Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Mars 2017

N° 2016/27/CGE/SG

RAPPORT ETUDIANT LA POSSIBILITE DE CREER UN COMMISSARIAT A LA SOUVERAINETE NUMERIQUE

ooooo

PROJET DE RAPPORT AU PARLEMENT

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 armées*) ; 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.

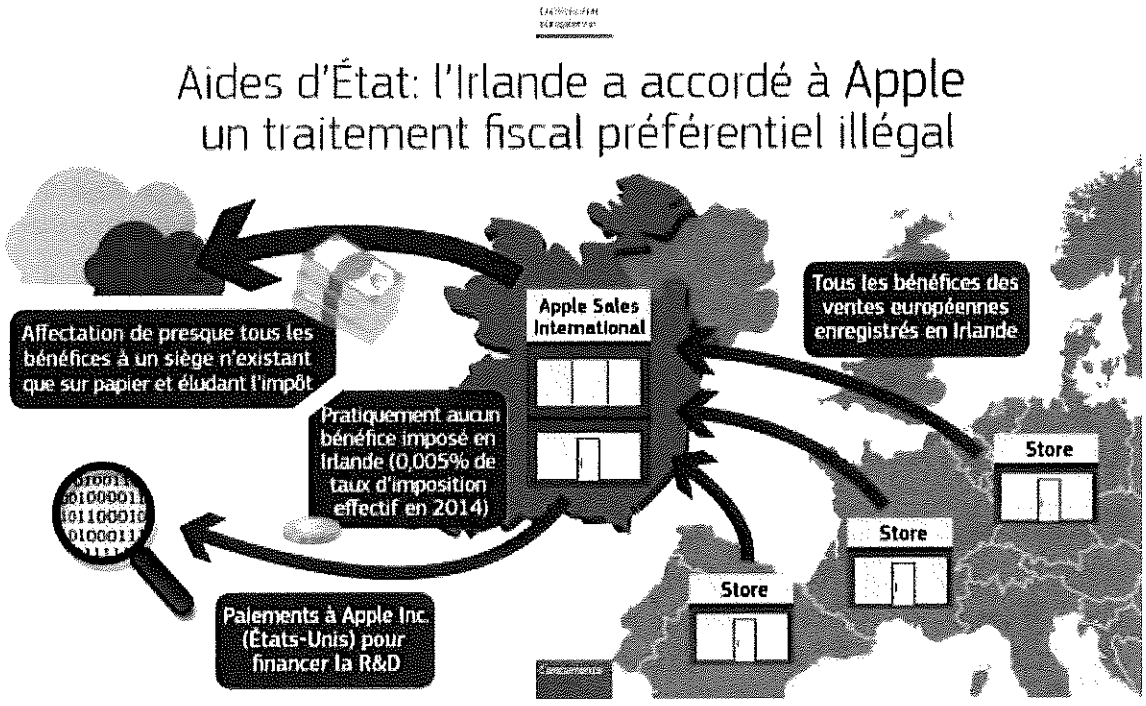
La santé est l'un des secteurs dont on attend le plus d'évolutions générées par le numérique, notamment grâce aux objets connectés et au diagnostic à distance. Le développement de la santé connectée permettrait de relever plusieurs défis en matière de santé publique : une réponse (*partielle*) aux déserts 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 rapport*) 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 19 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)