une meilleure circulation des données entre les administrations, et des mécanismes de gestion des identités (SSO : Single Sign On) conformes au Règlement eIDAS de l'Union européenne et gérés par France Connect.

4.3 La protection des données

Elle a fait l'objet du RGPD (Règlement général de la protection des données UE 2016/679) qui entrera en vigueur le 25 mai 2018 s'efforce de légiférer sur la localisation des données au sein de l'Union européenne et sur leur portabilité.

- L'obligation d'une acceptation des Conditions générales d'utilisation des sites Web par les internautes (loi pour la confiance dans l'économie numérique du 21 juin 2004, et décret du 9 mai 2007) va dans le même sens.
- La libre circulation des données étant fortement souhaitée par les entreprises, des clauses de confiance sont élaborées (cf. Safe Harbor invalidé et remplacé par le Privacy Shield) mais pas toujours respectées. La réglementation européenne sur le Free flow of data est toujours en discussion.

Un effort significatif a été fait ces dernières années au niveau de l'administration et des OIV en faveur de la souveraineté numérique de la France.

En revanche, dans le cadre de la transformation numérique de l'économie, la tâche à accomplir reste immense et doit faire l'objet d'une forte mobilisation des pouvoirs publics au profit des acteurs privés, notamment les PME.

5 LES OPTIONS D'ORGANISATION

5.1 Un engagement fort des pouvoirs publics est indispensable

Comme indiqué précédemment, la souveraineté numérique peut avoir plusieurs significations : la protection des données sensibles de l'administration, la protection des données des entreprises, la protection des données personnelles des citoyens, la maîtrise de la transformation numérique de la société afin qu'elle ne se fasse pas exclusivement par des acteurs étrangers détournant la valeur ajoutée hors de France…

Mais les différentes mesures envisageables citées ci-dessus sont souvent communes à plusieurs de ces thèmes de souveraineté et sont de nature très diverses, concernant plusieurs acteurs. Même lorsqu'il s'agit d'acteurs publics, il s'agit souvent d'impulsions données sur une thématique donnée pour laquelle il existe déjà un pilote au sein de l'administration.
Par exemple, la Commande publique est déjà encadrée par la règlementation et possède une direction opérationnelle (la DAE), de telle sorte qu'on imagine mal une nouvelle entité (Commissariat…) qui serait chargée de la commande publique sous prétexte que les achats publics ont une incidence sur la souveraineté. La protection des données personnelles est déjà pilotée par une autorité administrative indépendante (la CNIL) qui ne pourrait être rattachée à une nouvelle structure puisque sur ce sujet il s'agit essentiellement de proposer des lois ou Règlements français ou européens.
Les aspects qui justifient en revanche l'existence d'une structure sont la capacité de réflexion interne, le pouvoir de décision et d'attribution de fonds budgétaires et la capacité de pousser des projets de lois, directives et règlements en France et à Bruxelles.

Dans ces conditions, l'impulsion à donner sur les différents dossiers de la souveraineté numérique relève soit de la vision d'un dirigeant éclairé (façon Steve Jobs ou Al Gore), soit d'une équipe disposant à la fois d'une capacité de réflexion élevée et d'une autorité suffisante sur les différents ministères ou directions générales.

Néanmoins, la mission tient à rappeler en préambule qu'il ne sert à rien de créer des structures s'il n'y a pas de volonté politique pour considérer que la transformation numérique est un enjeu majeur qui nécessite des moyens et des actions. Un organisme non soutenu politiquement ne constituerait qu'une lourdeur administrative supplémentaire. A contrario, une structure, dotée de leviers d'action, peut être un relais efficace pour relayer une volonté.

Recommandation n° 1.	La création d'une nouvelle structure doit s'accompagner d'une politique renforcée en faveur de la transformation numérique de l'économie.

5.2 Pour la sphère étatique, une nouvelle structure ne semble pas s'imposer

Un certain nombre d'entités interministérielles (SGDSN, SGMAP/ DINSIC…) concernées par la souveraineté numérique de la sphère étatique au sens large (Etat, collectivités locales, OIV) existent déjà. L'administration a joué son rôle par la mise en place du RGS[3] pour les systèmes d'information déployés par les autorités administratives, ou via la LPM 2013- 1168 pour les OIV. Ces actions sont assez structurantes et garantissent un niveau raisonnable de souveraineté. Si elles ne s'appliquent parfois que partiellement aux collectivités locales ou à la fonction hospitalière, c'est que le pouvoir de l'Etat sur ces entités reste limité.

Comme indiqué plus haut, les orientations relèvent plus de choix politiques que d'une absence de structure.

A l'examen de quelques cas où la souveraineté de la sphère régalienne peut être menacée, il apparait que la création d'un commissariat n'apporterait pas grand-chose :

- Le domaine véritablement sensible est déjà régi par le classifié de défense avec des sanctions pénales prévues en cas d'infraction. La France dispose encore d'une capacité souveraine à produire des équipements de chiffrement, et un chiffrement souverain validé par l'ANSSI est obligatoire pour le transit du classifié de défense sur des réseaux publics
- Sur les autres réseaux, pour lesquels le risque est moindre l'usage de produits Microsoft (Windows, Outlook) ou de routeurs étrangers peut poser problème mais ces décisions se font aujourd'hui en concertation avec la DINSIC, qui relève du premier ministre, et peut aisément provoquer une réunion interministérielle. Le choix de Microsoft office à l'Education nationale, qui peut effectivement être critiqué car il oriente des millions de jeunes vers ces produits à la fois payants et non souverains, n'a pas été fait sans une information du premier ministre.

  Le choix d'ouvrir les réseaux ministériels aux réseaux sociaux fait également l'objet de débats avec la DINSIC, et peut facilement être arbitré par le premier ministre s'il le souhaite.

  D'autre part, les réseaux étatiques sont plus ou moins contraints d'utiliser des commutateurs et routeurs Cisco ou Juniper parce qu'il n'y a rien d'autre sur le marché. Ceci est un problème industriel et non un problème d'organisation de l'Etat, et la création d'une filière nationale de routeurs destinée à l'administration semble hors de portée en raison des couts et de la position hostile aux aides d'Etat de la Commission européenne.
- Pour les OIV, leur interlocuteur naturel sur ces questions de souveraineté est le SGDSN et le dialogue avec l'ANSSI (qui dépend du SGDSN) est bon. Le CGE a d'ailleurs proposé dans un rapport récent d'aller plus loin que l'usage des sondes dans les obligations faites aux OIV d'utiliser des produits certifiés, mais ce genre d'initiatives se fait naturellement dans le cadre de la LPM ou de la directive NIS, et l'introduction d'un nouvel acteur ne ferait que compliquer le dialogue avec les OIV.

  L'interdiction d'utiliser certains équipements dont on peut estimer qu'ils posent problème (Commutateurs Huawei…) est difficile à réaliser dans le contexte européen de libéralisation des Télécom mais n'est pas complètement impossible grâce à l'article L35-6 du CPCE. Néanmoins, l'usage d'une telle procédure, qui a déjà été envisagée mais non retenue par le SGDSN et le Ministère de l'économie[4] n'est pas très liée à l'existence d'un commissariat.

[3] Décret RGS 2010-112 du 2 février 2010, pris en application de l'ordonnance 2005-1516

[4] Cette procédure devrait être justifiée pour éviter des recours en justice, et nécessiterait un dédommagement des opérateurs, au motif qu'on leur impose des coûts supplémentaires.

Ces exemples mettent en lumière le fait que ce n'est pas forcément la souveraineté de la sphère étatique qui est menacée mais la souveraineté globale par le biais de l'usage généralisé du numérique dans la société.
Enfin, le dialogue entre la DINSIC et l'ANSSI est actuellement de bonne qualité, ne justifiant donc pas une structure nouvelle de coordination.

Recommandation n° 2.	Pour la sphère régalienne, la création d'un commissariat à la souveraineté numérique ne se justifie pas car les structures actuelles apparaissent à même de régler ou faire arbitrer les choix de l'administration.

5.3 L'opportunité d'une nouvelle structure peut se poser pour donner une impulsion nouvelle à la transformation numérique de l'économie et le maintien de la souveraineté du pays

IL semble logique d'estimer que l'entité envisagée devrait appliquer la politique définie par le gouvernement et en outre disposer d'un certain pouvoir vis-à-vis des services de l'Etat. Ceci exclut donc des structures externes à l'administration comme les Autorités administratives indépendantes ou le Conseil national du numérique.

- Les différentes structures existantes qui sont concernées par cette problématique sont :

Le secrétariat d'Etat au numérique rattaché au Ministère de l'économie

Des directions ou services interministériels

- Le SGDSN, avec ses directions comme PSE ou l'ANSSI et ses relais HFDS dans les ministères. La problématique de souveraineté est centrale au SGDSN, sa compétence numérique est forte également mais elle est plus orientée vers la Cyber-défense que vers la montée en puissance de futures licornes
- La DINSIC et le SGMAP ont un rôle central sur l'usage du numérique dans les administrations, mais leur influence sur l'économie en général est très limitée
- Le SGAE a un rôle de négociation international mais est plus dans une position de recueil/ synthèse des positions des ministères que d'action
- Le CGSP (France Stratégie) propose une stratégie mais a peu de pouvoir d'action
- Le CGI (Commissariat général à l'investissement), BPI France…

Des directions de ministères

- La DGE en charge de la transformation numérique, via plusieurs de ses services : le SEN, le CISSE, l'Agence du numérique
- La DAE, la DG Trésor, la Direction de la législation fiscale
- Plus beaucoup de directions de ministères notamment aux ministères de la Défense, de l'Education nationale…

- Enfin, une liste d'objectifs de la structure peut être ébauchée, afin de pouvoir définir en temps utile des décrets d'attributions et de pouvoir ensuite évaluer son action. Pour chacun des objectifs, est indiqué l'intitulé du service qu'il faudrait impulser :

- Accroître la valeur ajoutée et la part de marché des acteurs français dans le domaine des réseaux, des services informatiques et du Cloud ⓞ ARCEP, DGE, AC, BPI France, CGI
- Accroître la part de marché des fournisseurs français de services sur le marché des plateformes utilisées par les utilisateurs français ⓞ DGE, BPI France, CGI
- Accroître le taux de retour (impôts en France) des acteurs du Web par rapport au chiffre d'affaires qu'ils réalisent en France ⓞ MEF (DGFIP/ DLF), SGAE
- Conserver la maîtrise de la fabrication de composants : la structure peut être au niveau européen, mais la France doit disposer de la capacité de produire les composants qu'elle désire dans des conditions de sécurité auditables, notamment dans le domaine cryptologique et cybersécurité ⓞ DGE
- Développer l'innovation : soutien aux PME innovantes, augmentation des capacités d'action en Capital risque ⓞ MEF (BPI France, DGE)
- Faire évoluer la commande publique afin de pouvoir favoriser l'emploi local et les PME (*Small Business Act*) dans le domaine du numérique ⓞ MEF, SGAE & UE
- Favoriser l'usage de logiciels libres au sein de l'administration et des collectivités locales ⓞ MEF, MI (DGCL), SGMAP
- Le développement de l'administration électronique au profit des usagers ⓞ SGMAP

- La mission a examiné différents types d'organisation pour une entité chargée de la souveraineté numérique, sachant qu'il existe très généralement un conseiller à Matignon chargé du numérique :

5.3.1 La situation actuelle : un secrétariat d'Etat rattaché au Ministère de l'économie

Le Secrétariat d'Etat peut disposer des services de Bercy pour déterminer une stratégie mais manque de pouvoir pour l'appliquer, pour ce qui concerne les autres ministères.

5.3.2 Un ministre ou un secrétariat d'Etat rattaché au premier ministre, sans service associé

Une telle structure est susceptible de disposer d'un certain pouvoir vis-à-vis des autres ministres et de leurs directions générales, sans que ces directions générales ne craignent de voir leurs prérogatives rognées.

Néanmoins, cette organisation ne présente qu'un intérêt modéré par rapport à la situation actuelle : un pouvoir supplémentaire lié à la proximité avec le Premier ministre, notamment pour ce qui concerne les services rattachés au Premier ministre.

Il n'y a pas non plus de garantie de continuité de l'action, les orientations pouvant varier lors des remaniements ministériels.

5.3.3 Un Commissariat général à la transformation numérique rattaché au premier ministre (ou à un Secrétaire d'Etat rattaché au Premier Ministre), et disposant d'une petite équipe (une douzaine de personnes de haut niveau)

Cette option ne susciterait pas trop de conflits au sein de l'administration, mais suppose que la personnalité choisie ait d'une part une autorité et une compétence reconnue dans le domaine du numérique, et d'autre part ait, à titre personnel, la confiance du Premier ministre ou du Président de la République. C'est à cette condition qu'elle pourrait agir sur les services, et notamment agir au niveau financier, sans disposer nécessairement d'une enveloppe budgétaire.
Grâce à sa petite équipe d'experts, cette structure pourrait avoir une vision stratégique du domaine numérique.

5.3.4 Un Commissariat à la souveraineté numérique rattaché au premier ministre tel que dans l'exposé des motifs (Etablissement public)

Une telle structure ayant la forme juridique d'un établissement public aurait une capacité assez étendue d'analyse, et sans doute un certain pouvoir pour impulser les dossiers. Elle pourrait en outre disposer d'un budget d'intervention (à l'instar du CGI), et impulser plus directement des aides ou des prises de participation dans des start-ups. Le risque est néanmoins qu'assez rapidement, les directions d'administration s'organisent pour garder la maîtrise de leurs dossiers face à cette nouvelle structure, et qu'une bonne partie de l'énergie dans les directions et dans l'établissement public soit consacré à des luttes de pouvoir.
A la différence du CEA qui avait une mission aux contours bien définis (le nucléaire) et sur lesquels il pouvait avoir une maîtrise forte, un Commissariat au numérique ne pourrait en aucun cas être l'interlocuteur unique sur tous les sujets du numérique, lesquels touchent l'administration, les entreprises, et les citoyens dans un contexte souvent international multiforme.

5.3.5 Un Département « Transformation numérique et industrie du futur » au sein du Commissariat Général à la Stratégie et à la prospective (France Stratégie)

Une telle organisation permet de disposer de pratiquement autant de pouvoir qu'un commissaire en titre rattaché au Premier ministre, sans avoir l'inconvénient de risquer de provoquer des luttes de pouvoir face à une nouvelle structure. La capacité d'analyse de ce directeur de département, auquel pourraient être rattachés une demi-douzaine d'experts de haut niveau serait assez forte mais il ne s'agirait pas d'une structure opérationnelle.

5.3.6 Une structure administrative de coordination des aspects numériques pour les services rattachés à Bercy

Le cas de la souveraineté au sens Défense étant déjà partiellement traité par le SGDSN, l'essentiel des problématiques restantes relèvent de l'économie. Le Ministère de l'économie et des finances dispose historiquement d'un pouvoir important sur l'économie en général et sur les administrations en particulier grâce à la Direction du budget. Néanmoins, les différentes directions de Bercy ayant des missions et des objectifs non identiques (même si le but final est le même on comprend que la

DGE souhaite disposer de financements pour soutenir l'industrie tandis que la direction du Budget souhaite réduire le déficit de l'Etat), une coordination entre les directions pourrait être utile. Une structure administrative de coordination des aspects numériques, composée d'un petit nombre d'experts, pourrait analyser les positions des différentes directions et faire remonter une synthèse pour arbitrage par le ministre.

5.3.7 Une direction générale existante qui verrait son rôle étendu à l'ensemble des domaines de la souveraineté numérique

Cette organisation a l'avantage de résoudre les problèmes logistiques, de nombre de personnels ou d'enveloppe budgétaire. Les candidats possibles sont le SGDSN, le SGMAP (avec la DINSIC) ou la DGE, et éventuellement le SGAE, la DG Trésor ou la DGA (Direction générale de l'Armement).

Dans cette hypothèse, la direction concernée traiterait directement les dossiers relevant de son champ de compétence et donnerait des directives aux autres directions. Cette situation existe déjà sur certains dossiers, comme l'usage du classifié de défense piloté par le SGDSN ou l'achat obligatoire de véhicules électriques par les administrations piloté par le MEEM. Il faut toutefois étudier la situation au cas par cas en fonction du tropisme naturel de la direction retenue :

Il faut sans doute distinguer l'hypothèse d'un service rattaché au Premier ministre et une direction d'un ministère.

Service du Premier ministre
Le SGDSN aurait une autorité naturelle mais une tendance à privilégier les sujets de défense par rapport aux sujets de transformation numérique de la société.
Le SGAE, très orienté sur la négociation internationale risque de privilégier des consensus européens et a peu d'expérience pour donner des directives aux administrations ou pour gérer des fonds de capital-risque.

Direction d'un ministère
En l'occurrence, le ministère qui semble le mieux placé serait celui de l'économie et des finances. La DGE, avec en son sein le SEN, le CISSE et l'Agence du numérique, semble un choix intéressant mais il n'est pas à l'abri de luttes de pouvoir à la fois internes à la DGE et vis-à-vis d'autres directions.

5.3.8 Une direction générale rattachée au Premier ministre qui regrouperait différents services existants

Une Direction générale ou un service pourrait regrouper la plupart des services qui ont une action forte dans le domaine du numérique : Un SGMAP étendu pourrait ainsi coiffer la DINSIC, l'ANSSI et une partie de la DGE (SEN, CISSE, Agence du numérique).
Cette option est toutefois relativement déstabilisante pour les directions concernées et leurs réseaux de correspondants et la plus-value de ce regroupement n'est pas flagrante vis-à-vis des objectifs cités ci-dessus.

5.3.9 Synthèse de l'analyse des structures envisagées

Plusieurs critères peuvent être envisagés pour évaluer les différents scénarios évoqués ci-dessus, notamment :

- L'autorité que pourra avoir l'entité sur les acteurs déterminants du dossier (ministères, directions générales, Assemblée nationale, Commission européenne…), et sa capacité financière à agir ;
- La capacité de réflexion et d'analyse pour déterminer la meilleure stratégie ;
- Le risque de lutte de pouvoir interne à l'administration entre la nouvelle entité et les directions existantes, de désorganisation des services, mais aussi la continuité de l'action lors des changements de gouvernement.

Au vu de ces critères et de ce qui a été exposé précédemment, seules les options 6.3.1, 6.3.3, 6.3.7 et 6.3.8 sont détaillées ci-dessous.

Un secrétaire d'Etat au Minefi, plus un conseiller à Matignon	
Avantages Permet une continuité des actions entreprises	Inconvénients Autorité limitée hors du MEF
Un Ministre plus un Commissaire général à la transformation numérique avec une petite équipe d'une douzaine de personnes	
Avantages Une autorité renforcée Le pouvoir de flécher des budgets Une capacité d'analyse Empiète peu sur les prérogatives des directions	Inconvénients Une structure nouvelle introduisant des lourdeurs administratives (coordination supplémentaire sur les dossiers, circuit de validation budgétaire modifié…)
Confier à une direction existante la responsabilité de la transformation numérique	
Avantages	Inconvénients
Pas de structure nouvelle, pas d'effectifs à recruter	Luttes de pouvoir, la direction retenue va vouloir donner des ordres aux autres directions La direction retenue impulsera plus son domaine propre (sur lequel elle est plus compétente) Risque de peu changer les choses
Une grande direction générale au numérique relevant du Premier ministre et regroupant l'ANSSI, la DINSIC et une partie de la DGE (CISSE, SEN, Agence du numérique)	
Avantages L'autorité et le pouvoir de traiter directement les dossiers Une capacité d'analyse approfondie	Inconvénients Une réorganisation des services, des méthodes de travail à revoir (réseaux d'interlocuteurs…) Des services communs (RH…) à réorganiser Une conduite du changement pour coordonner les directions fusionnées

A la lumière de ces analyses, il peut y avoir un intérêt à donner une impulsion nouvelle à la transformation numérique de l'économie, mais qu'aucune structure ne se dégage néanmoins très nettement.

La dernière option citée (grande direction générale du numérique relevant du premier ministre) n'apparaît toutefois pas opportune car trop déstabilisante. Qu'il soit plus efficace ou non à terme que le système actuel, ce genre de réorganisation qui a des incidences lourdes en termes de locaux et donc de personnels, peut se traduire par une période de flottement de 2 ans qui est plutôt une régression par rapport à l'objectif. Le besoin ne justifie donc pas une telle évolution.

Dans le cadre du redressement de l'économie numérique et afin de rendre effective une priorité sur la transformation numérique de la société, la création d'un Commissariat général à la transformation numérique a un sens. Mais ce commissariat devrait rester une petite structure d'experts de haut niveau, avec un chef ayant la confiance des plus hautes autorités de l'Etat, et capable de flécher des budgets, donner des orientations aux directions concernées (DGFIP, DGE, DINSIC, ANSSI) et négocier avec autorité à Bruxelles.

Recommandation n° 3.	Sous un certain nombre de conditions préalables (volonté forte du gouvernement d'agir pour la transformation numérique en France et à Bruxelles), la création d'un Commissariat général doté d'une petite structure (une douzaine d'experts de haut niveau) avec des leviers d'action pourrait donner une nouvelle impulsion à la transformation numérique de la France.

5.4 Un autre choix, plus politique, est de miser sur une nouvelle dynamique européenne

L'analyse préliminaire montre bien que la France n'est pas seule dans son retard sur le numérique, mais que c'est l'Europe entière qui s'est faite distancer par les USA.

La réussite véritable de la transformation numérique passe par une prise de conscience des enjeux en particulier par le niveau européen qui seul permettrait de disposer d'un marché suffisant pour que se développent les nouveaux services dans ce contexte où les effets de réseau sont importants. Certains sujets (fiscalité, levée de barrières réglementaires intra-européennes sur les données, politique d'achat, politique industrielle…) relèvent du niveau européen et ne peuvent être traités unilatéralement.
Plutôt que d'essayer d'obtenir des concessions ponctuelles de nos partenaires européens sur tel ou tel secteur, avec une efficacité limitée, il est possible aussi de donner plus de pouvoir aux instances européennes et leur demander en contrepartie d'assumer la réussite de cette transformation numérique : une autorisation de l'UE pour des aides d'Etat à certaines entreprises du secteur numérique sera difficile à négocier et moins productive si seuls les acteurs français utilisent les produits ou services concernés. A contrario, une politique industrielle volontariste de l'UE, associée à une sensibilisation des entreprises européennes sur leur intérêt à privilégier l'usage de produits européens, la libre circulation des données sur le sol européen et non avec l'extérieur, la fin du dumping fiscal de certains Etats, la mise en place d'un fonds de Capital-risque européen puissant… pourraient recréer en Europe les champions comparables à ceux des USA.

Mais un tel choix européen suppose une volonté politique non seulement de la France, mais aussi de ses partenaires, et elle implique sans doute une révision du Traité de Lisbonne. Elle suppose aussi que la France transfère ou partage certaines compétences (le choix de privilégier tel ou tel secteur économique, l'acceptation d'un pouvoir accru des instances européennes en matière budgétaire et fiscale) au profit d'une autre souveraineté espérée sur les outils du numériques (OS, navigateurs, moteurs de recherche, acteurs de l'intermédiation, des réseaux sociaux…).

Ceci reste un choix politique, mais dans cette hypothèse, les instances en charge du numérique devraient se trouver au niveau de l'UE, et un commissariat au numérique ne se justifie plus au niveau France dès lors que l'impulsion est européenne. Mais il faudrait alors de manière transitoire, une équipe de négociateurs plus politiques pour définir ces nouvelles règles du jeu.

Recommandation n° 4.	Dans l'hypothèse d'un nouvel élan européen et d'un transfert de certaines compétences vers les instances européennes en vue d'aboutir à un marché unique européen du numérique et la création de nouveaux champions, une structure de commissariat national ne se justifie plus. En revanche cette transition vers plus d'Europe nécessiterait, à titre temporaire, une équipe de négociateurs.

ANNEXES

Annexe 1 : Lettre de mission

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

SECRETARIAT D'ETAT CHARGE DU NUMERIQUE ET DE L'INNOVATION

LA SECRETAIRE D'ETAT

Paris, le 13 OCT. 2016

Monsieur,

L'article 29 de la loi n°2016-1321 du 7 octobre 2016 pour une République numérique prévoit que le Gouvernement remette un rapport étudiant la possibilité de créer un Commissariat à la souveraineté numérique rattaché aux services du Premier ministre, ainsi que les moyens et l'organisation nécessaires au fonctionnement de ce Commissariat. Selon l'article, les missions de ce Commissariat devraient concourir « à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège ».

La souveraineté numérique est un enjeu clé pour toute nation en général, et pour la France en particulier : l'indépendance, la maîtrise et la pérennité des technologies que l'Etat et ses concitoyens emploient au quotidien doivent sont des objectifs permanents pour lesquels nous devons nous assurer que les moyens pour les atteindre sont bien mis en place. C'est notamment pour cette raison qu'ont été créés ces dernières années la DINSIC[1], l'ANSSI[2], et plus récemment encore le CISSE[3], qui chacun dans leurs domaines d'attribution, contribuent à la souveraineté numérique de notre pays.

Favorable à un travail d'étude sur ce sujet, je vous demande de réaliser sous l'autorité de mon cabinet, un projet de rapport au Parlement traitant de cette question, notamment sous l'angle des données et de leur protection, des logiciels et systèmes d'exploitation, notamment des logiciels libres, des matériels informatiques et de leur production, et de la capacité du pays à assurer son indépendance numérique grâce à l'innovation

[1] Direction Interministérielle du numérique et du système d'information et de communication de l'Etat
[2] Agence nationale pour la sécurité des systèmes d'information
[3] Commissaire à l'information stratégique et à la sécurité économiques, au sein de la Direction générale des Entreprises

Monsieur Luc ROUSSEAU
Vice-président du Conseil général de l'Economie,
de l'Industrie, de l'Energie et des Technologies
120 rue de Bercy
75572 PARIS Cedex 12

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES
139 rue de Bercy - Télédoc 143 - 75572 Paris cedex 12

Je vous invite à cet effet à rencontrer les parlementaires qui sont à l'initiative de cet article ajouté par la Commission des Lois de l'Assemblée nationale, que j'informerai de la démarche, mais aussi les services de l'Etat abordant cette question : DGE[4], DINSIC, ANSSI, CISSE, ainsi que les autres ministères compétents le cas échéant. La rencontre de la CNIL, d'acteurs industriels du secteur et des associations professionnelles les représentant, des acteurs finançant ces filières industrielles et d'innovation, pourrait également être éclairante pour vos travaux.

Vous pourrez si nécessaire me proposer différentes options d'organisation permettant d'assurer les missions concourant à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs.

Je souhaite que vous me remettiez vos premières pistes de réflexion à la mi-décembre 2016, pour une remise finale du projet de rapport au premier trimestre 2017.

Dans l'attente de la conclusion de vos travaux, je vous prie de croire, Monsieur, à l'assurance de ma parfaite considération.

Axelle LEMAIRE

[4] Direction générale des entreprises

Annexe 2 : Liste des personnes rencontrées :

Parlementaires et personnes à l'origine de l'amendement adopté :

- Mme Delphine BATHO, Députée
- Mme Catherine MORIN-DESAILLY, Sénatrice
- M. Pierre BELLANGER, PDG de SKYROCK accompagné de M. Jean-Luc ARCHAMBAULT, Président de LYSIOS

Autorités administratives indépendantes :

CNIL :

- M. Edouard GEFFRAY, Secrétaire général

Autorité de la Concurrence :

- Mme Virginie BEAUMEUNIER, Rapporteure générale
- M. Nicolas DEFFIEUX, Rapporteur général adjoint
- M. Joël TOZZI, Rapporteur général adjoint
- M. David VIROS, Chef du service du Président

Gouvernement :

Cabinet de M. Manuel VALLS, Premier Ministre :

- M. Georges-Etienne FAURE, Conseiller technique « numérique »

Cabinet de Mme Axelle LEMAIRE, Secrétaire d'Etat chargée du numérique et de l'innovation :

- M. Bertrand PAILHES, Directeur de Cabinet
- M. Alexandre TISSERANT, Directeur de Cabinet Adjoint

Administrations :

SGDSN :

- M. Jean-Marie DESMARTIS, conseiller industrie et numérique auprès du SGDSN
- M. Guillaume POUPARD, Directeur général de l'ANSSI
- M. Christian DAVIOT, Conseiller stratégie auprès du DG de l'ANSSI

DINSIC

- M. Henri VERDIER, Directeur
- M. Xavier ALBOUY, Chargé de mission

DGE :

- M. Pascal FAURE, Directeur général
- M. Jean-Baptiste CARPENTIER, Commissaire à l'Information Stratégique et à la Sécurité Economiques (CISSE)
- Mme Cécile DUBARRY, chef du Service de l'Economie Numérique

DAJ :

- M. Jean MAÏA, Directeur
- M. Michel LEJEUNE, Sous-Directeur « Droit public et droit européen et international »
- Mme Valérie SERVICE-TSETOU-LEBON, adjointe au Chef du bureau « Droit public général et constitutionnel »
- Mme Caroline LEMASSON-GERNIER, consultante bureau « Droit public général et constitutionnel »
- M. Pierre LABRUNE, Chef du bureau « Droit financier »

Ministère de la Défense :

- Vice-Amiral Arnaud COUSTILLIERE
- M. Laurent CELERIER, Capitaine de vaisseau
- M. Frédéric VALETTE, Ingénieur en chef de l'armement

Organismes rattachés :

Conseil National du Numérique

- M. Godefroy BEAUVALLET, Vice-président
- M. Yann BONNET, Secrétaire général
- M. Yan KREWER, Rapporteur

INRIA :

- M. Antoine PETIT, PDG
- M. Claude KIRCHNER, Conseiller du PDG
- M. François SILLION, Directeur général délégué à la Science

Associations :

Institut de la souveraineté numérique :

- M. Bernard BENHAMOU, Secrétaire général

APRIL (Association pour la Promotion et la Recherche en Informatique Libre) :

- M. Fréderic COUCHET, Délégué général
- M. Etienne GONNU, Affaires publiques

CINOV-IT (Chambre professionnelle des TPE et PME du numérique) :

- Alain PRALLONG, Président
- Marie PRAT, Administratrice

SYNTEC Numérique (Syndicat professionnel des entreprises de services du numérique) :

- M. Laurent BAUDART, Délégué général
- M. Sébastien DUPLAN, Délégué aux relations institutionnelles
- Mme Philippine LEFEVRE, Déléguée aux relations institutionnelles

Entreprises :

Alain Bensoussan Avocats :

- M. Alain BENSOUSSAN

Gemalto :

- M. Frédéric TROJANI, Directeur général délégué
- M. Jean-Claude PERRIN, Directeur général stratégie et marketing

OVH :

- M. Alban SCHMUTZ, Vice-président développement stratégique

TALENTSOFT :

- M. Jean-Stéphane ARCIS, PDG
- M. Joël BENTOLILA, Directeur Technique

Annexe 3 : Glossaire

AC	Autorité de la concurrence
ANSSI	Agence nationale de la Sécurité des systèmes d'information
ARCEP	Autorité de Régulation des communications électroniques et des Postes
CGEIET	Conseil général de l'économie, de l'industrie, de l'énergie et des technologies
CGI	Commissariat général à l'investissement
CISSE	Commissariat à l'information stratégique et à la sécurité économiques
CNIL	Commission nationale de l'informatique et des libertés
CNN	Conseil national du numérique
DAE	Direction des achats de l'Etat
DAJ	Direction des affaires juridiques (MEF)
DGCL	Direction générale des Collectivités locales
DGE	Direction générale des entreprises
DGFIP	Direction générale des finances publiques
DGT	Direction générale du Trésor
DINSIC	Direction interministérielle du numérique et du système d'information et de communication de l'Etat
DLF	Direction de la législation fiscale (DGFIP)
ETI	Entreprise de taille intermédiaire
GAFAM	Google, Apple, Facebook, Amazon, Microsoft
IGF	Inspection générale des finances
LPM	Loi de programmation militaire
MEF	Ministère de l'économie et des finances
OIV	Organisme d'importance vitale
OS	Operating system (système d'exploitation)
PME	Petites et moyennes entreprises
RGPD	Règlement général sur la protection des données
RGS	Référentiel général de sécurité
RIE	Réseau interministériel de l'Etat
SEN	Service de l'économie numérique (DGE)
SGAE	Secrétariat général aux Affaires européennes
SGDSN	Secrétariat général à la Défense et à la sécurité nationale
SGMAP	Secrétariat général pour la modernisation de l'action publique
SSO	Single Sign On
USTR	United States Trade Representative

Annexe 4 : bibliographie

La souveraineté numérique, de Pierre BELLANGER (Editions Stock, janvier 2014)

L'âge de la multitude, de Nicolas COLIN et Henri VERDIER (Editions Armand Colin, mai 2015)

Economie du bien commun, de Jean TIROLE (Presses Universitaires de France, mai 2016)

Rapport d'information sur l'Union européenne, colonie du monde numérique (Sénat, Mme Catherine MORIN-DESAILLY 20 mars 2013) : https://www.senat.fr/rap/r12-443/r12-4431.pdf

Rapport d'information sur le développement de l'économie numérique française (Assemblée Nationale, Mmes Corinne ERHEL & Laure de La RAUDIERE 14 mai 2014) : http://www.assemblee-nationale.fr/14/pdf/rap-info/i1936.pdf

Rapport d'information sur les objets connectés (Assemblée nationale, Mmes Corinne ERHEL & Laure de La RAUDIERE 10 janvier 2017) : http://www.assemblee-nationale.fr/14/pdf/rap-info/i4362.pdf

Note « Tirer parti de la révolution numérique » (France Stratégie mars 2016) : http://francestrategie1727.fr/wp-content/uploads/2016/03/17-27-revolution-numerique-web.pdf

Note « Mobiliser l'épargne pour le financement des start-ups » (France Stratégie janvier 2017) : http://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/2017-2027-actions-critiques-financement-startup-web-ok.pdf

Guide d'hygiène informatique (ANSSI janvier 2017) :

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

La performance économique et sociale des start-ups numériques en France (Baromètre EY – France digitale 2016) : http://www.ey.com/Publication/vwLUAssets/ey-barometre-france-digitale-performance-economique-sociale-startups-numeriques/$FILE/ey-barometre-france-digitale-performance-economique-sociale-startups-numeriques-fr.pdf

Liens utiles :

- http://www.economie.gouv.fr/files/files/PDF/Rapport_numerique_dans___accords_commerciaux_internationaux.pdf (rapport CGE - IGF « Accord plurilatéral sur le commerce des services et partenariat transatlantique pour le commerce et l'investissement : enjeux numériques des négociations » avril 2016)
- https://syntec-numerique.fr/note-position/circulation-donnees-europe (Positon de Syntec Numérique sur la circulation des données en Europe, 2 janvier 2017)
- https://ustr.gov/sites/default/files/ARH-AMF-DTWG-Letter-1-13-17-FINAL.pdf (Office of the United States Trade Representative – Letter from Deputy USTR Robert Holleyman to USTR Froman 13-01-2017);
- https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf (Office of the United States Trade Representative)