N° 4299

___

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 29 juin 2021

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA MISSION D'INFORMATION [1]

sur le thème **« Bâtir et promouvoir une souveraineté numérique nationale et européenne ».**

ET PRÉSENTÉ PAR

M. JEAN-LUC WARSMANN, Président,

ET

M. PHILIPPE LATOMBE, Rapporteur,

Députés.

___

TOME I

RAPPORT

(1) La composition de cette mission figure au verso de la présente page.

La mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne » est composée de : M. Jean-Luc Warsmann, *président ;* Mmes Virginie Duby-Muller, Danièle Hérin, MM. Denis Masséglia, Jean-Michel Mis, *vice-présidents* ; M. Philippe Latombe, *rapporteur*, Mme Valéria Faure-Muntian, M. Philippe Gosselin, Mmes Marietta Karamanli, Amélia Lakrafi, *secrétaires* ; Mme Laetitia Avia, MM. Xavier Batut, Éric Bothorel, Moetai Brotherson, Mmes Frédérique Dumas, Paula Forteza, MM. Thomas Gassilloud, Bastien Lachaud, Christophe Lejeune, Mme Marion Lenne, MM. Philippe Michel-Kleisbauer, Jérôme Nury, Pierre Person, Pierre-Alain Raphan, Mme Nathalie Serre, *membres*.

SOMMAIRE

Pages

INTRODUCTION

La crise sanitaire que nous avons vécue a fait la démonstration de la formidable dépendance de la France et de l'Europe vis-à-vis des solutions et matériels numériques non européens. Les outils utilisés afin de poursuivre une activité à distance ont été, dans leur grande majorité, américains. Au même moment, nombre de problématiques numériques ont refait surface, de la protection des données de santé aux enjeux de cyber-sécurité, face aux attaques informatiques qui ont notamment touché des collectivités territoriales et des structures de soins. Dans ce contexte compliqué, la question de la souveraineté numérique est réapparue avec force. La France et l'Europe doivent en faire la priorité de leurs politiques pour répondre à la demande de protection des citoyens, de compétitivité des entreprises, et, enfin, à une double exigence d'efficacité et de transparence des institutions publiques.

Dans ce contexte, le groupe MODEM a demandé et obtenu la création d'une mission d'information pour s'attacher aux conditions et moyens pour « Bâtir et promouvoir une souveraineté numérique nationale et européenne. »

La mission d'information, qui a tenu quatre-vingt-trois auditions, pendant plus d'une centaine d'heures, a ordonné celles-ci selon plusieurs thématiques, dans l'intention de faire suivre chaque constat de propositions opérationnelles :

– la base industrielle – industrie électronique et industrie du numérique, infrastructures – dont l'appréciation objective de la situation permet de mesurer la dépendance qu'il convient de réduire et le réalisme des objectifs à atteindre ;

– la compétitivité des entreprises, différentes autant par leur spécialisation que par leur taille, mais qui, toutes, évoluent dans un monde où la concurrence globale amplifie l'impact de leurs atouts comme de leurs handicaps ;

– la capacité des acteurs publics à piloter aussi bien les politiques de numérisation des administrations – leurs procédures, les relations avec leurs agents, leurs usagers et leurs fournisseurs – que les politiques de soutien à l'écosystème et aux filières d'avenir ;

– la compréhension des enjeux de la cybersécurité et de la mobilisation qu'ils requièrent de la part de tous, ce qui va bien au-delà des seules missions régaliennes ;

– l'impératif de la formation, dans toutes ses dimensions : de l'école à l'université, de la culture générale du numérique à la recherche de pointe, de l'utilisation des outils du quotidien à la maîtrise des algorithmes ;

– le rôle de l'Europe comme puissance normative, scientifique et économique, sans perdre de vue la dimension géopolitique qui interroge la possibilité d'un modèle numérique européen.

Votre rapporteur a tenu à hiérarchiser, selon l'urgence d'agir, les propositions découlant du constat sans fard auquel il s'est astreint, ce qui l'a conduit à définir quatre axes de propositions :

– premier axe : garantir la résilience de nos infrastructures ;

– deuxième axe : faire confiance à nos entreprises technologiques ;

– troisième axe : mettre la souveraineté numérique au cœur de l'action publique ;

– quatrième axe : mettre le citoyen au cœur des politiques numériques.

Votre rapporteur tient à remercier le président Jean-Luc Warsmann pour sa présidence attentive, l'ensemble de ses collègues qui ont participé aux travaux de la mission et toutes les personnes qui ont accepté d'être auditionnées pour leur approche, leur compréhension de la souveraineté numérique nationale et européenne, et pour la volonté d'action persévérante qu'ils ont tous appelée de leurs vœux, action dont dépend la faculté pour la France et ses partenaires européens de tenir leur rang – un rang à la mesure de leurs capacités – dans le monde et à l'âge numériques.

30 PROPOSITIONS CLÉS

AXE 1 : GARANTIR LA RÉSILIENCE DE NOS INFRASTRUCTURES

Ambition n° 1 : Garantir la sécurité de nos réseaux

Proposition n° 2 : Renforcer les contrôles mis en œuvre par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) sur la qualité du déploiement des réseaux fixes (page 42).

Proposition n° 3 : Maintenir une exigence maximale de sécurité vis-à-vis des déploiements 5G (page 43).

Ambition n° 2 : Faire face l'accroissement réel de la menace cyber

Proposition n° 1 : Créer un « comité numérique de crise » réunissant les opérateurs, les grands acteurs du numérique et les pouvoirs publics en cas de difficulté majeure sur les réseaux numériques (page 40).

Proposition n° 19 **:** Former les citoyens aux gestes-barrières face au risque cyber (page 66).

Proposition n° 40 : Accélérer la mise à niveau des équipements numériques des collectivités territoriales et des structures de soins pour garantir leur résilience (page 120).

Ambition n° 3 : **Assumer le coût de notre souveraineté numérique**

Proposition n° 34 : Augmenter les moyens financiers et les effectifs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour répondre à la croissance de la menace cyber (page 109).

Proposition n° 35 : Consentir un engagement financier inédit à destination des acteurs de la protection numérique au sens large, c'est-à-dire la plateforme Pharos, le groupement d'intérêt public Action contre la Cybermalveillance (ACYMA) et le parquet national cyber (page 109).

Proposition n° 39 : Veiller à ce que la trajectoire définie au sein de la loi de programmation militaire pluriannuelle soit en adéquation avec l'état de la menace et le niveau d'ambition porté par la France dans ce domaine (page 119).

Proposition n° 41 : Appliquer une doctrine de l'autonomie technologique maximale en matière de renseignement et de cyberdéfense en faisant du recours à des technologies extra-européennes une exception devant être motivée (page 122).

AXE 2 : FAIRE CONFIANCE A NOS ENTREPRISES TECHNOLOGIQUES

Ambition n° 4 : **Faire de nos entreprises technologiques une priorité nationale**

Proposition n° 26 : Privilégier, en matière de commande publique, le recours aux solutions d'acteurs technologiques français ou européens (page 98).

Proposition n° 27 : Exiger de l'Union des groupements d'achats publics (UGAP) des délais raisonnables dans le traitement des demandes de référencement des acteurs de l'offre numérique française (page 98).

Proposition n° 31 : Renforcer le soutien public à destination de la French Tech, pour encourager ses membres à « chasser en meute » (page 100).

Ambition n° 5 : Accélérer les projets européens de « reconquête » numérique.

Proposition n° 57 : Garantir au sein de Gaia-X une gouvernance et une conduite de projets conformes aux ambitions exprimées par ses membres fondateurs afin d'éviter que cette initiative ne devienne un instrument au service de la croissance d'acteurs déjà dominants (page 160).

Proposition n° 58 : Accélérer le déploiement d'une constellation européenne de satellites en orbite basse (page 162).

Proposition n° 60 : Renforcer les moyens mis en œuvre dans le cadre des projets importants d'intérêt européen commun (PIEEC) et adopter à chaque reprise des calendriers ambitieux de déploiement (page 164).

AXE 3 : METTRE LA SOUVERAINETÉ NUMÉRIQUE AU CŒUR DE L'ACTION PUBLIQUE

<u>Ambition n° 6</u> : Faire de l'État le moteur d'une politique de souveraineté numérique assumée.

– Défendre cette ambition au plus haut niveau de l'État

Proposition n° 45 : Créer un ministère du numérique, doté d'une administration et de moyens propres, et chargé de porter les politiques numériques aux niveaux national, européen et international (page 133).

Proposition n° 46 : Mettre en place un briefing hebdomadaire du Président de la République sur les questions technologiques en s'inspirant du modèle américain (page 133).

Proposition n° 65 : Mettre le numérique au cœur de la présidence française de l'Union européenne au premier semestre de l'année 2022 (page 178).

– Faire évoluer rapidement les pratiques de l'administration

Proposition n° 13 : Favoriser la circulation des compétences numériques au sein du secteur public (page 62).

Proposition n° 52 : Imposer au sein de l'administration le recours systématique à des solutions numériques françaises lorsque leur niveau de performance est satisfaisant pour les usages concernés (page 138).

Proposition n° 53 : Imposer au sein de l'administration le recours systématique au logiciel libre en faisant de l'utilisation de solutions propriétaires une exception (page 138).

AXE 4 : METTRE LE CITOYEN AU CŒUR DES POLITIQUES NUMÉRIQUES

Ambition n° 7 : Simplifier la vie des citoyens grâce au numérique.

Proposition n° 10 : Accélérer le déploiement de l'identité numérique en France (page 59).

Proposition n° 17 : Développer une culture de la transparence vis-à-vis des données utilisées par la puissance publique dans le cadre de ses interactions avec les citoyens (page 65).

Proposition n° 50 : Créer un portail public rassemblant l'ensemble des offres numériques françaises disponibles (page 135).

Proposition n° 15 : Créer un guichet numérique unique d'accès de chaque citoyen à l'ensemble des services publics, lui permettant aussi d'être informé en temps réel de l'utilisation de ses données par l'administration (page 63).

Proposition n° 16 : Créer un numéro d'identification unique afin de mettre fin aux difficultés que rencontrent les administrations pour identifier les administrés et partager leurs informations de façon efficace (page 65).

Ambition n° 8 *:* Se donner les moyens de protéger leurs données personnelles

Proposition n° 5 : Renforcer les effectifs de la commission nationale de l'informatique et des libertés (CNIL) dans le cadre du projet de loi de finances pour 2022 (page 47).

Proposition n° 6 : Simplifier le processus de sanction mise en œuvre par la commission nationale de l'informatique et des libertés (CNIL) au sein des dossiers de moyenne et de faible intensité afin de renforcer sa capacité à prononcer les « mesures correctrices » prévues par le RGPD (page 47).

Proposition n° 7 : Intégrer de façon systématique au sein des arbitrages techniques des projets numériques les enjeux ayant trait à la souveraineté numérique, en particulier concernant la protection des données personnelles et la localisation des données en Europe (page 50).

PREMIÈRE PARTIE : COMPRENDRE LA SOUVERAINETÉ NUMÉRIQUE

I. UNE REMISE EN CAUSE DE LA SOUVERAINETÉ DES ÉTATS ?

A. LA RÉVOLUTION NUMÉRIQUE FAIT ÉVOLUER LES PRÉROGATIVES CLASSIQUES DE L'ÉTAT

La « révolution numérique » transforme en profondeur nos sociétés, en faisant émerger de nouveaux usages et de nouveaux rapports entre les citoyens. Cette rupture est incontestable et incontestée, bien qu'elle échappe en partie aux efforts mis en œuvre pour la définir. On parle ainsi tantôt de « révolution numérique » (1) , tantôt d'une nouvelle « ère numérique, nouvel âge de l'humanité » (2) , ou encore de l'émergence d'un « âge de la multitude » (3). Certains parlent même d'un « nouveau désordre numérique » (4) lorsqu'il s'agit de pointer les évolutions à l'œuvre et la façon dont elles bouleversent les équilibres établis. Force est de constater, néanmoins, que ces différentes tentatives peinent à appréhender cet ensemble de changements profonds qui affectent la société dans son ensemble.

Quelques éléments souvent rappelés en donnent toutefois une idée assez fidèle : la révolution numérique se traduit par la facilitation et l'accélération inédite de la circulation de l'information, le dépassement des frontières physiques par le cyberespace, l'émergence de nouveaux objets et usages et, *in fine*, la construction d'un nouveau système d'échanges économiques et symboliques qui accorde une place inédite à l'individu-usager de services numériques.

Cette révolution technologique ne saurait évidemment épargner les États, qui se sont historiquement construits comme régulateurs monopolistiques de la vie en société, et définissent leur puissance, c'est-à-dire leur souveraineté, comme l'exercice d'un pouvoir normatif autonome sur une population dans un territoire donné délimité par des frontières.

Selon une acception largement partagée, le numérique viendrait remettre en cause, en profondeur, la souveraineté des États. La célèbre déclaration d'indépendance du cyberespace de John Perry Barlow, en 1996 souvent citée, en démontrerait l'intention : *« Gouvernements du monde industriel, vous géants*

---

(1) Une mission d'information commune portant sur « les droits de l'individu dans la révolution numérique » avait par exemple été instituée en 2010 au sein de l'Assemblée nationale en reprenant cette expression dans son intitulé.

(2) Gilles Babinet, L'Ère numérique, un nouvel âge de l'humanité, Le Passeur, 2014.

(3) Henri Verdier, Nicolas Colin, L'âge de la multitude : Entreprendre et gouverner après la révolution numérique, Armand Colin, 2012.

(4) Olivier Babeau, Le nouveau désordre numérique, Buchet-Chastel, 2020.

fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit (…). Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté où nous nous rassemblons. » (1). La puissance publique se verrait ainsi progressivement dépossédée de ses prérogatives les plus essentielles, comme le fait de battre monnaie, d'être capable de soumettre à l'impôt les activités économiques, ou encore de réguler les contenus pour préserver la société des propos haineux et de la violence. Le caractère transnational des géants du numérique et leur poids économique en feraient, en outre, des acteurs intouchables s'imposant sur un nombre croissant de marchés, face à une puissance publique en recul et incapable de les réguler, faute d'outils adaptés et de moyens de faire prévaloir ses règles au sein de l'espace numérique.

B. LA PUISSANCE PUBLIQUE EST CERTES CONCURRENCÉE MAIS ENCORE « MAÎTRESSE À BORD »

Les travaux de la mission d'information font apparaître une réalité plus nuancée quant à l'impact réel du numérique sur l'exercice par l'État de sa puissance souveraine.

Il est difficilement contestable, certes, que le numérique interroge la souveraineté des États, dans la mesure où il vient travailler en profondeur le périmètre et les modalités de leur action au sein des frontières nationales, dont la portée apparaît plus réduite dans le cyberespace que dans le monde réel. Cette situation a été souvent rappelée lors des auditions, par exemple celle de M. Nicolas Brien, directeur général de France Digitale, qui estime que nous vivons, à l'heure actuelle, « *un moment « Compagnie des Indes orientales »,* en référence au fait que, pour découvrir, exploiter et réguler le Nouveau monde, « *des acteurs privés se sont par le passé dotés d'attributs régaliens* ». Comme le relève M. Nicolas Brien, avec *« l'émergence des géants technologiques, notamment américains, les États n'ont plus le monopole des attributs régaliens de la souveraineté comme le cadastre, le fait de battre monnaie, le monopole de la violence physique légitime, l'état civil. Il est de notoriété publique que le fisc grec préfère aujourd'hui utiliser Google Maps plutôt que son propre cadastre* […] [ou] *que Facebook détient davantage de photos d'identité de chacun d'entre nous que n'importe quel service de renseignement* » (2).

Deux phénomènes nourrissent cette dynamique, comme l'a rappelé M. Julien Nocetti, docteur en sciences politiques, chercheur associé à l'Institut français des relations internationales, lors de son audition (3) :

– un premier phénomène « *de dépeçage des prérogatives souveraines des États* » par les géants américains « GAFAM » et chinois « BATX », qui se traduit,

(1) Cité par Mme Pauline Türk, Définition et enjeu de la souveraineté numérique, Cahiers français, mars-avril 2020, p.18.

(2) Audition de M. Nicolas Brien, 25 février 2021.

(3) Audition de M. Julien Nocetti, 11 mars 2021.

par exemple, par le fait que « *sur le plan monétaire, le projet Libra porté par Facebook pourrait, à terme, prendre de vitesse l'Union africaine dans son ambition de relier les États africains par le biais d'une monnaie unique* » pour ne citer que cet exemple ;

– un second phénomène de *« déspatialisation »* qui vient affecter, notamment, *« notre manière de penser les relations internationales et la géopolitique* [qui] *repose* [originellement] *sur l'idée d'espace, de frontière, de territoire »*, alors qu'il existe déjà « *une réalité du rapport de pouvoir dématérialisé, qu'il est très difficile de juridiciser* ».

Ce constat, qui repose sur des éléments factuels indiscutables, doit néanmoins être nuancé en raison de son approche très stato-centrée. En effet, si ce dernier, en tant qu'acteur public central, perçoit légitimement cette concurrence comme remettant en cause certaines de ses prérogatives, il convient d'observer, d'une part, qu'il reste à l'heure actuelle encore largement « maître à bord » en ce qui concerne ses missions fondamentales (1) et, d'autre part, que le numérique est un vecteur puissant de transformation et d'efficacité que l'État entreprend de mobiliser à son avantage. La « perte » de souveraineté de l'État peut donc se traduire par des gains d'efficacité au profit des citoyens, mais aussi de l'État lui-même, qui fait évoluer ses modes d'intervention vers un meilleur partage entre ce qu'il est capable de faire et ce qu'il convient de déléguer à des acteurs spécialisés.

Aussi, la question de la souveraineté numérique doit-elle moins être pensée en termes de « gains » et de « pertes » qu'en termes de redistribution de la puissance d'action des acteurs publics et privés au sein de l'espace numérique et physique. Il est donc important, sur ce sujet, de faire « la part des choses » entre les nombreux apports du numérique, la nécessité de trouver de nouveaux équilibres satisfaisants dans une sphère numérique où les règles de fonctionnement sont différentes, et les interdits et missions dont l'État doit conserver impérativement la compétence pour protéger les intérêts nationaux et les droits fondamentaux des citoyens.

C. LE NUMÉRIQUE EST DÉSORMAIS UN PUISSANT LEVIER D'INFLUENCE ET DE SOUVERAINETÉ POUR LES ÉTATS

Pour votre rapporteur, la façon d'appréhender la question de la souveraineté numérique doit donc être inversée : le numérique ne vient pas remettre fondamentalement en cause la souveraineté des États, il rebat simplement les cartes des relations de pouvoir entre ces derniers au niveau international et constitue un puissant levier d'influence à court et moyen terme. Les tensions entre les États-Unis et la Chine en matière d'approvisionnement en semi-conducteurs, question critique, ou la fermeture du marché chinois à des géants américains comme Facebook ou

(1) On notera, sur ce point, qu'aucun GAFAM ne vient sérieusement contester l'hégémonie des États quant à la gestion de la monnaie, en dépit de certaines tentatives, tandis que les règles de régulation qui s'appliquent sur les réseaux sociaux, c'est-à-dire les conditions d'utilisation de ce type de services, doivent respecter le cadre juridique national et un niveau d'exigence renforcé, par exemple, quant au retrait des contenus.

Twitter par exemple, sans oublier de mentionner, pour l'Union européenne, la mise en place du règlement général sur la protection des données (RGPD), constituent autant d'exemples de la dimension profondément politique et géopolitique de cette question.

Votre rapporteur est convaincu que l'enjeu est désormais moins de s'interroger sur l'évolution des prérogatives classiques de l'État, que sur la façon dont la France peut, dans un contexte où l'autonomie absolue est impossible, maximiser ses atouts et réduire ses dépendances, en s'appuyant sur le levier de puissance que constitue aussi l'Union européenne.

C'est cette approche que, pour son caractère pragmatique et opérationnel, les membres de la mission d'information ont choisi de retenir dans leurs travaux, en interrogeant l'ensemble des différentes couches du numérique :

– *le hardware*, c'est-à-dire les infrastructures numériques, incluant les réseaux et les centres de données, les fibres optiques transocéaniques, IXP (*Internet Exchange Points* – centres d'interconnexion entre réseaux des différents opérateurs) et les équipements informatiques, incluant les serveurs et les systèmes d'exploitation (qui sont hébergés dans les centres de données) ;

– et *le software*, c'est-à-dire l'ensemble des applications et/ou logiciels utilisés.

Votre rapporteur relève d'ailleurs l'existence d'une interaction croissante entre ces deux couches, *via* la virtualisation des réseaux par exemple, qui doit être prise en compte, bien qu'elle complexifie évidemment encore davantage l'appréhension de ce que pourrait être une « politique » de la souveraineté numérique nationale et européenne.

Le cyberespace : quelle définition ?

Dans son glossaire, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) définit le cyberespace comme un *« espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisés de données numériques »*. Ce dernier peut également être appréhendé par son contenu : il rassemble en effet *« l'ensemble des données numérisées (logiciels et documents textuels, sonores, graphiques ou visuels) disponibles sur l'Internet et les infrastructures matérielles et logicielles qui leur confèrent l'ubiquité. »* [(1)] .

Le numérique peut être décrit suivant un modèle en quatre couches :

– une couche physique : les infrastructures, fibres optiques transocéaniques, IXP (*Internet Exchange Points* – centres d'interconnexion entre réseaux des différents opérateurs) … ;

– une couche commande et contrôle (C&C) : le DNS (*Domain Name System* – système des noms de domaines), les tables et les protocoles de routage, les logiciels qui les implémentent ;

– une couche logique : les données publiées, les logiciels qui permettent d'y accéder et de les transformer : serveurs Web, moteurs de recherche, navigateurs, CDN (*Contents delivery networks – réseaux de diffusion de contenus*), systèmes de chiffrement … ;

– une couche cognitive : l'esprit et l'intellection des internautes organisés par la sémantique et la syntaxe des interfaces d'accès à la couche logique.

Source : Laurent Bloch, L'Internet, vecteur de puissance des États-Unis, géopolitique du cyberespace, nouvel espace stratégique, Éditions Diploweb, mars 2017.

II. QU'EST-CE QUE LA SOUVERAINETÉ NUMÉRIQUE ?

La souveraineté numérique constitue d'abord et avant tout une ambition politique forte, celle d'une autonomie stratégique à conquérir de la France et de l'Europe en matière d'équipements et de technologies numériques. Les nombreuses auditions menées ont fait apparaître qu'il existe une grande variété de définitions de la souveraineté numérique. Plusieurs approches possibles se dégagent des travaux conduits, qu'il convient d'articuler pour aborder les enjeux juridiques, économiques, et culturels d'une véritable politique de la souveraineté numérique.

A. UNE NOTION POLYMORPHE AU CŒUR DU DÉBAT POLITIQUE

1. Une préoccupation récente qui date du milieu des années 2000

Les premières réflexions françaises sur la question de la souveraineté numérique datent du milieu des années 2000, avec la publication dès 2006 d'une contribution de MM. Bernard Benhamou et Laurent Sorbier dans la revue *Politique*

(1) Laurent Bloch, L'Internet, vecteur de puissance des États-Unis, géopolitique du cyberespace, nouvel espace stratégique, Éditions Diplomweb, mars 2017.

étrangère (1) . Comme le rappelle Mme Pauline Türk, professeur de droit public, dans son article « Définitions et enjeux de la souveraineté numérique », l'apparition du concept de « souveraineté numérique » est néanmoins souvent associée à la publication par M. Pierre Bellanger, d'un ouvrage portant explicitement ce titre, *La souveraineté numérique*, en 2014 (2) . Cette même année, l'organisation d'Assises consacrées à ce sujet débouchait d'ailleurs sur la création d'un Institut de la souveraineté numérique, association chargée de nourrir le débat public et la réflexion des décideurs *via* la publication de *Cahiers de la souveraineté numérique*. Lors de son audition, M. Bernard Benhamou, secrétaire-général de cet institut, s'est d'ailleurs réjoui de voir que « *le thème de la souveraineté numérique est devenu plus familier, parce qu'il est abordé quasiment quotidiennement dans la presse »,* alors que *« tel n'était pas le cas à l'époque [de la création de cet institut] »* (3) .

2. Un regain d'intérêt dans le contexte de la crise sanitaire

L'émergence dans le débat public du thème de la « souveraineté numérique » reste relativement récente, comme l'ont rappelé plusieurs des acteurs auditionnés. Ainsi, Mme Karine Picard, directrice générale d'Oracle France, a-t-elle relevé qu'Oracle, société américaine qui fait partie des cinq grandes sociétés qui fournissent des *clouds* dans le monde faisait aujourd'hui *« face à une montée de la souveraineté, pas uniquement en France. Nous le constatons depuis cinq ans dans plusieurs pays, même en Angleterre. Même s'il est extrêmement proche des États-Unis, ce pays est très souverain en ce qui concerne ses données. Nous observons une même émergence en Allemagne, en France, dans les pays du Nord, au Moyen-Orient. Cette résurgence de la souveraineté n'est pas nouvelle. Depuis de nombreuses années, en tant qu'éditeurs américains, nous avons pris conscience de cette demande.* » (4) . Sur le sujet du *cloud* et des solutions souveraines, lors de la même audition, Mme Servane Augier, directrice générale déléguée de 3DS OUTSCALE**,** avait abondé en ce sens au sujet des offres *cloud* « souveraines » estimant qu'aujourd'hui *« après avoir été pas mal galvaudé, voire un peu tabou pendant quelques temps, le mot revient fortement. Après la promulgation du Cloud Act en 2018 et après que le confinement a révélé que la France et l'Europe étaient dépendantes de beaucoup de continents sur de nombreux sujets, dont le numérique, il est très important et très agréable, pour nous qui apportons des solutions souveraines, de voir que le sujet revient sur le devant de la scène et que les entreprises et les administrations se mobilisent pour essayer de faire en sorte que les offres souveraines existent et perdurent »* (5) .

---

(1) Bernard Benhamou, Laurent Sorbier, « Souveraineté et réseaux numériques », Politique étrangère, 2006/3.

(2) Pierre Bellanger, La souveraineté numérique, Paris, 2014.

(3) audition de M. Bernard Benhamou, 29 octobre 2020.

(4) Audition de Mme Karine Picard, 9 février 2021

(5) Audition de Mme Servane Augier, 9 février 2021.

Cette ambition politique a en effet longtemps été considérée comme peu réaliste voire anachronique, dans un monde ouvert et alors que le numérique dépasse évidemment largement le cadre des frontières nationales. C'est au fond tout le sens de l'interrogation de notre collègue, M. Pierre-Alain Raphan, lors d'une audition sur la *blockchain*, le 27 avril 2021 : *« dans ces auditions, nous parlons de gouvernance, nous essayons de réfléchir à un système de gouvernance, mais finalement, ces systèmes numériques sont-ils gouvernables ? Peut-on réguler un espace qui n'a pas de frontières sans une gouvernance globale qui serait partagée par l'ensemble des usagers et des utilisateurs ? Est-ce une utopie ? Peut-on avoir une gouvernance sur un territoire donné qui serait l'Europe, mais qui n'aurait pas forcément les mêmes objectifs que les autres régions du monde ? »*

La crise sanitaire et la situation de forte dépendance numérique des pays membres de l'Union européenne ont donné une actualité nouvelle à cette interrogation dans un contexte où, d'une part, certains pays asiatiques ont largement utilisé le numérique pour suivre leurs citoyens, avec des enjeux éthiques évidents, et où, d'autre part, il a fallu réfléchir à la mise en place d'un passeport sanitaire européen. La Commission européenne est à l'origine, le 17 mars 2021, de la création d'un certificat européen intégrant une preuve de vaccination, un résultat de test négatif ou une preuve de rétablissement du Covid depuis moins de six mois. L'approbation définitive de cette proposition par le Parlement européen, le 8 juin 2021, rend ce certificat obligatoire, à partir du 1er juillet, pour les déplacements dans l'espace européen (1) .

Ces dernières années, de nombreuses publications sont intervenues à cet égard, parmi lesquelles plusieurs notes de la Fondation pour l'innovation politique (2) ou encore un ouvrage collectif rédigé sous la direction de Mme Pauline Türk et M. Christian Vallor en 2018. En outre, la question de la souveraineté numérique est également présente dans un certain nombre de publications des acteurs institutionnels du secteur, comme l'ARCEP (3), le CNNum (4) ou l'ANSSI (5). Le Parlement, enfin, n'est pas en reste : il s'est saisi de cet enjeu à plusieurs reprises, essentiellement dans diverses missions de contrôle. Plusieurs rapports d'information de l'Assemblée nationale et du Sénat ont approché cette question de façon incidente, quand bien même leur objet ne reprenait pas *stricto sensu* cette expression. Un rapport sénatorial dédié à la question du « devoir de souveraineté numérique » a été publié en 2019 (6) . Ce sujet n'a néanmoins pas fait

(1) Le 6 avril 2021, la porte-parole de la Maison Blanche, Mme Jen Psaki, avait affirmé que, pour sa part, le gouvernement américain ne soutient pas et ne soutiendra pas un système qui demanderait aux Américains d'avoir un certificat. Il n'y aura pas de base de données fédérale sur les vaccinations ni d'obligation fédérale de vaccination. (Source AFP).

(2) Il s'agit en particulier des notes rédigées par M. Farid Gueham en 2017 (Vers la souveraineté numérique) et plus récemment par M. Emmanuel Combes en 2021 (Souveraineté économique : entre ambitions et réalités).

(3) Autorité de régulation des communications électroniques, des postes, et de la distribution de la presse.

(4) Conseil national du numérique.

(5) Agence nationale de la sécurité des systèmes d'information.

(6) Rapport n° 7 (2019-2020) présenté par M. Gérard Longuet au nom de la commission d'enquête le 1er octobre 2019.

l'objet d'une traduction concrète sur le plan législatif, bien que la *loi pour une République numérique* [(1)] ait comporté un article demandant la réalisation d'un rapport visant à instituer un « Commissariat à la souveraineté numérique ». Cette idée a d'ailleurs été finalement abandonnée.

B. UNE GRANDE DIVERSITÉ DE DÉFINITIONS

Les auditions menées font apparaître une grande diversité de définitions de cette notion, en dépit d'une forme de consensus quant aux éléments fondamentaux qui pourraient sous-tendre une « politique de la souveraineté numérique ».

Au cours de ses travaux, votre rapporteur a souhaité interroger cette notion à travers un ensemble de questions simples, pour en retenir la définition la plus opérationnelle possible :

– Quels sont les grands « principes » que recouvre la notion de souveraineté numérique ?

– Quel peut être le contenu concret de cette politique pour être efficace et réaliste ?

– Quel peut être le juste périmètre d'une politique de la souveraineté numérique ?

1. Trois grands principes pour l'État : liberté de choix, maîtrise technologique et réversibilité

Pour répondre à la question des « principes » de la souveraineté numérique et du contenu d'une telle politique, votre rapporteur souhaite se référer aux propos tenus lors de son audition par M. Nadi Bou Hanna, directeur interministériel du numérique [(2)]. Ce dernier avait en effet tracé, à cette occasion, à grands traits, un cadre utile pour penser cette question. Pour M. Bou Hanna, il ne peut y avoir de souveraineté numérique pour la puissance publique, sans :

– la liberté pour la puissance publique d'effectuer librement des choix stratégiques et technologiques en matière de numérique, et donc, en un sens, de choisir également « *ses dépendances* » ;

– la capacité de la puissance publique à maîtriser ses choix, ce qui implique de disposer « *des expertises qui permettent d'évaluer les risques et les solutions ainsi que d'internaliser certaines fonctions* ». Comme l'indique M. le directeur interministériel du numérique : « *la souveraineté numérique n'est pas possible si une partie des fonctions les plus critiques ne sont pas internalisées* » ;

(1) Loi n° 2016-1321 du 7 octobre 2016.

(2) Audition de M. Nadi Bou Hanna, 21 janvier 2021.

– enfin, corollaire du principe de liberté, la possibilité pour la puissance publique de revenir sur certaines de ses décisions, c'est-à-dire « *mettre fin à des projets, changer de prestataire, sans se retrouver de fait pris dans une chaîne de dépendances sur laquelle nous n'avons plus de pouvoir* ». Cela correspond de fait au principe de réversibilité.

Ces trois principes sont constitutifs d'une autonomie stratégique de l'État, mais aussi d'une forme de « résilience » indispensable pour *« résister aux conséquences d'une crise ou d'une agression et retrouver le plus rapidement possible un fonctionnement normal, même si celui-ci est différent du fonctionnement précédent »* (1) . Comme l'a précisé Mme Naomi Peres, secrétaire général adjointe pour les investissements d'avenir, lors de son audition (2), cette dernière terminologie a été préférée à celle de souveraineté numérique dans le PIA 4, bien qu'elle renvoie davantage au volet défensif de ce concept.

Cette conception peut être déclinée d'une façon similaire au niveau européen, comme l'a rappelé Mme Lorena Boix Alonso, directrice chargée de la stratégie et de la diffusion des politiques à la Direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne, lors de son audition le 19 novembre dernier. Pour cette dernière, la souveraineté numérique est « *d'une importance capitale et fait partie d'un concept plus large, celui de la souveraineté stratégique* » en ce qu'elle rejoint largement l'enjeu de résilience car « *n'importe quelle dépendance, même minime, à l'égard de technologies numériques développées et produites en dehors de l'Union européenne pourrait rendre vulnérables ces différents secteurs de notre économie et de notre société* […] [et] *mettre en péril non seulement notre économie, mais également notre sécurité, nos valeurs démocratiques et nos droits fondamentaux* ». Il est donc indispensable que l'Europe développe « *des projets susceptibles d'aboutir à des alternatives européennes dans les technologies et stratégies clés* » (3) .

2. Une dimension à la fois défensive et offensive

Lors de son audition, M. Thomas Courbe, directeur général des entreprises, a précisé le contenu d'une politique de la souveraineté numérique du point de vue de l'État. Cette dernière comprendrait deux volets, en intégrant à la fois *« la capacité* [de l'État] *à établir les règles qui permettront d'utiliser le numérique, de contrôler les impacts de ses usages et à disposer de l'autonomie sur les principales technologies qui vont conditionner ces usages du numérique »* (4) .

Au sein de son premier volet, sur la définition de règles, trois éléments revêtent, selon lui, une importance particulière : la sécurité numérique, la protection

(1) Audition du Secrétariat général pour l'investissement,11 mars 2021

(2) Idem.

(3) Audition de Mme Lorena Boix Alonso, 19 novembre 2020.

(4) Audition de M. Thomas Courbe, 8 octobre 2020.

des données, et, enfin, la régulation des grands acteurs ainsi que des plateformes, structurants dans ce domaine.

Au sein de son second volet, sur la maîtrise technologique**,** M. Thomas Courbe a mentionné **six technologies critiques :** les semi-conducteurs et la microélectronique, le super calcul, l'Intelligence artificielle, le *cloud* et la maîtrise de la donnée, la cybersécurité. Ces six techniques font l'objet de plans dédiés, financés au titre du plan de relance et des investissements d'avenir.

Une politique de la souveraineté numérique comprend donc nécessairement à la fois un volet offensif et défensif.

Son volet défensif s'appuie principalement sur la régulation. La puissance publique doit être en mesure de réguler les acteurs qui évoluent dans la sphère numérique, conformément aux valeurs qu'elle défend. Comme le relève le secrétaire d'État au numérique, M. Cédric O, *« une entreprise dont le siège social et le patron sont américains est différente d'une entreprise dont le siège social et le patron sont européens par leur culture, par leur approche de la question des valeurs de l'entreprise et par la capacité d'influence des États »* [(1)] . Au niveau européen, l'approche défensive se matérialise ainsi par la proposition de Règlement de la Commission *Digital Services Act (DSA)*, qui vise à une meilleure régulation des contenus en ligne. L'approche défensive implique également de conserver la maîtrise opérationnelle du numérique : en cas de crise, l'État, les administrations, les entreprises et les citoyens doivent toujours avoir accès à leur environnement numérique essentiel. Le développement de la cybersécurité est ainsi, à l'échelle nationale, une composante essentielle du pilier défensif de la souveraineté.

Ce volet défensif comprend également la nécessité de « *nous protéger des pratiques commerciales déloyales en appliquant les règles internationales, garantir la réciprocité des accès aux marchés internationaux, lutter contre les effets de distorsion des subventions étrangères dans notre marché unique et* […], [d'] *adapter le cadre européen de la concurrence pour garantir qu'il réponde aux défis de la transition verte et de la transformation numérique* » [(2)] . Il inclut enfin évidemment les outils de protection économique de nos entreprises stratégiques et la réduction du risque extraterritorial.

Son volet offensif implique, en revanche, de développer un écosystème numérique, de manière à favoriser l'éclosion d'entreprises du numérique ayant vocation à devenir des champions mondiaux. Or, à l'heure actuelle, la plupart des grandes entreprises du numérique sont étrangères, à l'image des GAFAM aux États-Unis et des BATX en Chine. Ce volet renvoie donc évidemment aux politiques de financement des acteurs technologiques, aux politiques de recherche et d'innovation, et, enfin, à la capacité de la puissance publique à maintenir un cadre attractif et compétitif pour les acteurs économiques critiques. Du point de vue des

(1) Audition de M. Cédric O, 22 octobre 2020.

(2) Audition de Mme Lorena Boix Alonso, 19 novembre 2020.

opérateurs de communications électroniques français, qui ont été auditionnés, la souveraineté numérique implique d'avoir « *des opérateurs solides, des infrastructures fortement déployées, redondantes, accessibles sur l'entièreté du territoire* » ainsi que la capacité à travailler « *en confiance* » avec les autorités sur les différents sujets qui animent le secteur, et donc d'interroger aussi les différences de fiscalité entre ces acteurs et certains acteurs dominants du numérique [(1)].

Un équilibre doit ainsi être trouvé entre un pilier défensif, qui a jusqu'à présent été le principal moyen d'action des institutions nationales et européennes à travers la régulation, et un pilier offensif qui doit prendre de l'ampleur. Ce dernier doit être renforcé en France et dans les États membres de l'Union européenne, de manière à favoriser l'émergence d'un tissu productif d'entreprises technologiques et numériques, vecteur d'innovations.

3. Une ambition à co-construire avec l'ensemble des acteurs nationaux et nos partenaires européens

Quant au périmètre d'une telle politique, deux derniers éléments ressortent des auditions menées par la mission d'information.

Une politique de souveraineté numérique nationale implique nécessairement de mobiliser l'échelon européen. L'Union européenne dispose en effet d'une taille suffisante pour que les tentatives de régulation des acteurs du numérique aient un poids réel et que les entreprises puissent se positionner de façon compétitive sur les différents segments du marché numérique. Cette double nécessité plaide en faveur d'un modèle ouvert d'autonomie stratégique partagée, qui correspond *de facto* à une « *troisième voie* » « *dans une conception* [de cette ambition] *qui n'est ni protectionniste, ni hégémonique* », comme l'a rappelé M. Henri Verdier, ambassadeur du numérique [(2)] . Ce dernier a insisté à juste raison sur quatre éléments qui semblent décisifs à votre rapporteur pour construire une souveraineté numérique nationale et européenne : la sécurité & la cybersécurité, la puissance de création, une puissance normative maîtrisée, et, enfin, une autonomie des ressources utilisées.

En outre, la souveraineté numérique ne peut être l'apanage des seuls États : les entreprises, notamment grâce aux solutions innovantes qu'elles proposent, et les citoyens, dans leurs usages, doivent participer à cette co-construction. La table-ronde réunissant les différentes associations représentatives des collectivités territoriales a témoigné d'une vraie maturité sur les sujets numériques et d'une volonté de participer à cette co-construction, aussi bien de la part des régions que des départements et des villes. Les acteurs locaux ont ainsi insisté, lors de leur audition sur les « *enjeux de sécurité, de résilience, de maîtrise »* propre à la question

(1) Audition du 26 novembre 2020.

(2) Audition de M. Henri Verdier, 15 octobre 2020.

de la souveraineté numérique. Ceci doit être salué [1] . Il ne saurait y avoir de souveraineté numérique sans la pleine mobilisation de ces derniers.

Il ressort de ces différents éléments qu'une politique de souveraineté numérique ne peut être envisagée qu'en conjuguant trois dimensions essentielles :

– *une approche juridique*, pour garantir un cadre protecteur des droits et libertés des citoyens, et réguler l'action des grands acteurs ;

– *une approche économique* pour stimuler le potentiel d'innovations des acteurs nationaux et encourager la constitution d'écosystèmes compétitifs ;

– et, enfin, *une approche libérale ou citoyenne*, qui mobilise les citoyens en les sensibilisant aux enjeux politiques de leurs usages.

C. TROIS DIMENSIONS PRINCIPALES À ARTICULER

1. L'approche juridique : renforcer la capacité de régulation de la puissance publique

La question de la souveraineté numérique doit être appréhendée, d'abord, sous l'angle juridique, ce qui revient à s'interroger sur la capacité de l'État « *de n'être obligé ou déterminé que par sa propre volonté* » [2] . La souveraineté recouvre en effet, selon l'Assemblée générale des Nations-Unies le « *droit inaliénable de choisir et de développer son système politique, économique, social et culturel sans aucune forme d'ingérence de la part de n'importe quel État* » [3] .

Dans cette perspective, promouvoir une forme de souveraineté numérique nationale et européenne revient à défendre la capacité de l'État à imposer ses règles dans l'espace physique et numérique, et à ne pas admettre, sans y consentir, que d'autres règles puissent régir cet espace, que celles-ci émanent d'acteurs privés mais aussi d'autres acteurs publics comme les États. Cette distinction, entre souveraineté numérique interne et externe, a été rappelée par M. Thibaut Douville, professeur des Universités, lors de son audition, cette notion recouvrant à la fois, dans l'ordre interne, « *la possibilité d'adopter des normes et de les faire appliquer dans l'environnement numérique* » [ainsi que, dans l'ordre externe], « *la capacité de l'État à demeurer indépendant* » [4].

---

(1) Table ronde organisée le jeudi 10 décembre 2020 consacrée aux collectivités territoriales, avec M. Ariel Turpin, délégué général de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA), Mme Valérie Nouvel, vice-présidente du département de la Manche, Mme Ann-Gaëlle Werner-Bernard, conseillère parlementaire de l'Assemblée des départements de France (ADF), M. Guilhem Denizot, conseiller innovation de l'ADF, et M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France.

(2) Louis Le Fur, État fédéral et Confédération d'États, Paris, 1896, p.443.

(3) Résolution n°2131 (XXe session) de l'Assemblée générale des Nations Unies du 21 décembre 1965, documents officiels, supplément n° 14.

(4) Audition du Pr Thibaut Douville,11 mars 2021.

Cette approche intègre, en conséquence, à la fois les enjeux de régulation de l'Internet, des réseaux sociaux, et la protection des droits fondamentaux des citoyens et des intérêts nationaux, mais aussi la question de l'extraterritorialité de certaines législations étrangères, qui pourraient venir remettre en cause les intérêts précités. Elle comprend donc *de facto* une forte dimension géostratégique tout en interrogeant aussi les modalités d'exercice de la puissance normative souveraine sur des terrains et dans des contextes nouveaux.

2. L'approche économique : soutenir l'émergence d'écosystèmes technologiques compétitifs

La souveraineté numérique comprend évidemment une importante dimension économique : le « monde numérique » repose sur l'existence d'acteurs privés parfois dominants qui innovent et vendent des services numériques ou des équipements indispensables à son fonctionnement matériel.

Cette approche est évidemment complémentaire de l'approche juridique de la souveraineté numérique, puisque les « champions du numérique » constituent autant des vecteurs d'influence et de *soft power* évidents pour leurs États d'origine, et qu'il convient donc aussi de pouvoir disposer des outils nécessaires pour protéger les « pépites » françaises ou européennes.

La promotion d'une forme de souveraineté numérique nationale et européenne implique également de travailler à l'émergence d'écosystèmes compétitifs et performants au sein des différentes strates du numérique pour satisfaire les besoins numériques domestiques, mais aussi exporter ces matériels et services.

3. L'approche culturelle et libérale : promouvoir l'autonomie des citoyens dans la sphère numérique à l'âge de la multitude

Toute réflexion sur la construction d'une souveraineté numérique ne saurait faire l'économie de la question des usages et du modèle de valeurs promu dans le cadre juridique au sein duquel ces usages s'effectuent.

Dans cette perspective, en partant du point de vue du citoyen-usager, la défense de sa souveraineté numérique correspond à la nécessité de garantir ses droits et libertés dans le cyberespace, ainsi que sa capacité à choisir entre les fournisseurs de services numériques, afin de ne pas être captif de l'un d'entre eux en raison des spécificités de l'économie numérique. Cette dernière approche comprend donc à la fois les enjeux relatifs à la protection des données, à l'interopérabilité des plateformes, et, par ailleurs, l'enjeu du modèle et des valeurs à défendre dans le cyberespace.

D. PLUSIEURS LEVIERS D'ACTION POSSIBLES POUR LES DÉCIDEURS PUBLICS

Pour parvenir à une souveraineté numérique nationale et européenne, plusieurs leviers peuvent être mobilisés, de nature politique, économique et juridique.

1. Les leviers politiques

Le premier levier politique est la coopération diplomatique entre États pour défendre une approche ouverte du monde numérique. L'avenir économique de la France dans le cyberespace repose en effet sur l'entraide européenne. Or, tous les États ne partagent pas cette approche : la coopération diplomatique est à ce titre essentielle, pour défendre le modèle conforme aux valeurs françaises et européennes d'un monde numérique libre et ouvert. La coopération diplomatique doit également permettre, dans une économie mondialisée, de garantir la continuité des chaînes d'approvisionnements et le partage de technologies. En ce sens, la construction d'une souveraineté numérique doit permettre d'éviter la répétition de l'échec de la crise sanitaire de 2020, durant laquelle les tentatives de coopérations technologiques n'ont pas abouti.

Le second levier politique est la préservation des intérêts nationaux face aux tentatives de déstabilisation. Les États et les entreprises doivent être en mesure de lutter contre les attaques malveillantes, de manière à protéger leurs données et celles des citoyens.

2. Les leviers économiques

Le levier économique le plus important est la politique industrielle et concurrentielle, qui favorise l'apparition d'entreprises technologiques innovantes. Il s'agit ainsi de disposer de compétences suffisantes sur le territoire, mais aussi de dispositifs d'accompagnement à la création, puis au développement d'entreprises du numérique. Le levier industriel est ainsi la composante essentielle du pilier offensif de la souveraineté numérique.

La fiscalité est le second levier de politique publique en matière économique. Les États doivent trouver un équilibre entre deux objectifs, qui peuvent parfois être contradictoires. D'une part, l'équité fiscale doit conduire à la juste taxation des entreprises du numérique qui, par leurs caractéristiques, ne bénéficient pas toujours d'un établissement stable sur le territoire où elles délivrent leurs services. D'autre part, la fiscalité est également un élément d'attractivité, qui peut contribuer à attirer des entreprises technologiques sur le territoire, afin d'accroître le tissu productif de ce secteur.

3. Les leviers juridiques

Les leviers juridiques s'appuient en grande partie sur la régulation et participent, à ce titre, de l'approche défensive de la souveraineté numérique. Il s'agit, d'abord, de garantir la protection des intérêts nationaux et européens contre certaines pratiques : il en va ainsi des deux propositions de Règlement de la Commission, le *Digital Services Act* en matière de régulation des contenus en ligne, et le *Digital Market Act* qui vise à instaurer un nouveau modèle de régulation du comportement concurrentiel des grandes plateformes sur le marché européen.

Les leviers juridiques peuvent également avoir une utilité pour se prémunir contre les normes d'autres États, d'application extraterritoriale. À titre d'exemple, les États-Unis ont adopté en 2018 une loi fédérale sur l'accès aux données de communication, notamment opérées dans le *cloud*. Cette loi permet aux instances de justice américaines de solliciter auprès des fournisseurs de services opérant aux États-Unis, les communications personnelles d'un individu sans que celui-ci en soit informé, ni que son pays de résidence ne le soit, ni que le pays où sont stockées ces données ne le soit [(1)]. Selon Mme Servane Augier, directrice générale déléguée de 3DS OUTSCALE, « *dans le contexte réglementaire actuel, la souveraineté s'entend du fait de n'être absolument pas soumis à des réglementations extra-européennes. J'entends par là que l'on ne peut pas prétendre être souverain si l'on est soumis au Cloud Act*. » [(2)] .

La bonne articulation de ces différents leviers, et des différentes dimensions de la souveraineté numérique évoquées précédemment est indispensable pour renforcer le niveau de souveraineté numérique de la France et de l'Union européenne. En effet, contrairement à d'autres États, l'Europe connaît un niveau de dépendance élevé dans ce domaine, qui l'expose mécaniquement à des difficultés importantes en cas de crise.

III. UNE ABSENCE ÉVIDENTE DE SOUVERAINETÉ NUMÉRIQUE NATIONALE ET EUROPÉENNE

Si le numérique réinterroge les attributs de souveraineté de tous les États, ces derniers ne sont pas en situation d'égalité vis-à-vis des évolutions afférentes à cette dynamique.

A. LA CHINE ET LES ÉTATS-UNIS ONT RÉUSSI À BÂTIR LEUR SOUVERAINETÉ NUMÉRIQUE SUR DES MODÈLES TRÈS DIFFÉRENTS.

Actuellement, les États-Unis et la Chine sont les deux États qui possèdent le niveau d'indépendance numérique le plus important, pour des raisons tenant à l'existence d'acteurs numériques de taille critique qui disposent de parts

(1) C. Fischer, The cloud Act : A dangerous expansion of police snooping on Cross-Border Data, Electronic Frontier Foundation, 8 février 2018.

(2) Audition de Mme Servane Augier, 9 février 2021.

importantes du marché numérique mondial (GAFAM) et/ou d'un marché domestique profond tout en manifestant cette intention (BATX).

Cette autonomie, toujours relative et incomplète par définition, repose, pour les États-Unis, sur une puissance financière et technologique sans égal, qui se traduit par un fort potentiel d'innovation**,** dans un domaine où il est extrêmement difficile, pour les concurrents, de rattraper le retard pris. On peut la qualifier de souveraineté numérique « ouverte », dans la mesure où elle prend appui sur un ensemble d'acteurs privés et se traduit plutôt par une expansion de la sphère numérique américaine au-delà des frontières nationales de ce pays.

Dans le cas de la Chine, la construction d'une souveraineté numérique « fermée » procède plutôt de facteurs politiques (défense du modèle chinois, protection des institutions). Elle traduit une forme de « *régionalisation de l'Internet* » évoquée par M. Sébastien Soriano, alors président de l'ARCEP, lors de son audition (1) . Cette souveraineté numérique nationale repose sur l'existence d'infrastructures, d'équipements et de logiciels nationaux, ainsi que sur le refus de l'usage des outils étrangers, en particulier américains (2). Elle est évidemment éminemment politique, puisqu'elle constitue un instrument de promotion du modèle politique chinois.

Au-delà de leurs différences profondes, force est de constater que ces modèles de conquête d'une forme d'autonomie stratégique numérique maximale possèdent deux points communs qu'il convient de relever : une forte volonté politique, d'une part, et le recours à la puissance publique dans un rôle de sélection ou d'encouragement des acteurs numériques les plus prometteurs, *via* le levier de la commande publique, d'autre part. Comme l'a rappelé en effet M. Bernard Benhamou, déjà précédemment cité, « *les technologies fondamentales utilisées aujourd'hui dans l'iPhone, pour quasiment la totalité d'entre elles, ont été développées sur des crédits fédéraux américains. L'Internet, le premier, a été développé sur fonds fédéral militaire, [et] l'on pourrait parler des écrans tactiles, des interfaces vocales, des interfaces en réalité augmentée. Pratiquement toutes les technologies clés ont pu être développées parce que la puissance publique a largement investi dans leur développement, parce que la puissance américaine, depuis plus de cinquante ans, a développé un mécanisme appelé le Small Business Act, c'est-à-dire une loi orientant une partie significative de la commande publique vers des PME innovantes* » (3).

(1) Audition de M. Sébastien Soriano,10 décembre 2020.

(2) Facebook, par exemple, est interdit en Chine, mais dispose de son équivalent Tencent Qzone.

(3) M. Bernard Benhamou, audition du jeudi 29 octobre 2020.

B. L'EUROPE RESTE DANS UNE SITUATION D'HÉTÉRONOMIE NUMÉRIQUE PROBLÉMATIQUE EN DÉPIT DE SES ATOUTS

À l'inverse de la Chine et des États-Unis, l'Europe se trouve actuellement dans une situation de forte dépendance numérique, même si les situations des États membres sont évidemment variables, certains d'entre eux, dont la France, étant dans une position plus favorable que d'autres pays en raison de leurs ressources propres.

Votre rapporteur souhaite insister sur le caractère problématique de cette situation alors que l'Europe dispose, en théorie, d'atouts importants et d'une puissance économique et financière collective équivalente à celle des pays précédemment pris en exemple. Certains blocages, d'ordre politique, économique, financier et culturel expliquent néanmoins que les écarts se soient creusés rapidement, et que la situation actuelle ne soit pas satisfaisante.

En un mot, et comme l'a bien résumé M. Bernard Benhamou, secrétaire-général de l'Institut pour la souveraineté numérique, nous sommes malheureusement pour l'instant « *en situation hautement défensive* ». Il nous faut donc « *absolument réfléchir à une possibilité de rebond, à une nécessité de rebond par rapport à cela. Cette nécessité doit prendre appui sur les faiblesses que nous notons aujourd'hui dans les acteurs du numérique, faiblesses en termes de confiance, faiblesses en termes de sécurité et de protection des données, faiblesses en termes de protection des processus démocratiques* » [(1)].

Les nombreuses auditions menées aboutissent à ce constat sévère : l'Europe reste encore un « nain numérique » en dépit d'atouts indéniables et d'acteurs parfois bien positionnés dans des secteurs critiques, ce qui apparaît d'autant plus frustrant. Cette dépendance se manifeste tout au long des maillons de la chaîne de valeur du numérique, ou de ses différentes couches, pour reprendre le modèle précédemment évoqué. Sans prétendre à l'exhaustivité, il est possible de relever un certain nombre de faiblesses structurelles qui restent problématiques.

1. Une dépendance vis-à-vis des matériaux et composants fondamentaux des équipements numériques

L'Union européenne se trouve, d'abord, dans une situation de dépendance quasi-totale vis-à-vis des métaux rares indispensables pour produire les équipements numériques, que ces derniers soient attenants aux terminaux ou aux infrastructures. À l'heure actuelle, la Chine fournit 98 % des terres rares lourdes nécessaires à l'Union européenne, la Turquie 98 % du borate et l'Afrique du Sud 71 % des platinoïdes, pour ne citer que ces trois exemples. S'il existe incontestablement un niveau de conscience élevé de cette problématique, l'Union européenne ayant lancé un plan dédié à ce sujet, il n'en demeure pas moins que ce premier élément de dépendance reste une contrainte importante pour envisager toute forme sérieuse d'autonomie numérique, en plus de rendre plus difficile la maîtrise de l'empreinte environnementale du numérique.

(1) Audition de M. Bernard Benhamou, 29 octobre 2020.

L'Union européenne se retrouve également dans une position de forte dépendance vis-à-vis de la production de semi-conducteurs, composants pourtant indispensables au fonctionnement des équipements numériques, et dont l'importance ira croissant avec les progrès de l'Intelligence artificielle. Le marché mondial des semi-conducteurs, représente une valeur de 440 milliards de dollars. La moitié des composants produits et vendus est destinée au marché des ordinateurs, des smartphones et des mémoires. Or, comme le relève M. Thierry Tingaud, président du comité stratégique de filière (CSF) « Industries électroniques », alors « *qu'il existe une prise de conscience* [de cet enjeu] *au niveau mondial* », qui se traduit par le fait que « *la Chine, les États-Unis mais aussi le Japon, la Corée et Taïwan consentent des investissements massifs pour avoir un leadership* […] *dans ce domaine* », les acteurs européens ne sont pas, pour l'heure, fournisseurs de ces éléments, qui restent produits par un nombre très restreint d'acteurs que sont « *Intel, Qualcomm, Broadcom,* [ainsi que] *les trois fabricants de mémoires dynamiques dans le monde* » (1). Les vives tensions intervenues il y a quelques mois entre la Chine et les États-Unis sur ce sujet, pendant la crise sanitaire, donnent à voir, là aussi, la situation problématique dans laquelle se retrouve l'Europe, en dépit de l'existence d'acteurs, notamment français, qui disposent d'une vraie compétence sur certains des segments de ce marché.

Sur ce sujet, également, le soutien de longue date de projets importants d'intérêt européen commun, (PIEEC), et la perspective d'une alliance européenne pour l'électronique (2) constituent des éléments positifs, qui peuvent être salués. La localisation d'infrastructures de production en Europe, pour limiter les risques de sur-dépendance, notamment des équipementiers numériques vis-à-vis de leurs fournisseurs, doit être encouragée.

2. L'Europe reste encore un « nain numérique » sur le plan économique

La faiblesse de l'Union européenne en matière de production d'équipements et de terminaux numériques constitue un élément de fragilité indiscutable. La majorité des matériels utilisés sont en effet non-européens.

Sans prétendre à l'exhaustivité, quelques exemples de marchés clefs suffisent à indiquer la domination des équipements numériques chinois et américains, au niveau global.

Le marché des PC, qui a connu une hausse forte en 2020 avec plus de 300 millions d'ordinateurs personnels vendus, est dominé par le chinois Lenovo (24 % de part de marché), qui devance les acteurs américains HP (22,4 %), Dell Technologies (16,6 %), Apple (7,6 %) et Acer Group (6,9 %) (3) .

---

(1) Audition de M. Thierry Tingaud, 8 octobre 2020.

(2) Le commissaire européen, M. Thierry Breton, a fait part de sa volonté de voir se constituer une alliance européenne dédiée aux processeurs et technologies des semi-conducteurs en vue de doubler la capacité de production de ces derniers en Europe d'ici 2030.

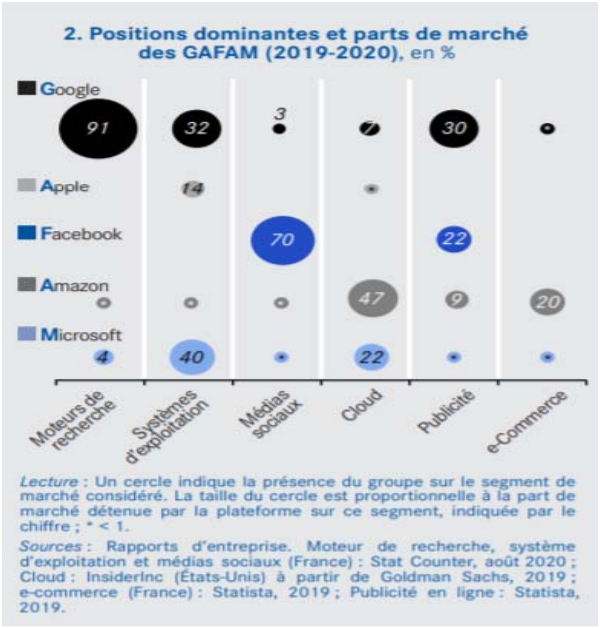
(3) Source : IDC - https://www.phonandroid.com/ventes-de-pc-le-marche-connait-sa-plus-forte-croissance-depuis-10-ans.html

Il en va de même sur le marché européen et mondial des smartphones. Au niveau européen, l'acteur coréen Samsung dispose des parts de marché les plus élevées (32 % au premier trimestre 2021), devant l'américain Apple (22 %) et le chinois Xiaomi (18 %) et les deux acteurs chinois Oppo (6 %) et Huawei (2 %) (1) . Les parts de marché mondiales respectent *grosso modo* cet ordre de classement.

Les écarts sont encore plus importants pour la partie *software*, par exemple en ce qui concerne les systèmes d'exploitation. Au niveau mondial, la domination des acteurs américains est incontestable, qu'il s'agisse des solutions pour les PC de Windows, qui devance de loin le second acteur du marché, Apple, ou des OS pour les terminaux mobiles, dont le marché est réparti entre Google (Android) et Apple (iOS). Elle se répercute logiquement en termes de pouvoir de marché de ces deux acteurs au bénéfice de leurs magasins d'applications respectifs.

Les parts de marché des GAFAM sur un certain nombre de marchés critiques, telles que rappelées au sein de la note du Conseil d'analyse économique d'octobre 2020 « Plateformes numériques : réguler avant qu'il ne soit trop tard » témoignent de ce puissant différentiel entre acteurs européens et américains.

PARTS DE MARCHÉ DES GAFAM (2019-2020)



Source : Conseil d'analyse économique

(1) https://news.strategyanalytics.com/press-releases/press-release-details/2021/Strategy-Analytics-Global-Smartphone-Shipments-Surge-to-340-Million-units-Up-24-YoY-in-Q1-2021/default.aspx

Sur les principaux marchés numériques, l'Europe n'est donc pas parvenue à se doter d'acteurs de taille critique, ce qui fait dire à juste titre, à M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique que, face aux « *grands acteurs non européens, qu'ils soient américains (Google, Apple, Amazon, Microsoft) ou chinois (Baidu, Alibaba, Tencent, Huawei, Xiaomi)*[, il] *manque dans ces acronymes des lettres européennes* » (1) .

Cette absence d'acteurs critiques sur le marché mondial du numérique ne signifie pas qu'il n'existe pas, sur des segments spécifiques, des acteurs européens d'influence mondiale. Elle s'explique par un ensemble de facteurs au sein desquels la politique de la concurrence européenne joue une part non négligeable. Le marché européen du numérique reste encore, par bien des aspects, un simple agrégat de marchés nationaux, ce que démontre son éclatement par exemple en matière de communications électroniques. L'Europe comprend en effet un nombre très important d'acteurs, dans un contexte économique de prix bas qui entrave la constitution de marges suffisantes et réduit mécaniquement leur capacité à investir et à peser au sein de nouveaux marchés, en plus de produire parfois des effets de distorsions préjudiciables.

3. Une situation quotidienne de dépendance numérique vis-à-vis d'outils et de services non-européens

Le numérique étant d'abord un nouveau mode de vie et de fonctionnement de nos sociétés, il convient de traduire concrètement la réalité de cette absence de souveraineté numérique européenne dans le quotidien de ses usagers, pour mieux en comprendre les conséquences, notamment en cas de crise.

Au quotidien, les citoyens européens achètent des terminaux qui sont produits par des acteurs non-européens avec des composants asiatiques et fonctionnent sur des systèmes d'exploitation américains. Ils utilisent les services des magasins d'application américains et effectuent leurs recherches en ligne en mobilisant de façon majoritaire le moteur de recherche Google. Ils utilisent enfin massivement les réseaux sociaux, créés et régulés par des acteurs américains. Ils procèdent à leurs achats en ligne en recourant au leader du marché, l'américain Amazon. Enfin, la pratique croissante du streaming est dominée, elle aussi, par des acteurs américains (Netflix, Amazon Prime, Disney +) dont la puissance financière est supérieure aux acteurs européens (OCS, Canal + à la demande), bien que ces derniers proposent une offre différente qui rencontre son public.

Cet état manifeste de dépendance numérique, qui se traduit par l'absence d'acteurs européens de premier plan, est problématique, pour deux raisons :

– en cas de tensions géopolitiques, de multiples angles d'influence s'offrent à certains acteurs géopolitiques, qui auront forcément la tentation d'employer leurs leviers d'influence respectifs ;

(1) Audition de M. Bernard Benhamou, 29 octobre 2020.

– un mouvement d'entraînement vers de nouvelles dépendances se crée, en raison du caractère stratégique de certains des domaines cités, comme le marché des systèmes d'exploitation par exemple.

4. Une multitude de causes explique cette situation

Elle procède d'un ensemble complexe de causes qui doit être étudié et a été au cœur des travaux de la mission d'information. Parmi les nombreuses contributions des acteurs entendus, le constat selon lequel « *l'Europe cumule des faiblesses déjà bien identifiées en matière de souveraineté numérique, qu'il s'agisse de facteurs internes ou externes* » mis en avant par M. Julien Nocetti, est pertinent. M. Nocetti relève en effet, à juste raison, pour les facteurs internes, « *l'insuffisante intégration du marché numérique, les problématiques de financement de l'innovation, les divergences politiques entre États membres* » et, pour les facteurs externes, des « *stratégies de puissances prédatrices et éprouvées* » de la part des États-Unis et de la Chine (1).

S'agissant des facteurs internes, les auditions ont largement confirmé ce diagnostic : positionnement différents des États membres sur ces sujets, avec des éléments de résistance, voire d'opposition, entre souveraineté nationale et européenne sur le numérique, difficultés des entreprises technologiques à se financer sur le marché européen, notamment sur les « tickets » les plus importants, capacités d'anticipation et de veille technologique insuffisantes, au niveau européen, pour articuler une action efficace sur des projets d'ampleur, réticences, enfin, à soutenir la création de champions européens en raison d'un primat accordé à la politique de la concurrence sur la « politique industrielle » européenne, longtemps secondaire. Il est possible d'ajouter à cette liste l'encadrement strict, et peut être excessif, de la commande publique, et sa mobilisation parfois insuffisante au sein des États membres, dans une optique de stimulation de l'innovation et de l'offre technologique privée.

S'agissant des facteurs externes, il est incontestable que l'avance d'un certain nombre d'acteurs américains a pu créer le sentiment d'un retard difficile, voire impossible à rattraper sur certains segments, ce qui est exact. Les auditions font apparaître que l'Europe et ses États membres ont souvent été réticents à utiliser des outils de protection d'un certain nombre d'acteurs critiques, faute d'outils parfois, faute de souhaiter les utiliser aussi dans certains cas. Sur le plan diplomatique, la défense des intérêts numériques européens a pu être insuffisante, pour des raisons liées à des divergences entre les États membres, ou considérée comme secondaire au sein des instances internationales, même si la situation s'est améliorée à mesure même de la place croissance du numérique au sein des sujets politiques.

(1) Audition de M. Julien Nocetti, 11 mars 2021.

En conséquence, votre rapporteur ne peut que plaider pour l'amplification de la dynamique mise en œuvre ces derniers mois, sur le sujet de la souveraineté numérique, au niveau européen. Cette dynamique doit être soutenue également au niveau national, pour valoriser au mieux les différents atouts dont dispose la France, à savoir un écosystème tech dynamique et des capacités de financement des entreprises importantes, des entreprises bien positionnées sur certains segments clefs, un réel savoir-faire en matière de formation aux technologies de pointe et, enfin, une commande publique forte dont la mobilisation doit être réinterrogée à l'aune de ces enjeux.

DEUXIÈME PARTIE : BÂTIR UNE SOUVERAINETÉ NUMÉRIQUE NATIONALE ET EUROPÉENNE

I. UNE POLITIQUE DE SOUVERAINETÉ NUMÉRIQUE AU SERVICE DES CITOYENS.

Une politique de souveraineté numérique ne peut se construire qu'en partant des citoyens, dont les usages constituent le cœur du numérique. Comme l'a rappelé M. Sébastien Soriano, alors président de l'Autorité de régulation des communications électroniques, des postes, et de la distribution de la presse (Arcep), « *dans nos sociétés démocratiques modernes, la première souveraineté à laquelle il faut être attentif, c'est celle des individus, en particulier leur capacité à faire des choix* » (1). Avant de se poser la question de la régulation, indispensable pour garantir que le citoyen puisse « *exercer son libre arbitre, dans la sphère réelle comme dans la sphère virtuelle* » (2), il convient de lui assurer un accès performant à des réseaux efficaces et résilients.

A. CRÉER LES CONDITIONS DE LA CONFIANCE DANS LE NUMÉRIQUE

1. Répondre à la demande de connectivité des citoyens

a. Une accélération indispensable des déploiements fixe et mobile

L'égal accès à des infrastructures numériques est une condition indispensable de la confiance des citoyens dans le numérique. Il ne peut en effet y avoir de débats sur les usages du numérique lorsque persiste le sentiment que ce dernier viendrait creuser les inégalités. Il existe actuellement une forte demande de connectivité aux réseaux « fixe », *via* la fibre, et « mobiles », *via* la 4G, qui doit être entendue. Il est en effet impératif de permettre à chacun de bénéficier des avantages du numérique. Il convient également d'éviter que la défiance ne s'installe, et ne vienne nourrir d'autres craintes liées, par exemple, au déploiement de la 5G (3) .

Les auditions font apparaître qu'en matière de rythme de déploiement, la France se positionne favorablement par rapport à ses voisins européens, grâce à une politique volontariste menée dans le cadre du plan France Très Haut Débit (4) et du

---

(1) Audition de M. Sébastien Soriano, jeudi 10 décembre 2020.

(2) Idem.

(3) Lors de son audition le 10 décembre 2020, M. Ariel Turpin, délégué général de l'AVICCA avait ainsi exprimé cette crainte dans les termes suivants : « l'arrivée de la 5G a un impact négatif sur le déploiement du *« New Deal »* et de la 4G. En effet, même lorsque les élus et les habitants étaient très favorables à l'arrivée de la 4G, nous constatons une réactivation des oppositions et des associations locales qui rend compliqué même le développement de la 4G ».

(4) Le Plan France Très Haut Débit a été lancé en 2013 pour permettre à l'ensemble des citoyens de bénéficier du très haut débit d'ici 2022. Il fixe comme objectif l'accès au très haut débit (> 30 Mbit/s) pour tous en 2022.

New Deal mobile [1] . L'Observatoire du très haut débit [2], publié par l'AVICCA et InfraNum avec l'appui de la Banque des territoires, indique en effet que la France est le marché le plus dynamique d'Europe sur la période de septembre 2019 à septembre 2020, en nombres d'abonnés au THD (+ 2,8 millions) et de foyers raccordables (+ 4,6 millions). En outre, au niveau global, comme l'a relevé M. Sébastien Soriano, si en 2014 « *la France était dernière au classement européen du très haut débit et avant-dernière pour la 4G* », elle est aujourd'hui « *le pays d'Europe où la fibre se déploie le plus en valeur absolue selon le classement IDATE Digitaworld* ». Les investissements au sein du secteur des télécoms ont en effet fortement augmenté lors cette période, en passant de 7 milliards d'euros en 2014 à plus de 10 milliards d'euros en 2019.

Votre rapporteur salue évidemment ces progrès, mais conserve à l'esprit que le classement de la France, au niveau européen, en termes d'infrastructures numériques, reste décevant. Selon l'index DESI 2020 publié par la Commission européenne, notre pays se classe en effet en 18e position, et possède encore « *de vastes portions de zones moins densément peuplées et de zones rurales qui ne sont toujours pas couvertes* » [3]. Une accélération des déploiements est donc indispensable.

b. Une poursuite des déploiements pendant à la crise sanitaire

i. État des lieux des déploiements « fixe »

Pour les déploiements « fixe », M. Sébastien Soriano a indiqué qu'environ « *16 millions de prises ont été installées au cours des cinq dernières années* ». D'après les chiffres publiés par l'ARCEP dans son Observatoire du haut débit et du très haut débit (T4 2020), « *à la fin du quatrième trimestre 2020, 28,6 millions de locaux étaient éligibles à des services à très haut débit, toutes technologies confondues, dont 21,7 millions en-dehors des zones très denses* » [4] . Le nombre d'abonnements à haut et très haut débit atteint désormais 30,6 millions (dont 14,7 millions d'abonnements THD), soit une hausse du nombre d'accès de 2,7 % (+ 800 000) en 2020, « *croissance qui n'avait pas été aussi élevée depuis trois ans* » [5].

Comme l'ont rappelé les opérateurs, le rythme de déploiement très élevé en 2019, avec 4,8 millions de lignes déployées, a été maintenu en 2020, ce qui constitue

---

(1) Le New Deal mobile est un accord passé entre l'État et les opérateurs dans le but d'accélérer le déploiement de la couverture mobile 4G en France. Il fixe notamment comme objectif le passage en 4G de tous les sites des opérateurs et la couverture d'un ensemble de zones blanches dans le cadre d'un dispositif spécifique de « couverture ciblée ». Il comprend, par ailleurs, d'autres obligations liées notamment à la couverture des axes routiers et ferroviaires.

(2) InfraNum-Avicca, Observatoire du Très Haut Débit, 9e édition, 2021.

(3) Commission européenne, Indice relatif à l'économie et à la société numériques, France, 2020, p.8.

(4) https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/observatoire-des-abonnements-et-deploiements-du-haut-et-tres-haut-debit/observatoire-haut-et-tres-haut-debit-abonnements-et-deploiements-t4-2020.html

(5) Idem.

déjà une performance notable. Pendant la crise, les déploiements se sont en effet poursuivis à un rythme réduit, « *de l'ordre de 20 %, 30 % ou 40 %* » d'après les opérateurs, quand la plupart des autres secteurs, le BTP par exemple « *étaient à 90 % à l'arrêt* » (1) .

Votre rapporteur considère que les acteurs de ce secteur ont ainsi fait la démonstration de leur résilience et de leur capacité à assurer la maintenance des réseaux, dans un contexte de « choc d'usages » qui avait légitimement suscité des inquiétudes au mois de mars 2020. Il souhaite également saluer la capacité de dialogue et d'action concertée du Gouvernement, de l'ARCEP et des opérateurs qui ont permis à notre pays de pouvoir compter pleinement sur ses réseaux numériques pour faire face à la crise sanitaire. Il considère, enfin, que les instances de dialogue mises en œuvre pendant la crise pour échanger avec les acteurs grands consommateurs de bande passante doivent être pérennisées, de sorte à pouvoir être mobilisées avec encore davantage de rapidité en cas de nouvelle crise.

Proposition n° 1 : Créer un « comité numérique de crise » réunissant les opérateurs, les grands acteurs du numérique et les pouvoirs publics en cas de difficulté sur les réseaux numériques.

ii. État des lieux des déploiements mobiles

Les déploiements mobiles en 4G progressent également à un rythme important ces dernières années, conformément aux objectifs fixés dans *New Deal* mobile. La couverture mobile du territoire est ainsi passée, en surface, « *de 46 % en 2018, au moment de la signature du « New Deal mobile », à 76 % au milieu de l'année 2020* », ce qui a permis à « *notre pays,* [qui] *était classé vingt-sixième sur vingt-huit,* [de se situer] *maintenant en milieu de tableau* » (2) , selon M. Sébastien Soriano, alors président de l'ARCEP.

Sur le premier volet du *New Deal* mobile, c'est-à-dire l'engagement des opérateurs à basculer tous leurs sites mobiles en propre en 4G d'ici la fin de l'année 2020, les opérateurs considèrent qu'ils sont « *quasiment à l'objectif* » (3), constat qui semble partagé par l'ARCEP.

Sur le dispositif de couverture ciblée, destiné à améliorer la disponibilité de la 4G en zones peu denses, ces mêmes opérateurs indiquent avoir « *atteint l'objectif de déploiement du nombre de pylônes, sauf pour une vingtaine de pylônes qui n'ont pas pu être installés dans les délais* [en raison soit de] *difficultés liées à des*

(1) Audition de M. Olivier Riffard, directeur des affaires publiques de la Fédération française des télécoms, M. Anthony Colombani, directeur corporate de Bouygues Telecom, Mme Claire Perset, secrétaire générale adjointe de SFR et Mme Ombeline Bartin, responsable des relations institutionnelles de Free mobile, 26 novembre 2020.

(2) Audition de M. Sébastien Soriano, jeudi 10 décembre 2020.

(3) Audition de M. Olivier Riffard, directeur des affaires publiques de la Fédération française des télécoms, M. Anthony Colombani, directeur corporate de Bouygues Telecom, Mme Claire Perset, secrétaire générale adjointe de SFR et Mme Ombeline Bartin, responsable des relations institutionnelles de Free mobile, 26 novembre 2020.

oppositions de riverains soit [de] *difficultés liées à l'absence d'autorisation administrative d'accès à des sites classés* » [(1)].

Ces éléments indiquent donc que le *New Deal* mobile est entré **«** *en phase industrielle* », mais que les efforts engagés doivent se poursuivre et s'amplifier.

c. Des progrès indéniables mais des inégalités persistantes à résorber

Comme l'ont indiqué les représentants des collectivités locales, *« le New Deal mobile et le plan France Très Haut Débit sont globalement un succès mais nous ne pouvons pas ignorer qu'il reste des problèmes de connexion, que l'inachèvement de la couverture numérique fixe et mobile produit des inégalités dans l'accès au numérique »* [(2)] .

En effet, il reste encore des zones blanches à couvrir, *via* le déploiement des réseaux d'initiative publique, d'une part, et le déploiement de la 4G puis que de la 5G, d'autre part.

Sur la partie « fixe », on ne peut que noter que la zone d'initiative publique connaît une grande variété de rythmes de déploiement des réseaux en fonction des modèles choisis et des dates de lancement de ces projets. Si l'année 2021 devrait être celle du « pic des RIP » avec une prévision de déploiement de 6,2 millions de prises, seuls 31 % des locaux de cette zone étaient couverts par la fibre FttH au niveau national et un peu moins de la moitié (47 %) par le très haut débit au quatrième trimestre 2020, ce qui laisse entrevoir l'ampleur du chemin qu'il reste à parcourir.

L'enjeu de la complétude des déploiements doit également être adressé (6,5 millions de prises à déployer d'ici 2025). En ce sens, le plan de relance, qui a abondé les crédits du plan France Très Haut Débit pour le déploiement des réseaux d'initiatives publiques, constitue un excellent signal envoyé en faveur d'une reprise aussi rapide que possible du rythme nominal des déploiements fixes dans les territoires où les attentes sont fortes.

Votre rapporteur insiste sur l'enjeu de la qualité des déploiements, ce sujet étant régulièrement revenu dans les échanges menés, notamment au sujet du recours au mode STOC [(3)] . Le bon équilibre doit être trouvé pour garantir une résilience des réseaux déployés. C'est la raison pour laquelle votre rapporteur invite l'ARCEP et les services du Gouvernement à faire preuve d'une grande vigilance sur ce point.

---

(1) Idem.

(2) Table ronde consacrée aux collectivités territoriales, avec M. Ariel Turpin, délégué général de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA), Mme Valérie Nouvel, vice-présidente du département de la Manche, Mme Ann-Gaëlle Werner-Bernard, conseillère parlementaire de l'Assemblée des départements de France (ADF), M. Guilhem Denizot, conseiller innovation de l'ADF, et M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France, jeudi 10 décembre 2020.

(3) Le mode STOC (sous-traitance opérateur commercial) consiste, pour un opérateur d'infrastructure, à faire réaliser par l'opérateur commercial le raccordement final du client.

Proposition n° 2 : Renforcer les contrôles mis en œuvre par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) sur la qualité du déploiement des réseaux fixes.

Sur la partie « mobile », enfin, l'enjeu sera évidemment d'approfondir la couverture en 4G, et de préparer le déploiement de la 5G, dont une partie des sites sera implantée en zones rurales conformément au cahier des charges auquel les opérateurs ont consenti lors de l'attribution des premières fréquences sur la bande 3,5 GHZ.

d. Déployer la 5G sans faire de compromis sur la sécurité

Le déploiement de la 5G sur le territoire national constitue un enjeu de souveraineté pour la France et l'Europe à plusieurs titres :

– cette technologie va offrir des gains d'efficacité importants au sein de l'industrie et permettre l'émergence de nouveaux usages dans des domaines variés, de la santé à l'agriculture en passant par la robotique, l'industrie 4.0 etc. Il s'agit d'un élément de compétitivité indispensable pour le développement de nos acteurs industriels nationaux et l'anticipation d'éventuelles ruptures technologiques ;

– cette technologie va également participer à moyen-terme à la couverture mobile du territoire, conjointement avec les déploiements en 4G. C'est en ce sens que le cahier des charges fixé par l'ARCEP prévoit qu'une partie des sites 5G sera progressivement déployés en zone rurale. De ce point de vue, la dynamique engagée devrait conduire, selon M. Sébastien Soriano, à ce que « *la 5G des villes et la 4G + des champs* [offre] *un service quasiment équivalent dans toute la France* » afin de veiller à « *éviter l'apparition de fractures territoriales* » [(1)] ;

– enfin, cette technologie présente des caractéristiques qui lui donnent une certaine sensibilité en matière de sécurité. La virtualisation des réseaux et le déploiement d'un nombre important d'équipements sur le territoire national impliquent une vigilance particulière afin de réduire le risque d'exposition des réseaux numériques à des problématiques de sécurité.

Les auditions font apparaître une situation nationale en cours d'amélioration concernant les réticences au déploiement de la 5G, grâce au dialogue nourri entre les maires et les opérateurs, sur le terrain, mais également un retard incontestable de la France et de l'Europe par rapport aux États-Unis et à la Chine dans ce domaine. De ce point de vue, les craintes exprimées, par exemple, par M. Anthony Colombani, directeur des affaires publiques chez Bouygues Telecom, semblent plus que fondées : « *Dans l'opinion publique et chez certains élus, nous constatons une véritable méfiance, parfois même une vraie défiance, ce qui a conduit certains d'entre eux à prendre des moratoires qui créent évidemment des difficultés pour nous. Il ne faudrait pas que cette opposition larvée à la 5G, parfois violente*

(1) Audition de M. Sébastien Soriano, jeudi 10 décembre 2020.

puisqu'une quarantaine d'antennes ont brûlé en France, nous fasse prendre du retard. C'est un point extrêmement important. » (1).

Votre rapporteur ne peut donc qu'encourager les pouvoirs publics à se mobiliser pour défendre la 5G, d'une part, et à tenir le calendrier des déploiements prévu, d'autre part, afin de s'assurer de minimiser le retard existant dans ce domaine. Il souhaite néanmoins insister, en même temps, sur le fait qu'aucun compromis ne doit être fait sur la sécurité de ces déploiements.

Proposition n° 3 : Maintenir une exigence maximale de sécurité vis-à-vis des déploiements 5G.

Le cadre offert par la loi du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles est en effet pertinent. Il existe néanmoins probablement des marges de progrès en ce qui concerne les délais de traitement des dossiers et la transparence qui peut être offerte aux opérateurs sur les raisons des refus d'autorisation d'exploitation.

Proposition n° 4 : Assurer un traitement rapide des demandes d'autorisation d'exploitation d'équipements 5G. Garantir également une transparence des critères de décision mis en œuvre dans ce cadre.

2. Protéger de façon effective les données personnelles des citoyens

a. Des attentes fortes de la population sur la souveraineté des données

La protection des données est une préoccupation majeure des Français et la condition légitime de leur confiance dans le numérique. Cette vigilance est largement partagée au sein de la population, comme l'a rappelé M. Gwendal Le Grand, secrétaire-général adjoint de la commission nationale de l'informatique et des libertés. Les études récentes sur cette question « *montrent une profonde aspiration de maîtrise des personnes sur leurs données* [puisque] *87 % des Français se déclarent sensibles à la protection des données* » (2).

La capacité de protéger les données des citoyens français est donc un enjeu de souveraineté auquel les citoyens sont très sensibles (3). Selon un sondage IFOP publié en avril 2021 (4) , 69% des Français estiment que la souveraineté des données est un enjeu majeur et 72 % des Français se disent opposés à ce que leurs données personnelles soient stockées en dehors de l'Union européenne. Ainsi que l'a résumé M. Michel Paulin, directeur général d'OVHcloud, une vraie prise de conscience a

(1) Audition de M. Anthony Colombani, 26 novembre 2020.

(2) Audition de M. Gwendal Le Grand, 25 mars 2021.

(3) Audition commune de Mme Servane Augier, directrice générale déléguée de 3DS OUTSCALE, M. Michel Paulin, directeur général d'OVHcloud, et Mme Karine Picard, directrice générale d'Oracle France, 9 février 2021.

(4) IFOP, « les Français et la souveraineté numérique », avril 2021.

eu lieu sur ce sujet. Les Français sont désormais « *extrêmement attentifs sur les domaines de la santé, des données financières, des données publiques. Ils estiment que les données doivent être en France ou en Europe et qu'il doit y avoir une garantie que les acteurs ne puissent pas faire circuler ces données ou métadonnées.* […] *D'une certaine façon, tous les débats passés sur la localisation des données, leur traitement, leurs flux, et l'impact de Schrems II démontrent que ces sujets sont d'actualité et impactent les vies des entreprises et des citoyens* » (1).

b. Un niveau de protection en Europe sans équivalent dans le monde

En matière de protection des données, s'il est évident que la confiance « ne se décrète pas », force est de constater néanmoins que l'Union européenne et ses États membres garantissent un niveau de protection des données personnelles de leurs citoyens sans équivalent dans le monde.

Le cadre juridique actuel est le résultat de plusieurs décennies d'action résolue visant à répondre aux défis politiques, économiques et géopolitiques posés par la question de la protection des données.

Comme l'a rappelé M. Gwendal Le Grand, en France, cette dynamique a d'abord été impulsée à l'occasion de l'adoption de la loi pour l'informatique et les libertés, en 1978, dont l'article premier « *a donné naissance à la CNIL* [et posé] *le principe selon lequel l'informatique doit être au service de chaque citoyen et ne porter atteinte ni à une entité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles et publiques* ». Cette loi a permis d'imposer « *quatre types de nouveaux droits citoyens* [dans ce domaine] *: les droits d'information, d'opposition, d'accès et de rectification* » (2).

À partir des années 1990, ensuite, face aux défis économiques et à l'explosion d'Internet, l'Europe s'est dotée « *d'une directive en 1995, qui reprend les principes de la loi Informatique et Libertés* », puis « *en 2002,* [d']*une directive dite « on Privacy » (Vie privée et communication électronique)* [qui a reconnu] *la spécificité du secteur des communications électroniques, avant que cette dernière évolue le 25 mai 2018 en Règlement général sur la protection des données* » dans un contexte où désormais les GAFAM « *sont devenues hégémoniques et* [où] *de nombreuses avancées technologiques, comme les objets connectés, les techniques de profilage, de surveillance, les outils de contrôle, les algorithmes et le développement des cyberattaques,* [ont nourri] *la conscience collective de devoir revoir à la hausse le niveau de protection des données personnelles. Les révélations d'Edward Snowden aux débuts des années 2010 en sont le symbole* » (3).

Ce Règlement général sur la protection des données est construit autour de cinq axes majeurs, comme l'a rappelé le secrétaire général adjoint de la CNIL (4) :

---

(1) Audition de M. Michel Paulin, 9 février 2021.

(2) Audition de M. Gwendal Le Grand, 25 mars 2021.

(3) Idem.

(4) Idem.

– le renforcement quantitatif et qualitatif du droit des personnes *via* notamment une meilleure explication de la loi Informatique et Libertés, et l'apparition de nouveaux droits, comme le droit à l'oubli, le droit à la portabilité et la possibilité de mener des actions de groupe ;

– la responsabilisation de l'ensemble des acteurs de traitement de données, publiques et privées, sur la base de principes de minimisation de la collecte, de limitation de la durée de conservation et d'obligation de sécurité pour garantir à tout moment le respect du règlement général sur la protection des données. Le RGPD est d'ailleurs fondé sur la notion de risques présentés par les traitements, tant en volume qu'en sensibilité des données. En clair, plus l'acteur est important dans l'écosystème numérique, plus ses obligations et ses responsabilités sont nombreuses ;

– le renforcement du pouvoir de sanction administrative des différentes CNIL au niveau européen. Les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial d'une entreprise, l'option majeure étant appliquée. La gamme des sanctions est également élargie ;

– la mise en place d'un nouveau modèle de gouvernance de la régulation, inédit au niveau européen, au travers d'un guichet unique pour les entreprises et d'un guichet unique pour les citoyens ;

– la libre circulation des données sur l'ensemble du territoire de l'Union et un principe inédit d'extra-territorialité, selon lequel il s'applique à tous les acteurs dès lors qu'un organisme cible des citoyens européens.

Le règlement général sur la protection des données, qui ne connaît pas d'équivalent dans le monde, est progressivement devenu « *un instrument de soft power* [et]*de diplomatie* », de sorte à ce que, selon M. Gwendal Le Grand, il y a eu « *un avant et un après 25 mai 2018 au niveau mondial* ». En effet, suite à son adoption « *des pays ont procédé à la mise à jour de leur cadre national en matière de protection des données, afin de continuer à commercer avec l'Europe. Tel est le cas de la Suisse, du Japon, de la Corée du Sud, du Bénin ou de l'Australie. Des processus législatifs sont en cours dans d'autres pays comme la Tunisie ou le Burkina Faso. Des États ont*, [en outre], *pour la première fois, adopté un cadre juridique général de protection des données personnelles comparable au RGPD dans ses principales dispositions. Tel est le cas de la Californie avec le* California Consumer Privacy Act (CCPA) *adopté en octobre 2018 et entré en application le 1er janvier 2020. Le Brésil a adopté son règlement en 2019. En Inde, la Cour suprême a* [également] *consacré, en 2017, le droit à la protection de la vie privée comme un droit fondamental* ». Ces nombreux exemples font la démonstration qu'en agissant au bon niveau et dans un timing satisfaisant, l'Europe peut peser sur la définition du modèle de valeurs mondial du numérique.

Ce cadre robuste de protection des données personnelles doit néanmoins constamment s'adapter aux évolutions technologiques. Les scandales récents de

fuites de données ou de captation par certains États (affaire Edward Snowden) plaident, en outre, en faveur d'une vigilance accrue sur les enjeux de transfert et de collecte des données. La localisation des données en Europe, le développement d'une offre *cloud* européenne compétitive capable de rivaliser avec les grands acteurs, et, enfin, la résistance vis-à-vis des tentations extraterritoriales doivent désormais constituer trois axes prioritaires dans cette optique.

c. Des moyens supplémentaires et une simplification des procédures de sanction sont indispensables pour assurer, en pratique, cette protection

La commission nationale de l'informatique et des libertés (CNIL) est chargée en France de la bonne application de ce cadre protecteur. Cette autorité administrative indépendante a connu un accroissement de sa charge de travail en raison d'un « *effet RGPD* » (1). Elle a en effet observé une forte augmentation du nombre de plaintes déposées. La CNIL a reçu, pour les années 2019 et 2020, environ 14 000 plaintes, soit une augmentation de 27 % par rapport à l'année 2018, cette dernière étant déjà « *une année record* » selon les mots de son secrétaire général adjoint.

La crise sanitaire a également renforcé l'acuité des problématiques liées à la protection des données personnelles, ce qui s'est traduit par une augmentation de 18 % du nombre de visites du site internet de la CNIL. La CNIL a également reçu près de 6 500 notifications de violations de données personnelles depuis 2018 et ouvert « *près de 1 200 dossiers en 2018, 2 300 en 2019 et plus de 3 000 dossiers en 2020* » (2) . La CNIL procède également, dans son rôle de répression, à environ 300 contrôles formels par an, et réalise un certain nombre d'activités en coopération avec les autres autorités de protection des données personnelles des États membres. Elle a prononcé à ce jour « *plus de 550 sanctions représentant plus de 300 millions d'euros d'amendes* » (3) . Les montants des sanctions prononcées sont d'ailleurs « *nettement plus élevés qu'avant 2018, puisque le plafond est passé de 150 000 euros à 3 millions d'euros, voire 4 % du chiffre d'affaires mondial d'une entreprise* » (4).

Force est de constater que les missions de la CNIL tendent à s'accroître, et que l'Autorité, en dépit de l'évolution à la hausse de ses effectifs (245 agents en 2021 contre 225 en 2020), peut difficilement exercer ses missions de façon ambitieuse dans les conditions actuelles mises à son activité. Ainsi que le rappelle à juste raison M. Gwendal Le Grand, la France présente, selon les chiffres de la Commission européenne, « *le troisième plus mauvais ratio pour son nombre d'agents de la CNIL rapporté au nombre d'habitants* » (5) . Cette situation n'est pas tenable dans la durée.

---

(1) Audition de M. Gwendal Le Grand, 25 mars 2021.

(2) Idem.

(3) Idem.

(4) Idem.

(5) Audition de M. Gwendal Le Grand, 25 mars 2021.

Dans ces conditions, votre rapporteur estime que les pouvoirs publics doivent assumer le coût d'une protection effective des données des citoyens français. Il préconise donc de revoir fortement à la hausse les effectifs de la CNIL, selon une trajectoire beaucoup plus ambitieuse que les prévisions actuelles.

Proposition n° 5 : Renforcer les effectifs de la commission nationale de l'informatique et des libertés (CNIL) dans le cadre du projet de loi de finances pour 2022.

Les échanges menés avec la CNIL font également apparaître que les procédures de sanction applicables aux dossiers de moyenne ou faible intensité ne sont pas adaptées au traitement d'un flux de plaintes aussi important. Il semble donc indispensable de simplifier et d'enrichir les procédures dont dispose la CNIL pour prononcer les différentes « mesures correctrices » prévues par le RGPD. Ainsi que l'a indiqué la CNIL, dans un échange postérieur à son audition, le cadre juridique actuel ne lui permet d'adopter, en pratique, chaque année, qu'environ « *50 mises en demeure* [ainsi qu'] *une dizaine de décisions de la « formation restreinte », compétente en matière de sanctions. Cette dizaine de décisions ne correspond, en outre, pas nécessairement à des sanctions.* [Enfin], *le président de cette formation ne dispose d'aucune faculté de prendre seul les décisions les plus simples (injonction de produire ou non-lieu) ».*

Votre rapporteur considère que le Parlement doit faire preuve d'un haut niveau d'ambition à l'occasion de l'examen actuellement en cours du projet de loi « 4D », et en particulier de son article 51, qui concerne directement cette question.

Proposition n° 6 : Simplifier le processus de sanction par la CNIL pour les dossiers de moyenne et de faible intensité, afin de renforcer sa capacité à prononcer les « mesures correctrices » prévues par le règlement général sur la protection des données (RGPD).

d. Des évolutions récentes du droit de l'Union européenne utiles pour contrer les risques de transfert de données non conformes au règlement général sur la protection des données (RGPD).

La consolidation du cadre actuel de protection des données s'est effectuée *via* l'action de la Cour de justice de l'Union européenne, à l'occasion de contentieux relatifs au transfert de données en dehors de l'Union, c'est-à-dire vers des pays tiers.

Son arrêt Schrems II en date du 16 juillet 2020 a réaffirmé la nécessité, pour procéder à pareil transfert, que ces données bénéficient d'une protection équivalente au sein des pays tiers. Il constitue une nouvelle étape au sein d'un contentieux « *assez ancien* », comme l'a rappelé le Pr Thibaut Douville, professeur des universités, l'autorité irlandaise de protection des données ayant formulé « *par deux fois, des questions préjudicielles qui ont conduit la Cour de justice à rendre un arrêt* » [(1)] . La Cour avait en effet déjà invalidé, en 2015 suites aux révélations de l'affaire Edward Snowden « *le Safe Harbor, premier accord transatlantique sur le*

(1) Audition du Pr Thibault Douville, 11 mars 2021.

transfert des données des citoyens européens aux États-Unis » qui était « *utilisé par plusieurs milliers de sociétés aussi bien aux États-Unis que dans d'autres pays* » (1).

Cet arrêt apparaît, en outre, relativement « *inattendu du point de vue de sa solution, car le contentieux qui a amené à l'arrêt Schrems II ne portait pas sur la validité de la décision d'adéquation Privacy Shield, mais sur le recours à des clauses contractuelles-types par Facebook pour transférer des données aux États-Unis* » (2) . Par cette décision, la Cour de justice de l'Union européenne a en effet invalidé le *Privacy Shield,* c'est-à-dire la décision d'adéquation qui permettait le transfert de données à caractère personnel vers un pays tiers, en l'espèce les États-Unis. Cette annulation repose sur un constat simple : à la date du jugement, « *les États-Unis n'offraient pas* [de] *protection* [des données] *équivalente* » à celle existant en Europe. La Cour a en effet relevé que les personnes concernées « ne bénéficiaient *« ni de droits effectifs et opposables, ni d'un droit à un recours juridictionnel »*, dans la mesure où, notamment, « *le médiateur mis en place par les États-Unis, en tant qu'autorité chargée de protéger les données à caractère personnel des citoyens européens, ne présent[e] pas de garantie d'indépendance et ne dispos[e] pas d'un pouvoir permettant d'adopter des dispositions contraignantes en matière de protection des données*. » (3). Elle s'est appuyée, pour rendre sa décision d'annulation, sur « *la protection du droit au respect de la vie privée garanti par l'article 7 de la Charte des droits fondamentaux, la protection du droit au respect des données à caractère personnel et son régime exprimé à l'article 8 de la Charte des droits fondamentaux et enfin, sur l'article 47 de la Charte des droits fondamentaux qui consacre le droit à un recours juridictionnel au titre des droits protégés par cette Charte* » (4).

L' invalidation du *Privacy Shield* par la décision Schrems II a constitué « *un cataclysme dans les activités économiques* », dans la mesure où « *65 % de l'offre* cloud *est offerte par Amazon, dont une partie des serveurs se situe aux États-Unis* » (5). Nombre d'acteurs économiques auditionnés ont en effet indiqué être « en attente » de davantage de clarté sur les conséquences de l'arrêt Schrems II. Les acteurs publics sont d'ailleurs dans une situation similaire, lorsqu'ils se sont orientés pour l'hébergement de leurs données vers des acteurs non européens. Prenant l'exemple du *Health Data Hub*, le Pr Thibault Douville estime ainsi que, même si Microsoft stocke un certain nombre de données en Europe, la réalisation d'opérations de traitement sur les données, qui sont « *pour partie, conduites grâce à un transfert temporaire* via *des serveurs américains* » pourraient être cause d'« *une non-conformité au droit de l'Union à la suite de l'arrêt Schrems II* » (6) .

---

(1) Audition de M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique, 29 octobre 2020.

(2) Audition du Pr Thibault Douville, 11 mars 2021.

(3) Idem.

(4) Idem.

(5) Idem .

(6) Idem..

Lors de son audition [1], la directrice de cette structure, Mme Stéphanie Combes, a d'ailleurs indiqué qu'une étude sur les conséquences de la décision Schrems II avait été commandée par ses services à ce sujet.

Le *Health Data Hub* : une plateforme unique de recherche sur les données de santé

Le *Health Data Hub* est un groupement d'intérêt public créé par la loi du 24 juillet 2019 portant organisation et transformation du système de santé, à la suite de la remise au président de la République du rapport de Cédric Villani sur l'Intelligence artificielle. Cette plateforme remplace l'Institut national des données de santé (INDS), créé par la loi en 2016.

Le *Health Data Hub* poursuit l'objectif de garantir un accès aisé, unifié, transparent et sécurisé aux données de santé pour améliorer la qualité des soins et l'accompagnement des patients. Cette plateforme est un guichet unique pour les projets de recherche médicale. Elle met à disposition des chercheurs un catalogue de données, ainsi qu'une plateforme sécurisée et une palette d'outils pour les traiter. L'utilisation de ces données est soumise à un processus strict d'autorisation qui implique le comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES) et la CNIL.

Le *Health Data Hub* regroupe 56 parties prenantes réparties en neuf collèges représentant respectivement l'État, la Caisse nationale d'assurance maladie, les organismes d'assurance maladie complémentaires, le secteur de la recherche et de l'enseignement, les établissements de santé, les professionnels de santé, les agences, opérateurs et autorités administratives indépendantes, les usagers et enfin les industriels.

En 2020, le *Health Data Hub* avait lancé un appel à projet, accompagné 27 projets pilotes et 9 projets Covid. Huit projets de recherche ont été autorisés, cette même année, par la CNIL. Une vingtaine de partenariats sont par ailleurs en cours de discussion avec des responsables de données.

Source : audition du Health Data Hub par la mission d'information.

En tout état de cause, cet élément de risque supplémentaire aurait pu être évité en recourant à des solutions françaises ou européennes, dont il n'apparaît pas, au regard des auditions menées, qu'elles auraient été trop peu performantes pour justifier pareil arbitrage. Les contraintes calendaires et politiques ne sauraient suffire en effet à justifier le recours à un prestataire américain quand il existe une offre française ou européenne suffisamment compétitive.

Votre rapporteur considère que la décision Schrems II est positive et qu'elle démontre la capacité de l'Union européenne à défendre de façon effective la protection des données des citoyens. Il estime que cette décision plaide en faveur de la localisation des données sur le sol européen et de l'émergence d'offres de *cloud* souverain ainsi que de contraintes juridiques effectives sur les offres des acteurs non-européens pour garantir le respect du modèle numérique défendu par l'Union européenne. Ces éléments doivent être intégrés par les pouvoirs publics lorsqu'il

(1) Audition de Mme Stéphanie Combes, 18 février 2021.

s’agit d’effectuer des choix techniques pour mener à bien les projets numériques existants.

Proposition n° 7 : Intégrer de façon systématique au sein des arbitrages techniques des projets numériques les enjeux ayant trait à la souveraineté numérique, en particulier concernant la protection des données personnelles et la localisation des données en Europe.

Votre rapporteur considère également que l’arrêt Schrems II souligne la question centrale de l’extra-territorialité de la législation américaine, qui pourrait conduire, sur le fondement du *Cloud Act* ou de la section 702 du *FISA*, à ce que les autorités des États-Unis contraignent des entreprises à communiquer certaines données personnelles en leur possession. Ce risque lié à l’existence de législations extraterritoriale a d’ailleurs été explicitement reconnu dans la décision en référé du Conseil d’État du 14 octobre 2020 (1) .

(1) Extrait de la décision précitée, considérant 17 : « ll ne peut ainsi être totalement exclu, sur le plan technique, que Microsoft soit amenée à faire droit à une demande des autorités américaines fondée sur l'article 702 du FISA, ce qui méconnaîtrait alors les articles 28 et 48 du règlement général sur la protection des données, cités au point 5, qui interdisent qu'un sous-traitant transfère des données à caractère personnel vers un pays tiers si ce n'est sur instruction du responsable du traitement ou en vertu d'une obligation prévue par le droit de l'Union européenne ou d'un État membre, et que puisse être reconnue ou rendue exécutoire une décision d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel, sauf sous certaines conditions qui ne seraient en l'espèce pas remplies. ».

***Health Data Hub* et protection des données de santé**

La création du *Health Data Hub* et l'accélération de son déploiement dans le cadre de la crise sanitaire ont donné lieu à plusieurs recours d'associations de défense des droits devant le Conseil d'État.

Le Conseil national du logiciel libre (CNLL) et plusieurs autres associations ont saisi une première fois le juge des référés du Conseil d'État à la fin du mois de mai et au début du mois de juin 2020 pour lui demander de suspendre l'exécution de *l'arrêté du 21 avril 2020* qui autorisait le *Health Data Hub* à récolter différentes données de santé pour la gestion de l'urgence sanitaire et l'amélioration des connaissances sur le covid-19.

Cette requête s'appuyait notamment sur les modalités d'hébergement des données, celles de leur anonymisation, ainsi que sur le risque qu'elles puissent faire l'objet de transfert vers des pays tiers.

Dans *une décision du 19 juin 2020*, le juge des référés du Conseil d'État a rejeté les conclusions des requérants, en s'appuyant notamment sur le contenu du contrat conclu avec Microsoft le 15 avril 2020, et sur le fait que les possibles transferts de données aux États-Unis pour des besoins de maintenance s'inscrivaient dans le cadre de la décision d'adéquation de la Commission européenne de 2016, ainsi que le permet le RGPD. Le juge des référés a néanmoins demandé à la plateforme de communiquer sous cinq jours à la CNIL tous les éléments relatifs aux procédés de pseudonymisation utilisés afin qu'elle puisse les vérifier.

L'invalidation du Privacy Shield, par *l'arrêt Schrems II de la Cour de justice de l'Union européenne en date du 16 juillet 2020* est venue remettre en cause la base juridique de cette première décision. Les associations requérantes ont en conséquence à nouveau saisi le juge des référés le 28 septembre 2020 pour lui demander de suspendre le traitement des données liées à l'épidémie de covid-19 au sein du *Health Data Hub* en raison des risques d'atteinte au droit au respect de la vie privée liés aux possibles transferts de données vers les États-Unis.

Dans *une nouvelle décision en date du 14 octobre 2020* le juge des référés du Conseil d'État a rejeté les conclusions des requérants tendant à la suspension immédiate du traitement de données sur la plateforme, en s'appuyant notamment sur *un arrêté ministériel pris le 9 octobre 2020* interdisant tout transfert de données à caractère personnel dans le cadre de ce contrat. Il a reconnu, en revanche, l'existence d'un risque et, eu égard aux limites afférant à l'office du juge des référés, demandé au *Health Data Hub* de continuer à travailler avec Microsoft, sous le contrôle de CNIL, afin de renforcer la protection des droits des personnes concernées sur leurs données personnelles, dans l'attente d'une solution pérenne permettant d'écarter tout risque d'accès aux données personnelles par les autorités américaines, comme présenté par le secrétaire d'Etat au numérique le jour même de l'audience. Ce dernier s'est en effet engagé au nom du Gouvernement à transférer l'hébergement du *Health Data Hub* sur des plateformes françaises ou européennes. Un délai de deux ans a été retenu pour procéder à ce transfert dans des conditions satisfaisantes.

Source : auditions de la mission d'information – site internet du Conseil d'État

Sur ce sujet, les auditions ont fait apparaître des réponses pour le moins contrastées, pour ne pas dire contradictoires, selon les acteurs entendus.

Les représentants d'IBM ont ainsi affirmé explicitement lors de leur audition, qu'en tant que « *société française indépendante, opérant en France* », leur entreprise n'était pas *« soumise à la juridiction d'autorités gouvernementales étrangères qui lui demanderaient de communiquer des données, que ce soit au titre du Cloud Act ou de toute autre législation équivalente* ». Ils ont également souligné, en outre, que « *depuis trois ans, le Cloud Act* [n'avait eu] *aucun impact sur l'accès aux données de clients français d'IBM, ou de tout autre client d'IBM situé hors des États-Unis* » (1).

À l'inverse, les représentants de Google France, ou d'Amazon Web Services, par exemple, ont explicitement admis être soumis au *Cloud Act* et donc à ce type de demandes, en précisant néanmoins qu'ils utilisaient de façon systématique les voies de recours prévues pour les contester (2) . Ils ont également indiqué que ces demandes restaient extrêmement rares, pour ne pas dire exceptionnelles (3).

Les échanges intervenus sur l'impact de la soumission de ces entreprises au FISA ne témoignent donc pas d'une grande clarté quant à la portée réelle de cette législation. Néanmoins, comme l'a rappelé M. Gwendal Le Grand, secrétaire général adjoint de la CNIL, bien que « *la section 702 du FISA n'apporte pas de précision sur la portée extraterritoriale des ordres à produire* », elle « *ne restreint pas ces demandes aux seules données stockées sur le territoire américain, ce qui implique un possible accès à des informations en dehors du territoire américain. Il n'y a donc pas de doute sur le caractère extraterritorial des acquisitions* [ainsi que] *des interceptions fondées sur l'Executive Order 12333* ». Pour ce qui concerne le Cloud Act, « *un responsable de traitement ou un fournisseur de communications électroniques ou de services informatiques distants, dont les traitements sont soumis au RGPD, pourrait devoir répondre à un mandat des autorités américaines en vertu du* Cloud Act*. Un sous-traitant de responsable de traitement américain, établi dans l'Union européenne, peut* [donc] *être destinataire d'un mandat des autorités américaines pour les données qu'il sous-traite* » (4).

---

(1) Audition de Mme Diane Dufoix-Garnier, directrice des affaires publiques, et M. Michel Gesquiere, responsable des ventes d'IBM, 9 mars 2021.

(2) Auditions du 18 mars 2021.

(3) C'est ce qu'a indiqué, par exemple, M. Fenitra Ravelomanantsoa, responsable des affaires publiques, de Google France, lors de son audition le 18 mars 2021 : « Quand des autorités adressent à Google cloud une demande d'accès aux données d'un tiers, notre politique est de la soumettre à une équipe de juristes chargés d'en vérifier la validité (sa conformité à la loi, le statut de l'émetteur et l'ampleur raisonnable des données sur lesquelles elle porte). Quand l'un au moins de ces points ne donne pas satisfaction, nous opposons un refus. Nous nous considérons comme des processeurs sous-traitant des données et non comme leur propriétaire. Nous invitons les autorités qui souhaitent y accéder à en formuler la demande directement au client à qui elles appartiennent. Quand une demande nous semble recevable, nous notifions son exécution à l'entreprise concernée. Dans le cas contraire, nous nous tenons prêts à la contester devant la justice. Par souci de transparence, nous publions un rapport semestriel des demandes qui nous parviennent. Celles qui visent les entreprises n'en représentent qu'une très petite part et, parmi elles, les demandes suivies d'effet forment une infime minorité. Google cloud n'a communiqué aucune donnée des entreprises de sa clientèle suite à une demande gouvernementale. Nous n'avons en outre identifié aucune demande d'un gouvernement national en vue d'obtenir des informations sur un autre gouvernement national ».

(4) Audition de M. Gwendal Le Grand, 25 mars 2021.

Face à ce constat d'exposition effective au risque extraterritorial, votre rapporteur considère qu'il est impératif que l'Europe et la France mobilisent leurs arsenaux juridiques respectifs pour refuser l'application extraterritoriale de normes de cette nature.

Proposition n° 8 **:** Réaliser un état des lieux de l'arsenal juridique national permettant de s'opposer à la communication d'informations à une puissance étrangère et former les acteurs publics à ce type d'outils.

L'actualisation et le renforcement, le cas échéant, de *la loi de blocage du 26 juillet 1968*, conformément aux recommandations formulées au sein du rapport « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » remis au Premier ministre par notre collègue M. Raphaël Gauvain en 2019 est également souhaitable.

Proposition n° 9 : Actualiser et renforcer, le cas échéant, *la loi de blocage du 26 juillet 1968*, conformément aux recommandations formulées au sein du rapport « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » remis au Premier ministre par M. le député Raphaël Gauvain en 2019.

e. Un nouvel équilibre sur la question de la conservation généralisée des données de connexion

i. Un encadrement croissant par le droit européen

La conservation des données de connexion des utilisateurs par les opérateurs de communications électroniques pose évidemment la question centrale du juste équilibre entre protection des données et nécessité, pour lutter contre la criminalité grave et le terrorisme, de les conserver pour les exploiter utilement.

Le droit de l'Union européenne a encadré de façon croissante les possibilités de conservation des données des utilisateurs. Ainsi que l'a rappelé le Pr Thibault Douville, « *cette dynamique jurisprudentielle trouve son origine dans la directive européenne de mars 2006 sur la conservation des données de communications électroniques* [...] [qui] *prévoit la conservation généralisée d'un certain nombre de données liées aux communications électroniques, qu'il s'agisse de données d'identification des utilisateurs ou de métadonnées* ». Dans un arrêt « Digital Rights » en date du 8 avril 2014, la Cour a en effet invalidé cette directive en affirmant le principe de l'interdiction du stockage et de la conservation généralisée de l'ensemble des données de connexion. Elle s'est appuyée, à cette fin, sur le fait que la directive de 2006 « *n'opérait aucune différenciation entre les différents objectifs poursuivis par le législateur : la conservation des données était déconnectée du but poursuivi, soit de prévention d'atteinte à la sécurité publique ou de lutte contre la criminalité grave* » [(1)].

(1) Audition du Pr Thibault Douville, 11 mars 2021.

La Cour de justice de l'Union européenne s'est à nouveau prononcée sur ce sujet, à l'occasion de ses *arrêts Tele2 et La Quadrature du Net*, « *en reprenant des solutions similaires et en apportant des précisions quant à ces arrêts antérieurs* ». Elle a notamment mis en avant, à cette occasion, « *une échelle de mesures pouvant être adoptées selon le but poursuivi : lutte contre le terrorisme, lutte contre la criminalité grave ou protection de la sécurité publique. En fonction du but poursuivi, les mesures de conservation des données varient : elles peuvent être des mesures de conservation généralisée mais temporaire, des mesures de conservation ciblée et temporaire, des mesures de conservation uniquement des données d'identification des utilisateurs. Les solutions apportées par les différents arrêts ne sont qu'une application de l'exigence de proportionnalité entre la protection des données, d'une part, et le but poursuivi, d'autre part* » (1).

ii. L'arrêt « French Data Network » : un équilibre subtil qui maintient la possibilité d'une large collecte des métadonnées des utilisateurs

Cette question a enfin connu une actualité importante et récente, à la suite de l'arrêt de l'assemblée du contentieux du Conseil d'État « French Data Network » en date du 21 avril 2021, qui est venu concilier les règles nationales et le droit européen dans cette matière, *via* une interprétation neutralisante de la portée de la jurisprudence de la Cour de Justice de l'Union européenne.

Le Conseil d'État a en effet opté pour une solution audacieuse consistant à annuler de façon limitée un certain nombre de textes réglementaires, pour des raisons tenant à leur absence de proportionnalité (sur le périmètre des données collectées dans certaines circonstances) ou à l'absence d'avis « contraignant » pour les activités de renseignement (2), sans néanmoins mettre fin à la collecte des données de connexion *stricto sensu*.

Le raisonnement du Conseil d'État s'effectue en plusieurs étapes.

Le Conseil d'État a refusé, d'abord, d'exercer un contrôle de l'*ultra vires*, c'est-à-dire du respect par les organes européens de leur compétence, dans un esprit de conciliation vis-à-vis des institutions européennes. Il a néanmoins réaffirmé, en même temps, la primauté de la Constitution dans l'ordre juridique interne.

---

(1) Idem.

(2) Le dispositif de cette décision d'assemblée du contentieux du Conseil d'Etat prévoit ainsi l'annulation :

– *des décisions du Premier ministre refusant d'abroger l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* « en tant que ces dispositions réglementaires « d'une part, ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation autres que les données d'identité civile, les coordonnées de contact et de paiement, les données relatives aux contrats et aux comptes et les adresses IP à la sauvegarde de la sécurité nationale et, d'autre part, ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale ».

– *des décrets du 11 décembre 2015 et du 29 janvier 2016* « en tant seulement qu'ils permettent la mise en œuvre des dispositions des articles L. 851-1, L. 851-2, L. 851-4 et du IV de l'article L. 851-3 du code de la sécurité intérieure sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiée ».

Il a ensuite estimé, dans le cas d'espèce, que les exigences constitutionnelles que sont la sauvegarde des intérêts fondamentaux de la Nation, la prévention des atteintes à l'ordre public, la lutte contre le terrorisme et la recherche des auteurs d'infractions pénales ne bénéficiaient pas, en droit européen, d'une protection équivalente à celle que garantit la Constitution, et qu'un contrôle de leur bon respect par les règles du droit européen s'imposait en conséquence.

À l'issue de son contrôle, le Conseil a considéré que la conservation généralisée des données existant en droit français est bien justifiée par une menace pour la sécurité nationale, conformément à la jurisprudence de la Cour de Justice de l'Union européenne.

Pour la poursuite des infractions pénales, le Conseil d'État a jugé en revanche illégale l'obligation de conservation généralisée des données, tout en relevant, pour ces infractions, que la solution « suggérée » par la Cour de Justice de l'Union européenne concernant la conservation ciblée des données de connexion pose des difficultés « [n'était] *ni matériellement possible, ni – en tout état de cause – opérationnellement efficace. En effet, il n'est pas possible de pré-déterminer les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu où elle sera commise* ». Les juges ont relevé, en revanche, que « *la méthode de « conservation rapide » autorisée par le droit européen* », permettait de *« s'appuyer sur le stock de données conservées de façon généralisée pour les besoins de la sécurité nationale, et peut être utilisée pour la poursuite des infractions pénales ».*

La solution dégagée revient, comme le résume, le Pr Bertrand Brunessen, professeur à l'Université Paris I, à estimer que « *les données de connexion étant de toute façon conservées au titre de la sécurité nationale, la question de la conservation (ciblée ou non) ne se pose plus, en pratique pour les enquêtes pénales puisque, de fait, l'autorité judiciaire est en mesure d'accéder à ces données. Ainsi, « aussi longtemps que » les questions de sécurité nationale justifieront la conservation généralisée de ces données, la question de la conciliation entre le droit de l'Union et le droit constitutionnel ne se posera pas en pratique ».* Ainsi que le relève le Pr Bertrand Brunessen, cette solution « *a le mérite de temporiser une situation, qui, de toute façon, est appelée à évoluer avec l'adoption proche du Règlement e-privacy* » [(1)].

Cette solution devrait donc conduire les pouvoirs publics à actualiser le cadre réglementaire existant, en maintenant la possibilité de conserver les métadonnées, mais en prévoyant un périmètre et des modalités conformes au droit européen et un contrôle mis en œuvre par une autorité indépendante lorsqu'il s'agit de données conservées à des fins de renseignement. L'avis de la commission nationale de contrôle des techniques de renseignement (CNCTR) sur ce sujet n'était en effet pas contraignant jusqu'à ce jour, même si, comme le relève le Conseil d'État

(1) https://blog.leclubdesjuristes.com/larret-french-data-network-du-conseil-detat-un-dialogue-des-juges-en-trompe-loeil/

« *en pratique, le Premier ministre n'a jamais outrepassé un avis défavorable de la CNCTR pour l'accès des services de renseignement à des données de connexion* ».

Votre rapporteur considère que la solution dégagée semble équilibrée et devrait permettre une juste conciliation entre les impératifs de sécurité et de protection des données. Il prend note, néanmoins, des choix différents qui ont pu être effectués par d'autres pays voisins, et souhaite rappeler en conséquence l'impérieuse nécessité de conserver un dialogue fructueux entre juges nationaux et juges européens sur cette question complexe.

B. FAIRE DU NUMÉRIQUE UN LEVIER DE SIMPLIFICATION ET D'ÉMANCIPATION INDIVIDUELLE

1. Mettre en place rapidement une identité numérique pour les citoyens

La mise en place d'une identité numérique présente des enjeux évidents en termes de souveraineté numérique. Comme l'a rappelé le Pr Thibaut Douville, l'identité numérique « *traduit* [en effet] *l'aptitude des États à exercer leur souveraineté numérique* ». L'État étant « *le détenteur naturel de l'identité de tous ses concitoyens* [puisqu'il] *a le monopole de l'émission des titres d'identité* », il a dès lors « *naturellement vocation à proposer une solution d'identification électronique à ses citoyens* [pour] *favoriser l'émergence d'un socle de confiance en ligne et réaffirmer sa place dans l'environnement numérique* » (1).

a. Un outil utile pour simplifier et sécuriser la vie numérique des citoyens

L'identité numérique, c'est-à-dire « *la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources* » (2) au sein de la sphère numérique, est un prérequis indispensable pour garantir un niveau de confiance élevé des citoyens dans le numérique. Cette technologie doit en effet permettre à chacun de bénéficier à la fois d'un niveau de sécurité adapté à ses usages et d'une plus grande simplicité dans sa vie quotidienne numérique. Les usages de l'identité numérique seront en effet variés, aussi bien publics (disposer d'un document d'identité, voter en ligne, accéder à différents services en ligne dans les domaines de l'éducation, de la santé, de la justice, ou encore des aides sociales) que privés (souscrire à une ligne téléphonique, ouvrir un compte bancaire par exemple).

Dans le contexte de la crise sanitaire, force est de constater que l'utilité d'une solution d'identité numérique régalienne n'a jamais été aussi évidente. La disponibilité d'une telle solution offrirait en effet de riches perspectives pour réaliser à distance nombre d'activités essentielles, d'une façon sécurisée. Ainsi que l'a relevé Mme Valérie Peneau, directrice du programme interministériel France Identité numérique, à terme « *rien ne s'opposera,* [par exemple] *à ce que l'identité*

(1) Audition du Pr Thibaut Douville, jeudi 11 mars 2021.

(2) Assemblée nationale, rapport d'information n° 3190 déposé par la mission d'information commune sur l'identité numérique, Mme Claude Hennion et M. Jean-Michel Mis, rapporteurs, 8 juillet 2020.

numérique soit interfacée avec un système de votation. Un tel système est d'ailleurs prévu concernant les élections professionnelles ainsi que le vote des Français de l'étranger. Je pense que le Conseil constitutionnel devra toutefois se prononcer sur cette évolution » (1).

Votre rapporteur considère donc que l'identité numérique offre de nombreuses possibilités pour simplifier un certain nombre de procédures et de pratiques. Son déploiement rapide est nécessaire, en outre, afin *« d'opérer une transformation de l'État en mettant le citoyen au cœur de la transmission de ses données entre administrations »* au bénéfice « [d']*une plus grande confiance dans le déploiement du numérique […] de[s] nouvelles technologies* » (2).

b. Un programme interministériel national « France Identité numérique » qui s'inscrit dans une dynamique européenne

En France, un programme interministériel France Identité numérique a été mis en place en 2018 afin de créer une identité numérique régalienne. Comme l'a rappelé sa directrice, Madame Valérie Peneau, le lancement de ce programme correspondait à la nécessité d'accélérer « *un processus qui avait connu plusieurs échecs par le passé, pour des raisons assez diverses. Cette nette accélération a été permise par le nouveau Règlement européen sur les cartes d'identité électroniques, les deux projets ayant été lancés de manière concomitante* » (3). Son objet consiste, en pratique, à dériver une identité dans la sphère numérique à partir d'un document d'identité physique, de façon, simple, fiable et sécurisé, en recourant à une *« interface cryptographique* [faisant] *le lien entre les données d'identité protégées dans la puce du titre et une application* » (4). La proposition de valeur supplémentaire de ce projet, par rapport à FranceConnect (2016), qui offre déjà une forme d'identité numérique en ligne, réside dans *« l'obtention d'une identité numérique très sécurisée »*, conformément à ce qui est prévu par le droit européen et notamment le règlement eIDAS (5) .

Le programme France Identité numérique s'inscrit plus globalement dans une dynamique européenne en faveur de l'interopérabilité et de la sécurisation des systèmes d'identité numérique nationaux. Lors de son audition, Mme Lorena Boix-Alonso, directrice chargée de la stratégie et de la diffusion des politiques à la Direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne avait d'ailleurs rappelé que la question de l'identité numérique figurait au sein du programme de la Commission européenne avant de préciser que cette dernière entendait « *faire une proposition qui vise à établir un cadre unique pour une identité numérique européenne qui soit universellement reconnue, sécurisée, fiable, et qui puisse être utilisée partout où nous nous*

---

(1) Audition de Mme Valérie Peneau,1er avril 2021.

(2) Audition du Pr Thibaut Douville,11 mars 2021.

(3) Audition de Mme Valérie Peneau, 1er avril 2021.

(4) Idem

(5) Règlement 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE .

identifions sur Internet. Cela ne signifie évidemment pas qu'elle remplacera les identités nationales, mais c'est quelque chose qui peut jouer un rôle fondamental. […] » (1).

La Commission européenne a présenté en ce sens, le 3 juin 2021**,** un projet de nouveau cadre européen relatif à la création d'une identité numérique européenne qui serait accessible à tous les citoyens, résidents et entreprises de l'Union. Ce nouveau portefeuille européen d'identité numérique sera accessible à toute personne souhaitant l'utiliser. Il offrira une multitude d'utilisations et garantira à l'utilisateur la maîtrise de ses données (2).

c. Un déploiement qui ne doit pas prendre davantage de retard

Le déploiement d'une solution d'identité numérique régalienne fait consensus au regard de la confiance que les citoyens accordent à l'État plutôt qu'aux acteurs privés dans ce cadre. Ces derniers ont néanmoins évidemment vocation à participer de l'écosystème de l'identité numérique (3).

Votre rapporteur soutient évidemment ce projet majeur pour la transformation numérique de notre pays. Il note que les collectivités territoriales y sont également très attachées, comme l'a indiqué, par exemple Mme Valérie Nouvel, vice-présidente du département de la Manche, « *le projet d'identité numérique renforcée peut nous* [les départements] *permettre d'être rapidement des champions en matière de souveraineté numérique, en conjuguant nos talents entre État et territoires.* […]. [Il] *conjugue en effet à merveille souveraineté numérique et inclusion numérique. Lancer ce chantier est pour nous une priorité absolue* ». Mme Valérie Nouvel avait néanmoins regretté, à cette occasion, le fait que ce même projet **«** *peine à progresser au niveau français* […] [étant] *souvent perçu comme une charge par l'État, tandis que les départements le voient comme une recette* » (4).

Votre rapporteur ne peut malheureusement que partager son constat : la France accuse un retard important en matière d'identité numérique par rapport à ses partenaires européens, ce qui est regrettable. Celui-ci peut s'expliquer en partie, certes, par les échecs que ce projet a connus précédemment (5). Il convient néanmoins de ne pas relativiser la situation actuelle, qui démontre, une nouvelle fois, la difficulté, pour l'État, de mener à bien des projets numériques d'ampleur pour des raisons tenant à la défiance existant vis-à-vis du numérique et au manque de maîtrise technique des acteurs publics sur des sujets aussi complexes.

---

(1) Audition de Mme Lorena Boix Alonso,19 novembre 2020.

(2) https://ec.europa.eu/france/news/20210603/proposition_identite_numerique_europeenne_fr

(3) Lors de son audition, Mme Valérie Peneau, directrice du programme ministériel France Identité numérique, a ainsi rappelé que « les sondages font état d'une plus grande confiance dans l'État que dans les acteurs privés ou commerciaux pour garantir les données d'identité » même si « des réticences apparaissent chez une partie de la population à propos de la transmission de ses données biométriques ».

(4) Audition sous forme de table-ronde consacrée aux collectivités territoriales,10 décembre 2020.

(5) Le détail des projets précédents ayant échoué est rappelé au sein du rapport d'information précité n° 3190 déposé le 8 juillet 2020 par la mission d'information commune sur l'identité numérique », p. 45-47.

Votre rapporteur relève qu'à l'heure actuelle, la France n'a toujours pas notifié son schéma d'identité numérique alors que les autres États membres de l'Union européenne « *ont souvent pris de l'avance, certains d'entre eux ayant déjà été notifiés à la Commission européenne* » (1). En outre, le calendrier initialement envisagé, qui devait permettre de déployer conjointement, à partir de l'été, une solution d'identité numérique effective avec la nouvelle carte d'identité électronique, ne sera pas respecté. Ce constat vient confirmer les inquiétudes formulées par les députés M. Jean-Michel Mis et Mme Christine Hennion dans un courrier en date du 22 mars 2021. Ce retard a été confirmé par Mme Valérie Peneau, qui a admis ne pas encore disposer « *du système d'information permettant d'exploiter cette dimension de l'identité numérique* […] *un décalage de quelques mois* [étant] *attendu* ». Mme Valérie Peneau a néanmoins indiqué que ledit décalage « *se retrouve dans les autres pays européens, où les cartes sont en général distribuées dans un premier temps, avant d'être accompagnées d'une offre numérique* ». Plusieurs éléments en sont les causes, selon elle, dont « *le fait que* [le programme FUN] *fait l'objet de recommandations de la part du Conseil national du numérique et de la mission parlementaire ad hoc de Mme Christine Hennion et de M. Jean-Michel Mis, qui ont déjà expertisé le projet* » (2), ce qui a conduit à compléter le cahier des charges concerné.

Votre rapporteur considère que l'absence de déploiement simultané de la carte nationale d'identité électronique (CNIe) et d'une solution d'identité numérique effective est extrêmement préjudiciable dans un contexte de retard persistant de la France sur ses voisins européens dans ce domaine et pour les citoyens français. Votre rapporteur invite les pouvoirs publics à redoubler leurs efforts pour que cette mise en œuvre soit la plus rapide possible.

Proposition n° 10 : Accélérer le déploiement de l'identité numérique en France.

Votre rapporteur estime, en outre, que ces difficultés sont tout à fait symptomatiques des limites réelles de la capacité de l'État à mener dans des conditions satisfaisantes des projets numériques de grande envergure, ce qui n'est pas satisfaisant. Une prise de conscience de ces carences est indispensable pour réformer les difficultés structurelles qui en sont la cause.

Proposition n° 11 : Engager une stratégie ambitieuse de montée en compétences au sein de l'État sur la gestion de projets numériques afin de ne pas répéter les erreurs du passé.

d. Des interrogations légitimes sur certains choix techniques

Au-delà du retard de déploiement d'une identité numérique utilisable par les citoyens français, les auditions ont fait apparaître l'existence d'un doute sur la capacité de l'État à proposer une carte d'identité électronique qui soit « à l'état de l'art » au regard des technologies disponibles. M. Cosimo Prete, dirigeant de

(1) Audition de Mme Valérie Peneau,1er avril 2021.

(2) Audition de Mme Valérie Peneau, 1er avril 2021.

l'entreprise CST + [1], a ainsi trouvé « *surprenant que la France ne soit pas capable de mettre en œuvre les meilleures solutions présentes sur son territoire* » et estimé que « *la moyenne d'âge des éléments de sécurité actuellement embarqués sur notre titre sécurisé dépasse la dizaine d'années, alors qu'il a paradoxalement été préconisé de limiter la durée de ce titre à dix ans, pour des raisons de sécurité* ». M. Prete a cité plusieurs exemples à l'appui de son propos, dont le choix d'une photo d'identité en noir et blanc « *fournie par une solution américaine, alors qu'IDEMIA ou Thales sont capables de produire une photo en couleur depuis plusieurs années* », et le recours à un « *cachet électronique visible (CEV), qui date d'il y a une dizaine d'années, alors qu'il serait possible de recourir à une norme universelle interopérable* » [2] . Le recours à des solutions technologiques non-européennes ne saurait en effet se justifier que par des écarts de performance importants.

Votre rapporteur prend acte des réponses apportées par les représentants de l'Agence nationale des titres sécurisés (ANTS) et de l'Imprimerie nationale (IN group). Mme Anne-Gaëlle Baudouin-Clerc, directrice de l'Agence nationale des titres sécurisés a en effet précisé que ces modalités techniques avaient fait l'objet d'un « *choix assumé* » et correspondaient notamment aux demandes des forces de l'ordre pour ce qui concerne la photo d'identité présente sur la CNIe. Concernant le cachet électronique visible, Mme Anne-Gaëlle Baudoin-Clerc a néanmoins indiqué avoir « *conscience que, pour l'Imprimerie nationale, le passage à la norme 105 aura des conséquences industrielles, notamment de modification de sa plateforme* » et estime que « *la situation a vocation à évoluer* » dans la mesure où « *parvenir à utiliser la norme 105 pour le pass sanitaire présentera un véritable intérêt* », même si « *la norme 105 a besoin* [pour l'heure] *de conforter sa gouvernance, ainsi que de clarifier ses conditions de sécurité et de souveraineté* » [3].

Pour sa part, le directeur des affaires publiques d'IN Group, M. Romain Galesne-Fontaine a démenti « *un quelconque défaut de maîtrise technique* [de] *l'Imprimerie nationale* [qui] *peut parfaitement produire des titres en polycarbonate qui contiennent de la couleur* », l'Imprimerie nationale ayant mis en œuvre cette technique « *à l'occasion de son partenariat avec le gouvernement monégasque* ». M. Romain Galesne-Fontaine a également ajouté que « *90 % de la centaine de pays qui, dans le monde, émettent des titres d'identité en polycarbonate, utilisent le système de gravure laser en tons de gris au cœur de la carte, choisi pour la CNIe française* » [4] .

---

(1) Audition de M. Cosimo Prete, 1er avril 2021.

(2) Lors de son audition, M. Cosimo Prete a détaillé son raisonnement concernant le caractère daté et inapproprié du modèle de CEV choisi : « Le CEV ayant été adopté sur notre CNI en est à sa version 101 et non 105. Par conséquent, chaque fois qu'un nouveau cas d'usage n'ayant pas été prévu par le CEV actuel se présentera, il sera nécessaire de réactualiser l'ensemble du système. À l'inverse, la version 105 du CEV a été validée selon la dernière norme AFNOR pour être universelle et interopérable, avec une mise à jour des différentes fonctionnalités. Nous nous fixons ainsi nos propres limites, en adoptant la version 101 et non 105 du CEV, alors que cette dernière pourrait être lue hors de France ».

(3) Audition de Mme Anne-Gaëlle Baudoin-Clerc, 1er avril 2021.

(4) Audition de M. Romain Galesne-Fontaine, 6 avril 2021.

Il n'appartient évidemment pas à la mission d'information de trancher des débats aussi techniques ressortant de l'appréciation légitime d'acteurs spécialisés. Votre rapporteur considère néanmoins qu'il est possible de s'interroger, au regard de la configuration actuelle de l'ANTS, et de ses moyens pour expertiser les solutions techniques, sur le risque d'un renversement des rôles entre l'ANTS, qui est censée être le donneur d'ordre, et l'Imprimerie nationale, qui doit répondre à ses exigences. De toute évidence, il existe des difficultés pour conserver des acteurs aux compétences avancées au sein de cette agence, pour des raisons tenant à l'attractivité perçue des missions proposées et au niveau de leur rémunération.

Dans ces conditions, votre rapporteur prend acte des efforts consentis par l'ANTS pour améliorer son attractivité. Il estime néanmoins que ceux-ci doivent être amplifiés pour lui permettre de réaffirmer sa complète capacité à jouer le rôle qui lui est dévolu, et à effectuer, sur ce type de projets, l'ensemble de ses choix en pleine connaissance de cause. Il plaide en conséquence pour la poursuite de l'accroissement de ses effectifs, revalorisés de six équivalents-temps-plein cette année. Il souhaite enfin insister sur l'importance du travail de veille technologique qu'elle doit pouvoir effectuer, afin d'être en état de « challenger » les choix techniques qui lui sont proposés lors des échanges menés avec ses différents interlocuteurs. Ces derniers ne sauraient être guidés par tout autre considération que celle d'offrir la meilleure garantie de sécurité possible pour les citoyens français.

e. Des difficultés symptomatiques dont il faut vite tirer les leçons

En définitive, votre rapporteur souhaite insister sur plusieurs points.

L'État, d'abord, doit améliorer sa capacité à attirer les compétences techniques afin que ses projets numériques puissent être menés dans les meilleures conditions possibles. Le *turnover* important qui peut concerner un certain nombre de projets numériques, dont celui sur l'identité numérique, est très préjudiciable au succès de ces initiatives, en raison des pertes de compétences qu'il génère dans des domaines ultra spécialisés. Cette question doit être au centre des préoccupations des décideurs publics.

Il est donc indispensable que **l'État mène des actions spécifiques pour améliorer sa maîtrise technique des projets numériques en recrutant des profils techniques par contrat de droit privé et en fidélisant ce précieux public**. Les conditions d'emploi proposées dans ce cadre doivent être attractives en termes de rémunération et de conditions de travail.

Proposition n° 12 : Renforcer le recrutement par contrat de droit privé de profils techniques, pour mener à bien les projets numériques de l'État et mettre en œuvre une stratégie de fidélisation pour les conserver au sein de la sphère publique.

Il convient, en outre, de mettre en place en son sein une doctrine « de la circulation des compétences » afin d'offrir des débouchés à ces profils fortement demandés.

Proposition n° 13 : Favoriser la circulation des compétences numériques au sein du secteur public.

Sur la mise en place d'une identité numérique, *stricto sensu*, un vrai travail de communication est nécessaire dans la mesure où cette question reste encore assez méconnue des citoyens français. Cette action reste encore largement à mener. Dans un contexte où la France est déjà en retard par rapport à ses voisins européens, on ne saurait sous-estimer les réticences qui pourraient se faire jour à l'occasion du déploiement effectif de l'identité numérique. Ce travail de communication doit également être réalisé à destination des acteurs privés, afin que ceux-ci puissent connaître « les règles du jeu » et le positionnement du Gouvernement sur le modèle économique de l'identité numérique.

Proposition n° 14 : Lancer une grande campagne de communication sur l'identité numérique.

Ce travail de communication devra être accompagné, à terme, d'une proposition d'accompagnement sur demande à l'utilisation de l'identité numérique, qui peut prendre des formes variées. À titre de simple illustration, en Estonie, ainsi que l'a présenté M. Arnaud Castaignet, directeur de la communication et des affaires publiques de Skeleton Technologies, ancien directeur des relations publiques du programme e-Residency du gouvernement estonien, « *lors du lancement de l'identité numérique, l'État estonien a décidé de former à son utilisation 15 000 personnes, qui ont chacune formé à leur tour dix de leurs concitoyens. L'idée de former les Estoniens tout au long de leur vie joue de ce point de vue un rôle clé* » (1). Cet enjeu doit être, dans tous les cas, anticipé en amont, pour garantir une inclusion aussi forte que possible.

Enfin, comme l'avaient déjà indiqué nos collègues Mme Christine Hennion et M. Jean-Michel Mis dans le rapport précité, il est indispensable de parier sur le dynamisme des collectivités territoriales, qui souhaitent pouvoir expérimenter l'identité numérique mais ont le sentiment, pour certaines, de ne pas avoir été entendues par l'État.

2. Créer une relation de confiance entre l'administration et les citoyens

Le déploiement d'une identité numérique ne doit être que la première étape d'une ambition de simplification administrative inédite de nos modes de fonctionnement habituels. Il faut en effet admettre, à l'heure actuelle, qu'en dépit des progrès indiscutables réalisés, le système administratif français conserve un niveau de complexité réel qui génère une défiance et un sentiment d'inefficacité. Dans ce domaine, les faits doivent désormais venir corroborer les discours régulièrement tenus sur la simplification administrative.

(1) Audition de M. Arnaud Castaignet,1er juin 2021.

Votre rapporteur est convaincu que le numérique, sans être la « solution miracle », offre néanmoins un puissant levier de transformation des relations entre l'administration et les citoyens. Il considère que deux mesures pourraient représenter une vraie rupture perceptible par les Français dans la vie quotidienne : la création d'un guichet unique pour accéder à l'ensemble des services publics et la création d'un identifiant unique numérique.

a. Mettre en place un guichet unique d'accès à l'ensemble des services publics

La création d'un guichet unique pour accéder à l'ensemble des services publics en ligne est souhaitable pour simplifier de façon effective la vie des citoyens. Ce projet dépend évidemment du déploiement d'une identité numérique permettant de réaliser en ligne les usages les plus complexes, qui nécessitent un niveau de sécurité élevé.

Votre rapporteur considère que la France, dans cette démarche, pourrait s'inspirer d'exemples étrangers, en particulier de celui du Luxembourg. Lors de son audition, M. Marc Hansen, ministre du numérique du Grand-Duché, a ainsi indiqué qu'il existait, dans son pays, une « *grande plateforme « guichet.lu », tenant lieu de guichet unique aux citoyens et aux entreprises souhaitant contacter les services publics par voie numérique* ». Cette plateforme permet d'accéder à l'ensemble des services publics luxembourgeois, car elle héberge *« un espace personnalisé « myguichet.lu », où chacun peut déposer aussi bien une demande de plaque d'immatriculation que de permis de pêche, par exemple »* [(1)]. Elle a été très utile pendant la crise sanitaire, ce que démontre son niveau de sollicitation inédit. Le nombre de démarches effectuées par son truchement est ainsi passé, en 2019, de 500 000 à plus de 1,8 million en 2020, en raison notamment des demandes d'aides ou d'appui des entreprises à destination du gouvernement luxembourgeois.

Proposition n° 15 : Créer un guichet numérique unique d'accès de chaque citoyen à l'ensemble des services publics, lui permettant aussi d'être informé en temps réel de l'utilisation de ses données par l'administration.

b. Créer un identifiant numérique unique pour chaque citoyen

Les auditions des ministres en charge du numérique de l'Estonie ou le Luxembourg font apparaître que l'ambition de simplification des procédures administratives ne pourra faire l'économie de la mise en place d'un numéro d'identification unique, afin de mettre fin aux difficultés que rencontrent les administrations pour identifier les administrés et partager leurs informations de façon efficace, sans avoir à solliciter à nouveau chaque citoyen pour récupérer des informations déjà disponibles.

Interrogé sur ce sujet, le secrétaire d'État chargé de la transition numérique, M. Cédric O, a relevé qu'à l'heure actuelle, le recours à cet identifiant unique était

(1) Audition de M. Marc Hansen, 3 juin 2021

« *interdit par la Commission nationale de l'informatique et des libertés (CNIL)* » [1]. Il s'agit là d'une position constante de cette autorité qui vise à éviter tout risque de création d'un fichier de population sur la base de cet identifiant. M. le secrétaire d'État a d'ailleurs indiqué que cette position était partagée par le Conseil d'État, qui « *au moment de la discussion sur le numéro de sécurité sociale, qui est en fait le seul identifiant, a estimé que l'usage de cet identifiant devait rester proportionné et qu'il n'était pas possible d'avoir un identifiant unique de l'administration* » [2].

En dépit de ces obstacles, et pleinement conscient du fait que « *l'avantage* [du modèle estonien est] *de ne pas avoir été bâti sur une administration datant de plusieurs centaines d'années et ayant ses propres processus* » [3] , votre rapporteur considère indispensable d'envisager la création de cet identifiant unique et de faire évoluer la perception de cet outil, en cantonnant le risque évoqué ci-avant par une complète transparence de l'administration sur l'utilisation des données des citoyens.

De ce point de vue, il est possible de s'inspirer, par exemple, du modèle luxembourgeois. M. Marc Hansen, ministre du numérique du gouvernement luxembourgeois, a ainsi indiqué que, dans son pays, les usagers de la plateforme unique d'accès à l'ensemble des services publics ont le droit de « *savoir à tout moment quelles administrations ont eu accès, au cours des six derniers mois, à la partie qui les concerne du Registre national des personnes physiques répertoriant les données des Luxembourgeois* ». En conséquence, « *si un service public a consulté les données d'un citoyen, sans que celui-ci comprenne pour quelle raison, cette personne peut interpeller le service en question, auquel il revient de s'expliquer. Il arrive par exemple à un père ou à une mère de ne pas comprendre pourquoi une administration a consulté ses données à la suite d'une demande de bourse déposée par son conjoint, pour leur enfant étudiant. Nous attachons une importance extrême à la transparence et au respect des données personnelles* » [4]. Cette logique positive de responsabilité et de confiance pourrait être utilement mise à profit en France dans le domaine du numérique.

Proposition n° 16 : Créer un numéro d'identification unique afin de mettre fin aux difficultés rencontrées par les administrations pour identifier les administrés et partager leurs informations de façon efficace.

Proposition n° 17 : Développer une culture de la transparence vis-à-vis des données utilisées par la puissance publique dans le cadre de ses interactions avec les citoyens.

(1) Audition de M. Cédric O, 22 octobre 2020.

(2) Idem.

(3) Idem.

(4) Audition de M. Marc Hansen, 3 juin 2021.

3. Former au numérique tous les citoyens dès le plus jeune âge

a. La maîtrise des savoirs numériques fondamentaux doit être une priorité

La formation aux compétences numériques doit être l'un des piliers d'une politique de souveraineté numérique. Chaque citoyen ne peut en effet rester maître de ses choix et vigilants face aux risques, que s'il maîtrise les codes du cyberespace. Ainsi que l'a résumé M. Edouard Geffray, conseiller d'État, directeur général de l'enseignement scolaire, « *chaque citoyen doit se doter d'une culture numérique* » [(1)]. L'univers numérique suppose en effet « des *modalités particulières d'exercice de l'esprit critique. La question des moyens de traduire nos valeurs dans le monde numérique se pose au quotidien. Chacun détient, en tant qu'utilisateur, un pouvoir, certes asymétrique mais toutefois réel, qu'il exercera comme il se doit, pour peu qu'il ait reçu une formation adaptée. Nous en revenons dès lors à la formation au numérique des élèves, qui suppose aussi bien une éducation aux médias d'information,* via *la lutte contre les fausses nouvelles, par exemple, qu'une formation plus technique* » [(2)]. Il faut en conséquence inculquer aux élèves « *l'esprit critique, la capacité de distanciation et la connaissance des outils numériques, tels que l'Intelligence artificielle ou les algorithmes, pour qu'ils comprennent comment le monde se modélise et comment leur volonté peut s'en trouver influencée* ». Cela revient à appliquer au numérique le précepte du positiviste Auguste Comte selon lequel « *il faut savoir pour prévoir et prévoir pour pouvoir* » [(3)].

La maîtrise des savoirs numériques va devenir, en outre, un élément de plus en plus différenciant sur le marché du travail, et dans la compétition économique entre les États. Cette primauté du capital humain numérique a été rappelée par M. Julien Nocetti, docteur en sciences politiques et chercheur associé à l'Institut français des relations internationales. Pour lui, il s'agit en effet de « *l'un des aspects les plus sous-estimés de ces enjeux de souveraineté numérique* » [(4)], qui doit être traité sous trois angles que sont sa formation, « *la rétention de nos cerveaux* » et enfin « *l'enjeu de [leur] captation* » [(5)]. M. Julien Nocetti relève d'ailleurs que c'est « *sur cet enjeu humain que la question du numérique prend une dimension quasi géopolitique, d'autant que nous l'avons trop longtemps sous-estimé, alors que les États-Unis peuvent s'enorgueillir d'une expérience extrêmement riche en la matière. Si l'Europe ambitionne de peser dans ce domaine et de s'affranchir, au moins partiellement, de ces formes de tutelle que je viens d'évoquer, elle doit nécessairement et urgemment répondre à cet enjeu de formation au long cours* » [(6)].

---

(1) Audition de M. Édouard Geffray, 4 mai 2021.

(2) Idem.

(3) Idem.

(4) Audition de M. Julien Nocetti, 11 mars 2021.

(5) Audition de M. Julien Nocetti, 11 mars 2021.

(6) Idem.

L'enjeu de la « *fuite des talents de haut niveau* » [(1)] a été abordé à plusieurs reprises lors des auditions de la mission, notamment par M. Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises (Cigref).

Votre rapporteur considère, au regard des échanges menés, que la formation aux compétences numériques est une priorité du Gouvernement, comme l'indiquent, par exemple, les propos tenus par le secrétaire d'État à la transition numérique : « *Dans le fond, je suis très optimiste sur cette question de la souveraineté numérique et de l'écosystème numérique ; en effet, je pense que la compétition mondiale pour la technologie est d'abord une compétition mondiale pour l'intelligence humaine. Or la France a cette intelligence humaine. Elle forme des ingénieurs, des chercheurs et des entrepreneurs parmi les meilleurs du monde. Il s'agit juste de les garder et qu'ils trouvent ici l'écosystème leur permettant de développer des entreprises qui seront demain parmi les meilleures du monde. Cela prendra un peu de temps mais elles y arriveront* » [(2)].

Votre Rapporteur est convaincu que cet apprentissage doit être mis en œuvre **dès le plus jeune âge et tout au long de la vie**. Il est en effet indispensable que l'appareil de formation français soit en capacité de transmettre de façon efficace et actualisée les savoir-faire permettant aux citoyens de garder la maîtrise de leur vie en ligne et de ne pas subir l'apparition de nouveaux usages. En ce sens, on ne rappellera jamais assez que **toute politique de souveraineté numérique ne peut exister sans des citoyens vigilants et informés sur le numérique.** C'est le sens des deux propositions suivantes, qui visent à réaffirmer la nécessité de former chacun aux compétences numériques tout au long de sa vie.

Proposition n° 18 : Former aux compétences numériques dès le plus jeune âge et tout au long de la scolarité et de la vie professionnelle.

Proposition n° 19 : Former les citoyens aux gestes barrières face au risque cyber.

b. Un certain retard de la France vis-à-vis de ses partenaires européens

Le niveau de maîtrise des compétences numériques en France reste encore insuffisant à l'heure actuelle. La France ne se classe en effet qu'en 17e position en matière de « capital humain » en Europe d'après l'indice relatif à l'économie et à la société numériques 2020 publié par la Commission européenne, soit un positionnement en-deçà de la moyenne européenne.

Cette mauvaise diffusion des compétences numériques est préjudiciable non seulement aux jeunes générations, qui ont plus besoin de disposer d'un socle solide de savoir-être et savoir-faire dans ce domaine, mais aussi pour l'ensemble des citoyens, dans la mesure où le numérique risque, dans le cas contraire, de renforcer certaines inégalités.

(1) Audition de M. Henri d'Agrain, 18 mars 2021.

(2) Audition de M. Cédric O, 22 octobre 2020.

Les auditions font apparaître un consensus sur l'existence d'un besoin de formation aux compétences numériques dans notre pays. Votre rapporteur ne peut en ce sens que souscrire aux propos tenus par le secrétaire d'État à la transition numérique, selon lequel la « *seule manière de combattre les nombreuses dérives du numérique, sur les fausses informations, sur la haine en ligne ou sur la puissance des grandes entreprises d'Internet, est de former nos concitoyens. Il faut les faire progresser et progresser nous-mêmes car nos concitoyens ne sont pas les seuls à être en retard* », mentionnant notamment le cas des « *serviteurs de l'État* [et] *hauts fonctionnaire* », avant d'admettre la nécessité d'une « *accélération sur ce sujet* » dans un contexte où « *un Français sur trois manque de compétences numériques de base* » (1).

Cette nouvelle étape à franchir doit s'appuyer sur les bases mises en place ces dernières années, tant en termes de formation aux compétences numériques que d'incitation à l'utilisation d'outils numériques pour renouveler les méthodes d'apprentissage.

c. L'effort de formation engagé par les pouvoirs publics doit être amplifié

L'approfondissement des apprentissages numériques est indéniable ces dernières années, ce qui doit être salué. Comme l'a rappelé M. Édouard Geffray, en effet, « *tous les élèves de seconde suivent désormais, suite à la réforme du lycée, un enseignement commun en sciences numériques et technologie (SNT) d'une heure et demie par semaine* » (2) . Une spécialité « nouvelles sciences de l'ingénieur » (NSI), créée en 2018 leur « *est ensuite proposée à raison de quatre heures hebdomadaires en première et six en terminale. Le programme de cette matière fournit une approche assez complète du numérique, allant de la technologie (le code) à l'éthique (le traitement des données personnelles) en passant par la compréhension globale de cet univers* » (3).

Une évaluation des compétences numériques des élèves intervient également à la fin du CM2 et en 6e. Le programme PIX permet ensuite de certifier le niveau des élèves en fin de troisième et de terminal afin de s'assurer qu'ils soient capables, au quotidien, « *d'évoluer dans l'univers numérique en y exerçant leurs droits et devoirs et, partant, une forme de souveraineté* » (4).

Enfin, l'apprentissage du code a également été introduit et renforcé dès l'école primaire (cycle 2 et cycle 3) ainsi qu'au collège (cycle 4) où l'on aborde ensuite les notions d'algorithmiques au sein des cours de mathématiques et de

---

(1) Audition de M. Cédric O, 22 octobre 2020.

(2) Audition de M. Édouard Geffray, 4 mai 2021.

(3) Cette option, suivie à l'heure actuelle par 9,5 % des élèves de première, a donné lieu à la création d'un Certificat d'aptitude au professorat de l'enseignement du second degré (CAPES) NSI, que suivra, en 2022, une agrégation NSI.

(4) Audition de M. Édouard Geffray, 4 mai 2021.

technologie. La programmation « *est également enseignée,* via *divers logiciels, dont le plus connu reste Scratch* » (1).

Sur ce dernier point, votre rapporteur ne peut qu'inviter les pouvoirs publics à prolonger leur effort, le code étant en définitive le nouvel alphabet du monde du numérique. Il nous faut donc nourrir l'ambition de rejoindre les pays les plus avancés dans ce domaine, c'est-à-dire les pays asiatiques et les États-Unis.

Proposition n° 20 : Développer l'apprentissage du code à l'école pour doter les élèves des fondamentaux de cet alphabet du monde numérique.

Il serait également extrêmement utile, dans cette optique, de développer l'esprit d'initiative dans ce domaine.

Ainsi que le relevait M. Alain Conrard, président de la commission digitale du mouvement des entreprises de taille intermédiaire (METI), « *nous manquons cruellement de formations et d'actions d'information auprès des publics les plus jeunes, spécialement ceux des collèges et lycées* […]. *Au sens large du terme, l'innovation gagnerait à intégrer les programmes de l'enseignement secondaire* » (2).

Cet apprentissage de l'innovation pourrait donc être intégré au sein de la formation initiale, de façon théorique et pratique.

Sur ce sujet, votre rapporteur considère que les propos tenus par M. Arnaud Castaignet, ancien directeur des relations publiques du programme e-Residency du gouvernement estonien, sont éclairants quant au chemin à suivre : *« Le développement du modèle numérique estonien a véritablement commencé en ce qui concerne l'éducation, par le raccordement des écoles à Internet et la formation des enseignants à l'utilisation des technologies numériques, ce qui a favorisé une meilleure compréhension des enjeux du numérique et l'émergence d'une culture de l'innovation et de l'entrepreneuriat, dès le plus jeune âge. Il existe beaucoup de junior-entreprises dans les lycées, voire les collèges. Comme ces initiatives ont débuté voici plus de vingt ans, les premiers étudiants formés au numérique sont aujourd'hui adultes. Ainsi, une grande part de la population estonienne est davantage formée que dans d'autres pays aux outils numériques* (3).

Il serait donc utile de faire évoluer les apprentissages technologiques du secondaire en ce sens, en s'appuyant sur l'existant, c'est-à-dire les enseignements technologiques actuellement mis en œuvre.

---

(1) Idem.

(2) Audition sous forme de table-ronde consacrée aux entreprises, comprenant le MEDEF, le METI et la CPME, 14 janvier 2021.

(3) Audition de M. Arnaud Castaignet,1er juin 2021.

Proposition n° 21 : Développer la capacité des établissements scolaires à former les élèves aux enjeux de l'innovation et soutenir la création de projets numériques.

Votre rapporteur note qu'un effort important a également été consenti sur le volet formation des enseignants. En 2020, plus de 200 000 d'entre eux se sont formés, *via* la plateforme de formation continue Canopé. M. Jean-Marc Merriaux, inspecteur général de l'éducation nationale, directeur du numérique pour l'éducation, a indiqué que le confinement avait permis de lever des craintes concernant le recours aux outils numériques dans le cadre des pratiques d'enseignement. Ainsi, alors que l'Éducation nationale répond à la règle de trois tiers qui prévaut en matière de transformation numérique, à savoir un tiers d'acteurs compétents et ouverts aux usages du numérique, un tiers d'hésitants, et un dernier tiers d'acteurs hostiles à ces évolutions, une étude d'un laboratoire de recherche attaché à l'université de Rennes et spécialisé dans le numérique et l'éducation a démontré que « *plus de 50 % des enseignants se déclaraient prêts à utiliser le numérique dans leur classe après le confinement* ». L'Éducation nationale a développé en outre « *sur la plateforme PIX, des modules spécifiques proposant aux professeurs des tests autonomes de positionnement, dans l'idée d'encourager, tout en la suivant, l'évolution de leurs compétences numériques tout au long de leur carrière* » et se fixe comme objectif, à terme, « *d'utiliser PIX pour certifier les compétences numériques des enseignants à l'issue de leur formation initiale* » [(1)] et d'atteindre en outre 250 000 enseignants formés chaque année *via* la plateforme de formation à distance M@gistère.

La diffusion du numérique au sein des pratiques d'enseignement semble actuellement en bonne voie. Selon l'enquête PROFETIC, qui porte sur les pratiques des enseignants en matière de numérique éducatif, 9 enseignants sur 10 reconnaissent les bénéfices pédagogiques du numérique et l'utilisent pour préparer leurs cours dans le premier degré, et plus de 92 % des enseignants du second degré l'utilisent pour construire des séquences d'activités en classe [(2)], notamment grâce au déploiement des espaces numériques de travail (ENT).

Toutes ces initiatives doivent être poursuivies et amplifiées pour fournir aux futurs citoyens les clés du monde numérique et aux entreprises des salariés disposant d'un socle satisfaisant de compétences numériques. Il existe en effet encore des carences sur ce dernier point. C'est le sens du propos de M. Henri d'Agrain, délégué général du Cigref, qui invite en effet les pouvoirs publics à « *ne pas baisser le niveau d'exigence de la formation des ingénieurs, notamment ceux orientés vers les métiers du numérique* » et relève que les efforts menés doivent être approfondis puisqu'à l'heure actuelle, « *le nombre d'élèves qui choisissent, en fin de seconde, la spécialité « Numérique et sciences informatiques (NSI) » est assez faible et très peu de filles figurent parmi eux* ». La spécialité NSI ne se trouve en outre, selon lui, pas en bonne position dans le cadre actuel où « *l'une des trois*

(1) Audition de M. Jean-Marc Merriaux, mardi 4 mai 2021.

(2) Ministère de l'éducation nationale, de la jeunesse et des sports – Enquêtes Profetic 2017 et 2018.

spécialités de première est abandonnée en terminale. […]. *Or ce sont ces étudiants qui, à travers Parcoursup, choisiront ensuite les voies de formation des métiers du numérique dans l'enseignement supérieur* » (1). Il convient donc de prendre en compte ces critiques et de faire évoluer certains paramètres le cas échéant.

4. Former les salariés aux savoir-faire numériques généraux et avancés

a. Un impératif alors que la France est aussi en retard dans ce domaine

La formation des salariés aux savoir-faire numériques généraux et avancés est un levier indispensable pour numériser notre économie *« par le bas* » et faire en sorte que le numérique soit un vecteur de progrès. Comme l'a rappelé M. Bruno Sportisse, président-directeur général de l'Institut national de recherche en sciences et technologies du numérique (INRIA), défendre la souveraineté numérique implique impérativement de « *s'assurer un vivier de talents et de compétences. La transformation numérique ne se réussira pas autrement.* […]. *[L]'enjeu de la formation initiale et continue* [..] *constitue* […] *la clé de voûte de toute politique à mener dans ce domaine* » (2).

Sur ce sujet, en dépit des progrès réalisés, la France accuse un certain retard. Dans son rapport présenté pour le lancement du Pacte productif 2025, le Gouvernement relevait ainsi que : « *la numérisation de la société française progresse mais doit être accélérée. Nos entreprises et notre administration ont pris du retard dans la numérisation. En 2019, la France n'était que 15ème sur 28 dans le classement de la Commission européenne relatif à l'économie et la société numériques. Seulement 15 % des entreprises françaises utilisent le* cloud *contre 18 % en moyenne dans l'Union européenne. On compte par ailleurs 132 robots pour 10 000 personnes dans l'industrie manufacturière en France : il y en a 1,4 fois plus en Italie et 2,3 fois plus en Allemagne.* » (3).

Ce constat d'une forme de retard français a été largement partagé par les différents acteurs auditionnés par votre rapporteur. Il a été résumé utilement par M. Renaud Vedel, préfet, et coordinateur de la stratégie nationale pour l'Intelligence artificielle : « *En ce qui concerne la formation, nous n'avons encore parcouru qu'entre un tiers et la moitié du chemin, au regard de la transformation et de l'émergence des formations qu'exige la vague technologique. La formation ne doit pas reposer uniquement sur la formation initiale, bien que de très importants efforts sont à fournir sur ce plan. Nous devons également revitaliser les connaissances ou procéder à l'entraînement de certains acteurs qui n'opèrent pas directement sur l'IA mais qui auraient la capacité d'investir le sujet. Dans le monde professionnel, il faut également que les fonctions comme les ressources humaines, le marketing, le business deviennent capables de comprendre et d'intégrer les systèmes d'IA dans leurs façons de raisonner* » (4).

---

(1) Audition de M. Henri d'Agrain, 18 mars 2021

(2) Audition de M. Bruno Sportisse, jeudi 18 mars 2021.

(3) Pacte productif 2025, rapport diagnostic et enjeux du Pacte productif, octobre 2019, p.15.

(4) Audition de M. Renaud Vedel, 6 mai 2021.

M. Renaud Vedel a néanmoins relevé, en même temps qu'un « *important effort [est en cours] de ce point de vue* » et que « *l'offre de formation s'étoffe grandement* » [(1)].

Comment la demande de compétences numériques requises a-t-elle évolué entre 2012 et 2018 ?

Les travaux de Pôle Emploi et de France Stratégie indiquent que les compétences numériques sont en train de devenir un facteur de plus en plus différenciant entre les salariés, entreprises et secteurs d'activité.

La maîtrise des systèmes informatiques et de télécommunications (conception et exploitation), l'usage et le paramétrage de logiciels et l'installation d'infrastructures numériques, sont ainsi parmi les premières compétences en croissance, traduisant la hausse continue des métiers de cadres. Elles sont, en effet, particulièrement mobilisées par les professions de l'informatique et des télécommunications (ingénieurs et cadres de l'industrie, du bâtiment, des transports) et les cadres administratifs, financiers et commerciaux dont l'emploi continue de progresser.

Selon l'OCDE, ces compétences numériques complexes vont prendre à l'avenir de l'ampleur dans l'économie, en raison des besoins croissants en matière de maintenance des structures informatiques et de télécommunication et de sécurité et protection informatiques.

Source : France Stratégie Pôle Emploi, Cartographie des compétences par métiers, La note d'analyse, n° 101, mai 2021.

Il est donc indispensable d'augmenter les capacités de la France à former massivement les salariés aux compétences numériques. Cela implique, en pratique, de bien comprendre la nature de la « demande de compétences » émanant des acteurs privés pour orienter de façon efficace le système de formation professionnelle.

b. Une demande accrue de compétences numériques générales et spécialisées

Les besoins en compétences numériques déclarés par les employeurs sont variés. D'après les enquêtes annuelles « Besoins en main-d'œuvre (BMO) » réalisées par Pôle Emploi, les employeurs recherchent à recruter des salariés disposant de plus en plus à la fois de compétences numériques classiques (maîtrise des usages bureautiques de l'ordinateur, dans ses principales fonctions (messagerie, traitement de texte, tableurs, recherche d'information sur Internet) mais aussi de compétences expertes ou spécialisées, même lorsque le métier proposé n'a pas de lien direct avec le secteur du numérique. Cela témoigne d'une prise de conscience, au sein des entreprises, en particulier pour les plus grandes, de la valeur ajoutée que le numérique peut apporter à leur activité (*via* la maîtrise par le salarié d'un logiciel spécialisé, de la configuration de logiciels, programmation, ou encore de l'utilisation de machines automatisées ou de robots).

(1) Idem.

Ainsi que l'indique l'étude de Pôle Emploi *« pour un même métier, les établissements de moins de cinq salariés ont davantage d'exigences à l'égard des compétences numériques de base ou de compétences plus pointues et spécifiques (savoir configurer des logiciels spécialisés, savoir produire du code informatique). Ces exigences s'inscrivent dans une demande de polyvalence plus importante des salariés. De même ces compétences sont davantage recherchées par les employeurs ayant des projets de recrutement portant sur des emplois durables. En revanche, pour un même métier, les compétences en matière de manipulation des robots et de machines automatisées sont plus demandées dans les établissements de plus de 100 salariés. La probabilité que cette compétence soit jugée indispensable dans ces grands établissements est multipliée par deux par rapport à un établissement de 10 à 19 salariés. Ce résultat est cohérent avec l'intensité d'utilisation des robots, plus importante dans les grandes entreprises. »* (1).

En fonction du caractère indispensable, utile ou superflu pour les employeurs des compétences numériques, six groupes de métiers peuvent être distingués :

– les métiers avec un usage limité des outils numériques ;

– les métiers concernés par la conduite de machines automatisées ;

– les professions pour lesquelles la maîtrise d'outils spécialisés liés à l'activité de travail est demandée ;

– les métiers à forte intensité numérique ;

– les métiers à compétences numériques expertes ;

– les informaticiens et professionnels des télécommunications.

Le tableau présenté ci-dessous, décline pour ces catégories le type de compétences attendu et leur niveau de criticité.

(1) Pôle emploi, Quand les entreprises expriment leurs besoins de compétences numériques nouvelles, Éclairage et synthèses, n° 64, janvier 2021.

COMPÉTENCES NUMÉRIQUES ET MÉTIERS : UNE DEMANDE FORTE – DES BESOINS VARIÉS SELON LES SECTEURS D'ACTIVITÉ

LES MÉTIERS SELON LES COMPÉTENCES NUMÉRIQUES RECHERCHÉES : POIDS AU SEIN DES SECTEURS (EN %)

	Catégories de métiers selon les compétences numériques recherchées						
Secteur	Usage limité des outils numériques	Conduite des machines automatisées	Usage d'outils spécialisés	Métiers à forte intensité numérique	Métiers à compétences numériques expertes	Informaticiens et professionnels des télécommunications	Autres métiers*
Agriculture, sylviculture et pêche	36	37	1	7	4	1	14
Secteur agro-alimentaire	3	60	11	9	14	0	4
Industrie (hors agro-alimentaire)	4	41	1	13	36	2	3
Construction	55	8	1	11	23	1	1
Commerce	13	15	22	23	18	1	8
Transports et entreposage	34	15	0	22	9	1	18
Hébergement et restauration	77	6	1	5	3	0	7
Information et communication	1	2	1	20	25	42	9
Activités financières et d'assurance	1	2	2	79	8	5	4
Activités immobilières	8	15	3	38	16	1	19
Activités spécialisées, scientifiques et techniques	3	5	1	31	50	5	5
Activités de services administratifs et de soutien	9	21	2	15	8	1	44
Administration publique et enseignement	2	14	1	71	4	0	9
Santé	6	10	21	9	45	0	9
Action sociale	25	12	14	18	7	0	24
Arts, spectacles et activités récréatives	7	9	2	33	16	1	33
Autres activités de services	14	6	14	18	10	1	38
Ensemble des secteurs	16	17	7	24	19	2	16

*Les autres métiers désignent les métiers qui n'ont pas été classés en raison d'effectifs insuffisants: agents de sécurité, professions administratives de la fonction publique, techniciens et cadres de l'agriculture, cadres des transports, artistes, employés de maison.

Les catégories de métiers surreprésentées par rapport à l'ensemble des secteurs sont surlignées.

Lecture : dans le secteur de l'agriculture, les métiers pour lesquels l'usage des outils numériques est limité représentent 36% des effectifs salariés.

Sources : BVA-Pôle emploi, Enquête complémentaire Besoins en main d'œuvre 2018 ; Insee, Enquête emploi, 2015-2017.

Source : Pôle emploi, Quand les entreprises expriment leurs besoins de compétences numériques nouvelles, Éclairage et synthèses, n° 64, janvier 2021.

Les conclusions qu'il est possible d'en tirer, et qui sont largement partagées par les acteurs auditionnés sont les suivantes : **le numérique impactera l'ensemble des métiers, même de façon ponctuelle. Il est donc impératif d'anticiper ces changements rapides en proposant des formations spécifiques à l'ensemble des salariés pour éviter que des barrières de compétences ne se créent et ne viennent renforcer les inégalités existantes sur un marché du travail déjà fortement polarisé.**

c. Des pouvoirs publics qui se sont saisis de cette problématique

Il est incontestable que les pouvoirs publics ont pris la mesure de cette question, en mettant en place un certain nombre d'initiatives positives.

Un plan pluriannuel (2018-2022) d'investissement dans les compétences (PIC) a été lancé en septembre 2017 avec plusieurs objectifs principaux, dont celui d'amorcer la transition digitale de l'État et de construire une société de compétences par la transformation profonde de l'offre de formation et l'identification des projets innovants.

Ce plan vise à anticiper les conséquences de la « révolution numérique » qui va, d'après les anticipations proposées, conduire *« 50 % des emplois* [à se transformer] *dans les dix ans qui viennent »*, menacer de disparition 10 % à 20 %

des emplois en raison de l'automatisation et de la désintermédiation des tâches entraînées par la robotisation ou le numérique, et, enfin, créer des tensions sur les populations les plus faiblement diplômées, puisqu'à l'heure actuelle « *40 % des actifs ayant un niveau inférieur au Bac occupent des métiers à fort risque d'automatisation contre 5 % des actifs diplômés de l'enseignement supérieur* ».

Doté d'un montant de 14 milliards d'euros sur la période 2018-2022, composante du « grand plan d'investissements », le PIC est cofinancé par l'État et les entreprises *via* un financement dédié prévu dans le cadre de *la loi du 5 septembre 2018 pour la liberté de choisir son avenir professionnel*. Ce plan prévoit notamment le financement de 10 000 formations aux métiers du numérique, notamment par la Grande École du Numérique, accessibles à des publics peu qualifiés (« 10Knum »). Sa mise en œuvre est soutenue par le Haut-commissaire aux compétences et par France compétences.

France compétences

France compétences est un établissement public à caractère administratif créé en janvier 2019, en vue d'assurer le financement, la régulation et l'amélioration du système de la formation professionnelle et de l'apprentissage.

Placé sous la tutelle du ministre chargé de la formation professionnelle, France compétences a plusieurs missions :

– répartir les fonds mutualisés aux différents acteurs de la formation professionnelle et de l'apprentissage ;

– réguler la qualité de la formation ;

– émettre des recommandations sur les coûts, les règles de prise en charge et l'accès à la formation ;

– veiller à la bonne exécution de la réforme sur la formation professionnelle et de l'apprentissage.

France compétences joue également un rôle clé dans la transformation de l'offre de formation. En lien avec les branches, il participe à la construction des titres et des diplômes professionnels.

Doté d'une personnalité morale et d'une autonomie financière, France compétences est composée de cinq collèges représentant l'État, les organisations syndicales de salariés, les organisations patronales, les Régions et des personnalités qualifiées.

La convention d'objectifs et de performance de France compétences, conclue en avril 2020, qui fixe les orientations pour la période 2020-2022, a retenu comme premier axe stratégique celui de favoriser l'identification des besoins en compétences des personnes et des entreprises.

Source : site internet du ministère du Travail

En outre, plusieurs outils de dialogue entre les acteurs professionnels et l'État, qu'il s'agisse des contrats stratégiques de filières, ou encore des engagements de développement de l'emploi et des compétences (EDEC) comprennent des éléments liés aux enjeux de formation aux technologies numériques. Ces documents témoignent d'ailleurs souvent d'une réelle prise de conscience de ces enjeux dans

le monde professionnel, comme le montre, par exemple, le constat commun des signataires de l'accord-cadre national d'engagement de développement de l'emploi et des compétences pour la branche de la métallurgie dans le cadre des mutations liées à la transition numérique, qui vaut pour toute démarche de formation professionnelle dans tout secteur d'activité : *« Les liens entre introduction de technologies numériques et transformation du monde du travail sont très nombreux. Le numérique impacte les emplois, les métiers et les besoins en compétences, recompose l'organisation du travail et appelle à de nouvelles formes de collaboration. Aucun secteur professionnel n'échappe à ces transformations, qu'elles soient directement technologiques et/ou dans les usages, les modes de concurrence, le rapport au client, le renouvellement et l'adaptation des formations. Pour que ces évolutions soient porteuses d'emploi, des mesures d'accompagnement et d'anticipation sont nécessaires. »* (1).

Lors de leur audition, les représentants de la confédération française de l'encadrement-confédération générale des cadres (CFE-CGC) ont, pour leur part, considéré que la consolidation des résultats des différents engagements de développement de l'emploi et des compétences réalisés dans les différentes filières et les différents secteurs d'activité permettront d'obtenir une vision complète de l'impact de la transition numérique sur l'emploi. Selon eux, *« il s'avère complexe pour les entreprises de se projeter à cinq ou dix ans en matière de nouvelles compétences liées à l'Intelligence artificielle ou pour ce qui concerne les besoins qui seront les leurs à l'arrivée de jeunes salariés. Il convient donc de trouver cet équilibre entre le travail initial de prospective, mené par les organisations syndicales et patronales dans l'EDEC, et les propositions de formations aux nouvelles compétences »* (2).

Dans leur état des lieux du marché du travail et enjeux pour la relance, France Stratégie et le Conseil d'orientation pour l'emploi insistent en outre sur la considération selon laquelle *« la formation demeure une thématique prioritaire, pour toutes les parties prenantes. Celles-ci soulignent cependant des dysfonctionnements persistants dans les différentes dimensions : offre, institutions, financement, etc. Il existe de nombreuses structures de concertation et de très nombreux acteurs dans ce domaine de la formation professionnelle, mais pas de plan général susceptible de les coordonner. Les nombreuses priorités stratégiques de l'économie ne parviennent pas à se décliner clairement, ce qui favorise une vision adéquationniste de court terme sans d'ailleurs y parvenir, qui capte les financements au détriment du renforcement général des compétences au service d'un investissement dans les secteurs d'avenir. Les exercices de prospective des métiers sont antérieurs à la crise, et même si les initiatives sont nombreuses (campus des métiers et qualifications, comités d'orientation des grandes écoles, comités stratégiques de filières industrielles, etc.), il est difficile de stabiliser les*

(1) Accord signé le 7 novembre 2017, par l'État (déléguée générale à l'emploi et à la formation professionnelle), l'Union des industries et des métiers de la métallurgie (UIMM) et les représentants des syndicats CFDT, CFE-CGC, CFTC, FO.

(2) Audition de Mme Raphaëlle Bertholon et M. Nicolas Blanc, 20 avril 2021.

priorités d'un plan général de développement des compétences à moyen et long termes, d'autant plus que de nouveaux besoins en ressources humaines découlent de la crise comme du Plan de relance. La formation professionnelle demeure donc une thématique prioritaire de l'agenda social, et il reste essentiel de mieux anticiper les besoins de main-d'œuvre au niveau territorial, pour mieux planifier les formations. » (1).

Ces différents éléments plaident donc en faveur d'un vrai effort de prospective, de lisibilité, et d'action dans le cadre de la formation professionnelle, pour proposer à chacun des modules dédiés lui permettant de gagner en maîtrise des technologies numériques.

Proposition n° 22 : Proposer dans le cadre de la formation professionnelle des modules dédiés aux technologies numériques.

d. Des domaines de formation à prioriser au regard de leur haut potentiel

La prospective des métiers prioritaires pour amplifier l'accélération de la numérisation conduit bien sûr à insister sur l'importance des formations dans les domaines de pointe que sont notamment la cybersécurité, l'Intelligence artificielle et la blockchain.

i. La cybersécurité

La cybersécurité constitue un premier domaine qui doit être au cœur des priorités françaises en termes de formation.

Lors de son audition par la mission d'information, M. Michel Van Den Berghe, président de la mission Campus Cyber a en effet indiqué que la France souffrait à l'heure actuelle « *d'un manque de ressources en cybersécurité »*. Face à une menace croissante, cette situation n'est pas tenable et comporte le risque, pour la France, de « dévisser » progressivement au sein des classements internationaux, alors qu'elle est pour l'heure relativement bien positionnée dans ce domaine.

La création d'un campus cyber est une réponse à cette problématique. Ce campus rassemblera en effet « *plusieurs écoles pour pouvoir former plus de personnes dans [ce] domaine (…)*. Il a vocation à accueillir un ensemble de cyber-tech, d'acteurs de la formation numérique ainsi que l'ANSSI qui y sera également représentée pour rapprocher les différents acteurs de cet écosystème. M. Van Den Berghe a en outre précisé à votre rapporteur que « *l'école pour l'informatique et les techniques avancées (EPITA) créera un* bachelor *dédié à la cybersécurité. »*

S'agissant de la formation professionnelle continue, M. Michel Van Den Berghe estime que *« les formations doivent en premier lieu mettre à niveau les professionnels de la cybersécurité par rapport aux nouvelles typologies d'attaque.*

(1) France stratégie et Conseil d'orientation pour l'emploi, État des lieux du marché du travail et enjeux pour la relance, rapporteur M. Bruno Coquet, avril 2021.

Les pirates sont extrêmement créatifs et l'Internet des objets créera de nouvelles vulnérabilités. La 5G créera également de nombreuses possibilités de connexions d'objets et augmentera donc la vulnérabilité. Nous devons donc former les acteurs pour que les RSSI et les DSI soient mis à niveau. Nous essaierons en deuxième lieu de réaliser du rescaling *d'ingénieurs réseaux, d'ingénieurs de production informatique, de développeurs, plutôt que de laisser chaque entreprise mener ce travail de façon artisanale en son sein, nous voulons structurer la démarche, en nous faisant aider, par exemple, par l'ANSSI, qui pourrait dispenser des formations. »* (1).

Votre rapporteur salue la dynamique engagée dans ce domaine et invite les pouvoirs publics à poursuivre le déploiement de ce campus.

Proposition n° 23 : Poursuivre la dynamique de constitution d'un campus cyber.

ii. L'Intelligence artificielle

L'Intelligence artificielle constitue un second champ à investir massivement en termes de formation professionnelle.

L'Intelligence artificielle constitue, d'après le rapport de France Stratégie « Intelligence artificielle et travail », remis aux ministres en charge du travail et du numérique, en mars 2018, une forme de prolongement de la révolution numérique. Son développement offre un champ inédit d'usages et de possibilités, et devrait également conduire à automatiser un certain nombre de tâches. Le déploiement massif d'outils d'Intelligence artificielle favorisera, en outre, la diffusion des innovations, mais affectera évidemment les travailleurs, d'une façon différente selon la nature de leurs tâches.

En définitive, seul le rythme de diffusion de cette technologie reste incertain, car il dépend de considérations liées à l'automatisation, l'acceptabilité sociale, les compétences disponibles, les données disponibles ainsi que le cadre réglementaire. Comme l'indique en effet le rapport de France Stratégie précité : *« Des outils d'Intelligence artificielle vont être déployés progressivement dans de nombreuses activités. Leur diffusion va entraîner des transformations du travail qui passeront par des transformations des tâches et des métiers, donc des besoins de formation. Le renforcement des mécanismes de contrôle permis par l'Intelligence artificielle pourrait engendrer de nouveaux risques pour les travailleurs : les adaptations devront donc nécessairement passer par le dialogue social. Le scénario souvent avancé d'une transformation radicale et massive du travail apparaît toutefois peu crédible. Dans quelques secteurs ou sous-secteurs, l'occurrence d'un scénario disruptif n'est néanmoins pas exclue. Sa matérialisation s'appuierait sur une conjonction de facteurs : la capacité de l'Intelligence artificielle à fournir un service nouveau ; une demande forte des utilisateurs ; un cadre réglementaire*

(1) Audition de M. Michel Van Den Berghe,13 avril 2021.

obsolète ; enfin une concurrence internationale et l'arrivée de nouveaux acteurs sur le marché » (1).

Il convient donc de conduire, à l'échelle de la branche ou de la filière, des travaux de prospective sur le potentiel de l'Intelligence artificielle afin d'assurer un bon niveau d'information et d'anticipation des acteurs.

Votre rapporteur considère que sur la formation, la France s'est engagée dans la bonne direction mais que l'effort mis en œuvre doit être poursuivi. Comme l'a rappelé M. Renaud Vedel à l'occasion de son audition, les ambitions de la stratégie nationale IA sont élevées puisqu'il s'agit, à terme, de « *multiplier par deux, puis par quatre, le nombre de personnes formées, incluant des experts tels que des ingénieurs et des docteurs, mais pas seulement* ». Votre rapporteur partage l'analyse de M. Renaud Vedel, selon laquelle « a*u cœur de la bataille mondiale sur cet enjeu de souveraineté de l'IA, nous nous apercevons de l'existence d'un goulot d'étranglement, malgré la qualité de nos écoles d'ingénieurs, amenant à une tension en ce qui concerne le nombre de profils* ». Il convient donc d'encourager les doubles cursus thématiques, liant par exemple IA et santé, IA et agriculture, IA et industrie etc. Il sera également utile de pouvoir disposer d'un vivier « *de techniciens d'un niveau DUT ou licence, car une fois qu'un système d'IA est développé, il convient d'en comprendre les limites, les règles éthiques de fonctionnement, les alertes et être capable de préparer les données. Ces tâches ne nécessitent pas en elles-mêmes un haut niveau d'expertise, mais requièrent cependant une formation particulière.* » (2).

Cette dernière recommandation recouvre largement une proposition portée notamment par M. Nicolas Brien, directeur général de France Digitale, et que votre rapporteur soutient : faire des instituts universitaires de technologie (IUT) des centres d'excellence permettant à notre pays de disposer d'un vivier de techniciens du numérique.

Proposition n° 24 : Faire des instituts universitaires de technologie des centres d'excellence pour fournir à la France des techniciens numériques en nombre suffisant.

iii. La *blockchain*

Dans leur rapport, remis au gouvernement le 15 avril dernier, sur les verrous technologiques des *blochchains*, les chercheurs de l'Inria, du CEA-List et de l'Institut Mines-Télécom (IMT) ont dressé une cartographie des formations *blockchain* diplômantes dans l'enseignement supérieur en France.

Leur constat est celui d'une offre principalement localisée dans le bassin parisien (81 % des heures de formation), portant, à la fois, sur le cœur de la technologie *blockchain* et des formations techniques sur l'intégration d'une *blockchain* dans un système. Des formations en économie, finances et droit traitant

(1) France stratégie, Intelligence artificielle et travail, mars 2018.

(2) Audition de M. Renaud Vedel, 6 mai 2021.

de la problématique *blockchain* dans ces domaines complètent cette offre. La grande majorité des formations sont initiales (68 %), plus d'un cinquième en alternance. Les formations sont majoritairement dispensées en langue anglaise. Les comparaisons internationales font apparaître l'existence d'un faible nombre de cours technologiques orientés spécifiquement à cet égard dans les grandes universités, alors que les cours en finances, économie et droit sont nombreux. Cela démontre une claire appropriation du thème de la *blockchain* dans ces enseignements. Il reste qu'une petite proportion de programmes permet de former à l'ensemble des aspects de la technologie *blockchain* dans un cursus intégré. Il n'existe donc pas de retard proprement français.

Au total, les auteurs relèvent que l'offre de formation à la *blockchain* est en rapide développement, le système de formation académique en France n'étant pas en retard par rapport aux autres pays. Ils proposent, pour aller plus loin, de *« mettre en place un ou des parcours de formation mêlant un éventail de dispositifs pédagogiques modernes avec du coaching lors de sessions pratiques (par exemple lors de* coding bootcamp*) dédiées. Les professionnels doivent également être impliqués dans cette démarche. Au final, dans l'enseignement de la technologie* blockchain*, il s'agit de construire une approche pédagogique variée et agile dont la finalité est l'accélération de la formation pour pallier le manque actuel de diplômés et pour mettre rapidement sur le marché de jeunes recrutés opérationnels. »* (1).

Votre rapporteur considère que les pouvoirs publics doivent soutenir l'émergence de formations dans le domaine de la *blockchain*, afin de prendre de l'avance sur les autres pays. Les propositions de M. Rémy Ozcan, président de la Fédération française des professionnels de la *blockchain* (FFPB), pour faire de la France une « *blockchain nation* » pourraient être utilement étudiées. Ce dernier estime, en effet que « *le ministère de l'éducation* [nationale] *devrait inciter écoles et universités à intégrer dans leur offre de formation des modules* blockchains *»* et qu'il conviendrait « *de délivrer des formations à tous les corps professionnels, aussi bien aux métiers du droit, à l'École nationale de la magistrature (ENM), qu'à ceux de l'immobilier* », en adoptant « *une approche par corps de métier* » pour créer « *une sensibilisation progressive à l'impact de la technologie* blockchain *pour chaque secteur* » (2).

Proposition n° 25 : Accélérer le renforcement de l'offre de formation « *blockchain* » et soutenir la sensibilisation du monde professionnel au potentiel de cette technologie.

(1) Les verrous technologiques des blockchains. Rapport de l'Inria-CEA List-IMT, avril 2021.

(2) Audition de M. Rémy Ozcan, 22 avril 2021.

II. ACCÉLÉRER LA NUMÉRISATION DE TOUTES LES ENTREPRISES EN VALORISANT NOTRE ÉCOSYSTÈME TECHNOLOGIQUE

La crise sanitaire a démontré l'importance, pour les entreprises, de maîtriser les technologies numériques, dans un contexte où le numérique a conditionné la poursuite de leur activité à distance.

Le chemin à parcourir dans ce domaine est encore long puisqu'en 2019, près des deux tiers des TPE/PME n'avaient pas engagé de démarche de numérisation. Il existe, en outre, « un fossé » dans notre pays, comme l'a rappelé M. Jean-Noël de Galzain, président d'Hexatrust, organisation regroupant des *start-up*, des PME et des ETI spécialisées dans la cybersécurité, « *entre les privilégiés du numérique et un certain nombre de PME, ETI, artisans, professions libérales, commerçants, mais aussi tout un nombre d'organisations publiques de santé et de collectivités locales, qui ne sont pas équipés comme il se doit.* » (1).

L'accélération du recours aux outils numériques dans le cadre de la crise doit donc être mise à profit par les pouvoirs publics, alors que la France reste en retard sur la plupart des éléments de comparaison au sein des classements internationaux.

A. NUMÉRISER TOUTES LES ENTREPRISES POUR GAGNER EN COMPÉTITIVITÉ ET EN EFFICACITÉ

Selon la direction générale du Trésor, le degré de numérisation des entreprises françaises est comparable, dans une analyse globale, à celui observé en Europe, tant en ce qui concerne le recours à des outils numériques matures – progiciels de gestion, traitement automatisé des factures – que l'utilisation des technologies numériques comme le *cloud*, les données de masse ou l'Intelligence artificielle. En ce qui concerne le taux de robotisation, il est plus faible que dans d'autres pays européens mais considéré comme cohérent avec la structure sectorielle de l'économie et la population active (2).

Ce premier bilan appelle toutefois, dans le détail, plusieurs nuances. La direction générale du Trésor constate ainsi qu'en France comme dans le reste de l'Europe, les PME et *a fortiori* les TPE accusent, par rapport aux grandes entreprises, un retard dans l'adoption de toutes les technologies numériques, qui se traduit par une moindre connexion à l'Internet haut débit et très haut débit, un moindre recours aux logiciels de gestion, à la vente en ligne, au *cloud* et à l'analyse des données.

(1) Audition de M. Jean-Noël de Galzain, 11 février 2021.

(2) Trésor-Éco, Numérisation des entreprises françaises, n° 271, novembre 2020.

1. Une accélération de la numérisation pendant la crise mais un long chemin à parcourir, encore, pour les TPE et PME

La numérisation des entreprises, en particulier des plus petites, s'est accélérée en 2020, face à la nécessité, pour ces acteurs, de s'adapter aux contraintes de la crise sanitaire. Lors de son audition, Mme Bénédicte Roullier, directrice de France Num, a ainsi noté « *une progression évidente est visible dans les baromètres réguliers de la fédération du e-commerce et de la vente à distance (Fevad) pour les volumes de vente en ligne* », ainsi qu'une « *nette progression des demandes de nom de domaine en « .fr »* » d'après les indicateurs de l'association français pour le nommage d'Internet en coopération, ce qui traduit certainement « une *augmentation de la présence sur Internet des TPE et PME* ». La crise a eu logiquement « *un impact positif de prise de conscience et constitue globalement une opportunité pour les filières numériques française, européenne et internationale, y compris pour les géants du Web (GAFAM)* » [1]. Mme Bénédicte Roullier a indiqué, en outre, que la crise sanitaire avait donné lieu à des « *actions de débrouillardise* » mises en œuvre par des TPE et PME, qui ont parfois improvisé un recours au « click and collect *ou [à] différentes solutions permettant à leurs clients de commander à distance et de venir chercher leurs produits* ». France Num a élaboré un guide à leur endroit, qu'elles ont pu utiliser lors du premier confinement.

Cette évolution positive, qui constitue un facteur de résilience pour ces entreprises, comme l'ont montré plusieurs travaux menés, notamment pendant la crise, par la Banque de France, ne doit néanmoins pas occulter le chemin qu'il reste à parcourir pour les petites entreprises en matière de numérisation. Il existe, en effet, comme le relève une étude de l'observatoire de l'emploi des cadres de l'Association pour l'emploi des cadres (APEC) sur la transformation numérique dans les PME publiée en mars 2019, un décalage persistant entre la diffusion d'usages numériques au sein de la population (sept consommateurs sur dix achètent et paient en ligne) et le niveau de maturité numérique des TPE et PME (une PME sur huit fait usage de solutions de vente en ligne), qui doit être résorbé.

D'après la même étude, on constate également un manque de structuration des projets de transformation numérique des TPE et PME. Nombre d'entreprises de cette taille mènent en réalité un projet informatique qui ne correspond pas à une véritable transformation. L'importance du diagnostic est trop rarement identifiée, ce dernier étant souvent réalisé en interne. Le niveau de maîtrise des enjeux numériques par les dirigeants d'entreprise reste, enfin, inégal, et les projets de numérisation d'une ampleur limitée (création d'un site Internet ou d'une page sur les réseaux sociaux etc.).

Le baromètre mis en œuvre par France Num permet de dresser un état des lieux de la numérisation des entreprises et de constater le chemin qu'il reste à parcourir au sein des TPE et PME. Ainsi que le relève Mme Bénédicte Roullier, ce baromètre indique que, sur la question des usages, « *68 % des TPE et PME sont*

---

[1] *Audition de Mme Bénédicte Roullier, 15 avril 2021.*

aujourd'hui convaincues des bénéfices concrets du numérique », ce qui laisse près d'un tiers d'entreprises non convaincues. Ce taux de convaincus atteint, en outre, 72 % sur le thème de la communication avec les clients, « *ce qui montre que le numérique appliqué à leurs problématiques leur parle, plutôt que le numérique en général* » (1).

En matière d'équipements numériques, si « *les dirigeants de TPE et PME sont des personnes très connectées* [puisque] *88 %* [d'entre eux] *possèdent un smartphone, seuls 37 % de leurs entreprises ont un site Internet institutionnel ce qui semble être un chiffre très particulier à la France* ». Les données de l'indicateur DESI 2020 démontrent globalement que « *la France est en retard en visibilité Internet, globalement et plus particulièrement par rapport aux pays du Nord. Le chiffre est encore plus bas pour les sites de e-commerce, puisque seulement 9 % des entreprises avaient un site au début de l'année 2020* ». En revanche, « *une spécificité de la France est que 40 % des entreprises ont un logiciel de gestion, ce qui nous met en tête du peloton européen. La France est donc assez faible en visibilité mais assez forte sur l'équipement en logiciel de gestion, ce qui est probablement lié à l'obligation – datant de 2018 ou 2019 – d'avoir un logiciel de caisse. Cette contrainte peut donc devenir un avantage pour les TPE et PME qui disposent ainsi de données de gestion* » (2).

France Num estime le nombre de TPE et PME à accompagner dans une démarche de numérisation **à** 2,6 millions d'entreprises. Elle a commandé en outre aux cabinets de conseil Boston Consulting Group et Ernst et Young une étude sur la relation des dirigeants de TPE et de PME à la transformation numérique de leur activité, afin de mieux comprendre leurs différents profils.

Cette étude, comme l'a rappelé Mme Bénédicte Roullier, détaille cinq attitudes à l'égard du numérique et de son développement qui doivent être prises en compte pour adapter les politiques de soutien et d'incitation à la numérisation :

– les dirigeants de type « prudent », qui n'ont pas de perspective de développement, et sont peu à l'aise avec le numérique. Leurs priorités portent sur la diminution de leurs charges, la fidélisation des clients et la protection de la réputation de l'entreprise. Pour 59 % d'entre eux, le numérique ne présente pas de réel bénéfice pour l'entreprise, même si la moitié d'entre eux est consciente du fait que le numérique est un moyen de communiquer avec ses clients : 15 % ont un site Internet institutionnel et 21 % une présence sur les réseaux sociaux, 4 % utilisent des plateformes d'échange de documents en ligne. Ce segment est estimé à 390 000 entreprises, plus particulièrement dans les secteurs des services à la personne et du tourisme/hébergement ;

– les dirigeants de type « demandeur », qui, sans être à l'aise avec le numérique, ne s'estiment néanmoins pas en retard par rapport à leurs pairs. Leurs

(1) Audition de Mme Bénédicte Roullier, 15 avril 2021.

(2) Idem.

priorités sont d'augmenter leur base client, de fidéliser leurs clients et d'accroître leur production. Pour 71 % de ces dirigeants, le numérique représente un réel bénéfice pour l'entreprise, 44 % ayant un site Internet institutionnel et 51 % une présence sur les réseaux sociaux. Mais (trop) rares sont ceux qui sautent le pas : 8 % seulement ont un site marchand, 6 % vendent seulement sur des places de marchés. Ce segment est estimé à 705 000 entreprises, en zone rurale, dans les secteurs de l'agriculture et du commerce-artisanat ;

– les dirigeants de type « réceptif », qui sont relativement à l'aise avec le numérique, et ne ressentent pas de retard par rapport à leurs pairs. Leurs priorités sont d'accroître leur visibilité, d'augmenter leur base clients et de faire évoluer leurs offres de produits et/ou de services. Pour 80 % de ces dirigeants, le numérique apporte un bénéfice réel à l'entreprise. Leur équipement numérique et leur utilisation des outils numériques sont déjà marqués : 47 % ont un logiciel de gestion, 18 % un site marchand, 11 % vendent en ligne sur une place de marché, 20 % achètent des mots clés pour être mieux référencés par les moteurs de recherche, 25 % utilisent des plateformes d'échange de documents en ligne, 55 % sont présents sur les réseaux sociaux. Ce segment est estimé à 650 000 entreprises, surtout dans le secteur de l'industrie ;

– les dirigeants de type « statique » sont aussi relativement à l'aise avec le numérique, sans se sentir en retard par rapport à leurs pairs. Leurs priorités visent la fidélisation de leurs clients, la protection de la réputation et la conformité avec la réglementation. Pour 68 % de ces dirigeants, le numérique représente un bénéfice réel pour l'entreprise. Ils utilisent des outils numériques pour gagner en efficacité : 17 % d'entre eux utilisent des plateformes d'échange de documents en ligne. Ce segment est estimé à 745 000 entreprises, dans les services spécialisés, les services à la personne et le tourisme-hébergement ;

– les dirigeants de type « opportuniste », qui ne sont pas représentatifs des dirigeants de TPE et de PME françaises. Entièrement autonomes avec le numérique et n'y rencontrant pas de frein, ils en sont passionnés. Ce segment est estimé à seulement 80 000 entreprises.

France Num

France Num est une initiative gouvernementale lancée en 2018 afin de soutenir la transformation numérique des TPE et PME. L'action des équipes de France Num consiste notamment :

- à animer l'écosystème des acteurs engagés dans la transformation numérique des TPE et PME, en facilitant leurs échanges et en les outillant ;
- à accompagner ces entreprises au passage à l'action en leur démontrant les bénéfices concrets de la transformation numérique et en les orientant vers les acteurs qui les accompagneront concrètement ;
- à mettre en place des actions de soutien et de financement dans ce cadre, ainsi que des actions de formations.

France Num fédère des actions qui vont de la sensibilisation jusqu'au passage à l'action.

Sensibiliser et mettre à disposition les ressources utiles

Le site Internet France Num met à disposition un ensemble de ressources variées, comprenant des articles de fond, un réseau d'experts numériques, des témoignages et retours d'expérience, des actualités sur les dispositifs nationaux et régionaux dédiés à la transformation numérique.

France Num propose également des actions de formation et de sensibilisation aux bénéfices concrets du numérique :

- Ma TPE a rendez-vous avec le numérique : formation en ligne pouvant être suivie à son propre rythme. Conçue en lien avec Fun-Mooc, la première session de ce Mooc (formation à distance capable d'accueillir un grand nombre de participants) a débuté le 25 janvier 2021, plusieurs sessions interviendront.
- Une campagne grand public de sensibilisation : le programme télévisé Connecte ta boîte sur BFM et RMC (connectetaboite.fr) depuis le 15 février 2021. Son principe consiste à suivre le processus concret de numérisation d'entreprises accompagnées par des experts.

Accompagner le passage à l'action

Cet accompagnement prend la forme de 10 000 diagnostics individualisés suivis d'un plan d'actions financé par le plan de relance. Ces diagnostics sont proposés gratuitement aux petites entreprises des secteurs du commerce et de l'artisanat par les chambres de commerce et d'industrie et les chambres des métiers.

France Num propose également des formations animées par des experts du numérique, en ligne ou en présentiel. Ce dispositif vise à accompagner 150 000 TPE/PME du secteur du commerce et de l'artisanat d'ici fin 2022.

Pour aider les entrepreneurs désireux d'engager leur transformation numérique à identifier des entreprises en mesure de les accompagner, France Num a constitué, en outre, un réseau d'experts du numérique : les activateurs France Num. Ce réseau compte aujourd'hui plus de 2 700 experts, offreurs de solution, conseillers privés ou publics (réseaux consulaires notamment), répartis sur l'ensemble du territoire.

Aider au financement de la transformation numérique

Plusieurs aides financières visent en outre à soutenir la transformation numérique des petites entreprises :

– des aides régionales : au-delà du plan de relance mis en œuvre par l'État, les collectivités territoriales, avec les Régions en fer de lance, soutiennent l'activité économique des TPE PME en leur proposant des aides financières à la transformation numérique.

– le chèque France Num de 500 euros est proposé, dans la limite des crédits disponibles, aux entreprises de moins de 11 salariés ayant fait l'objet d'une interdiction d'accueil du public à partir du 30 octobre 2020, ainsi qu'aux hôtels et hébergements similaires employant moins de 11 salariés. Il permet de financer tout ou partie de l'achat d'une prestation d'accompagnement à la transformation numérique ou d'acquisition d'une solution pour vendre en ligne, communiquer à distance avec ses clients ou encore promouvoir son activité sur Internet. 110 000 chèques financés par le plan de relance doivent être distribués. Un téléservice « cheque.francenum.gouv.fr » est ouvert depuis le 28 janvier 2021.

– la garantie de prêt France Num pour les entreprises souhaitant engager un processus de numérisation mais dont les ressources financières sont limitées. France Num propose, en lien avec la Banque européenne d'investissement (BEI), une garantie pour faciliter l'obtention d'un prêt bancaire. Le prêt est destiné aux entreprises de moins de 50 salariés ayant au moins trois ans d'existence. Le prêt d'un montant maximal de 50 000 euros bénéficie d'un taux de garantie de 80 %. Il est commercialisé par des réseaux bancaires partenaires.

Source : Direction générale des entreprises, ministère de l'économie, des finances et de la relance.

La direction générale des entreprises concentre ses actions au titre de l'initiative France Num sur 1,7 million d'entreprises relevant des segments « prudents, demandeurs et réceptifs » précités. Cette initiative vise, de façon concertée, en lien avec l'ensemble des acteurs, à lever les réticences qui peuvent exister en matière d'accompagnement vers la transformation numérique. Il s'agit, en somme, de mettre fin au paradoxe de l'existence de ressources numériques variées mais d'une absence de réflexe de ces entreprises consistant à se tourner vers des organismes ou des institutions professionnelles ou publiques.

Au total, l'accompagnement apparaît comme une problématique en soi, qui appelle un effort d'approche et de communication tenant compte de la diversité même des situations. Il importe de tenir compte de la réalité et des contraintes des TPE et des PME pour appeler leur attention de façon convaincante. Ainsi que le résume Mme Bénédicte Roullier, face à des TPE et PME qui n'ont « *pas toujours conscience de l'intérêt qu'a pour elles le numérique ou le vivent comme une sorte d'injonction au numérique* », France Num a vocation à accompagner ces entreprises dans une démarche de numérisation « *mais non à prescrire des solutions. Nous ne forçons pas les entreprises à se détourner d'offres de solution étrangères. Nous avons tous conscience que, actuellement, être référencé sur certaines plateformes ou moteurs de recherche internationaux est absolument indispensable. Notre but est plutôt d'embarquer les TPE dans le numérique, de les orienter vers les acteurs et les dispositifs les plus pertinents. France Relance a lancé plusieurs dispositifs,*

mais les entreprises restent libres de leurs choix entrepreneuriaux, de recourir à des solutions françaises ou étrangères. Nous voulons seulement qu'elles le fassent en connaissance de cause, qu'elles sachent que la gestion de leurs données sera différente selon la solution choisie » (1).

En somme, le but de France Num « *n'est donc pas uniquement de leur proposer des solutions françaises mais aussi de les convaincre de l'intérêt de se numériser et de les accompagner au mieux lorsqu'elles entreprennent cette démarche de digitalisation* ». C'est la raison pour laquelle, précise-t-elle, le réseau France Num « *inclut des acteurs privés, donc des offreurs de solutions. France Num est géré en partenariat avec les régions. Nous présentons notre réseau de façon territoriale car la relation de confiance de la TPE s'établit avec un contact de proximité. Nous travaillons sur l'animation du réseau avec les régions et avec les filières numériques régionales. Nous avons un enjeu de qualité de la description sur la base de données des activateurs pour permettre à une TPE de choisir en connaissance de cause, les critères pouvant aller du respect du Règlement général sur la protection des données (RGPD) au fait que la société est française ou non, mais nous ne référençons pas uniquement des sociétés françaises ou européennes »* (2).

Votre rapporteur salue les efforts engagés dans ce cadre, et le soutien du plan de relance à cette initiative. Il relève également qu'il est au fond assez logique, que des petites entreprises puissent avoir tendance à recourir à des solutions *« ready made »*, proposées par les intégrateurs, qui privilégient la facilité et le prix, quels que soient les enjeux d'indépendance technologique nationale et européenne. Il lui semble important, sur ce sujet, de se placer en effet dans une logique d'accompagnement objectif visant à faire connaître l'offre française et européenne, tout en prenant en compte les besoins des entreprises accompagnées. Il est également essentiel de les sensibiliser aux stratégies de « captivité » déployées par certains acteurs, et qui peuvent prendre la forme, par exemple, de « kits de bienvenue », dont certains ont été critiqués lors des auditions, notamment pour les *start-up*. Mme Servane Augier, directrice générale déléguée de 3D Outscale, a ainsi relevé qu'un certain nombre de *start-up* ayant utilisé ce *welcome kit*, cherchent à s'en émanciper dans un deuxième temps. *« Elles utilisent ce welcome kit. On ne va pas leur reprocher d'utiliser ce qu'on met à leur disposition, mais elles se rendent vite compte du risque important de perte de maîtrise. En effet, quand on utilise la panoplie des services de nos concurrents, on ne maîtrise plus l'infrastructure technique et le système d'information qu'on est en train de déployer »* (3). Les petites entreprises doivent donc être sensibilisées vis-à-vis de ces pratiques pour prendre leurs décisions en connaissance de cause.

(1) Audition commune de Mme Bénédicte Roullier,15 avril 2021.

(2) Idem.

(3) Audition de Mme Servane Augier, 9 février 2021.

Cette position d'accompagnement réaliste s'impose d'autant plus qu'il existe encore certaines limites dans l'offre numérique française et européenne, qui concernent cette fois-ci l'ensemble des entreprises et administrations nationales.

Comme le relève M. Jean-Claude Laroche, vice-président du Club informatique des grandes entreprises françaises (Cigref), il existe actuellement une *« situation d'extraordinaire dépendance »* des grandes entreprises et administrations adhérentes du Cigref à l'égard d'acteurs ou de solutions non européens : *« C'est vrai dans le domaine des logiciels. Typiquement, nous utilisons des systèmes d'exploitation, tels que Windows de Microsoft, et des suites bureautiques de Google ou de Microsoft comme Microsoft Office, Word, Excel, etc. Ces solutions sont américaines. Le moteur de recherche très souvent utilisé est Google. Il en va de même pour les outils de communication, avec les solutions comme Zoom, Teams, BlueJeans, Verizon ou Skype, qui sont américaines. Notre dépendance est presque totale. En ce qui concerne les matériels, la situation n'est guère plus brillante dans la mesure où, par exemple, nos* data centers *sont très souvent constitués de composants américains. Les routeurs dont sont munis les* data centers *de nombre de nos adhérents sont souvent de marque Cisco. C'est également vrai pour le matériel qui équipe les bureaux. Les ordinateurs personnels sont souvent fabriqués en Chine, avec des composants américains conçus et parfois développés en Israël. »* (1).

M. Stéphane Volant, président du Club de la sécurité et de la sûreté des entreprises, partage ce constat : *« la plupart des entreprises n'utilisent pas de solution française ni de solution européenne. Le marché des solutions françaises ou européennes des entreprises représenterait 10 % à 15 % des entreprises à l'heure actuelle. La raison n'est pas que les entreprises ne sont pas patriotes, surtout lorsqu'il s'agit d'entreprises publiques ou de défense. Ce n'est pas non plus parce qu'elles refusent de travailler avec des solutions françaises. Il y a deux raisons possibles : soit les solutions françaises sont inaccessibles et non compétitives, soit elles n'offrent pas les mêmes fonctionnalités ni la même ergonomie que les solutions internationales »* (2).

Sur ce sujet, votre rapporteur défend une position pragmatique, favorable à l'offre française et européenne mais consciente que certains segments sont moins compétitifs que certaines solutions extra-européennes. Dans le domaine de la sécurité, par exemple, il ne suffit pas d'insister sur le caractère souverain d'une solution pour répondre aux besoins des entreprises utilisatrices. Il faut répondre à ce besoin à un coût qui ne soit pas exorbitant et pour des fonctionnalités et une ergonomie toutes deux concurrentielles. Les acteurs auditionnés par la mission d'information ont ainsi considéré que le coût de la souveraineté représente un supplément maximum envisageable de l'ordre de 10 % à 15 %, lorsqu'il est envisagé comme une assurance.

---

(1) Audition de M. Jean-Claude Laroche, 18 mars 2021.

(2) Audition de M. Séphane Volant, 11 février 2021.

Quant au choix de passer au *cloud*, Mme Karine Picard, directrice générale d'Oracle France a pu insister en outre sur la force des acteurs américains qui est d'offrir un tout : l'infrastructure, la plateforme et le SaaS. *« Cela permet à certaines entreprises de rationaliser leur schéma directeur, de prévoir les intégrations, de faciliter la construction et le* move to cloud *d'un certain nombre de processus. Au départ, les entreprises privées ont fait des choix de* cloud *département par département. La présence de multiples acteurs* cloud *à l'intérieur d'une entreprise peut engendrer des problématiques de sécurité, de transmission de données, des problèmes légaux. Il existe un besoin de rationaliser, en termes tant de sécurité des données, de souveraineté, que de flux entre les différents départements des entreprises. Peu d'acteurs en Europe peuvent fournir ce type d'offre, cette gamme de services pour les entreprises privées »* (1).

Pour autant, la question des limites de l'offre numérique française ou européenne ne doit pas être appréhendée comme relevant d'un dernier « baroud d'honneur ». Des exemples de succès peuvent d'ailleurs être mis en avant, comme celui des progiciels de gestion de la logistique, de la comptabilité, des ressources humaines développés par l'éditeur allemand SAP AG. Il est question ici de choix avisés d'anticipation et d'investissement.

2. Des ETI et grandes entreprises convaincues par le numérique, et qui doivent accélérer leurs investissements

Les entreprises de taille intermédiaire se sont davantage saisies de l'enjeu de la transformation numérique. L'enquête annuelle dite « Baromètre de la maturité digitale des ETI », réalisée à la demande du Mouvement des entreprises de taille intermédiaire (METI), conjointement avec la société d'investissement Apax Partners et le cabinet Ernst & Young et associés, montre, année après année, depuis 2017, un approfondissement de la transformation numérique des ETI. Dans le baromètre 2019, 61 % des entreprises interrogées se déclaraient en cours de déploiement de leur stratégie digitale et 8 % affirmaient avoir atteint un stade de pleine maturité, sans différences entre les entreprises de *BtoB* et de *BtoC*.

Le premier type de projet d'investissement envisagé cible l'amélioration de l'expérience client, devant la collecte et l'exploitation organisée des données et la cybersécurité.

Dans le baromètre 2020, il apparaît que 71 % des ETI interrogées veulent accélérer leurs investissements dans le digital. La moitié des ETI estime également que la crise a accéléré le déploiement d'outils d'amélioration de l'expérience client et de transition vers le marketing digital. Pour plus de 85 % des entreprises interrogées, les domaines prioritaires d'investissement demeurent l'amélioration de l'expérience client par le digital, le déploiement des outils collaboratifs digitaux, la modernisation des infrastructures de technologies de l'information et la cybersécurité.

(1) Audition de Mme Karine Picard, 9 février 2021.

Comme l'a relevé M. Alain Conrard, président de la commission digitale du METI, la manière d'aborder la transformation numérique dans les entreprises revêt un caractère décisif : *« 71 % des ETI estiment que leurs direction générale et direction des systèmes d'information (DSI) portent principalement la transformation numérique en leur sein. En pratique, cette transformation se heurte à plusieurs obstacles : la résistance au changement, le défaut de vision partagée, des difficultés à intégrer les nouvelles compétences, la nécessité que les décideurs appréhendent les conséquences profondes de la transformation sur leur entreprise. Je pense ici à celles de l'Intelligence artificielle, des mégadonnées* (big data) *ou de l'Internet des objets* (IoT)*, sur l'organisation et le modèle même des entreprises, leurs canaux et modes de production. Les ETI n'investissent pas encore assez dans ces sujets qui déterminent pourtant en partie leur performance future »* [(1)].

Le caractère différenciant du facteur taille en matière de numérisation des entreprises ne doit pas faire oublier l'existence d'intérêts convergents entre les grandes entreprises et leur environnement économique. Il existe en effet une dynamique de numérisation des entreprises au sein des filières, comme le montre, par exemple, le contrat de filière du Comité stratégique de filière de l'industrie aéronautique (2018-2022). À partir du constat d'une filière « à deux vitesses » au regard des impératifs de l'industrie du futur entre, d'une part, les grands groupes, dont les « feuilles de route » sont en place et, d'autre part, la vision insuffisamment claire des solutions à mettre en œuvre de la part des PME et ETI, un parcours d'accompagnement individualisé de ces dernières a été mis en place en ce qui concerne les premières étapes de la transformation digitale, l'accélération du déploiement d'outils transverses propres à la filière pour une meilleure efficacité collaborative (AirSupply, Airdesign, Air Collab) et la sécurisation des systèmes d'information et de production (AirCyber). Il en va de même au sein de la filière des industries et technologies de santé, dont le contrat de filière comprend un volet d'accompagnement du développement des PME, afin de permettre la montée en compétences stratégique et managériale de leurs dirigeants et stimuler une relation partenariale durable et globale propre à initier, faciliter ou apporter des solutions aux PME dans leurs relations avec les grands comptes donneurs d'ordres.

Votre rapporteur souhaite insister, à ce stade, sur une idée-force : **les ETI et grandes entreprises doivent être ambitieuses dans leurs investissements technologiques pour anticiper les gains de productivité que ces technologies vont apporter dans les prochaines années.** Cela implique de bien mesurer le rapport de force avec leurs concurrents étrangers et de privilégier une approche pragmatique. Pour M. Michel Paulin, président d'OVHcloud : *« il faut choisir ses batailles. Pour certaines d'entre elles, il vaut mieux faire des alliances ouvertes, conformes aux règles de l'Europe sur la protection des données. Pour d'autres domaines – la sécurité, l'Intelligence artificielle, le* big data *– l'Europe a des solutions extrêmement innovantes. Il faut les aider, comme le font les autres régions, qui sont capables de créer des écosystèmes aux États-Unis, en Inde, en Russie, au Japon, en Corée, en Chine, pour faire émerger les acteurs qui auront la taille*

(1) Audition de M. Alain Conrard, 14 janvier 2021.

suffisante pour les investissements nécessaires. Il existe un écosystème à travers la filière française et européenne » (1).

3. Des technologies numériques indispensables pour peser dans le monde numérique de demain

Les auditions font apparaître **plusieurs segments technologiques clés** qui seront de plus en plus critiques pour les entreprises dans les prochaines années.

Les technologies quantiques ont un potentiel très élevé dans cette optique. Pour Mme Diane Dufoix-Garnier, directrice des affaires publiques d'IBM (2), le quantique constitue un champ entier, encore à ses prémices, malgré la rapidité des progrès. À côté de l'investissement dans cette technologie (dans les ordinateurs, les simulateurs, etc.), l'enjeu est de constituer des écosystèmes, par exemple avec de grandes entreprises françaises et des universités, pour développer les algorithmes quantiques qui seront probablement au centre des usages de demain. Selon elle, une technologie n'a pas d'intérêt si elle n'offre pas un usage pour l'industrie de demain, la santé de demain, les villes intelligentes, etc. Il existe donc un enjeu pour la France à se positionner à la pointe de ces technologies dans leur dimension « offre ». Il s'agit d'investir en R&D et de développer les compétences, dans une logique d'écosystème, certains acteurs ayant déjà, de manière propre, beaucoup investi dans ces technologies.

Le *cloud* hybride constituera une stratégie structurante des prochaines années. Selon Michel Gesquiere (3), responsable des ventes d'IBM**,** le *cloud* hybride est censé combiner « *le meilleur des deux mondes* ». En fonction de la criticité des applications concernées, qui est très différente dans le domaine industriel, bancaire ou des biens de grande consommation, il s'agit d'offrir le choix de localiser les applications ou les données dans des environnements privés (plus protecteurs) ou dans des environnements publics, ces derniers offrant plusieurs avantages à l'impact économique extrêmement important (une économie d'échelle et une automatisation très importante, le recours à des logiciels libres, une grande flexibilité etc.).

L'Intelligence artificielle verra sa place considérablement accrue dans les années à venir. Déjà déployée dans le domaine de l'expérience « client », elle servira également d'assistant pour accroître la performance des employés. L'automatisation des processus industriels passera également par l'Intelligence artificielle. L'accroissement du nombre de données liées à l'*IoT* et à la 5G, fera de l'Intelligence artificielle l'instrument de leur transformation en éléments de compétitivité et d'automatisation des performances.

---

(1) Audition de M. Michel Paulin, 9 février 2021.

(2) Audition de Mme Diane Dufoix-Garnier, 9 mars 2021.

(3) Audition de M. Michel Gesquiere, 9 mars 2021.

4. Certains obstacles persistent pour anticiper les évolutions à venir

L'appréciation des capacités d'anticipation des grandes entreprises et les difficultés qu'elles peuvent rencontrer dans leur montée en gamme technologique ont fait l'objet de plusieurs remarques lors des auditions.

Ont été mis en exergue, notamment :

– le niveau insuffisant d'investissement des entreprises françaises sur les technologies d'avenir. Pour M. Nicolas Brien, directeur général de la fédération de *start-up* France Digitale, la responsabilité du retard français en matière numérique est celle des dirigeants des sociétés du CAC 40, peu visionnaires, sans prescience des transformations numériques à venir sur les *business models* et n'investissant pas au niveau requis : *« nos opérateurs français sont encore en train de déployer les pylônes 4G quand leurs concurrents allemands ou sud-coréens déploient les premiers réseaux de télécommunications quantiques »* (1) ;

– la difficulté de faire d'une entreprise innovante un géant technologique. Pour M. Éric Baissus, président-directeur général de Kalray, il convient de surmonter une forme de tropisme d'exclusivité technologique de la part des *start-up* : *« aujourd'hui, en France, on croit encore que vous pouvez créer une société, quand vous avez une technologie. J'ai tendance à dire que, quand vous avez une technologie, vous n'avez fait que 20 % du travail, vous devez encore déployer un effort considérable pour transformer une technologie en une société commerciale pérenne, leader de son marché. L'effort à fournir est largement sous-estimé. Beaucoup de financements aujourd'hui sont plus liés à de la technologie (même si les mentalités sont en train d'évoluer) qu'au positionnement produit, à la mise au point d'une offre mature, à l'accès au marché. C'est bien d'avoir une technologie différente, mais la différence en soi n'a pas de valeur. Il faut avoir une différenciation sur le marché. »* (2) ;

– l'effet d'éviction lié à la dimension mondiale du marché technologique. Pour M. Michel Van Den Berghe, alors directeur général d'Orange Cyberdéfense, un phénomène de survalorisation de certaines entreprises rend prohibitif leur achat par des entreprises européennes. *« Orange Cyberdéfense a mis Alcide à son catalogue et a incité ses propres clients à acheter ses solutions, en prenant en charge les problématiques de référencement et d'achat.* In fine, *Alcide a été rachetée par une société américaine, pour un montant de 100 millions d'euros. Personne en France ne peut investir 100 millions d'euros pour acheter Alcide. Cette valorisation est complètement délirante. La valorisation des cibles du marché de la cybersécurité est pour nous de l'ordre de 20 à 25 % de l'EBITDA. Je ne peux pas demander au conseil d'administration de valider l'acquisition d'une entreprise pour un montant de vingt à vingt-cinq fois son EBITDA, Le marché est survalorisé. Aucune entreprise française ne peut débourser 100 millions d'euros pour acheter Alcide, qui réalise 8 millions d'euros de chiffre d'affaires. Lorsque vous achetez*

(1) Audition de M. Nicolas Brien, 25 février 2021.

(2) Audition de M. Éric Baissus,30 mars 2021.

une entreprise vingt-cinq fois la valeur de son EBITDA, cela signifie qu'il faut vingt-cinq ans pour rentabiliser l'investissement. Il faut donc être certain que les synergies d'acquisition permettront de diviser le coût par deux. Dans notre métier, les valorisations sont de manière générale un peu délirantes. Les grands acteurs américains sont visionnaires dans la transformation numérique et achètent des start-up *qui ont déjà développé des solutions, pour ne pas avoir à le faire eux-mêmes. Même s'ils ont commencé à travailler dans le domaine, mais qu'une* start-up *est allée plus vite, ils l'achètent, la mettent à leur catalogue et sont en avance sur le marché. »* (1).

Il faut évidemment relever qu'une entreprise américaine mondialisée comme Cisco conteste une telle appréciation et s'en remet à la véracité des prix de marché. Pour M. Laurent Degré, président directeur général de Cisco Systems France, *« si ces sociétés sont achetées à ces prix, cela signifie qu'il existe de la compétence et de l'expertise en France. II s'agit donc d'une bonne nouvelle. Par ailleurs, ce n'est pas de la survalorisation, mais une valorisation de la compétence qui a un prix sur ce marché. La question se pose ensuite de savoir si nous avons la capacité de le faire, au niveau français ou européen, mais c'est une autre discussion. Il n'y a pas de survalorisation de ces sociétés, mais une simple valorisation de leur compétence. »* (2) ;

– la nécessité de dépasser un certain nombre de stéréotypes. Pour M. Jean-Noël de Galzain, président d'HEXATRUST, organisation qui regroupe des *start-up*, des PME et des ETI spécialisées dans la cybersécurité : *« Arrêtons de croire que nous allons changer le monde en investissant de l'argent dans les grandes entreprises. Si nous réservons de l'argent aux PME,* start-up *et ETI, et si leurs propositions de valeur séduit les utilisateurs, alors nous parviendrons à attirer les grands intégrateurs, les grands financeurs et les grandes banques. Le cercle vertueux fonctionnera, puisque nous créerons de nouveaux besoins et de nouveaux marchés. Il me paraît urgent de considérer le fait qu'un certain nombre d'entrepreneurs ne sont pas attirés par l'idée de devenir milliardaires à tout prix. D'aucuns associent le profil du patron à la volonté de* « s'en mettre plein les poches », *mais il faut avoir à l'esprit qu'un certain nombre d'entrepreneurs sont séduits par l'idée de créer des géants mondiaux comme Schneider Electric, Alstom et d'autres sociétés françaises qui ont fantastiquement bien réussi. Or, pour y parvenir, ils ont besoin d'un certain nombre d'instruments qui fonctionnent, à savoir des solutions de sortie pour les investisseurs, c'est-à-dire des solutions permettant de réaliser, sans avoir à revendre là où les capitaux sont les plus nombreux, là où ils s'achètent le plus cher »* (3).

(1) Audition de M. Michel Van Den Berghe,13 avril 2021.

(2) Audition de M. Laurent Degré, 13 avril 2021.

(3) Audition de M. Jean-Noël de Galzain, 11 février 2021.

B. SOUTENIR LE DÉVELOPPEMENT DE L'ÉCOSYSTÈME DEEPTECH FRANÇAIS ET EUROPÉEN

1. Mobiliser davantage le levier de la commande publique au service de l'innovation

a. La commande publique est insuffisamment orientée vers les entreprises technologiques nationales et européennes.

Le contenu de la commande publique a un impact évident sur la nature de la transformation numérique de nos administrations et sur la construction d'une forme de souveraineté numérique nationale ou européenne.

L'achat public se situe au confluent de deux préoccupations :

– répondre aux besoins des administrations publiques par la sélection du soumissionnaire le « mieux-disant » à la suite, par exemple, d'un appel d'offres ;

– tirer parti de la dépense publique en termes de politique économique et de soutien aux entreprises. Par lui-même, le processus d'achat public permet d'injecter des liquidités dans l'économie et de soutenir financièrement les entreprises. La commande publique représentait ainsi 87,5 milliards d'euros en 2019, selon le baromètre de l'Assemblée des communautés de France (AdcF) et de la Banque des territoires. Il ressort des auditions le sentiment largement partagé qu'une part de la commande publique doit être utilisée comme un levier de développement de l'écosystème technologique français et européen.

En l'état actuel du droit de l'Union européenne, insérer une préférence généralisée pour les entreprises nationales dans les marchés publics du numérique est impossible. Le *Buy American Act* adopté en 1933 ou le *Small business Act*, visant à réserver certains marchés publics aux PME, adopté en 1953 aux États-Unis, n'ont pas d'équivalent au sein de l'Union européenne.

Buy European Act* et *Small Business Act

Le *Buy European Act* et le *Small Business Act* sont deux projets de réforme du droit économique européen en faveur d'une préférence européenne en matière d'achat public. Ils s'inspirent de l'adoption aux États-Unis du *Buy American Act* en 1933 et du *Small Business Act* en 1953.

Souvent confondus, ces deux propositions possèdent une logique semblable mais s'inscrivent dans une perspective et un périmètre légèrement différents.

La création d'un *Buy European Act* viserait à favoriser dans les procédures de marché public les entreprises qui localisent leur production eu Europe, voire à exclure de la commande publique les entreprises qui ne respectent pas cette obligation. La défense d'un *Buy European Act* était une proposition du candidat Emmanuel Macron, afin de réduire la dissymétrie dans l'accès à la commande publique. Il existe en effet une inégalité d'accès dans ce domaine, en raison d'un degré d'ouverture des marchés publics de l'Union européenne plus important que chez ses partenaires mondiaux. Bien que ce ne soit l'objectif principal du *Buy European Act,* le fait de favoriser les entreprises européennes au sein des marchés publics serait évidemment bénéfique pour les PME européennes.

La création d'un véritable *Small Business Act* permettrait de réserver une partie des marchés publics aux PME. Son objectif premier est donc d'abord de viser le développement des petites entreprises européennes.

Source : mission d'information

À l'heure actuelle, les entreprises étrangères peuvent candidater aux appels d'offres des administrations sans restrictions spécifiques. Dès lors, dans le secteur du numérique, les entreprises les « mieux-disantes » et aux offres les plus intéressantes, en termes de performance ou de sécurité, peuvent être des entreprises en dehors du territoire de l'Union, ou non contrôlées par des acteurs européens. Lors de son audition, la directrice du *Health Data Hub* a par exemple justifié le recours à Microsoft pour l'hébergement des données de santé, en raison de ses services managés de sécurité et des exigences de performance, notamment en matière de *deep learning* (1). La taille des géants du numérique leur offre, en outre, assez souvent, un avantage compétitif important face aux offres nationales ou européennes

La temporalité des besoins des administrations publiques peut également conduire à privilégier une solution aisément accessible, déjà développée et disponible. La « demande » de solutions numériques émanant des administrations publiques repose en effet sur une attente de fiabilité, de simplicité et de rapidité qui favorisent par construction les grands acteurs. Dès lors les petites ou moyennes entreprises (PME) ou les entreprises de taille intermédiaire (ETI) peuvent rencontrer des difficultés d'accès à la commande publique, en matière numérique, en raison notamment de la position hégémonique de certains acteurs dans ce secteur.

(1) Audition de Mme Stéphanie Combes, 18 février 2021.

L'article L. 2153-1 du code de la commande publique prévoit le principe d'égalité de traitement des opérateurs économiques issus de l'Union européenne avec ceux d'États parties à l'accord sur les marchés publics de l'Organisation mondiale du commerce (OMC). Les entreprises françaises, européennes, ou extra-européennes sont ainsi traitées de façon similaire, limitant l'emploi de la commande publique comme outil de politique économique pour développer le tissu productif local en matière numérique.

Contrairement aux idées reçues, il existe, en revanche, un certain nombre d'outils permettant de favoriser, dans certaines circonstances, une offre nationale ou européenne (*infra*).

Votre rapporteur considère donc que la commande publique doit davantage être prise en compte par l'État comme un outil de stimulation de l'offre privée et de soutien à la création d'un écosystème d'entreprises du numérique. Pour parvenir à cet objectif, il est essentiel de promouvoir l'exemplarité de l'État dans sa doctrine d'achat public, notamment à destination des acteurs technologiques français.

b. Le cadre juridique actuel offre des marges de manœuvre via plusieurs dérogations au principe d'égalité de traitement

À droit constant, plusieurs dispositions permettent de favoriser le recours à des solutions françaises ou européennes dans les procédures d'achat public, qui peuvent s'appliquer dans des domaines en lien avec le numérique.

Un premier type de dérogations tient à la nature de l'achat :

– *pour les marchés publics de défense*, le droit de la commande publique autorise une dérogation au principe d'égalité de traitement entre les candidats. L'article 97 de l'instruction générale interministérielle n°1300 du 30 novembre 2011 sur la protection du secret de la défense nationale autorise par exemple l'apposition d'une mention « Spécial France »[(1)]. Cette dernière implique de ne retenir que des sociétés françaises dans des domaines qui comportent un enjeu de nature stratégique. La mise en œuvre de ce dispositif s'appuie sur un travail de certification effectué par l'ANSSI ;

– *pour les opérateurs de réseaux* (eau, énergie, transports), l'article L.2153- 2 du code de la commande publique permet d'écarter les offres composées à plus de 50 % de produits provenant d'États tiers à l'Union européenne, n'ayant pas signé l'accord sur les marchés publics de l'OMC. Cet article ne s'applique toutefois qu'aux seuls opérateurs de réseaux ;

– *pour les achats innovants*, une expérimentation est en cours jusqu'au 24 décembre 2021 afin de dispenser de publicité et de mise en concurrence les

(1) Le dernier alinéa de l'article 97 de cette instruction dispose : « aucune entreprise candidate de droit étranger ne peut être retenue lorsque l'exécution du contrat conclu (…) implique la détention ou l'échange d'informations ou supports classifiés portant la mention « *Spécial France* » ».

achats de produits innovants au-dessous de 100 000 euros. Au 1er janvier 2021, 174 marchés ont été déclarés selon cette procédure, pour un montant total de 11 millions d'euros. Le principal frein au recours à ce dispositif est l'incertitude entourant la notion d'achat innovant.

Un deuxième type de dérogation est prévu par l'article L.2153-2 du code de la commande publique, qui pose un principe d'égalité de traitement entre les opérateurs économiques issus de l'Union européenne avec ceux des États parties à l'accord sur les marchés publics de l'OMC. Cet article intervient en transposition de l'article 25 de la directive européenne 2014/24 du 26 février 2014 (1). Le principe d'égalité de traitement n'a ainsi pas vocation à être respecté vis-à-vis des États non parties à cet accord.

Le troisième type de dérogation correspond au respect des exigences sociales, environnementales, ou à la nécessité d'assurer la sécurité des informations et des approvisionnements. L'article L.2112-4 du code de la commande publique prévoit que l'acheteur peut ainsi exiger une localisation de tout ou partie du marché sur le territoire des États de l'Union européenne afin de prendre en compte ces exigences.

Lors de son audition, Me Thierry Dal Farra**,** associé du cabinet UGGC Avocats a souligné qu'un dernier type de dérogation, sans être expressément prévu, **tient à la pratique de la commande publique** : la structuration des contrats et des contraintes d'exécution peut influer sur l'origine des entreprises susceptibles de remporter les marchés. Par exemple, **l'allotissement géographique et technique**, sous réserve qu'il ne soit pas incohérent, est de nature à favoriser la candidature de PME implantées localement, tout en pouvant réduire l'intérêt des plus grands opérateurs à candidater (2). Mme Laure Bédier, directrice des affaires juridiques au ministère de l'Économie, des Finances et de la Relance relève ainsi qu'« *il est très important de connaître l'offre nationale pour pouvoir adapter la demande en conséquence* […]. *Les critères doivent être pondérés de manière à ce que le prix ne soit pas le seul élément pris en compte dans la sélection* » (3).

c. Une modification des pratiques d'achat public est indispensable

Une meilleure connaissance du droit de la commande publique paraît nécessaire, en particulier dans le domaine du numérique. Mme Laure Bédier a ainsi plaidé pour une plus large diffusion des outils déjà existants et pour une meilleure communication sur les possibilités offertes par le code de la commande publique. Le recours plus large à l'allotissement pourrait ainsi, dans l'immédiat, être une piste à privilégier, indépendamment de la création du *Small Business Act* européen, que beaucoup d'acteurs appellent de leurs vœux (4).

---

(1) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE.

(2) Audition de Me Thierry Dal Farra, 28 janvier 2021.

(3) Audition de Mme Laure Bédier, 28 janvier 2021.

(4) Audition de Mme Laure Bédier, 28 janvier 2021.

Pour votre rapporteur, l'information sur les outils permettant de privilégier le recours aux acteurs français, à droit constant, doit ainsi être renforcée. De même, ces acheteurs doivent être formés aux enjeux de souveraineté numérique afin que cet objectif soit pleinement pris en compte lors du recours à un prestataire externe.

Les pratiques de l'Union des groupements d'achats publics (UGAP) sont également sources d'interrogations. L'UGAP est une centrale d'achat, responsable de la publication des appels d'offres pour les clients publics. Lors de son audition, M. Edward Jossa, président de l'UGAP, a insisté sur les limites du rôle de la centrale d'achat *: « l'UGAP n'est pas une autorité de prescription. La logique de l'UGAP est de fournir ce qu'on lui demande. La valeur ajoutée de l'UGAP est de sécuriser les procédures de mise en concurrence, d'appliquer correctement le code de la commande publique, de faire gagner du temps aux clients, de procéder à des économies. Nous sommes là pour faciliter de meilleurs prix et pour faciliter la commande. En revanche, si l'État décide qu'une partie des applications des ministères doivent obligatoirement bénéficier de la labellisation SecNumCloud, et que nous avons instruction de ne vendre que des produits labellisés SecNumCloud, alors nous l'appliquerons »* (1).

Interrogé par notre collègue, M. Éric Bothorel, sur le point de savoir si les référencements de l'UGAP sont encore adaptés à l'évolution du marché des logiciels qui intègre davantage de services que de produits et sur la façon dont l'UGAP conseillerait concrètement une petite agglomération se trouvant face à des choix de *cloud*, le président de l'UGAP a répondu : *« la manière classique de travailler de l'UGAP recouvre les étapes suivantes : conseil, puis devis, puis commande. Sur un certain nombre de solutions, comme le marché multi-éditeurs ou le marché* cloud*, tout notre travail consiste à incorporer des outils d'aide à la décision dans notre dispositif de commande. Cet outil d'aide à la décision repose sur un système de questions et réponses : le client entre les données relatives à ses besoins et à sa commande. Capgemini, titulaire du marché, est responsable d'entretenir une application d'aide aux choix qui permet d'objectiver les critères guidant la prise de décision. Cela permet d'éviter une forme d'arbitraire qui présente un risque pour l'UGAP tout comme pour le client public. »* (2).

Or, plusieurs entreprises auditionnées ont fait état de difficultés de référencement dans les dossiers de l'UGAP, limitant ainsi leur accès à la commande publique. Au regard de l'innovation sur le marché du numérique et de la nécessaire adaptation à l'état du marché, les procédures de référencement à l'UGAP doivent être fluides et rapides, afin de ne pas éloigner durablement des entreprises de l'achat public. En outre, l'UGAP privilégie les solutions prêtes à l'emploi, limitant la place des jeunes entreprises, dont les solutions innovantes sont en cours de développement.

(1) Audition de M. Edward Jossa, 21 janvier 2021.

(2) Idem.

Pour votre rapporteur, il ne fait pas de doute que l'UGAP doit s'attacher à modifier ses pratiques de référencement, afin de permettre un accès accru des entreprises françaises du numérique à la commande publique.

Proposition n° 26 : Privilégier, en matière de commande publique, le recours aux solutions d'acteurs technologiques français ou européens.

Proposition n° 27 : Exiger de l'Union des groupements d'achats publics (UGAP) des délais raisonnables dans le traitement des demandes de référencement des acteurs de l'offre numérique française (page 98).

Proposition n° 28 : Créer un guide d'information des acteurs publics sur les outils de la commande publique, afin d'encourager, notamment, la pratique de l'allotissement, le recours par les collectivités au « dialogue compétitif » en matière de numérique et l'usage de la mention « Spécial France », toutes mesures qui permettront de rendre plus systématique le recours aux acteurs français au sein de la commande publique.

d. Une évolution du droit de la commande publique national et européen sont également souhaitables

À court terme, la France fait toute diligence au sein du groupe de travail « marchés publics » du Conseil de l'Union pour obtenir un accord sur une modification de la directive 2014/23/CE [(1)], en vue d'étendre la dérogation prévue à l'article L.2153-2 du code de la commande publique au-delà du champ des opérateurs de réseaux. Une telle extension pourrait en effet conduire à offrir davantage de souplesse aux administrations publiques dans leur processus de sélection des offres, en particulier dans le domaine du numérique, et leur permettrait de sélectionner en priorité des entreprises françaises ou européennes.

À moyen terme, les systèmes de labellisation et de certification devraient être développés :

– concernant la labellisation, il convient de relever qu'au sein de la direction interministérielle au numérique (DINUM), la mission Label élabore actuellement un label destiné à la commande publique française, afin d'orienter les décideurs vers l'achat de solutions nationales ou européennes. Lors de leur audition, M. Jacques de La Rivière, président et fondateur de Gatewatcher et Mme Louise Bautista, représentante de TheGreenBow, deux entreprises du numérique françaises, ont fait part de leur pleine approbation d'une telle initiative [(2)] ;

– concernant la certification, plusieurs normes existent, en particulier s'agissant de garantir la sécurité du *cloud* (SecNumCloud, HDS en matière de santé, ISO 27001). Néanmoins, ces certifications ne vont pas au-delà de la sécurité des solutions techniques, sans prendre en compte les questions de souveraineté. Ainsi, selon M. Michel Paulin, directeur général d'OVHcloud, les certifications devraient prendre en compte plusieurs critères, comme la localisation des données et

(1) Directive 2014/23/UE du Parlement européen et du Conseil du 26 février 2014 sur l'attribution de contrats de concession.

(2) Audition de Mme Louise Bautista et M. Jacques de la Rivière, 14 janvier 2021.

métadonnées en Europe, leur accessibilité par des législations de pays hors de l'Union européenne, la soumission à des droits extraterritoriaux, et la conformité aux demandes d'autorisation des pays tiers conformes au RGPD [1].

Votre rapporteur estime nécessaire d'intégrer, à moyen terme, dans les normes existantes (SecNumCloud, HDS, ISO 27001) le principe selon lequel l'hébergeur ne doit pas être soumis à des lois extraterritoriales.

Enfin, il est souhaitable de soutenir, à moyen-terme, l'adoption d'un *Small Business Act* pour répondre aux attentes fortes et légitimes manifestées par les acteurs auditionnés dans le cadre de la présente mission.

Compte-tenu du droit du marché intérieur et des libertés de circulation, un *Small Business Act* n'est pas envisageable à l'échelle nationale, mais seulement à l'échelle européenne. En termes politiques, l'adoption d'un *Buy European Act* ou d'un *Small Business Act* à l'européenne paraît difficilement réalisable à court terme puisqu'une refonte du droit de la commande publique européen serait nécessaire, ce qui nécessite un accord entre les États membres. Au surplus, ce dispositif nécessiterait une négociation avec l'Organisation mondiale du commerce (OMC). En effet, c'est l'OMC qui a accordé des dérogations aux règles du commerce international pour permettre aux États-Unis, à la Corée du Sud et au Canada d'adopter des mesures législatives visant à favoriser leurs entreprises nationales dans les marchés publics.

Il n'en ressort pas moins des auditions que l'adoption d'un tel dispositif contribuerait fortement, à moyen et long terme, à l'affirmation d'une souveraineté numérique européenne et au développement d'un écosystème d'entreprises digitales européennes qui en est le corollaire**.** Un tel dispositif permettrait en effet de contraindre les acheteurs publics au choix de solutions françaises, au-delà de la simple recommandation. Lors de son audition, M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique, a ainsi insisté sur l'importance du *Small Business Act* aux États-Unis, lequel a permis, par exemple, le développement de la société SpaceX dans le domaine spatial, en fort lien avec les commandes de la NASA, agence publique [2].

Quand bien même la France part relativement isolée face aux autres États membres sur ces sujets, un groupe de réflexion sur l'évolution du cadre européen de la commande publique pourrait être utilement créé pour parvenir, à moyen terme, à l'adoption d'un *Small Business Act* européen.

(1) Audition de M. Michel Paulin, 9 février 2021.

(2) Audition e M. Bernard Benhamou, 29 octobre 2020.

Proposition n° 29 : Lancer une mission d'expertise sur les enjeux de souveraineté de la commande publique, afin d'identifier les leviers permettant de faire évoluer le cadre juridique actuel, en faveur de la prise en compte des enjeux de sécurité numérique, de gestion et de localisation des données en Europe.

Proposition n° 30 : Faire évoluer les pratiques et le cadre juridique de la commande publique :

Au niveau national :

– En intégrant le principe selon lequel l'hébergeur ne doit pas être soumis à des lois extra-européennes dans les normes de sécurité existantes (SecNumCloud, HDS, ISO 27001) ;

– En intégrant dans les clauses administratives générales des marchés (CCAG) des obligations liées à la localisation des données en Europe, sous peine de condamnation pénale des dirigeants du *cloud* ;

– En soutenant une « culture du risque » chez les acheteurs publics (sécurisation juridique) et en améliorant leur formation aux aspects extra-juridiques de la commande publique.

Au niveau européen :

– En mettant en place rapidement un *Small Business Act* ;

– En étendant à d'autres produits le régime de préférence communautaire existant dans les infrastructures ;

– En clarifiant l'article 25 de la directive européenne de 2014 pour identifier précisément les cas dans lesquels une offre d'un État tiers peut être écartée.

2. Faciliter l'accès de nos *deeptech* aux financements européens

Des solutions de financement significatives existent, à l'échelon national, pour faciliter la création de *start-up*. Bpifrance mène une action volontariste en ce sens, qui nécessite d'être poursuivie et clarifiée afin d'assurer une lisibilité maximale au sein du paysage des aides au soutien à l'innovation français.

Les *deeptech* peuvent ainsi bénéficier de bourses qui leur sont spécifiquement dédiées : les bourses *« French Tech Emergence* ». Si les bourses « *French Tech* » peuvent être sollicitées par toutes les *start-up* innovantes, les bourses « *French Tech Emergence* » (de 50 000 euros à 90 000 euros) sont spécifiquement destinées à soutenir les innovations de rupture à forte dimension technologique.

Un effort de financement particulier et ciblé est ainsi réalisé en faveur des *deeptech* grâce à des subventions directes, à la mise à disposition d'avances remboursables, de prêts d'innovation, ou encore de prêts d'amorçage.

Cette action de soutien doit se poursuivre et l'écosystème doit travailler à approfondir ses coopérations afin de « chasser en meute ».

Proposition n° 31 : Renforcer le soutien public à destination de la French Tech, pour encourager ses membres à « chasser en meute » (page 100).

Les *deeptech :* quelle définition ?

Selon la définition donnée par Bpifrance, ce terme désigne les *start-up* qui proposent des produits ou des services sur la base d'innovations de rupture. D'après la définition proposée en 1997 par Clayton Christensen, une innovation est dite « de rupture » (*disruptive innovation*) lorsqu'elle crée, transforme ou détruit un nouveau marché.

Une entreprise de la *deeptech* est ainsi une forme particulière de *start-up*, ce dernier terme désignant une entreprise innovante à fort potentiel de croissance et de spéculation sur sa valeur future.

Source : Bpifrance-création.fr & Stratégie.gouv.fr

i. Des progrès incontestables au niveau national

Selon M. Paul François Fournier, directeur exécutif en charge de l'innovation chez Bpifrance, le nombre de *start-up* accompagnées par la banque publique a triplé depuis 2013-2014 pour atteindre près de mille par an aujourd'hui. Cette évolution trouve son origine dans les mutations induites par l'irruption du digital dans la vie économique : « *avec le digital, l'innovation a complètement changé et le modèle le plus créateur de valeur est maintenant celui des* start-up*. Même si les filières traditionnelles continuent à être innovantes, les* start-up *sont aujourd'hui l'outil de création de valeur au début du processus d'innovation* » [(1)].

Pour Mme Liliane Devryer, directrice de projets « Technologies et solutions numériques émergentes » au sein de la direction générale des entreprises (DGE), les dispositifs *deeptech* ont permis, en 2020, d'injecter un million d'euros au bénéfice des *start-up* investies dans le développement de la *blockchain* [(2)]. Bpifrance poursuit ainsi une politique de soutien à la création de *start-up* technologiques.

Des financements permettent aussi d'accompagner la croissance des *start-up*. C'est le deuxième axe de l'action de Bpifrance. Pour cela, la banque publique cherche à créer des conditions favorables à la création d'un environnement dynamique de capital-risque. Le développement de fonds d'investissement est essentiel pour permettre aux entreprises de croître et de se développer. Les programmes d'investissement d'avenir ont permis à Bpifrance d'investir afin d'augmenter la taille de ces fonds.

La dynamique de maturation de cet écosystème est incontestable. Le capital-risque français est en effet passé de deux milliards d'euros en 2013-2014 à plus de cinq milliards d'euros cette année. Certains de ces fonds représentent déjà

(1) Audition de M. Paul-François Fournier, 15 avril 2021.

(2) Audition de Mme Liliane Devryer, 29 avril 2021.

plus d'un milliard d'euros. En 2020, 80 levées de fonds de vingt millions d'euros ont eu lieu, contre seulement une quarantaine en 2016, et douze levées de fonds de 100 millions d'euros ont eu lieu en 2020, contre six en 2016. La progression est donc significative.

En conséquence, la poursuite de l'action publique dans ce domaine, avec la pérennisation du plan *deeptech* qui a débuté il y a deux ans, est souhaitable. La dynamique de maturation de l'écosystème de capital-risque doit être poursuivie.

Au cours de son audition, M. Paul-François Fournier a néanmoins rappelé que Bpifrance n'avait pas vocation à se substituer aux fonds d'investissement, qui doivent « prendre le relais » pour financer ces innovations.

Ces différents éléments confirment, pour votre rapporteur, l'analyse présentée dans le rapport de M. Philippe Tibi sur la difficulté qu'ont les *start-up* à financer, non pas leurs premiers stades de développement, mais ceux nécessitant des levées de fonds très significatives. Leur croissance est en effet ralentie par le manque de financement en *late stage* (levée de fonds supérieure à 30-40 millions d'euros). Dans ce rapport, M. Philipe Tibi constate que les fonds français sont rarement capables de financer des « tickets supérieurs » à 30 millions d'euros. Cela est problématique dans la mesure où la dernière levée permettant à une entreprise de devenir une « licorne » [(1)] dépasse généralement les 100 millions d'euros. Il est donc nécessaire de poursuivre la dynamique engagée et d'accroître l'attention portée à la croissance quantitative et qualitative du nombre de fonds *late stage* et *global tech*. L'objectif est d'obtenir à terme dix fonds de capital-innovation gérant plus d'un milliard d'euros [(2)].

Proposition n° 32 : Accélérer le développement du marché du capital-risque et l'harmonisation du marché des capitaux en Europe pour réduire le différentiel d'attractivité avec les États-Unis et éviter le départ de pépites européennes pour des raisons liées à la recherche de financements.

Ce bilan appelle une remarque relative au double enjeu d'attractivité et de souveraineté qu'implique le fait d'attirer des capitaux étrangers au sein de cet écosystème. La rentabilité des fonds de capitaux français croît, ce qui les rend plus attractifs pour les capitaux étrangers. C'est une bonne chose : la souveraineté économique en matière de financement d'entreprises nationales ne saurait signifier qu'il faut que les entreprises technologiques françaises ne soient financées que par des fonds français. M. Paul François Fournier dresse un constat tout à fait similaire sur ce point : « *Nous ne croyons pas pouvoir construire un écosystème qui ne soit pas un minimum ouvert sur le reste du monde* », avant d'ajouter ne pas croire : « *qu'un écosystème français uniquement financé sur les fonds français soit pérenne* » [(3)]. Des fonds américains ou des fonds étrangers peuvent permettre de

---

[1] *Une « licorne » est une* start-up *dont la valeur est estimée à plus d'un milliard de dollars.*

[2] *Philippe Tibi, « Financer la quatrième révolution industrielle », juillet 2019.*

[3] *Audition de M. Paul-François Fournier, 15 avril 2021.*

consolider l'écosystème des *start-up* françaises et leur donner accès à un réseau de compétences ou à un réseau de relations.

En même temps, il convient, sur ce sujet, de trouver un juste équilibre. Aussi avantageux que soit le recours à ces fonds, il n'est pas sans risque puisqu'il peut favoriser les actes de prédation, ou encore les transferts technologiques. Cela peut impliquer, notamment, une vigilance des pouvoirs publics vis-à-vis des stratégies de prédation. Un certain nombre d'outils existent dans ce domaine, ce qui fait dire à M. Thomas Courbe, directeur général des entreprises au ministère de l'Économie des Finances et de la Relance, que les investissements étrangers en France, font l'objet d'un contrôle déjà étroit [(1)]. Les enjeux de sécurité et d'ordre public, qui peuvent être opposés à la libre circulation des capitaux, sont entendus dans un sens assez large. Le nombre de secteurs susceptibles de protection a d'ailleurs été revu à la hausse dans un objectif de préservation de la souveraineté.

M. Thomas Courbe a toutefois souligné que le sujet est beaucoup moins avancé à l'échelon européen. Ainsi, le règlement 2019/452 entré en vigueur récemment sur le contrôle des investissements étrangers dans l'Union se révèle décevant [(2)]. Il n'instaure pas véritablement un contrôle de l'investissement, mais favorise plutôt l'échange d'informations.

ii. À l'échelon européen, des efforts à poursuivre pour financer les *deep tech* et soutenir le développement d'un écosystème européen

Le nombre de dispositifs existants, tant à l'échelon européen, qu'à l'échelon national pour appuyer le développement des *start-up* est important. En France, avec la crise sanitaire, un nouvel outil, *French Tech Bridge*, a été créé. Il s'ancre dans un paysage déjà très fourni et parfois peu lisible (Bourses *French Tech*, *bourses French Tech Emergence*, plan *Deeptech*, fond *French Tech* souveraineté, les concours d'innovation, un fond *French Tech accélération* etc.). Un réel effort de lisibilité devrait être mené pour clarifier les aides disponibles, et les critères d'éligibilité associés.

Pour votre rapporteur, il serait utile que l'ensemble des aides disponibles pour soutenir les *start-up* et les *deeptech* soient répertoriées dans un tableau ou un fichier unique, en détaillant les critères associés à chaque aide, et incluant l'ensemble des concours d'innovation bénéficiant d'une dotation publique.

Lors de son audition, M. Jean-Noël de Galzain, président d'HEXATRUST a également insisté sur l'importance de faciliter l'accès aux financements pour les PME et les ETI : le taux des prêts qui leur sont proposés par la Banque européenne d'investissement sont prohibitifs. Il importe ainsi de veiller à flécher certains

---

[1] Audition de M. Thomas Courbe, 8 octobre 2020.

[2] Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union.

financements à destination des ETI, PME et *start-up* pour leur permettre de se financer plus aisément [1].

Enfin, il conviendrait de ne pas amoindrir les efforts déjà réalisés en faveur du financement du volet R&D, notamment à l'échelon européen. En effet, selon Mme Mariya Gabriel, commissaire européenne, le budget consacré au second pilier du programme Horizon Europe est en recul. Les 52 milliards prévus sont insuffisants [2].

Le troisième pilier du programme Horizon Europe présente en revanche une originalité intéressante avec la création d'un Conseil européen de l'innovation. Son ambition est de soutenir la création de « licornes » européennes en identifiant les *start-up* et PME les plus prometteuses. Les *start-up* et PME seront directement financées dans leur phase de développement la plus risquée : le passage de la recherche à la commercialisation. Le Conseil européen de l'innovation a commencé à fonctionner : 5 000 entreprises ont déjà été soutenues pour un total de quatre milliards d'euros. Un enjeu important dans le développement du Conseil européen de l'innovation tient au soutien des États membres. Ces derniers viennent pourtant d'amputer son budget de 200 millions d'euros. Il importe de continuer à soutenir les propositions européennes en faveur de l'innovation et d'y consacrer des moyens suffisants, à la hauteur des ambitions affichées.

De plus, l'impérative utilisation de la langue anglaise lors de la rédaction des dossiers visant des demandes de financement, à l'échelon européen, est susceptible d'engendrer des difficultés pour certaines entreprises. Autoriser la rédaction du dossier de candidature en langue française permettrait de faciliter et d'accélérer les procédures pour les entreprises candidates.

Concernant la promotion de l'innovation, l'acquisition de brevets représente un enjeu majeur. Lors de son audition, M. Charles Thibout, chercheur associé à l'Institut des relations internationales et stratégiques (IRIS) [3], a souligné l'importance des brevets dans la stratégie de puissance des GAFAM : ces acteurs ont largement bénéficié de l'externalisation de l'innovation *via* le rachat de brevets et de *start-up*. M. Didier Patry, directeur général de France Brevets a quant à lui relevé que la France devrait s'imprégner de la pratique consistant à acquérir des brevets plutôt que de se concentrer exclusivement sur la recherche et le développement interne. Ainsi, de très nombreux brevets sont disponibles sur le marché, qu'ils proviennent d'entreprises privées ou de laboratoires de recherche publics français [4].

Votre rapporteur considère donc qu'il est important de soutenir le financement des acquisitions de brevets par les *start-up* et les *deeptech* pour accélérer leur croissance, et soutenir efficacement l'innovation.

---

[1] Audition de M. Jean-Noël de Galzain, 11 février 2021.

(2) Audition de Mme Mariya Gabriel, 1er octobre 2020.

(3) Audition de M. Charles Thibout, 12 novembre 2020.

(4) Audition de M. Didier Patry, 17 décembre 2020.

Proposition n° 33 : Encourager les entreprises françaises à développer des stratégies de captation de brevets, afin de leur permettre de résister aux pratiques agressives de leurs concurrents étrangers.

3. Protéger nos « licornes » face aux tentations de prédation

En 2021, la France comptabilisait quatorze « licornes » (*start-up* dont la valeur est supérieure à un milliard de dollars). Elle se situe à la troisième place au sein de l'Union européenne, derrière l'Allemagne (seize licornes) et le Royaume-Uni (vingt-neuf licornes) [1]. À titre de comparaison, parmi les 372 « licornes » décomptées à la mi-juillet 2019, 182 étaient américaines, 94 chinoises et 45 étaient européennes [2].

Les États-Unis et la Chine possèdent une puissance d'investissement sans équivalent et ciblée sur les entreprises les plus valorisées. Le directeur exécutif en charge de l'innovation de Bpifrance a souligné, sur ce sujet, que près des trois quarts des ventes de parts des *start-up* françaises se réalisent auprès d'investisseurs français ou européens, et seulement 17 % auprès d'investisseurs américains. Toutefois, les parts acquises par les investisseurs américains sont en moyenne trois fois plus valorisées que celles acquises par les investisseurs européens. Les « licornes » françaises sont donc tout particulièrement exposées à un risque de prédation et de possible captation technologique [3].

Pour les protéger, il est nécessaire que les fonds d'investissement français et européens continuent de croître. Il importe aussi de rapprocher les industries traditionnelles et les entreprises de la *deeptech* afin de créer des possibilités de coopération et de rachat. Faisant le constat que le tissage entre l'écosystème du digital et celui des entreprises françaises souffre d'imperfections, Bpifrance a lancé la plateforme de mise en relation *Tech in Fab*.

La nécessité de ce rapprochement procède de deux constats. M. Paul François Fournier se dit ainsi convaincu que *« nous allons vers une révolution de la* deep tech*, c'est-à-dire que les industries traditionnelles connaîtront la même rupture que le digital, avec des* start-up *venant disrupter les industries traditionnelles »*. En outre, il importe que les *start-up* qui atteignent leur limite, en termes de capacité de distribution, par exemple, puissent être rachetées par les filières traditionnelles françaises ou européennes pour les intégrer et leur faire profiter de leur réseau de distribution et savoir-faire [4].

---

[1] *Direction générale du trésor, « Levées de fonds et licorne : où en est la France ? », 4 juin 2021.*

[2] *Philippe Tibi, « Financer la quatrième révolution industrielle », juillet 2019.*

[3] *Audition de M. Paul-François Fournier, 15 avril 2021.*

[4] *Idem.*

Il faut également souligner l'existence d'autres variables permettant de préserver l'intégrité des « licornes » françaises et européennes. C'est le cas notamment de la fluidité du marché. Il convient, comme l'a souligné M. Jean-Noël de Galzain, président d'HEXATRUST, de « *massifier et de fluidifier le marché européen* » pour que les entreprises, PME et *start-up* puissent avoir un accès plus rapide au marché des utilisateurs [1]. Ce constat est également partagé par M. Benoît Darde, administrateur de *Syntec Numérique*, qui considère que le numérique a moins besoin de subventions, qu'il n'a besoin de marchés et d'opportunités de *business* [2], et par le général Grégoire de Saint-Quentin, président du cabinet de conseil Petra advisors : « *les* start-up *progressent moins vite grâce aux subventions qu'aux commandes, car celles-ci donnent confiance aux investisseurs* » [3].

L'effort de réalisation d'un marché unique numérique en Europe doit être poursuivi afin d'offrir aux « licornes » des perspectives de développement et de croissance avantageuses en France et en Europe.

L'État doit également exercer son rôle de gardien vigilant face aux stratégies de prédation économique**.** Le ministère de l'Économie, des Finances et de la Relance, a ainsi identifié plus de 250 menaces visant des entreprises de secteurs stratégiques au cours de l'année 2020. Le contexte de crise sanitaire a en effet augmenté les risques de stratégies agressives en raison de la fragilisation des fonds propres de certaines entreprises. Ces stratégies offensives peuvent prendre des formes très variées, de la prédation classique aux accords commerciaux avec transferts de technologie, en passant par des tentatives de déstabilisation informatique.

Votre rapporteur souhaite donc saluer, à l'occasion de ce rapport, l'action de ce ministère, en particulier de son service de l'information stratégique et de la sécurité économique, ainsi que celle de Bpifrance, et inciter le Gouvernement à maintenir ce niveau de vigilance.

C. DÉVELOPPER UNE CULTURE DE LA CYBERPROTECTION AU SEIN DES ENTREPRISES

1. Un impératif de vigilance face à l'accroissement de la menace cyber

La capacité des entreprises françaises à résister à une attaque cyber est un élément de souveraineté économique qui doit être, plus que jamais, pris en compte. La menace cyber a en effet connu une croissance importante qui correspond à une dynamique historique à laquelle est venue se greffer le facteur d'accélération qu'a été la crise sanitaire.

---

[1] *Audition de M. Jean-Noël de Galzain, 11 février 2021.*

[2] *Audition de M. Benoît Darde, 25 février 2021.*

[3] *Audition du Gal d'armée Grégoire de Saint-Quentin, 22 avril 2021.*

La tendance à l'augmentation de la menace cyber correspond, d'abord, assez logiquement, au développement des activités numériques. Ainsi que l'a résumé M. Arnaud Dechoux, responsable des affaires publiques « Europe » de l'entreprise Kaspersky, alors qu'en « *1994, on détectait un nouveau virus ou fichier malveillant par heure : le rythme est passé à un virus par minute en 2006, un virus par seconde en 2011* » [(1)]. Ces chiffres continuent d'ailleurs à augmenter puisqu'ils sont passés de 350 000 virus détectés chaque jour en 2019 à 428 000 en 2020. Cette progression de 25 % des détections en un an est évidemment due à la situation de crise sanitaire et de prolifération de la menace cyber qui s'en est suivie. Elle s'explique, selon M. Dechoux par « *l'élargissement de la surface d'attaque : augmentation du temps passé sur Internet, du travail à distance, avec des équipements souvent moins bien protégés que ceux des entreprises, et recours à des ressources éducatives en ligne* »[(2)].

Les échanges conduits avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Fédération française de la cybersécurité confirment une dynamique inédite de la menace cyber dans le cadre de la crise sanitaire. Lors de son audition, M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information a précisé qu'en *« 2019,* [l'ANSSI est intervenue] *dans une cinquantaine de cas pour des questions de cybercriminalité ; en 2020, pour quelques 200 cas »,* en ajoutant que « c*e quadruplement en un an est très inquiétant ; la courbe est véritablement exponentielle, et la tendance est la même en ce premier trimestre 2021, avec une quarantaine d'opérations actuellement ouvertes à l'ANSSI* ».

De son côté, le groupement d'intérêt public Action contre la cybermalveillance (GIP ACYMA) a indiqué à votre rapporteur que 10 500 entreprises et 2 100 collectivités l'ont sollicité pour une assistance en 2020, le plus souvent pour des rançongiciels. Cette menace arrive désormais en tête du classement en 2020, alors qu'elle n'était qu'en 6e position pour les entreprises et pour les collectivités en 2019.

Les chiffres communiqués par M. David Ofer, président de la Fédération française de la cybersécurité démontrent une exposition générale des organisations et des acteurs économiques face au risque cyber. Ainsi, en 2020, « *selon une étude d'un spécialiste de la cybersécurité, 91 % des organisations françaises ont été la cible de cyberattaques* […] *et 60 % ont subi plusieurs actes malveillants. 75 % et plus des attaques sont faites par des* ransomwares *(rançongiciels) en France comme dans le reste du monde* » avant de rappeler, par ailleurs, « *qu'une cyberattaque n'est pas forcément une paralysie du système d'information* » [(3)].

---

[1] *Audition de M. Arnaud Dechoux,13 avril 2021.*

[2] *M. Arnaud Dechoux a d'ailleurs ajouté à ce propos :* « Dans ce dernier cas, nous avons vu d'autres types d'attaques, comme celles par déni de service (DDoS), qui se sont beaucoup développées lors du premier confinement en mars dernier, et la semaine dernière encore en France. Ceci est dû aussi bien sûr au développement des objets connectés ».

[3] *Audition de M. David Ofer, 30 mars 2021.*

La crise sanitaire a donc été un catalyseur pour les cyberattaques, la numérisation massive, forcée et rapide des entreprises ayant mécaniquement élargi le champ des possibles pour les acteurs malveillants du cyberespace. Ce constat est partagé par M. Alain Assouline, coprésident de la commission « Innovation et économie numérique » de la confédération des petites et moyennes entreprises (CPME) : « *La crise sanitaire de 2020 a, pour nombre d'entreprises, marqué le début de leur transformation numérique* […]. *Par effet de symétrie, les cyberattaques ont cru de 400 % pendant la période* »[1]. Cette transformation digitale parfois subie, et souvent mise en œuvre à marche forcée, a mécaniquement créé des vulnérabilités, dont des assaillants ont tenté de tirer profit.

Votre rapporteur considère que l'état actuel de la menace cyber appelle un niveau de vigilance inédit. Les chiffres relatifs au risque cyber sont d'ailleurs sous-estimés par construction, puisqu'ils sont « *basés sur les déclarations des attaques, sur les plaintes des victimes et sur les interventions de l'ANSSI et des forces de l'ordre* » [2]. Cela fait dire, à M. David Ofer, qu'il existe « *une différence colossale entre le nombre d'attaques non référencées et le nombre de plaintes déposées* » [3]. Trop peu de plaintes sont en effet déposées par les victimes sur ce sujet. D'après les éléments fournis à la mission, la France se situe au niveau international à la septième place avec 1 640 plaintes déposées par des victimes en 2020. Le Royaume-Uni arrive en tête de ce classement, 216 000 plaintes, suivi par le Canada (5 300), l'Inde (2 930).

Votre rapporteur insiste donc sur la diffusion nécessaire d'une culture de la cybersécurité à destination des entreprises, mais aussi des acteurs publics face à une menace globale et multiforme, et à une véritable « *montée en compétences des cyberattaquants* » pour reprendre les propos tenus par M. Arnaud Dechoux [4]. Cela implique notamment de connaître les acteurs vers lesquels il faut se tourner en cas de difficulté, et de déposer plainte en cas d'attaque, pour favoriser le partage d'information et le suivi du risque cyber par les pouvoirs publics.

2. Une prise de conscience à construire avec les entreprises

Les auditions font apparaître, en effet, que les acteurs privés, notamment les TPE/PME, ne perçoivent pas de façon concrète la gravité que peut avoir une attaque informatique sur la vie d'une entreprise. Ces attaques sont pourtant « *extrêmement dangereuses pour l'économie française dans la mesure où elles mettent en péril la pérennité des entreprises qui la composent* ». Elles ont souvent des conséquences dramatiques. Selon M. David Ofer, près de « *50 % des PME qui ont subis une cyberattaque paralysante disparaissent dans les six mois qui suivent* ». En outre, selon lui, « *les grands groupes, à l'instar de Sopra Steria, récemment victime d'une attaque, s'ils ne sont pas menacés d'extinction, perdent, s'ils ne font rien, 20 % de*

---

[1] *Audition de M. Alain Assouline, 14 janvier 2021.*

[2] *Audition de M. David Ofer, 30 mars 2021.*

[3] *Ibidem.*

[4] *Audition de M. Arnaud Dechoux, 13 avril 2021.*

leur valorisation six à huit mois après l'attaque ». Une meilleure prise en compte du risque cyber est donc un impératif de souveraineté économique.

Cette prise de conscience reste aujourd'hui inégale. Pour M. Jérôme Notin, directeur général du GIP ACYMA : « *Les grandes entreprises s'en préoccupent assez, grâce à l'ANSSI et à la loi de programmation militaire, par exemple, mais pas les PME. Leurs patrons* […] *pensent ne présenter aucun intérêt pour les cybercriminels, puisqu'ils ne possèdent ni fichier clients ni propriété intellectuelle. Les événements de 2020 ont pourtant démontré que la menace cyber touchait tout le monde. Bloquer le réseau d'une PME prend quelques heures à un cybercriminel, qui en retire plusieurs milliers d'euros. Même si peu d'entreprises « passent à la caisse », et tant mieux, une telle opération reste rentable* » [(1)].

Il existe donc incontestablement **un défi de la sensibilisation au risque cyber à destination des entreprises, en particulier pour les plus petites**. Votre rapporteur identifie à ce propos plusieurs leviers d'action permettant de réaliser des progrès à court et moyen terme.

À court terme, il est indispensable que les pouvoirs publics mettent en œuvre une communication proactive sur le risque cyber**,** à destination des entreprises, sur le modèle, par exemple, des spots télévisés diffusés à destination des citoyens sur les risques informatiques pendant la crise sanitaire. D'après M. Jérôme Notin, une « *grande campagne de sensibilisation, sur le modèle de celle de la sécurité routière* » devrait être lancée par les pouvoirs publics prochainement sur ce sujet. Selon lui, il ne manque « *que des moyens financiers* », mais *« il suffit d'une volonté politique pour les débloquer* » [(2)]. Un guide à destination des TPE et PME concernant les gestes d'hygiène numérique a d'ores et déjà été élaboré en partenariat avec l'ANSSI, les chambres de commerce et d'industrie (CCI), les chambres de métiers et de l'artisanat (CMA) et le GIP ACYMA.

Votre rapporteur souhaite également insister sur la nécessité, pour l'État, d'assumer le coût financier de la promotion de la cybersécurité auprès des citoyens et des entreprises. Il salue, à cet égard, la mise en place d'une stratégie d'accélération sur la cybersécurité, annoncée par le Président de la République au mois de février 2021, dans le cadre du programme d'investissements d'avenir n° 4.

Il convient désormais d'engager un effort financier inédit ciblant les principaux acteurs de la chaîne de la protection numérique au sens large, soit l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA), le parquet national cyber, ainsi que la plateforme Pharos.

---

[1] *Audition de M. Jérôme Notin, 6 avril 2021.*

[2] *Audition de M. Jérôme Notin, 6 avril 2021.*

Proposition n° 34 : Augmenter les moyens financiers et les effectifs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour répondre à la croissance de la menace cyber.

Proposition n° 35 : Consentir un engagement financier inédit à destination des acteurs de la protection numérique au sens large, c'est-à-dire la plateforme Pharos, le groupement d'intérêt public Action contre la Cybermalveillance (ACYMA) et le parquet national cyber.

La stratégie nationale pour la cybersécurité

Dans le cadre du plan « France Relance » et du 4ème Programme d'investissement d'avenir (PIA 4), le Gouvernement a annoncé le 18 février 2021 le lancement d'une stratégie nationale pour la cybersécurité.

Cette stratégie suit un objectif double : accompagner le développement d'une filière au potentiel économique et technologique important, garantir la sécurité numérique de la France et sa maîtrise technologique dans ce domaine.

Le financement de cette stratégie, qui correspond à un investissement total de 1,039 milliard d'euros, est réparti entre une part publique majoritaire (720 millions d'euros) et une part privée (319 millions d'euros).

Cette stratégie s'articule autour des cinq priorités suivantes :

– Développer des solutions souveraines et innovantes de cybersécurité ;

– Renforcer les liens et synergies entre les acteurs de la filière ;

– Soutenir la demande (individus, entreprises, collectivités et État) par un effort de sensibilisation et la promotion d'une offre nationale ;

– Former davantage de jeunes et professionnels aux métiers de la cybersécurité

– Soutenir les entreprises de la filière en fonds propres.

Son déploiement est en cours et a déjà donné lieu à des actions concrètes, avec le lancement des programmes et équipements prioritaires de recherche (PEPR), le soutien aux projets du Campus Cyber, le Grand Défi cyber ou encore la mise en place d'un « observatoire des métiers et des qualifications de la sécurité du numérique ».

Source : auditions de la mission d'information

Les auditions font également apparaître l'utilité de la démarche de labellisation des offres et la nécessité d'amplifier cette dynamique. Votre rapporteur salue, à cette occasion, les premiers efforts consentis en ce sens, *via* la création d'un label CyberExpert, dont bénéficient aujourd'hui 55 prestataires aux compétences vérifiées.

Proposition n° 36 : Labelliser les prestations de cybersécurité pour renforcer la visibilité des acteurs privés sur la qualité des offres disponibles sur le marché.

À moyen terme, la promotion de la souveraineté numérique implique de travailler à l'émergence d'une offre française et européenne aussi complète et

compétitive que possible. À l'heure actuelle, M. Jérôme Notin le relève à juste titre : « *On trouve bien quelques acteurs français et européens de cybersécurité, mais il subsiste de nombreux « trous dans la raquette ». Ni les particuliers, ni les entreprises, ni les collectivités territoriales ne disposent pour l'heure d'une offre à cent pour cent souveraine. Un travail considérable reste à mener* » [1]. La variété de cette offre est également importante afin de permettre aux entreprises de taille réduite de bénéficier de produits conformes à leurs besoins et à leurs moyens financiers.

Sur ce premier point, il est donc nécessaire que les acteurs publics et privés travaillent à la structuration de l'offre française de cybersécurité, en renforçant sa diversité et sa lisibilité pour les acteurs concernés (*voir proposition n° 42*).

Enfin, il est également impératif de travailler à la couverture par les acteurs assurantiels du risque cyber, qui reste tout à fait insuffisante à l'heure actuelle. Ce marché ne représente actuellement que 40 millions d'euros, ce qui est très faible au regard des montants du marché assurantiel. Il faut donc encourager les acteurs de l'assurance à compenser leur futur « *manque à gagner sur les polices d'assurance automobile en proposant de couvrir les risques cyber* », alors que vont apparaître dans les prochaines années des véhicules autonomes.

Le développement de ce type de produits présente en effet un double avantage. Il permettra à la fois d'améliorer la quantification de l'impact des attaques informatiques sur les acteurs économiques et incitera beaucoup plus fortement ces derniers à intégrer ce risque au sein des aléas qu'il convient d'anticiper.

La mise en place d'un observatoire de la menace cyber à l'initiative du GIP ACYMA est une excellente initiative de ce point de vue. Elle permettra en effet de donner davantage de visibilité sur le nombre d'acteurs touchés et le coût du risque cyber [2] , et facilitera en conséquence l'appétence des acteurs économiques à le financer. L'investissement nécessaire pour une entreprise dans la cybersécurité correspond à une fourchette allant de 5 et 10 % de son « budget numérique ».

Proposition n° 37 : Systématiser la couverture du risque cyber dans les polices d'assurance.

Proposition n° 38 : Renforcer la sensibilisation des acteurs privés vis-à-vis du coût du risque cyber. Travailler également à l'amélioration des techniques de quantification de ce risque.

3. Une prudence nécessaire face au risque croissant d'espionnage économique

La protection contre l'espionnage économique est une nécessité alors que le numérique offre une palette nouvelle de possibilités pour récupérer des informations stratégiques. La numérisation accélérée d'un certain nombre d'entreprises, dans le contexte de la crise sanitaire, a mécaniquement créé des

1 Audition de M. Jérôme Notin, 6 avril 2021.

(2) Au niveau mondial, le coût du risque cyber est estimé pour 2021 à 6 000 milliards de dollars.

vulnérabilités, et donc des possibilités de pré-positionnement potentiels de la part de services de renseignement étrangers.

L'actualité récente a donné à voir, par exemple, des tentatives d'espionnage industriel à destination des laboratoires de recherche développement des vaccins contre la Covid-19. Le constat d'une recrudescence des pratiques d'espionnage industriel a été confirmé par un certain nombre d'acteurs auditionnés, dont l'entreprise américaine IBM, qui a indiqué avoir observé, par exemple, une campagne mondiale de *phishing* à l'encontre des entreprises en lien avec le développement du vaccin, comme la firme Pfizer, attaquée par un groupe de *hackers* chinois [(1)].

Votre rapporteur note, sur ce sujet, que les acteurs compétents sont pleinement mobilisés pour assurer de manière effective la protection des intérêts français. Leur action est notamment orientée par le service de l'information stratégique et de sécurité économique (SISSE), qui appartient au ministère de l'Économie, des Finances, et de la Relance. La publication régulière d'un « flash ingérence » par la direction générale de la sécurité intérieure (DGSI) démontre la vigilance importante des pouvoirs publics sur ce sujet.

Il n'en demeure pas moins que cette vigilance doit être partagée, ce qui implique la diffusion d'une culture de la sécurité numérique. Une sensibilisation spécifique des acteurs des technologies à forte valeur ajoutée doit être mise en œuvre, de façon préventive, et non uniquement lorsqu'un risque est identifié par les services. Cette dynamique, qui est déjà en partie à l'œuvre d'après les éléments dont dispose votre rapporteur, doit être poursuivie et amplifiée. Cette sensibilisation doit évidemment porter sur les choix technologiques effectués ou à effectuer par les acteurs, qui ne sont pas neutres sur les risques évoqués ci-dessus. Elle doit également être entendue au sens large et concerner les sous-traitants et fournisseurs des entreprises ciblées.

[1] *Audition de M. Michel Gesquiere, 9 mars 2021.*

III. MOBILISER LA PUISSANCE PUBLIQUE POUR DÉFENDRE LA SOUVERAINETÉ NUMÉRIQUE FRANÇAISE ET EUROPÉENNE

A. LA CYBERDÉFENSE, COMPOSANTE VITALE DE NOTRE SOUVERAINETÉ NUMÉRIQUE

1. Une ambition nationale qui doit s'appuyer sur l'échelon européen

La cyberdéfense est une composante essentielle de la souveraineté numérique française. Elle vise à protéger les infrastructures et acteurs stratégiques nationaux contre les menaces. Elle comprend de ce fait un volet défensif et un volet offensif qui doivent être articulés de façon complémentaire.

La politique de cyberdéfense française repose évidemment sur l'action de l'État au niveau national. Elle mobilise en ce sens un certain nombre d'acteurs et d'instances spécialisés (*infra*).

La politique de cyberdéfense revêt néanmoins également une dimension européenne face au besoin de disposer d'une masse critique suffisante pour peser dans le cyberespace. Ainsi que le relève le général de division aérienne Didier Tisseyre, commandant de la cyberdéfense française, c'est *« à l'échelle européenne qu'il est nécessaire de penser la souveraineté numérique. Les États membres doivent relever le défi de la quantité et de la qualité des ressources humaines et capacitaires à détenir pour pouvoir conquérir leur autonomie stratégique* ».

Cette dimension européenne ne doit donc pas être négligée, comme l'a rappelé M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique. Ce dernier a en effet insisté sur l'importance *« de définir de nouvelles modalités de discussions avec nos partenaires européens et autres pour engager des actions concertées, mais respectueuses de la souveraineté de chacun.* » [(1)].

Votre rapporteur est en accord avec ces premiers éléments de constat. Il considère en effet que l**a cyberdéfense française doit reposer sur des capacités autonomes garantissant la souveraineté nationale mais qu'elle ne saurait toutefois, pour ce même motif, être cantonnée au sein des seules frontières nationales**. Il est en effet nécessaire que la France s'appuie sur une coopération avancée avec ses alliés et qu'elle porte, au sein des institutions européennes, la volonté intacte de construire des outils technologiques européens. Il s'agit en effet d'une condition essentielle pour minimiser progressivement les dépendances technologiques de l'Europe vis-à-vis de certains pays tiers.

---

[1] *Audition de M. Bernard Benhamou, 29 octobre 2020.*

2. Une politique nationale de cyberdéfense en phase de consolidation

En France, la mise en œuvre de la politique de cyberdéfense relève de l'État, mais fait intervenir un ensemble d'acteurs au service de la sécurité numérique nationale.

Le modèle de cyberdéfense française se caractèrise par une spécificité : la séparation entre le défensif et l'offensif. Ce choix vise en effet à limiter les conflits d'intérêts et à simplifier en conséquence la relation de confiance entre les différents acteurs concernés. Il n'empêche pas une coordination fine entre ces deux domaines *via* la gouvernance du centre de coordination des crises CYBER, le C4.

Le centre de coordination des crises CYBER (C4)

La coordination nationale s'appuie sur les mécanismes de gouvernance mis en place à la suite de la revue stratégique de cyberdéfense (RSC) de février 2018.

Le C4 a notamment pour mission de permettre :

– de partager l'analyse de la menace, préparer et coordonner les différents acteurs des ministères ;

– de traiter les crises d'origine CYBER ne nécessitant pas l'activation d'une cellule de crise interministérielle (CIC).

Son organisation comprend notamment :

– un niveau stratégique, qui se réunit de façon mensuelle ou de circonstance, sous la présidence du SGDSN, et coordonne notamment des groupes de travail et le plan d'action de la revue stratégique de cyberdéfense ;

– un niveau TECHOPS, qui permet le partage de l'analyse des modes opératoires adverses et de la menace.

Source : auditions de la mission d'information

Cette coordination s'effectue également au plus haut niveau dans le cadre du Conseil national du renseignement, qui est présidé tous les quinze jours par le Président de la République, et rassemble les six services du premier cercle du renseignement (DGSE, DGSI, DRM, DRSD, Direction du renseignement des douanes – DNRED – et Tracfin).

La direction du renseignement militaire (DRM)

La direction du renseignement militaire (DRM) est le service de renseignement des armées. Elle est placée sous l'autorité du chef d'état-major des armées.

La DRM figure parmi les services de renseignement du premier cercle, qui rassemble les services militaires (direction du renseignement et de la sécurité de défense DRSD, direction générale de la sécurité extérieure DGSE, DRM), les services du ministère de l'économie et des finances (Tracfin, Douanes), et la direction générale de la sécurité intérieure DGSI du ministère de l'intérieur. Pour rappel, le deuxième cercle de la communauté nationale du renseignement comprend les activités de renseignement des ministères : par exemple, le renseignement pénitentiaire, le renseignement des services territoriaux (préfectures).

La DRM exerce à titre principal les trois missions suivantes :

– l'appui aux opérations, en cas de déploiement des forces armées dans le monde, en complément des moyens d'action du commandement des forces ;

– l'anticipation, à une échelle de temps de six, douze, dix-huit mois, avec un objectif prédictif par l'élaboration de scénarios éclairant les responsables de la Défense, militaires ou politiques. Un point de situation est périodiquement présenté devant le Conseil de défense ;

– la veille stratégique, à long terme, dans un arrière-fond marqué par le retour de l'État et de l'affirmation de puissance. L'approche en termes de menace potentielle prévaut alors.

Source : auditions de la mission d'information.

Le volet défensif de la cyberdéfense française est essentiellement géré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), service à compétence nationale, rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN), lui-même placé auprès du Premier ministre. Créée en 2009, l'ANSSI a pour mission d'assurer la sécurité des systèmes d'information de l'État, d'appuyer les administrations et les opérateurs d'importance vitale face au risque cybernétique, de participer au développement des technologies de sécurité, et de promouvoir la culture de la cybersécurité auprès des citoyens et des entreprises. Elle est également impliquée dans la définition de la coopération avec d'autres États européens.

Comme l'a rappelé M. Guillaume Poupard, son directeur général, lors de son audition : « *Aujourd'hui, toutes les administrations ont un rôle à jouer dans le domaine cyber* ». L'ANSSI travaille donc avec l'ensemble des ministères, dans une approche transversale, qui correspond à la réalité actuelle de la menace.

La direction générale de la sécurité intérieure (DGSI) participe également de ce volet défensif. Rattachée au ministère de l'Intérieur, elle assure essentiellement trois missions que sont la lutte contre le terrorisme, la lutte contre l'espionnage et l'ingérence étrangère et, enfin, une action de protection économique face aux tentatives d'espionnage industriel. La DGSI contribue dans cette mesure à la prévention et à la répression de la menace cyber.

Le volet « offensif » de la cyberdéfense française ressort essentiellement des services du ministère des Armées, donc ceux de la Direction générale de la sécurité extérieure (DGSE), ou encore du commandement de la cyberdéfense (COMCYBER) et de la Direction générale de l'Armement (DGA).

La création du COMCYBER en 2017 a marqué l'aboutissement d'une phase de « montée en puissance » de la capacité de cyberdéfense du ministère des Armées depuis 2011.

Le commandement de la cyberdéfense (COMCYBER)

Placé sous l'autorité directe du chef d'état-major des armées, le commandement de la cyberdéfense (COMCYBER) est un commandement interarmées opérationnel et stratégique rassemblant, de façon hiérarchique ou fonctionnelle, l'ensemble des forces de cyberdéfense des armées françaises. Il dispose d'un centre d'opérations cyber colocalisé avec le centre de planification et de conduites des opérations (CPCO).

Créé en 2017, le COMCYBER a pour principales missions :

– la protection des systèmes d'information placés sous l'autorité du chef d'état-major des armées ;

– la conduite de la défense des systèmes d'information sur tout le périmètre du ministère des Armées, à l'exclusion de ceux de la direction générale de la sécurité extérieure (DGSE) et de la direction du renseignement et de la sécurité de la défense (DRSD) ;

– la conception, la planification et la conduite des opérations militaires de cyberdéfense, sous l'autorité du sous-chef d'état-major « opérations ».

Le COMCYBER participe également à la préparation de l'avenir et contribue à la politique RH du domaine cyber. Il coordonne la contribution des armées à la politique nationale et internationale de cyberdéfense, en participant notamment aux projets de coopération à travers la représentation militaire de la France à l'OTAN et l'UE, et coordonne la définition des besoins techniques spécifiques de cyberdéfense. Enfin, le COMCYBER assure la cohérence du modèle de cyberdéfense du ministère et sa coordination générale.

Le COMCYBER est membre du centre de coordination des crises cyber (C4) et contribue à l'analyse des crises d'origines cyber et à proposer des options de réponse.

Au-delà des entités régaliennes, le COMCYBER est au cœur d'un écosystème français de la cyberdéfense, en lien avec les industriels, les start-up et PME ainsi que les écoles et universités.

Fort de près de 3 400 cyber-combattants, le COMCYBER connaît un développement considérable ces dernières années pour faire face, dans le cadre des opérations militaires, aux nouvelles menaces pesant sur la France, et devrait compter environ 4 500 cyber-combattants à l'horizon 2025.

Source : auditions de la mission d'information.

La cyberdéfense française est désormais entrée dans une phase de consolidation qui doit se poursuivre. Les auditions indiquent que le modèle de séparation choisi entre les activités défensives et offensives est pertinent pour

prévenir les conflits d'intérêts entre acteurs et garantir une forme de confiance dans le partage d'information.

Les échanges menés font également apparaître dans ce domaine un changement d'état d'esprit qu'il faut saluer. La coopération entre services tend progressivement à devenir la règle et le refus de partager certaines informations une exception motivée par des raisons légitimes. Les acteurs auditionnés ont également mentionné un sentiment de maturité nouvelle, depuis plusieurs années, chez les décideurs publics et dans l'opinion publique. Le recours au renseignement s'est « normalisé » : il est désormais davantage considéré comme un outil de souveraineté légitime et utile pour permettre à la France de défendre ses intérêts.

3. Un impératif : rester parmi les puissances « cyber » de rang mondial

L'ambition nationale de la France en matière de cyberdéfense doit être de **rester parmi les puissances « cyber » de rang mondial**, quitte à être, pour reprendre une expression employée lors des échanges menés « *un petit parmi les grands* ». L'essentiel est en effet de **disposer de capacités d'action opérationnelles et autonomes** permettant au pouvoir politique d'être en état de prendre ses décisions de façon parfaitement souveraine.

L'état actuel de la menace plaide fortement en faveur d'un investissement puissant pour garantir à la France une capacité d'action dans le cyberespace autonome et aussi complète que possible. La gestion du risque cyber est déjà, et va devenir encore davantage dans les prochaines années, un enjeu décisif de sécurité nationale. Les auditions indiquent, en effet, **qu'est à l'œuvre depuis plusieurs années une « prolifération » de la menace cyber, qui se traduit par l'appétence de toutes les grandes puissances pour le développement et l'utilisation de capacités cyber**. Les conflits récents ont ainsi pu donner lieu à l'expérimentation d'outils cyber de toute nature. Ainsi que l'a résumé le commandant de la cyberdéfense, le général de division aérienne Didier Tisseyre, « *le retour à des politiques de puissance décomplexées menant des stratégies globales de remise en cause de l'ordre international, favorise les frictions. La compétition qui en découle, loin de geler les conflits, crée une situation propice également aux ambitions régionales de certains pays. Les conflits régionaux, allant parfois jusqu'à la haute intensité, impliquent ou sont instrumentalisés par les grands compétiteurs* ».

Dans ce contexte, **il est hautement probable que les adversaires de la France mobilisent de façon croissante ces capacités pour gagner en influence et défendre leurs intérêts**. Le principal risque à cette heure, pour la France et l'Europe, tient notamment, selon le commandant de la cyberdéfense, « *dans le déni d'accès, du jour au lendemain, à des ressources numériques essentielles, à l'occasion d'une crise avec l'une de ces puissances numériques ou avec son pays de rattachement, au titre de mesure de rétorsion/de coercition. Une telle situation aurait des conséquences directes sur la souveraineté européenne et française à très court terme, et indirectes à long terme* ». Dans un contexte de durcissement de la

conflictualité mondiale, *« avoir une cybersécurité défaillante est un risque : les failles peuvent être exploitées par des puissances étrangères pour obtenir des effets stratégiques à partir de notre espace numérique* ».

Au sein du nouveau champ de bataille que constitue le cyberespace, un pays en effet peut adopter, en somme, deux stratégies : se doter de capacités d'action et de riposte s'il en a les moyens, ou se trouver un protecteur, ce qui est difficilement compatible avec une défense ambitieuse de sa souveraineté. Les auditions menées ont permis de constater que **la France appartient au « club » des rares pays disposant de capacités autonomes en matière de cyberdéfense**. **Cette situation doit être préservée**. Elle est en effet la condition du maintien du niveau élevé de crédibilité dont la France jouit à cette heure dans ce domaine.

Votre rapporteur considère que plusieurs leviers peuvent être mobilisés en faveur de cet objectif :

– *les moyens financiers*, afin de s'assurer qu'ils suivent l'évolution de la menace ;

– *les technologies*, afin de disposer des meilleures capacités d'action tout en restant autonome ;

– *les compétences*, en améliorant l'attractivité des métiers de la cyberdéfense et en assumant une ouverture à des profils variés.

4. Les leviers d'une cyberdéfense efficace

a. Adapter les moyens budgétaires face à l'accroissement de la menace

L'accroissement de l'état de la menace cyber est indiscutable et doit être pris en compte par les pouvoirs publics. Cette évolution de la menace procède d'un élargissement du recours à l'outil cyber comme instrument de politique extérieure, selon des modalités qui dépendent du niveau d'avancement technologique respectif des pays concernés. La tendance, comme indiqué par M. Arnaud Dechoux, responsable des affaires publiques « Europe » de Kaspersky lors de son audition, est en outre à la sophistication de la menace [(1)].

Cet accroissement de la menace se traduit notamment, dans un contexte de dégradation de l'environnement international, que la crise Covid-19 et ses nombreuses conséquences fragilise encore davantage, par :

– *de nouvelles formes de conflictualité utilisant des modes d'action hybrides,* certains dans ce qu'on qualifie de « zone grise » et jouant avec le seuil de l'agression armée ;

---

[1] *Audition de M. Arnaud Dechoux, 13 avril 2021.*

– *une guerre de l'information*, permanente, de plus en plus préoccupante, qui passe notamment par les réseaux sociaux ;

– *une course aux armements technologiques* qui doit être conciliée avec le retour de la masse. Il est nécessaire de se préparer à la guerre de haute densité, y compris dans le domaine cyber ;

– *un retour de la « guerre sale » et un « nouvel âge de l'impunité » constaté dans le comportement de certains acteurs internationaux*. La Syrie en est un exemple ;

– *une accélération de la cybercriminalité*. Celle-ci ne cesse de progresser et de s'organiser en exploitant toutes les opportunités du cyberespace et en étant parfois les proxys, volontaires ou non, d'acteurs stratégiques.

L'attribution de moyens budgétaires à **destination des acteurs publics pour gérer leur cybersécurité et assurer une cyberdéfense efficace doit donc évoluer en conséquence**. Cette ambition doit concerner l'ensemble des acteurs publics, c'est-à-dire l'État, évidemment, mais également les collectivités territoriales et les structures de soins, dont la vulnérabilité a pu apparaître lors de la crise sanitaire.

Au sein de l'État, d'abord, **les moyens financiers et humains des acteurs de la cyberdéfense doivent être revus à la hausse, afin de prendre en compte l'état de la menace.** Dans cette perspective, votre rapporteur plaide en faveur d'une hausse du budget et des effectifs de l'ANSSI, d'une part, et souhaite **émettre un point de vigilance vis à vis de la loi de programmation militaire (LPM)** qui doit faire l'objet d'une veille pour s'assurer que son ambition correspond bien à l'évolution de la menace.

Proposition n° 39 : Veiller à ce que la trajectoire définie au sein de la loi de programmation militaire pluriannuelle soit en adéquation avec l'état de la menace et le niveau d'ambition porté par la France dans ce domaine.

Au sein des collectivités territoriales, ensuite, un effort de sensibilisation au risque cyber est nécessaire pour encourager ces acteurs à investir dans une protection efficace contre ce dernier. Ces derniers mois, plusieurs cyberattaques ont paralysé les services de collectivités, avec des conséquences importantes sur la continuité de leur action. Or, à l'heure actuelle, force est de constater que les situations entre collectivités sont très disparates sur la question de la cybersécurité. Cette situation doit donc être prise au sérieux et des efforts consentis dans ce domaine, avec l'accompagnement de l'État et des acteurs compétents.

Enfin, au sein des structures de soins, une vigilance particulière s'impose également. La crise sanitaire a démontré que les assaillants numériques n'hésitaient pas à s'en prendre à ces infrastructures, avec des conséquences d'une gravité potentiellement exceptionnelle au regard de la nature et des missions de ces établissements. **La montée en gamme de leurs équipements informatiques et de**

leur niveau de protection contre le risque informatique est indispensable et doit être poursuivie.

Proposition n° 40 : Accélérer la mise à niveau des équipements numériques des collectivités territoriales et des structures de soins pour garantir leur résilience.

Votre rapporteur souhaite insister, en conclusion de ce premier point, sur la nécessité de veiller à disposer d'une visibilité sur les progrès réalisés sur la montée en gamme proposée ci-dessus. Il s'agit en effet d'un travail de veille complexe puisque s'exerçant sur un périmètre extrêmement large. C'est le sens, notamment, des propositions formulées précédemment en faveur d'un ministère de numérique de plein exercice qui aurait une capacité de pilotage inédite de ces enjeux transversaux.

b. Conserver une autonomie technologique maximale au sein des activités sensibles

Votre rapporteur s'est également interrogé sur l'équilibre à rechercher entre performance des solutions technologiques et indépendance nationale, **puisqu'il n'est pas envisageable de voir la capacité opérationnelle des services de renseignement et de défense impactée à la baisse par le recours à des solutions dont ils deviendraient, finalement, en partie dépendants.**

Les auditions font apparaître, d'abord, que cette recherche d'autonomie technologique est partagée par un certain nombre de pays développés [(1)]. Dans le domaine du renseignement technique, force est de constater qu'il convient pour la France de continuer de prioriser une stratégie d'autonomie technologique maximale, ce qui préserve également la France de scandales d'espionnage tels que ceux qui ont touché plusieurs pays européens à la suite des révélations d'Edward Snowden. Plusieurs technologies critiques ont été évoquées lors des auditions, comme la cryptographie, l'Intelligence artificielle et le quantique. Elles ont trait au traitement et à la protection des données, afin d'être en capacité de valoriser leur collecte. Elles doivent être une cible prioritaire des investissements publics.

Votre rapporteur a conscience, qu'en Europe, un certain nombre d'États membres ne partagent pas l'idée d'une prévalence des équipements européens sur le recours aux équipements américains.

C'est le cas par exemple de la Lituanie comme l'a démontré l'audition du vice-ministre de la défense de ce pays, M. Margiris Abukevicius, qui a insisté sur la coopération transatlantique en matière de technologies et de cybersécurité, en des termes sans équivoque : « *Il est absolument critique d'aller au-delà du périmètre de l'Union européenne. Bien entendu, il est logique de promouvoir l'usage de produits européens pour préserver notre industrie. Néanmoins, il me paraît primordial d'élargir le périmètre de notre stratégie en matière de cybersécurité et de la concevoir dans l'alliance transatlantique. Dans d'autres domaines, les*

[1] *C'est le cas, par exemple, pour la Russie et la Chine ou encore Israël.*

exemples de coopération entre les États-Unis et l'Europe ne manquent pas, notamment en matière de sécurité. En tout cas, une alliance technologique entre les États-Unis et l'Europe aurait nécessairement un impact mondial. Dans cette alliance, chaque pays devrait promouvoir sa propre industrie et bâtir des chaînes d'approvisionnement efficaces. Notre vision doit toutefois porter au-delà de l'Union européenne pour inclure une dimension transatlantique, sachant qu'une coopération dans le domaine des technologies permettra certainement de revivifier cette alliance. » [(1)].

De même, M. Andrès Sutt, ministre du commerce et des technologies de l'information d'Estonie, a abondé dans ce sens en indiquant que *« la géopolitique s'applique bien entendu aussi aux domaines du numérique et de la cybersécurité. Les liens transatlantiques entre l'Union européenne et les États-Unis sont extrêmement forts et ces liens sont à l'avantage des deux parties. L'ordre mondial a bénéficié au monde entier et à tous les pays au cours de ces trente dernières années. Nous avons beaucoup à gagner à poursuivre cette alliance stratégique avec les États-Unis. Certes, nous avons parfois des différends et sommes concurrents dans certains domaines, mais nous sommes fondamentalement du même côté. Ce lien transatlantique fort va dans l'intérêt de l'Union européenne dans son ensemble mais aussi de chacun de ses membres. »* [(2)].

Votre rapporteur souhaite prendre évidemment une certaine distance vis-à-vis de ces positions exprimées : s'il en comprend les fondements, elles lui apparaissent néanmoins difficilement compatibles avec la construction d'une souveraineté numérique européenne.

Au niveau national, votre rapporteur est favorable au fait de **prioriser fortement le recours à des technologies françaises ou européennes.**

Cette approche maximaliste de l'autonomie technologique n'exclut pas néanmoins une forme de pragmatisme, dont l'utilisation du logiciel Gotham de Palantir par la DGSI est un exemple. S'il est évident que la situation actuelle n'est pas optimale, il est difficile de considérer qu'un autre choix était possible, au cours de l'année 2015, dans des circonstances très particulières et en l'absence d'alternative réelle. Il convient néanmoins de toujours envisager, dans ce cas, une « stratégie de sortie » à court ou moyen terme pour rester dans une logique de recours ponctuel et transitoire. De ce point de vue, la DGSI porte un projet ayant vocation à offrir une solution souveraine utile au service concerné, et le cas échéant à d'autres services de la communauté française du renseignement.

Dans un domaine proche, votre rapporteur souhaite également saluer la dynamique engagée autour du projet Artemis, qui doit permettre à la France de disposer d'une infrastructure souveraine de stockage et de traitement massif de données. Elle lui semble en effet démontrer la volonté des pouvoirs publics de défendre une doctrine de l'autonomie technologique maximale.

---

[1] *Audition de M. Margiris Abukevicius, 8 juin 2021.*

[2] *Audition de M. Andrès Sutt, 9 juin 2021.*

Proposition n° 41 : Appliquer une doctrine de l'autonomie technologique « maximale » en matière de renseignement et de cyberdéfense, en faisant du recours à des technologies extra-européennes une exception devant être motivée.

c. Soutenir, en conséquence, le développement des entreprises technologiques françaises et européennes

Le corollaire de la doctrine de l'autonomie technologique réside dans la capacité de la France à soutenir le développement de ses entreprises technologiques.

Les auditions font apparaître deux difficultés à ce sujet :

– *un déficit de financement des acteurs technologique***s**, qui s'explique par les limites du marché des capitaux national et l'insuffisante harmonisation du marché européen des capitaux, mais aussi par des réticences de certaines institutions européennes à offrir des conditions de financement satisfaisantes. Ce point a notamment été soulevé par M. Jean-Noël de Galzain, président d'HEXATRUST. Ce dernier a pris l'exemple de l'action de « *la Banque européenne d'investissement* [qui] *propose* [certes] *de l'aide, ce qui est un point positif* [mais à des taux] *de prêts allant de 13 % à 17 % par an* [ce qui est] prohibitif. ». Il a également ajouté que « *les solutions de financement existent, mais […] sont inaccessibles aux PME et aux ETI* » avant d'insister sur la nécessité de « *changer les mentalités* » sur ce sujet [1]. Des efforts sont néanmoins conduits au niveau national *via* la commande publique du ministère des Armées, ce qui doit être salué ;

– *des risques de captation des savoir-faire technologiques en matière de défense par des acteurs étrangers souhaitant s'approprier ces technologies*. Sur ce sujet, il convient « *de se donner les capacités de réagir* », pour reprendre les propos de M. Nicolas Blanc, délégué national au numérique, de la confédération française de l'encadrement–confédération générale des cadres (CFE-CGC), lors de son audition [2]. Plusieurs exemples de rachat problématique ont été évoqués lors des travaux de la mission, dont ceux des entreprises Sentryo et Alsid, rachetées respectivement par les deux sociétés américaines Cisco et Tenable. Il faut donc que l'État reste vigilant et proactif sur ce sujet, en utilisant les outils dont il dispose pour s'opposer à certaines opérations préjudiciables à la protection de la souveraineté nationale.

Votre rapporteur souhaite insister, en conséquence, sur un double impératif :

– d'une part, que l'écosystème français du capital risque se développe davantage et que les grandes entreprises françaises augmentent leurs acquisitions, pour fournir une alternative aux fonds d'investissements étrangers ;

---

[1] *Audition de M. Jean-Noël de Galzain, 11 février 2021.*

[2] *Audition de M. Nicolas Blanc, 20 avril 2021.*

– d'autre part, qu'un arsenal réglementaire plus contraignant soit mis en place, le cas échéant, pour protéger nos entreprises sensibles d'un rachat par des capitaux étrangers.

La dynamique engagée en faveur de la création d'un campus cyber lui apparaît évidemment très positive. Cette initiative devrait en effet faciliter les échanges entre acteurs publics et privés et favoriser une dynamique d'innovation. Comme le résume M. Michel Van Den Berghe, l'objectif est de « *structurer* [le] *marché de la cybersécurité* », en aidant *« à faire connaître ces PME, qui apportent de la cybersécurité dans les régions »*, pour créer « *un maillage, et faire en sorte que les gens se parlent pour élever le niveau global de cybersécurité.* »[1]. En rassemblant industriels, *start-up*, acteurs publics et le monde de l'enseignement et de la recherche sur un même campus, ce campus favorisera la circulation des compétences et le développement de solutions numériques innovantes.

Proposition n° 42 : Accélérer la dynamique de constitution d'un écosystème français et européen d'entreprises « cybertech ».

Votre rapporteur souhaite conclure ce point en rappelant **que le développement des entreprises technologiques françaises passe nécessairement par une phase d'internationalisation qu'il faut maitriser mais accepter**. Comme l'a rappelé M. Michel Van Den Berghe, président de la mission campus cyber : « *nos* start-up *doivent également pouvoir évoluer et s'internationaliser sans nécessairement aller chercher des fonds outre-Atlantique. Il ne faut plus que les entreprises françaises qui commencent à bien fonctionner sur le territoire national soient obligées de créer un siège social à San Francisco pour pouvoir rayonner aux États-Unis. Il est possible de procéder autrement, mais nous devons nous en donner les moyens. Nous devons conserver des entreprises françaises capables de s'adresser à des clients internationaux sans basculer leur siège social aux États-Unis.* »[2]. Il s'agit là d'une condition essentielle pour permettre à ces acteurs d'atteindre une taille critique.

d. Renforcer l'attractivité des métiers de la cyberdéfense

Enfin, il ne peut y avoir de politique de cyberdéfense efficace et opérationnelle sans un vivier de compétences « à l'état de l'art », ce qui implique de travailler sur la capacité de recruter et de fidéliser des profils techniques au sein des services de cyberdéfense.

Les auditions font apparaître que l'attractivité des métiers du « cyber » reste importante en raison du caractère prestigieux des services concernés, mais que les acteurs publics souffrent de la forte demande de compétences similaires dans le secteur privé, qui se traduit par des propositions de rémunération élevées, et un niveau d'attente en matière de qualité de vie.

---

[1] *Audition de M. Michel Van Den Berghe, 13 avril 2021.*

[2] *Audition de M. Michel Van Den Berghe, 13 avril 2021.*

Ce sujet a été notamment abordé par le général de corps aérien Jean-François Ferlet, directeur du renseignement militaire, lors de son audution : « *La difficulté est permanente. On ne forme pas assez de candidats en France. Il s'agit de nouveaux métiers dans une filière à fort potentiel. Une forme de « pillage » des talents est réalisée par les États-Unis et la Chine. Nous n'arrivons pas à être compétitifs dans la durée en termes de rémunération offerte, compte-tenu de la loi de l'offre et de la demande sur le marché, mais il est possible de fidéliser les talents, pour un temps, compte tenu de l'intérêt du travail à la DRM et s'agissant d'une génération en recherche de sens.* »

Votre rapporteur se réjouit du fait que les métiers de la cyberdéfense demeurent attractifs auprès des jeunes talents. Il considère que la mise en place d'un campus cyber est également très positive de ce point de vue et note les efforts d'action commune entre les différents services, *via* l'harmonisation, par exemple, des grilles de rémunération entre les différents services, comme l'a précisé M. Patrick Pailloux, directeur technique de la Direction générale de la sécurité extérieure, lors de son audition.

Votre rapporteur invite néanmoins les pouvoirs publics à amplifier leur démarche en ce sens, en mettant en œuvre les évolutions organisationnelles et managériales nécessaires pour améliorer le cadre de vie de ces profils qualitatifs. Il convient également de leur offrir des modalités attractives d'évolution de carrière au sein du secteur public *via* la formalisation, par exemple d'un parcours cyber au sein de la sphère publique. La mobilité de ces profils doit être d'abord considérée comme une force, même si elle n'exclut pas, évidemment, une nécessaire vigilance. Elle est en tout cas de plus en plus indispensable pour rester au meilleur niveau dans des secteurs d'activité technologiques très évolutifs par construction.

Proposition n° 43 : Recruter davantage de profils techniques issus du secteur de la sécurité numérique, en rehaussant les rémunérations proposées et en adressant la question de la qualité de vie au travail.

Proposition n° *44* : Formaliser un « parcours public » cyber offrant des débouchés aux profils à haute valeur ajoutée recrutés par les acteurs de la chaîne de défense et de sécurité nationale.

B. RÉUSSIR UNE TRANSFORMATION NUMÉRIQUE RAPIDE ET SOUVERAINE DES ADMINISTRATIONS PUBLIQUES

1. Des débats légitimes sur le contenu et la gouvernance de la transformation numérique des administrations publiques

La transformation numérique des administrations publiques est indispensable pour répondre aux attentes des citoyens et renforcer l'efficacité de l'action publique. Cette évolution profonde implique des enjeux de souveraineté au regard des partenaires choisis pour mener à bien les différents projets qui y concourent. À l'heure actuelle, nombre d'acteurs publics utilisent en effet des

solutions extra-européennes, parfois par nécessité, mais aussi par habitude et en raison de leur fiabilité parfois perçue comme meilleure que les produits concurrents.

La crise sanitaire a fait la démonstration du recours massif des particuliers mais aussi des administrations publiques aux solutions américaines. M. Nicolas Brien, directeur général de France Digitale, a considéré sur ce sujet que cela n'avait pas été *« tellement fait par choix, mais plutôt par paresse »*, soulignant par ailleurs, que la crise avait permis de constater « *qu'un processus grave était à l'œuvre : le désarmement technologique de l'État. (…). Cela se traduit de la manière suivante : dans les administrations, les personnes ne savent plus expertiser des solutions technologiques et se contentent de passer des contrats avec des intégrateurs (Capgemini, Sopra Steria, Onepoint). Cela peut donner l'illusion, comme ces intégrateurs sont français, que l'on achète français. Cela n'est pas du tout le cas : ces entreprises intègrent des solutions qu'ils ne produisent pas eux-mêmes et qui sont souvent des solutions sur étagère américaines. »* [(1)].

Abordant les moyens, pour l'État, de reprendre le contrôle de son expertise technologique, M. Nicolas Brien a considéré que cette expertise technologique retrouvée ne pourrait résulter que de l'alternative suivante :

– soit la nomination d'un *chief digital officer* dans chaque administration et ministère, leur réseau devant permettre de *« pousser la transformation digitale de l'État de manière offensive »* ;

– soit la création d'une direction générale du numérique, sous l'autorité du ministre du numérique, cette direction générale regroupant la French Tech, l'ANSSI, certaines compétences du Conseil national du numérique et de l'ARCEP ainsi que toutes les directions des systèmes d'information de l'État. Interrogé par votre rapporteur sur le point de savoir si la direction interministérielle du numérique (DINUM) ne constituait pas déjà cette direction centrale du numérique, M. Nicolas Brien a répondu : *« la DINUM n'est absolument pas cela. Aujourd'hui, l'expertise technologique est faible et éclatée. La DINUM n'est* [en effet] *pas capable de donner des instructions au DSI du ministère de la santé, par exemple. Dans ce cas de figure, le DSI s'en remettra au ministre de la santé »*. Dans cette configuration, la DINUM aurait vocation à devenir *« une administration aussi prestigieuse et puissante que la direction générale du Trésor. »*.

En regard de ces options, la gouvernance actuelle pourrait être qualifiée de troisième voie, si l'on s'en tient à la présentation qu'en a faite M. Nadi Bou Hanna, directeur interministériel du numérique : *« le système d'information de l'État repose sur le principe de subsidiarité. Chaque ministre, appuyé par sa direction du numérique, en est responsable sur son périmètre. La direction interministérielle du numérique (DINUM), placée sous l'autorité de la ministre de la transformation et de la fonction publiques, Mme Amélie de Montchalin, assure la cohérence d'ensemble, le portage stratégique en matière de numérique ainsi que l'animation*

[1] *Audition de M. Nicolas Brien, 25 février 2021.*

de cette équipe. Nous jouons donc un rôle de capitaine d'équipe. Nous intervenons auprès du gouvernement pour le conseiller, pour assurer une coordination fonctionnelle des directions du numérique, pour partager les bonnes pratiques et pour contrôler l'exécution des grands projets informatiques. Ma direction intervient également en soutien à l'innovation, en appui et en animation des acteurs de la GovTech. Enfin, la politique de la donnée est un axe de force très important de notre activité, qui conditionne la maturation des politiques publiques : la DINUM apporte un appui aux administrations sur la gestion de ce trésor. La DINUM assure également un rôle de création et d'exploitation de solutions. La résilience de l'État dans le domaine du numérique est directement portée par ma direction, avec l'appui des autres directions du numérique. Cette résilience repose sur le réseau interministériel de l'État, mais aussi sur la mise à disposition de solutions numériques pour assurer la continuité du service public, même quand les agents travaillent à distance. » [(1)].

Votre rapporteur a donc souhaité réfléchir à l'organisation des politiques numériques au sein de l'État et aux modalités de leur pilotage qui pourraient être les plus efficaces.

Il convient d'abord, en amont de toute réflexion, de conserver à l'esprit les travaux du sociologue des organisations M. François Dupuy [(2)]. Ce dernier critique, en effet, le raisonnement ordinaire postulant l'existence d'une meilleure et unique solution possible à un changement d'organisation, l'intelligence du dirigeant consistant à trouver cette solution et l'imposer à tous. Il convient de privilégier, à l'inverse, une approche pratique consistant non pas à rechercher une hypothétique meilleure solution, mais une première solution acceptable, dans un contexte et à un moment donné. Selon une telle approche, qui relativise d'une certaine façon le discours de l'anticipation et de la gestion prévisionnelle, transformer une organisation consiste à mettre les acteurs dans un contexte dans lequel ils trouveront des solutions différentes de celles adoptées précédemment.

Votre rapporteur est convaincu que la transformation numérique de l'État et de l'administration ne relève pas d'une approche du tout ou rien, mais plutôt d'un processus progressif.

Les auditions des ministres en charge de la transformation numérique de l'administration dans des pays, dont l'image est celle d'un parcours réussi, ont témoigné de l'opportunité d'une telle approche. M. Andrès Sutt, ministre du commerce et des technologies de l'information de la République d'Estonie, a souligné *: « Nous avons tiré de notre expérience un certain nombre de leçons. La première est l'importance de la simplicité. Pour cette raison, nous avons dû progresser étape après étape, en évitant le développement d'un énorme système qui serait très lourd et probablement peu efficace. Avancer petit à petit est une méthode qui s'est révélée efficace, mais il est essentiel qu'au final, le design soit bon et le*

---

[1] *Audition de M. Nadi Bou Hanna, 21 janvier 2021.*

[2] *François Dupuy, La faillite de la pensée managériale. Lost in management 2, Éditions du Seuil, 2015.*

système globalement bien conçu. Les plateformes partagées ont permis une implémentation plus rapide et efficace. Enfin, la confiance du public et la transparence sont des points clés. » [(1)]. Pour sa part, M. Marc Hansen, ministre délégué à la digitalisation du gouvernement du Grand-Duché du Luxembourg, a rappelé qu'*« entre experts ou, du moins, entre ceux qui s'y connaissent en matière de nouvelles technologies, il arrive de céder à la tentation de « faire de l'art pour l'art », selon l'expression française consacrée, c'est-à-dire de recourir à la numérisation en vue de la simple satisfaction que procure le basculement vers le numérique. Nous ne devons pas perdre de vue dans l'intérêt de qui nous agissons, et nous demander si notre travail apportera une plus-value aux autres en tant qu'êtres humains, dans leur travail ou leur vie quotidienne. Une administration qui utiliserait le numérique uniquement par attrait pour les nouvelles technologies risquerait de perdre la confiance des citoyens et des entreprises. Il faut toujours songer à l'individu et à ce que la digitalisation lui apporte. »* [(2)]. Loin de toute forme de solutionisme technologique, le numérique doit donc d'abord être mis au service d'une projet politique pour être soutenu et compris : simplifier la vie des citoyens.

Pour apprécier la situation française actuelle, on peut prendre comme point de départ, les prescriptions du décret du 22 décembre 1986 relatif au développement de l'informatique, de la bureautique et des réseaux de communication dans l'administration [(3)], puisqu'il a constitué le socle de la gouvernance numérique de l'État pendant près de trente ans. Il n'a en effet été abrogé que par le décret du 1er août 2014 relatif au système d'information et de communication de l'État.

Les objectifs et les choix de gouvernance de l'informatisation de l'administration étaient, à cette époque, les suivants :

– l'amélioration de la qualité et de l'efficacité du service public et la simplification des relations avec les usagers ;

– la responsabilité de chaque ministre dans la conduite de l'informatisation de son administration au travers de l'établissement d'un schéma directeur de l'informatique, de la bureautique et des réseaux de communication (objectifs et orientations de la politique informatique du ministère, plan de développement avec les différentes étapes de la mise en œuvre des systèmes d'information, les architectures correspondantes et les programmes de recrutement et de formation des personnels). Ce schéma directeur prenait en compte le respect des normes et leur évolution, l'ouverture à la concurrence en matière d'équipement et de sous-traitance, la sécurité des systèmes, la protection des libertés individuelles et le souci de coordination des systèmes d'information au niveau local ;

– l'animation et la coordination de l'informatisation de l'administration confiée au comité interministériel de l'informatique et de la bureautique présidé par le Premier ministre ou, par délégation, le ministre chargé de la réforme

[1] *Audition de M. Andrès Sutt, 9 juin 2021.*

[2] *Audition de M. Marc Hansen, 3 juin 2021.*

[3] *Décret n° 86-1301 du 22 décembre 1986.*

administrative. Le comité interministériel devait recueillir les informations concernant les réalisations et les projets informatiques, bureautiques et de réseaux de communication, veiller à la cohérence des systèmes de communication utilisés, recenser et examiner les problèmes d'intérêt commun, ou encore suivre la mise en œuvre des différents projets.

Le passage de l'âge de l'informatique à celui de la donnée s'est déroulé sur un fond de questions qui demeure étonnamment le même. Passer de modes de fonctionnement traditionnels, segmentés et séquentiels (organisation en « silos »), à des fonctionnement transversaux, horizontaux et par projets suppose de faire coopérer, sous la responsabilité d'un chef de projet, des entités bénéficiant jusqu'alors d'un haut degré d'autonomie. Dans cette démarche, la segmentation des fonctions de direction a été et reste l'obstacle majeur à la prise en compte de la complexité des organisations.

Pour l'administrateur général des données [(1)], dans son rapport au Premier ministre sur la gouvernance de la donnée de décembre 2015, une telle permanence d'approche explique pour une grande part la difficulté, rencontrée par l'administration, à prendre le tournant de la « révolution numérique » engagée. *« Si l'État a, de longue date, organisé son action autour de données scientifiques et administratives, il faut reconnaître que les choix d'organisation, les stratégies technologiques et les règles de gouvernance de ces données qui prévalent aujourd'hui encore résultent de choix organisationnels, de technologies et de cadres juridiques antérieurs à la révolution en cours. (…) Focalisé sur la fiabilité, la sécurité et la maîtrise des coûts, il a négligé l'interopérabilité, l'accessibilité et la capacité d'usage, et a donc toléré une culture de silos, des divergences de formats avec des qualités excessives ou au contraire dégradées, une sous-traitance excessive et une perte globale de souveraineté et d'autonomie sur ses propres données. »*

Le diagnostic effectué, il convient désormais de retracer succinctement le cheminement suivi en matière d'adaptation de la gouvernance de l'État aux nouveaux enjeux du numérique.

2. Des progrès incontestables ont été réalisés depuis 2011

Des progrès notables ont été effectués en faveur de la transformation numérique de l'État et de la gouvernance des politiques numériques.

En 2011, la création d'une direction interministérielle des systèmes d'information et de communication de l'État (DISIC) a constitué une étape décisive au sein de cette dynamique. Cette direction, placée sous l'autorité du Premier ministre et rattachée au secrétariat général du gouvernement, avait pour mission d'orienter, d'animer et de coordonner les actions des administrations de l'État visant

[1] *M. Henri Verdier assumait alors la responsabilité d'administrateur général des données.*

à améliorer la qualité, l'efficacité, l'efficience et la fiabilité du service rendu par les systèmes d'information et de communication.

Cette compétence d'orientation et de coordination s'est traduite par l'élaboration d'un cadre stratégique commun pour le développement des systèmes d'information et de communication des administrations de l'État et la recherche d'une mutualisation d'opérations (infrastructures, réseaux, services logiciels, systèmes de gestion) entre plusieurs administrations (1). La DISIC a défini dans ce cadre les démarches d'élaboration et d'actualisation des schémas directeurs des systèmes d'information et de communication des ministères (choix fonctionnels et technologiques) et les orientations à donner aux systèmes d'information à l'occasion de la réforme territoriale de l'État. Le directeur de la DISIC était informé, pour avis, de tout projet relatif au système d'information et de communication d'un certain montant.

En 2014, une nouvelle modernisation est intervenue avec la création, par décret, du système d'information et de communication de l'État. Ce dernier a permis de placer l'ensemble des systèmes d'information ministériels sous la responsabilité du Premier ministre. Il a consacré par ailleurs la notion de plan ministériel d'investissement pour les projets et activités de chaque ministère en ce qui concerne les systèmes d'information et de communication. Chaque plan devait être transmis pour avis au directeur de la DISIC, un avis conforme étant requis au-delà d'un certain montant.

La même année, est également créée la fonction d'administrateur général des données, placé sous l'autorité du Premier ministre (2). En concertation avec les administrations, l'administrateur général des données propose des stratégies d'exploitation des données produites, reçues ou collectées et élabore les moyens d'une meilleure exploitation des données (outils, référentiels et méthodologies).

---

[1] Décret n° 2011-193 du 21 février 2011.

[2] Décret n°2014-879 du 1er août 2014 et décret n° 2014-1050 du 16 septembre 2014.

La fonction d'administrateur général des données

Aux termes du décret n° 2014-1050 du 16 septembre 2014, qui institue sa fonction, l'administrateur général des données coordonne l'action des administrations en matière d'inventaire, de gouvernance, de production, de circulation et d'exploitation des données par les administrations – services centraux et déconcentrés de l'État ainsi que les établissements publics placés sous sa tutelle. Il organise, dans le respect de la protection des données personnelles et des secrets protégés par la loi, la meilleure exploitation de ces données et leur plus large circulation, notamment aux fins d'évaluation des politiques publiques, d'amélioration et de transparence de l'action publique et de stimulation de la recherche.

Initialement placé sous l'autorité du Premier ministre et rattaché au secrétariat général pour la modernisation de l'action publique, il est ensuite rattaché à partir de 2017 au directeur interministériel du numérique et du système d'information et de communication de l'État (DINSIC). Depuis 2019, le directeur interministériel du numérique (DINUM) exerce, à ce titre, cette fonction.

Source : Légifrance.

En 2015, un secrétariat général pour la modernisation de l'action publique (SGMAP) est institué, sous l'autorité du Premier ministre, comprenant une direction interministérielle pour l'accompagnement des transformations publiques chargée de plusieurs missions :

– la coordination et animation des travaux d'amélioration de l'action des administrations au profit des usagers ;

– la prise en compte des attentes des usagers, des agents et partenaires de l'État, l'amélioration et l'évaluation de la qualité de service ;

– la coordination des actions de simplification et d'allégement des formalités administratives ;

– l'animation de travaux de modernisation de la gestion publique ;

– le concours à l'adaptation de l'organisation des administrations de l'État à l'évolution de leurs missions et modes de gestion.

Une direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) [1] est également créée à cette occasion. La DINSIC reçoit alors une mission de coordination de l'action des administrations en vue de faciliter la réutilisation des informations publiques et administre le portail unique interministériel en vue de rassembler et mettre à disposition librement l'ensemble des informations publiques.

Cette dynamique de transformation s'est poursuivie en 2017, d'une façon différente. À la suite de la suppression du secrétariat général pour la modernisation

[1] *Décret n° 2015-1165 du 21 septembre 2015.*

de l'État, la direction interministérielle pour la transformation publique a été placée sous l'autorité du ministre chargé de la réforme de l'État. Elle est dirigée par le délégué interministériel à la transformation publique. La direction interministérielle du numérique et du système d'information et de communication (DINSIC) de l'État a quant à elle été placée, par délégation du Premier ministre, sous l'autorité du ministre chargé du numérique et rattachée au secrétariat général du gouvernement [(1)].

Enfin, deux évolutions en termes de gouvernance sont intervenues plus récemment :

– en 2019, la DINSIC a été transformée en direction interministérielle du numérique (DINUM) avec des objectifs similaires et chaque ministère met en place une structure de pilotage de ses actions en matière de numérique (transformation numérique des politiques publiques, développement des usages numériques, création et opération de services numériques, innovation numérique, exploitation du potentiel offert par les données, système d'information et de communication) [(2)].

– en 2021, a été désigné par chaque ministre, un administrateur ministériel des données, chargé d'élaborer la stratégie du ministère dans ce domaine, de coordonner les parties prenantes et d'être le point de contact des utilisateurs des données et des applications numériques dans son périmètre d'action, selon un positionnement hiérarchique lui permettant d'assurer ses missions en lien étroit avec les services du ministère. Il revient au directeur interministériel du numérique, en sa qualité d'administrateur général des données, algorithmes et codes sources, d'assurer la coordination. Il a également été désigné un référent « données, algorithmes et codes sources » auprès de chaque préfet de région pour accompagner les services déconcentrés de l'État [(3)].

---

[1] Décret n° 2017-1584 et décret n° 2017-1586 du 20 novembre 2017.

[2] Décret n° 2019-1088 du 25 octobre 2019.

[3] Instruction du Premier ministre du 27 avril 2021 sur la politique publique de la donnée, des algorithmes et des codes sources.

La direction interministérielle du numérique (DINUM)

La direction interministérielle du numérique a été créée en 2019 pour assurer un pilotage plus efficace des politiques numériques de l'Etat. Elle est placée sous l'autorité de la ministre de la transformation et de la fonction publiques, Mme Amélie de Montchalin.

Sa mission est d'assurer la cohérence d'ensemble de la politique numérique de l'Etat.

La DINUM intervient auprès du gouvernement pour le conseiller, assurer une coordination fonctionnelle des directions du numérique, partager les bonnes pratiques et et contrôler l'exécution des grands projets informatiques. Elle assure également un rôle de création et d'exploitation de solutions, et porte les enjeux de résilience numérique au sein de l'Etat, avec l'appui des autres directions du numérique.

Elle comprend une direction de programme TECH.GOUV dont l'objectif est d'accélérer la transformation numérique de l'Etat, ainsi que trois départements :

– un département « Infrastructures et services opérés » (ISO) pour concevoir et opérer les services d'infrastructures à valeur ajoutée mutualisés entre les administrations, dont le réseau interministériel de l'État ;

– un département « Etalab » pour coordonner la conception et la mise en œuvre de la stratégie de l'État dans le domaine de la donnée, dont ses composantes juridique et sociétale ;

– un département « Performance des services numériques » (PSN) pour la conception et le soutien à la mise en œuvre des plans d'action interministériels de mutualisation, dématérialisation, pilotage des projets et qualité des services numériques.

Dans le cadre du plan de relance, la DINUM est chargée de gérer une enveloppe de 500 millions d'euros destinée à soutenir les projets de l'État en s'appuyant autant que possible sur l'écosystème numérique français et européen.

Source : auditions de la mission d'information

3. Des réformes indispensables pour garantir un pilotage efficace des politiques numériques

Votre rapporteur souhaite formuler plusieurs remarques vis-à-vis de ces différentes évolutions.

a. La création d'un véritable ministère du numérique

Il relève, d'abord, que certains choix effectués font l'objet de critiques qui lui semblent légitimes. C'est le cas, en particulier, de la scission intervenue en 2017 qui a éloigné la DINSIC et la DITP. Pour le Conseil national du numérique, cette réforme a « *profondément réduit la capacité de réformer en profondeur le mode de fonctionnement et les missions de services publics. L'ancien SGMAP incarnait la cohérence entre les moyens mis en œuvre pour répondre aux enjeux de numérisation de l'État en portant une vision innovante et la mise en œuvre opérationnelle, technique et technologique de cette vision* » [(1)].

[1] *Conseil national du numérique, Transformation de l'État Dépasser la norme par la pensée design, Novembre 2019.*

Le CNnum recommande en conséquence de créer un ministère de la transformation de l'État et du numérique et le rapprochement dans une direction unique et interministérielle qui rassemblerait la DITP et les services de la DINUM en charge de la transformation numérique.

Votre rapporteur est favorable à cette proposition puisqu'il estime, en effet, qu'il est temps de passer « une étape supplémentaire » en consacrant l'existence d'un ministère du numérique de plein pied, doté d'une administration et de moyens propres, qui aurait pour mission de porter les politiques numériques au niveau national, européen et international. La gouvernance actuelle de ces politiques, qui doivent être pensées de plus en plus à l'échelle européenne et internationale, apparaît excessivement éclatée entre les ministères. Cette proposition recueille en outre de très nombreux soutiens au sein des acteurs de l'écosystème numérique et du Parlement. Elle avait d'ailleurs également été portée, il y a quelques mois, par notre ancienne collègue Mme Laure de La Raudière et par notre collègue M. Éric Bothorel, dans le cadre de leur groupe de travail créé au sein de la commission des affaires économiques de l'Assemblée nationale et consacré au suivi des conséquences de la crise sanitaire.

Proposition n° 45 : Créer un ministère du numérique, doté d'une administration et de moyens propres, et chargé de porter les politiques numériques aux niveaux national, européen et international.

Proposition n° 46 : Mettre en place un briefing hebdomadaire du Président de la République sur les questions technologiques en s'inspirant du modèle américain.

b. Une meilleure association des collectivités territoriales et du Parlement

Votre rapporteur souhaite, en outre, formuler deux autres propositions pour amplifier la transformation numérique des administrations publiques et améliorer le suivi des politiques numériques au Parlement.

Sur le premier point, votre rapporteur soutient un renforcement du volet numérique des contrats de plan État-régions. Cette demande légitime a été formulée par un certain nombre de collectivités territoriales lors des travaux menés par la mission d'information. La transformation numérique concerne en effet l'ensemble des administrations publiques et les collectivités territoriales doivent y trouver toute leur part.

Sur le second, il recommande de créer un document de politique transversale dédié aux politiques numériques, afin d'unifier leur suivi et de consacrer encore davantage leur importance lors des débats au Parlement sur le projet de loi de finances annuelle. À l'heure actuelle, ce suivi est rendu complexe par l'éclatement des différents projets menés, comme présenté ci-dessus.

Proposition n° 47 : Créer un document de politique transversale (DPT) dédié aux politiques publiques du numérique, en complétant en ce sens *l'article n° 128 de la loi n° 2005 – 1720 du 30 décembre 2005 de finances rectificative pour 2005*.

Proposition n° 48 : Renforcer le volet numérique des contrats de plan État-régions.

c. Une montée en gamme nécessaire des compétences et méthodes de gestion des projets numériques

Plusieurs autres évolutions sont également souhaitables, selon votre Rapporteur :

– *l'internalisation des compétences stratégiques au sein de l'État, qui est indissociable de toute forme de souveraineté numérique***,** comme le rappelait le directeur interministériel du numérique, M. Nadi Bou-Hanna : *« Je constate que 90 % à 95 % de la maîtrise des grands projets ou des technologies est aujourd'hui externalisée. Les couches d'externalisation s'empilent : elles impliquent des grands cabinets de conseil, l'assistance à maîtrise d'ouvrage, l'entreprise de maîtrise d'œuvre, l'opérateur externe… Au final, l'ordonnateur ne dispose pas d'une vue d'ensemble et ne maîtrise pas le dispositif. Il perd la main. Aucune forme de souveraineté numérique ne peut alors se développer.* » [1]. Le renforcement du recrutement par contrat de droit privé de profils techniques pour mener à bien les projets numériques de l'État doit y concourir, de même que la circulation des compétences numériques au sein de l'État, qui doit être encouragée.

– *le décloisonnement de l'administration*. De ce point de vue, l'annonce de la désignation d'administrateurs des données dans chaque ministère transpose, on peut l'espérer, la fonction de *« chief data officier »*, c'est-à-dire la responsabilité spécifique de faire émerger et mettre en œuvre des décisions ou des politiques publiques fondées sur la donnée. Il convient sur ce point de rechercher l'émergence d'un **«** État plateforme **».** Déjà suggéré par l'administrateur général des données, dans son rapport de 2015, il doit constituer le socle de la transformation numérique de l'administration. Le décloisonnement des relations entre les administrations doit leur permettre, avec l'accord des usagers, de prendre la responsabilité de recenser les différentes données disponibles et de leur offrir en retour un service personnalisé et simplifié. Un État plateforme faciliterait en effet les échanges entre administrations et avec les usagers au travers d'interfaces (API) sécurisées et sous le contrôle de l'utilisateur. Les fournisseurs de données et les fournisseurs de services pourraient s'appuyer sur le catalogue de référence des API disponibles. Cette stratégie implique de soutenir « l'extractibilité » des données *« by design »* et les choix d'architecture et de gouvernance permettant d'avancer vers l'utilisation en temps réel des données.

[1] *Audition de M. Nadi Bou Hanna, 21 janvier 2021.*

Proposition n° 49 : Accélérer la mise en œuvre d'une politique ambitieuse d'ouverture des données au sein des administrations publiques.

Proposition n° 50 : Créer un portail public rassemblant l'ensemble des offres numériques françaises disponibles.

– *la promotion de méthodes de gestions de projets modernes et efficaces*. Un travail de veille doit être mis en œuvre dans ce cadre par les acteurs pour moderniser leurs pratiques.

Proposition n° 51 : Assurer un travail de veille pour intégrer dans la gestion des projets numériques les méthodes de travail et d'organisation les plus performantes.

– *la volonté de promouvoir une démarche d'administration agile*. Les processus numériques de ce type développent les services et les systèmes à partir des besoins des utilisateurs, en organisant un retour d'expérience continu. De ce point de vue, FranceConnect, ouvert à toutes les administrations, permet au citoyen de se connecter à tout service public et de déterminer lui-même des échanges de données entre les différents systèmes pour simplifier des relations avec l'administration.

Le volet numérique du plan de relance

Le plan de relance intègre un volet numérique puissant, de l'ordre de 7 milliards d'euros investis sur deux ans, dont 2,3 milliards d'euros destinés à la transformation numérique de l'État, des territoires, et des entreprises, 300 millions d'euros destinés à la formation aux métiers du numérique et 800 millions d'euros investis dans le « numérique du quotidien » (plan France Très Haut débit et inclusion numérique ».

Les financements d'appels à projets correspondants portent sur les thèmes suivants :

– *l'amélioration de l'efficience des services publics*, par l'optimisation des fonctions supports (apport aux agents des données, des analyses et des simulations dont ils ont besoin au quotidien) et l'automatisation des tâches les plus répétitives (saisies multiples, contrôles de pièces, etc.). L'objectif poursuivi est de surmonter, par le levier numérique, des freins fréquemment rencontrés par les administrations (activités présentant une forte consommation de ressources, tâches répétitives à faible valeur ajoutée pour un agent qualifié, ruptures applicatives dans le système d'information). Ces projets pourront faire appel à l'Intelligence artificielle ;

– *la conception et l'accompagnement de la transformation des organisations et des métiers par le numérique*. Le projet peut porter sur le diagnostic du potentiel de transformation numérique du métier, du service ou de la structure, la construction d'une vision cible de cette transformation, et le déploiement de la trajectoire à suivre. Les projets ciblés ne peuvent pas se limiter à la refonte d'un système d'information métier ou au déploiement d'un équipement connecté. Le point de départ de la démarche doit consister en une réflexion sur les missions, les processus, les métiers, les organisations ou l'évolution des pratiques de travail, et non se limiter au déploiement d'un levier numérique pré-identifié. Les projets doivent être menés en associant les personnels concernés par la transformation ;

– *la transformation numérique des écosystèmes*. L'objectif est de permettre la mise en œuvre de politiques publiques au moyen de services numériques rassemblant les parties prenantes sur une même plateforme numérique. Les projets doivent prendre en compte l'évolution des pratiques numériques et des attentes des citoyens, agents, associations, entreprises (accessibilité des services numériques, démarches itératives de co-construction, respect des données personnelles, usages en mobilité, simplicité du langage administratif, etc. ;

– *la professionnalisation des filières numériques publiques*. L'objectif est d'attirer au sein des organisations publiques des experts du numérique ou de développer et faciliter la montée en compétences et la reconversion des professionnels déjà employés ;

– *l'extension territoriale des bonnes pratiques numériques visant à répliquer des projets et des solutions numériques mis en œuvre avec succès dans un service territorial de l'État ;*

– *la dématérialisation des démarches administratives*, dans un objectif de simplification de la vie quotidienne des citoyens.

Source : mission d'information

4. Une ambition de souveraineté qui implique des choix ambitieux

a. Faire du recours au logiciel libre un principe effectif au sein des administrations publiques

Le recours au logiciel libre au sein des administrations publiques doit être fortement encouragé et devenir un principe ne souffrant que d'exceptions dûment justifiées. Il s'agit, en effet, de réduire la part des solutions logicielles propriétaires, notamment non européennes, utilisées par défaut alors que des solutions alternatives ont fait la démonstration de leur utilité.

La défense de ce principe doit constituer, en effet, l'aboutissement de la politique menée en ce sens par l'État ces dernières années *via* :

– *l'instruction du Premier ministre du 19 septembre 2012***,** qui fixe les grandes orientations à suivre dans ce domaine. Le choix du logiciel libre y est considéré comme un choix raisonné devant la contrainte budgétaire croissante et la valorisation des compétences et de l'expertise professionnelle des équipes informatiques qui ne doivent pas être de simples acheteurs de solutions. Le logiciel libre, utilisé dans un contexte de développement agile, permet l'ajout de fonctions au fur et à mesure de la définition des besoins en rapport avec les utilisateurs, ce qui permet de procéder, d'une manière limitée, par « essais/erreurs ». Ce modèle nécessite également la mise en place d'une communauté de contributeurs et une approche modulaire, la constitution d'un réseau d'experts dans l'administration permettant de faire profiter l'ensemble des administrations des expertises ponctuelles nécessaires. Le logiciel libre n'étant pas synonyme de gratuité, il convient de veiller à assurer le contrôle des coûts de fonctionnement et de maintien de la performance dans le temps ;

– *l'article 16 de la loi du 7 octobre 2016 pour la République numérique* qui dispose que les administrations veillent à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information et encouragent l'utilisation des logiciels libres et des formats ouverts lors du développement, de l'achat ou de l'utilisation de tout ou partie des systèmes d'information ;

– *l'instruction du Premier ministre du 27 avril 2021 faisant de la politique de la donnée une priorité stratégique de l'État dans ses relations avec tous ses partenaires***,** qui insiste à nouveau sur le fait que cette ambition, outre le renforcement de l'ouverture des codes sources et des algorithmes publics, passe par l'usage du logiciel libre et ouvert. Lors de son audition, M. Stéfane Fermigier, co-président du conseil national du logiciel libre, s'il s'est réjoui de l'annonce par le Premier ministre de la création de la Mission « Logiciels libres » a regretté une situation contrastée quant à l'utilisation du logiciel libre dans l'administration : *« nous avons constaté des niveaux de maturité variables selon les administrations. Tout dépend des circonstances. Il suffit parfois d'un directeur des services informatiques (DSI) enthousiaste pour qu'une attitude proactive s'impose. Aujourd'hui, le constat s'impose que des ministères jusque-là fortement impliqués dans l'utilisation du logiciel libre semblent s'orienter vers d'autres solutions.*

Malgré la volonté de mettre en avant la notion de souveraineté, peut-être de manière trop abstraite, de plus en plus d'acteurs se tournent vers des fournisseurs de cloud *américains. Les contraintes qui en découlent risquent de contrecarrer à terme l'expansion des éditeurs de logiciels libres, mais aussi de l'industrie européenne du* cloud*. »* [(1)].

C'est dans cette optique que votre rapporteur souhaite faire du recours au logiciel libre une obligation au sein de l'administration, le recours aux solutions propriétaires devant devenir progressivement une exception.

Proposition n° 52 : Imposer au sein de l'administration le recours systématique au logiciel libre, en faisant de l'utilisation de solutions propriétaires une exception.

b. Privilégier le recours à des solutions numériques françaises et européennes au sein des administrations publiques

Dans le prolongement de cette idée, il convient également de privilégier, au sein des administrations, le recours systématique à des solutions numériques françaises, ou à défaut européennes, lorsque leur niveau de performance est satisfaisant pour les usages concernés.

Ce principe doit concerner l'ensemble des administrations publiques.

Proposition n° 53 : Imposer au sein de l'administration le recours systématique à des solutions numériques françaises, lorsque leur niveau de performance est satisfaisant pour les usages concernés.

c. Faire preuve de réalisme et de méthode pour mener à bien des projets dont le degré de complexité est souvent élevé

La gouvernance politique de la transformation numérique n'est pas simple à mettre en œuvre et nécessite une bonne compréhension de la contrainte technique qui la conditionne. L'exemple du *Health Data Hub* et des données de santé le démontre.

Une première difficulté tient aux conséquences « mécaniques » de la commande politique, lorsque celle-ci « fantasme » le pouvoir qu'aurait le politique d'imposer un calendrier technologique « ambitieux ».

Les acteurs auditionnés par la mission ont tous pointé les mêmes conséquences d'une approche de ce type :

– M. Dominique Pon, responsable ministériel du numérique en santé a souligné l'importance d'une commande politique techniquement avisée : *« S'agissant de la situation du Health Data Hub, je comprends que la commande politique donnée exigeait de construire une plateforme d'hébergement des données*

[1] *Audition de M. Stefane Fermigier, 1er juin 2021.*

de santé dans un cloud*, à très court terme et avec un niveau de sécurité très élevé. Cela signifie que, dans tous les cas, la commande politique court-termiste conduisait au choix d'un* cloud *qui n'était pas souverain. À l'état de l'art, compte tenu des délais et des exigences de sécurité donnés, il n'était pas possible de faire le choix d'un* cloud *souverain. »* (1) ;

– M. Nadi Bou Hanna, directeur interministériel du numérique a de même replacé la commande politique dans une confrontation avec la réalité du marché : *« le projet du Health Data Hub revêt un enjeu politique majeur et affichait un échéancier non négociable. Lorsque ce projet a été lancé, la seule plateforme qui était techniquement compatible avec l'ambition du projet, tel que cela a été analysé par le ministère de la santé, était celle de Microsoft. (…) Sur un projet de cette nature, nous n'allons dégrader ni le besoin client, ni la promesse politique. (…) Il n'y a pas de dogme s'agissant du Health Data Hub – il y a simplement un constat de réalité. Le souhait de l'ensemble des parties est que de nouvelles offres d'hébergement puissent émerger, qui remontent les couches, c'est-à-dire qui ne se contentent pas du niveau le plus bas (l'infrastructure) mais qui soient capables de remonter au niveau de la plateforme et des services à valeur ajoutée. »* (2) ;

– Mme Stéphanie Combes, directrice du groupement d'intérêt public dit *Health Data Hub*, a insisté sur le fait que, compte tenu des exigences de sécurité, de performance et de délai fixés par la commande politique, la solution du logiciel Azure de Microsoft était la seule à répondre à toutes ces exigences. *« Les acteurs français ne proposaient pas les fonctionnalités dont nous avions besoin. Si nous avions publié un marché public, Microsoft y aurait répondu et Microsoft l'aurait remporté. S'agissant du choix des partenaires technologiques, j'ai d'abord pensé à TeraLab et au centre d'accès sécurisé aux données (CASD) qui sont les acteurs de la statistique publique. Nous nous sommes tournés vers les solutions américaines très tardivement. Nous avons élargi nos recherches, lorsque nous nous sommes rendus compte que les acteurs n'étaient pas en mesure de répondre à notre cahier des charges. Nous avions un vrai problème si nous n'étions pas capables de mettre en place une plateforme de* data science *en santé avec des outils sur étagère. En fin de course seulement donc, nous avons commencé à interroger Microsoft, AWS et Google Platform. »* (3).

Après avoir insisté sur la considération selon laquelle *« Le HDH n'est qu'une surcouche. Les données de santé des Français ne sont, à 99 %, pas dans le HDH aujourd'hui. Elles sont stockées dans les* data centers *des différents hôpitaux, des laboratoires qui sont pour la plupart hébergés chez des Français »*, M. Cédric O, secrétaire d'État chargé de la transition numérique et des communications électroniques a insisté sur l'objectif poursuivi consistant, à la fois, dans la création de champions de la santé numérique et dans l'amélioration de la santé des Français : *« Cette décision a été prise dans le cadre de la présentation par le Président de la*

---

[1] Audition de M. Dominique Pon, 4 mars 2021.

[2] Audition de M. Nadi Bou Hanna, 21 janvier 2021.

[3] Audition de Mme Stéphanie Combes, 18 février 2021.

République du plan sur l'Intelligence artificielle en mars 2018. Elle a donné lieu à la consultation de dix-neuf entreprises sur l'outil mis à la disposition du HDH. La seule entreprise qui répondait début 2019 aux critères techniques de performance, de capacité à développer ces algorithmes, était Microsoft. Il a alors été décidé de démarrer tout de suite avec Microsoft une phase expérimentale de développement, parce que cette société était en avance dans le domaine de l'Intelligence artificielle. D'ailleurs, si vous discutez aujourd'hui avec les entreprises de l'Intelligence artificielle, elles vous feront toutes part de l'extrême avance des groupes américains » [(1)].

Votre rapporteur tient toutefois à présenter ici quelques remarques concernant la conception et la mise en œuvre du *Health Data Hub*. Il a en effet pu noter, à l'issue des entretiens et auditions qu'il a pu mener sur le sujet, que la construction du *Health Data Hub* s'est objectivement opérée sans tenir compte des solutions existantes, qui auraient pu être des modèles, et contre l'avis des autres co-concepteurs du projet ; que la réversibilité du système n'a pas été prévue à l'origine et que s'est manifestée une volonté assumée de continuer avec Microsoft, même contre les engagements des ministres, ce qui pose un réel problème de gouvernance. Voilà qui, selon votre rapporteur, peut engendrer à terme un problème de confiance des citoyens, vis-à-vis des conditions de protection et d'utilisation de leurs données de santé.

Une seconde difficulté au sein de ce type de projets peut tenir à la qualité de la donnée, qui est un enjeu décisif pour faciliter la réussite des projets numériques actuels et à venir avec le développement de l'Intelligence artificielle.

La capacité d'homogénéiser la donnée et de s'assurer de sa mise en forme, indispensable pour son traitement, est un sujet majeur comme l'avait déjà relevé le rapport remis au premier ministre, le 23 décembre 2020, par notre collègue M. Éric Bothorel sur la politique publique de la donnée, des algorithmes et des codes sources. Ce constat est partagé par le Pr Marc Cuggia, professeur des universités, praticien hospitalier au centre hospitalier universitaire de Rennes : *« nous sommes confrontés à des problématiques très complexes de qualité de données. En France, notre système de données de santé est extrêmement fractionné : aucun système d'information ne ressemble à un autre. L'enjeu de collecter les données et de les harmoniser est essentiel, et implique tout un panel d'acteurs. Cela implique des actions tout au long de la chaîne de production de données et d'expertise. C'est tout l'enjeu des centres de données cliniques. »* [(2)].

Le Dr Laurent Treluyer, directeur des systèmes d'information de l'Assistance publique-Hôpitaux de Paris (AP-HP), est aussi revenu sur ce point lors de son audition : *« il existe une notion de proximité s'agissant des données. Nous constatons tous la difficulté de mettre ensemble des données d'origines diverses*

---

[1] Audition de M. Cédric O, 22 octobre 2020.

[2] Audition du Pr Marc Cuggia, 18 février 2021.

dans un monde peu standardisé et non normalisé. Il est illusoire de rassembler dans un même entrepôt de données de santé, par exemple, l'ensemble des données de biologie et de vouloir en tirer de la valeur. Nous avons donc souhaité mettre en place la proximité avec la donnée et la proximité des outils avec nos chercheurs. » [(1)].

Une même démarche d'application de l'Intelligence artificielle pourra donc justifier des choix techniques différents en fonction des spécificités à prendre en compte pour la réussite à long terme du projet.

Le pilotage des projets de transformation numérique d'ampleur implique de suivre plusieurs principes, qui ont été résumés à votre rapporteur par Mme Élisa Salamanca, responsable du département web, Innovation, Données de la direction des systèmes d'information de l'Assistance publique-Hôpitaux de Paris (AP-HP)[(2)].

Il convient d'abord de **bien distinguer les différents cas d'usage**. Dans le cas de la construction d'un entrepôt de données médicales, il s'agit de la mise à disposition des données à des fins de recherche, de l'utilisation des données médicales pour piloter l'activité hospitalière et de la réutilisation des données pour l'innovation numérique.

Il convient ensuite de **refuser les *a priori* restreignant les marges de choix organisationnels ou techniques.** Par exemple**,** le choix de l'*open source* pour l'entrepôt de données résulte à la fois du constat de l'absence d'outil sur étagère et de ses avantages propres, tenant à l'existence d'une très grande communauté et à la garantie d'indépendance. Mais *« si d'excellents outils étaient mis sur le marché et qu'il était plus simple et moins coûteux de recourir à des logiciels sur étagère, nous le ferions. »* [(3)]. Ainsi, un outil existant sur le marché pour le pilotage de l'activité hospitalière a été retenu pour des motifs de rapport coûts/efficacité. Une même démarche vaut pour **la question du choix de l'infrastructure *on premise* ou en *cloud*.** La première considération expliquant le choix d'une infrastructure sur site tient aux préoccupations exprimées par les contributeurs à la donnée – la communauté médicale – en ce qui concerne la maîtrise de celle-ci et le transfert de données médicales à des tiers. La seconde considération tient à l'absence de besoin technique de recourir à des infrastructures de *cloud* extérieures, compte tenu de la puissance de calcul actuellement nécessaire. Mais le pragmatisme prévaut également en ce domaine : *« pour le moment, notre infrastructure supporte la charge de nos besoins en matière de puissance de calcul. Nous savons cependant que nous devrons faire face, à l'avenir, à des puissances de calcul supplémentaires auxquelles nous ne pourrons pas répondre. Il n'y a pas d'opposition au* cloud *de notre part. Nous sommes face à un vrai sujet technique. Nous menons actuellement*

---

[1] *Audition du Dr Laurent Treluyer, 4 mars 2021.*

[2] *Audition de Mme Elisa Salamanca, 4 mars 2021.*

[3] *Audition du Dr Laurent Treluyer, 4 mars 2021.*

des projets pilotes, des expérimentations et des collaborations avec différents fournisseurs de cloud *»* [1].

Il convient enfin de **penser la complémentarité des activités**. Le Pr Marc Cuggia a ainsi souligné le large partage d'expérience réalisé par le Ouest Data Hub avec les autres établissements en ce qui concerne la structuration des entrepôts de données, la qualité, la protection, la gouvernance et les usages : *« cela crée un effet d'entraînement national très important, qui se traduit par la mise en place d'entrepôts de données dans la plupart des CHU de France et dans les centres de lutte contre le cancer, ainsi que par la création d'équipes spécialisées dans ces domaines. »* [2].

Il est enfin souhaitable de veiller au respect d'un ensemble de prérequis au sein des projets numériques dont :

– l'intégration de la cybersécurité le plus en amont possible des choix de développement (principe de *security by design* et de *privacy by design*) ;

– la création et du maintien d'un lien de confiance avec les parties prenantes : la chaîne de confiance est fondamentale pour exploiter des données produites par différents services d'hôpitaux de manière transversale ;

– l'impératif de disposer de multiples compétences humaines au niveau requis. Le Pr Marc Cuggia y a insisté à partir de l'expérience du Ouest Data Hub : *« l'infrastructure ne fera pas l'innovation. L'enjeu principal réside dans le potentiel humain de formation et d'interdisciplinarité sur le terrain qui nous permettra d'avoir collectivement une chance de développer une souveraineté sur les enjeux du numérique en santé »* [3]. Il en a été de même de la part du Dr Laurent Treluyer, à partir de l'expérience de l'AP-HP : *« il s'agit de valoriser les activités d'un CHU avec toutes ses compétences : à la fois les compétences informatiques, de* data scientists*, de valorisation de la donnée et les compétences en recherche clinique. L'AP-HP réunit des personnes qui produisent de la donnée et des chercheurs cliniques. Cette confrontation permanente, qui s'incarne dans la notion de campus, crée de la valeur. »* [4].

Une démarche pragmatique de ce type peut manifestement trouver des champs d'application au-delà du seul domaine de la santé. Comme Mme Laurence Jay-Passot, déléguée générale du groupement de coopération sanitaire des hôpitaux universitaires du Grand Ouest (HUGO) l'a souligné : *« Le modèle de hub est absolument reproductible dans d'autres domaines, si on le conçoit comme un dispositif qui permet de mutualiser uniquement ce qui doit l'être et que l'on arrive à penser des systèmes de gouvernance agiles, qui continuent à s'appuyer sur toutes les compétences disponibles dans les centres locaux. Nous y croyons très fortement. Il existe plusieurs sujets – et les données massives en santé*

---

[1] *Audition du Dr Laurent Trelayer, 4 mars 2021.*

[2] *Audition du pr Marc Cuggia, 18 février 2021.*

[3] *Audition du dr Marc Cuggia, 18 février 2021.*

[4] *Audition du Dr Laurent Treluyer, 4 mars 2021.*

en sont un – pour lesquels le modèle de hub sera pertinent, s'il est dupliqué à l'échelle interrégionale sur l'ensemble du territoire. » [1].

Le Pr Marc Cuggia en a apporté la confirmation : *« ces réflexions dépassent les données de santé stricto sensu et s'appliquent également à des projets mettant en œuvre des approches similaires, en lien avec les citoyens. Je citerai trois expériences auxquelles nous sommes associés. D'abord, Rennes Métropole travaille à mettre au point un portail des données personnelles qui vise à exploiter les données de transport, d'énergie, de santé à des fins de recherche et d'innovation. Une réflexion de* hub *pourrait être mise en place à ces fins. Ensuite, l'université de Sherbrooke au Québec a mis en place un projet similaire de système d'information apprenant ; le projet Pulsar de l'université de Laval, enfin, fait le lien entre les données de santé et les données de territoires. Des projets d'innovation très importants existent donc, qui ont un lien très fort avec les citoyens. »* [2].

C. UNE CAPACITÉ D'ANTICIPATION À CONSOLIDER POUR ASSURER NOTRE AUTONOMIE STRATÉGIQUE

Les auditions indiquent que plusieurs segments technologiques doivent être au cœur des financements publics ces prochaines années. Les technologies de l'Intelligence artificielle, du *cloud*, de la *blockchain* ou encore de la cybersécurité sont, et seront encore davantage critiques dans les prochaines années, de même que celles de l'informatique quantique et les enjeux spatiaux. Des actions spécifiques sont prévues dans chacun de ces domaines, par l'intermédiaire de plans stratégiques et de financements dédiés.

C'est dans ce cadre que s'inscrivent les stratégies d'accélération mises en œuvre par le Gouvernement au sein du programme d'investissements d'avenir n° 4 et dans le cadre du plan de relance, comme l'a rappelé M. Thomas Courbe : « *Sur cette capacité à maîtriser la technologie comme un deuxième axe de la souveraineté numérique, toutes ces actions irriguent très fortement le plan de relance, et notamment son volet de soutien à l'innovation. Ce sera en particulier le cas pour tout ce qui sera financé dans le cadre du PIA, intégré dans ce plan de relance. Un certain nombre des stratégies que j'ai évoquées sur certaines de ces technologies seront soutenues par le plan de relance, y compris dans un cadre européen pour la plupart d'entre elles. Nous souhaitons, dans le cadre européen, promouvoir des Important Projects of Common European Interest (IPCEI). Les IPCEI sont ces nouveaux cadres d'action européens dérogatoires des régimes habituels d'aides d'État, expérimentés sur les batteries par exemple. Dans le domaine des batteries, ils ont finalement montré que l'on pouvait réintroduire une industrie nouvelle pour l'Europe. Nous voulons appliquer ces régimes sur le* cloud *et sur la microélectronique dans les prochains mois avec la Commission européenne, notamment dans le cadre d'un dialogue approfondi avec l'Allemagne »* [3].

---

[1] *Audition de Mme Laurence Jay-Passot, 18 février 2021.*

[2] *Audition du Pr Marc Cuggia, 18 février 2021.*

[3] *Audition de M. Thomas Courbe, 8 octobre 2020.*

Le programme d'investissements d'avenir (PIA)

Le programme d'investissements d'anir a été créé en 2010, à la suite de la remise du rapport Juppé-Rocard de 2009, qui insistait sur la nécessité pour la France de se doter d'un instrument de financement des secteurs et technologies critiques pour son économie sur le temps long.

Ce programme est piloté par le secrétariat général pour l'investissement (SGPI), placé sous la tutelle du Premier ministre.

Son objectif est de soutenir l'innovation et de permettre à la France d'augmenter son potentiel de croissance et d'emplois.

Trois programmes d'investissements d'avenir ont été lancés en 2010 (PIA 1 – 35 milliards d'euros), 2014 (PIA 2 – 12 milliards d'euros), et 2017 (PIA 3 – 10 milliards d'euros) dans ce but.

Dans le cadre de la crise sanitaire, et pour prolonger cet effort d'investissement, un programme d'investissements d'avenir n° 4 a été intégré au sein du projet de loi de finances pour 2021. Ses crédits viendront compléter et parfois soutenir les actions du plan de relance.

Doté d'une enveloppe de 20 milliards d'euros, dont 11 milliards d'euros intégrés au plan *France relance*, le PIA 4 soutient notamment la mise en œuvre de stratégies d'accélération dans des domaines critiques et l'approfondissement du marché du capital-risque français.

Source : Secrétariat général pour l'investissement (SGPI)

Votre rapporteur souhaite évoquer ici la situation de ces différents segments technologiques dont le soutien par la puissance publique est indispensable pour permettre à la France et à l'Europe de rester « dans la course technologique ».

1. La *blockchain*

Le développement de la technologie de la *blockchain* et de ses cas d'usage doit être une priorité pour la politique industrielle et technologique française

M. Rémy Ozcan, président de la fédération française des professionnels de la *blockchain* (FFPB) a rappelé le principe de cette technologie, qui consiste à attribuer « *à chaque produit une empreinte numérique unique, inscrite dans le registre partagé par tous les membres validateurs du réseau, lequel sollicitera la totalité du registre à chaque inscription d'une nouvelle information* » [(1)]. Le rapport de la mission parlementaire d'information, consacré à cette thématique et publié en 2018, définit cette technologie comme « *un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y*

[1] *Audition de M. Rémy Ozcan, 22 avril 2021.*

inscrire des données, selon les règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie » [(1)].

Pour M. Rémy Ozcan, les spécificités de la *blockchain* sont au nombre de cinq : la cryptographie, la signature électronique, le registre distribué, l'utilisation d'Internet et un système de « tokenisation ».

La *blockchain* présente des avantages évidents. Elle apparaît « *comme le moyen le plus rapide, fiable et sécurisé de transférer des actifs ou des données partout dans le monde* » et surtout « *par rapport à d'autres technologies existantes, la blockchain présente l'avantage de garantir l'intégrité des données et des informations inscrites dans son registre, du fait de ses composants intrinsèques : la cryptographie, la signature électronique, la distribution du registre, la décentralisation des validations* » [(2)].

Les cas d'usage possibles sont extrêmement variés (exemples : certifier des diplômes, des factures d'électronique, se financer par des émissions d'actifs numériques (*Initial Coin Offering, ou ICO*) etc.). Nombre d'usages apparaîtront, en outre, au fur et à mesure du développement de cette technologie.

La valorisation de ces cas d'usage nécessite néanmoins **d'octroyer une force probante à la *blockchain* en droit,** sans laquelle certains acteurs peuvent hésiter à recourir à cette technologie pour des raisons de sécurité juridique. Votre rapporteur souhaite donc porter à nouveau cette proposition, qui avait déjà fait l'objet de débats dans les travaux préparatoires de la loi relative à la croissance et la transformation des entreprises du 22 mai 2019 (loi PACTE).

Proposition n° 54 : Garantir en droit la force probante de la *blockchain* pour créer un cadre favorable au développement de cette technologie.

Dans cette optique, il serait également utile de **créer un système de certification des *blockchains***. Il est en effet nécessaire de s'accorder sur des critères pour garantir l'incorruptibilité du système. Toutes les *blockchains* ne peuvent, en l'état actuel de la technologie, être considérées comme ayant une force probante [(3)], ainsi que l'a relevé Mme Liliane Dedryver, directrice de projets au sein de la direction générale des entreprises[(4)]. La situation est en effet variable d'une *blockchain* à l'autre et doit être appréciée au cas par cas. L'établissement d'une certification, à l'échelon national, puis européen, fondée sur des critères prédéfinis est donc indispensable. La création d'un système de certification figurait d'ailleurs parmi les quatorze propositions du rapport de mission produit conjointement par le

---

[1] Assemblée nationale, rapport d'information sur les chaînes de bloc (blockchains), présenté par Mme Laure de La Raudière et M. Jean-Michel Mis, n° 1501 du 12 décembre 2018.

[2] Audition de M. Rémy Ozcan, 22 avril 2021.

[3] Audition de Mme Liliane Dedryver, 29 avril 2021.

[4] Audition de Mme Liliane Dedryver, 29 avril 2021.

CEA (Commissariat à l'énergie atomique et aux énergies alternatives), l'IMT (Institut Mines-Télécom) et l'Inria, très récemment, sur le sujet [1].

Proposition n° 55 : Lancer une réflexion sur la création d'un système de certification des blockchains conformément à la recommandation n° 7 du rapport IMT-CEA-INRIA « Les verrous technologiques des blockchains » publié en avril 2021.

Enfin, afin de sécuriser la filière, il serait nécessaire de pérenniser l'effort d'accompagnement et de financement entrepris, notamment par l'intermédiaire de la Task force *blockchain*.

2. L'Intelligence artificielle

L'Intelligence artificielle est une technologie numérique qui peut être définie comme la capacité, pour des systèmes, de faire preuve *« d'un comportement intelligent en analysant leur environnement et en prenant des mesures, avec un certain degré d'autonomie, pour atteindre des objectifs spécifiques »*. Son fonctionnement repose sur l'utilisation d'algorithmes entraînés à partir de jeux de données et capables de prendre, dans une certaine mesure, les décisions les plus efficaces en fonction de l'apprentissage réalisé.

Cette technologie, profondément transversale, modifiera en profondeur l'ensemble des activités humaines, au profit d'une automatisation plus forte, et d'une efficacité plus importante. Elle devrait en effet transformer toutes les activités économiques, en étant d'ailleurs « embarquée » de façon croissante directement au sein des objets, matériels et véhicules concernés. Comme l'a rappelé M. Renaud Vedel, préfet, et coordinateur de la stratégie nationale pour l'Intelligence artificielle, « *l'Intelligence artificielle est utilisée dans les traitements de signaux de l'industrie, du langage naturel, de la vision de l'image par ordinateur, de données de grandes dimensions, ainsi que dans la robotique. Il apparaît que la matrice de l'IA est à même de réaliser de plus en plus de tâches. Le fait qu'une machine, un robot ou un logiciel devienne capable de voir ou d'entendre va nécessairement changer notre rapport à l'autonomie* » [2].

Ses usages seront donc extrêmement variés. Cet enjeu a été résumé ainsi par M. Francesco Bonfiglio, directeur de l'initiative Gaia X : « *Il s'agit en réalité du domaine des domaines* […] *dans les prochaines années, nous serons submergés de services reposant principalement sur l'Intelligence artificielle* », avant d'insister sur le fait qu'au « *même titre que la plomberie transporte l'eau, l'Intelligence artificielle a besoin de données, et surtout de données de qualité* » [3]. Ce constat est partagé par M. Michel Gesquiere, responsable des ventes d'IBM : « *Le champ*

---

[1] *CEA, IMT et Inria, « Blockchain : 14 recommendations pour lever les verrous technologiques et techniques existantes », 25 mai 2021.*

[2] *Audition de M. Renaud Vedel, 6 mai 2021.*

[3] *Audition de M. Francesco Bonfiglio, 22 avril 2021.*

d'application de l'Intelligence artificielle s'accroîtra considérablement également dans les années à venir. Elle a déjà été déployée dans le domaine de l'expérience « client ». Elle servira aussi d'assistant pour accroître la performance des employés : c'est en ce sens qu'elle est envisagée dans notre partenariat avec le Crédit Mutuel. L'automatisation des processus industriels passera également par l'Intelligence artificielle. Avec l'IOT et la 5G, le nombre des données s'accroîtra et l'Intelligence artificielle permettra de les transformer en éléments de compétitivité et d'automatisation des performances » [(1)]. Pour prendre l'exemple d'un secteur d'activité traditionnel, l'agriculture, l'IA embarquée permettra ainsi, comme l'a souligné M**.** Thierry Tingaud, président du comité stratégique de filière « Industries électroniques » de développer une agriculture sélective : « *Une caméra serait installée sur un tracteur, avec de l'Intelligence artificielle embarquée, afin de savoir s'il est nécessaire de traiter ou non un pied de vigne. Soit l'agriculteur descend de son tracteur et regarde si le pied de vigne nécessite un traitement, soit cette analyse est réalisée automatiquement, via une caméra, par des logiciels d'Intelligence artificielle déterminant s'il faut déverser ou non de l'engrais ou des produits phytosanitaires. Cela constitue un bon exemple de ce qu'est l'Intelligence artificielle embarquée. Dans ce domaine, le champ d'application est infini. Cette Intelligence artificielle doit bien sûr être raisonnable et suivre les directions données par les rapports de la Commission européenne dans ce domaine* » [(2)].

Les industriels auditionnés, notamment ceux qui appartiennent à la filière des industries électroniques, entendent se positionner fortement sur l'IA embarquée et proposer à leurs clients des capacités d'Intelligence artificielle décentralisée conformes à leurs besoins. L'un des axes du contrat de filière « Industries électroniques » porte ainsi sur l'IA décentralisée, également appelée « *Edge computing* ». Les membres de cette filière souhaitent en effet progresser dans cette direction, comme l'a indiqué M. Thierry Tingaud, « *notamment avec les programmes d'accélération sur l'Intelligence artificielle actuellement élaborés avec la direction générale des entreprises (DGE), dans le but de pousser l'écosystème français et les coopérations nécessaires, à la fois au niveau du hardware (les algorithmes logiciels avec le CEA-List, l'Institut national de recherche en informatique et en automatique [INRIA] ou d'autres organismes) et les acteurs finaux que sont les utilisateurs de l'Intelligence artificielle* » [(3)].

Face au caractère révolutionnaire de cette technologie, la France et l'Europe doivent investir massivement et définir un cadre réglementaire permettant de défendre leur modèle éthique et politique.

L'Intelligence artificielle est en effet un domaine critique en matière de souveraineté numérique. Sa maîtrise constitue d'ailleurs l'un des éléments fondamentaux de la compétition économique et technologique que se livrent la Chine et les États-Unis. Comme l'a rappelé M. Julien Nocetti, cette question a

---

[1] *Audition de M. Michel Gesquiere, 9 mars 2021.*

[2] *Audition de M. Thierry Tingaud, 8 octobre 2020.*

[3] *Idem.*

suscité en effet des tensions entre ces deux pays : « *À l'origine, ce sont surtout les enjeux de propriété intellectuelle et de cybersécurité qui caractérisaient ces tensions. L'Intelligence artificielle s'est ensuite retrouvée au cœur de la rivalité sino-américaine, au point de cristalliser un certain nombre de peurs – notamment de déclassement – chez les Américains, eu égard à la montée en puissance de la Chine. Plus récemment, le dossier de la 5G a provoqué un regain de tensions entre les deux acteurs, avec notamment les performances internationales de la société Huawei* » (1). C'est pour cette raison, comme l'a rappelé M. Renaud Vedel, préfet, et coordinateur de la stratégie nationale pour l'Intelligence artificielle, que les États-Unis ont mis en place dès 2008 un plan technologie intitulé « Rester les meilleurs » afin de répondre aux ambitions du plan IA chinois décidé en 2007 et qui devait faire de ce pays un leader en Intelligence artificielle à l'horizon 2030 (2).

Cette criticité de l'IA s'explique par le fait que seuls les acteurs les plus puissants imposent toujours en partie leur modèle et de leurs valeurs, comme l'a rappelé M. Werner Stengg, membre du cabinet de Mme Margrethe Vestager : « *pour un dossier clé tel que l'Intelligence artificielle* [, si] *nous n'arrivons pas à devenir un acteur important dans son développement, il sera difficile de nous assurer que nos valeurs soient mises en avant. En étant seulement consommateurs de cette technologie, il sera en effet compliqué de refuser de l'utiliser si des éléments ne nous conviennent pas. Nous devons être forts et indépendants. Ce n'est pas une question de protectionnisme, mais d'indépendance et de compétitivité de notre industrie* » (3). Ce sont en effet les acteurs à l'origine de l'émergence de nouveaux usages qui définiront assez fortement la dynamique normative dans ce domaine. Il faut donc que la France et l'Europe soit en pointe afin d'être en capacité de défendre leur modèle de valeurs et leur conception du numérique.

La maîtrise du développement des usages de l'Intelligence artificielle, dans le domaine de la santé, par exemple, est critique comme l'a rappelé Mme Stéphanie Combes, directrice du *Health Data Hub* : « *J'ai une seconde crainte. J'entends beaucoup parler du* cloud *et de Microsoft, mais je n'entends pas beaucoup parler de la souveraineté des usages numériques de santé. Dans certains autres pays, et notamment aux États-Unis, ces questions avancent très vite. En mai 2018, le dispositif médical pour les examens de fond d'œil était le premier dispositif médical intégrant l'Intelligence artificielle à être autorisé par la Food and Drug Administration (FDA). Cela a constitué une très belle avancée et depuis, une trentaine d'autres dispositifs médicaux ont été autorisés par la FDA. Nous téléchargerons bientôt toutes ces applications sur nos téléphones, car elles proposeront des usages de santé extrêmement intéressants et performants ; mais elles n'auront pas été construites grâce à des données de patients français et l'on ne saura même pas si elles ont été développées dans le respect du Règlement général sur la protection des données (RGPD). Il faut donc garder en tête les questions sur la souveraineté des usages, afin de ne pas nous retrouver dans cinq ans à discuter*

---

[1] *Audition de M. Julien Nocetti, 11 mars 2021.*

[2] *Audition de M. Renaud Vedel, 6 mai 2021.*

[3] *Audition de M. Werner Stengg, 19 décembre 2020.*

de ces mêmes sujets car nous aurons pris du retard par rapport à d'autres acteurs. Il faut donc procéder à des arbitrages en ayant bien en tête tous les enjeux ayant cours au même moment. Cela n'est pas simple » [(1)]. Votre rapporteur partage ce point de vue et estime que la « souveraineté des usages » doit être un axe de réflexion pour les politiques numériques.

La situation de l'Europe en matière de maîtrise de l'Intelligence artificielle peut être résumée de la façon suivante : le retard pris sur l'IA appliqué aux données personnelles sera difficile à rattraper, mais il existe en revanche des opportunités pour l'Europe sur d'autres segments de l'IA, en particulier concernant le *B to B* et la santé. C'est le sens des propos tenus par le secrétaire d'État au numérique lors de son audition : « *Je considère en revanche que nous avons, pour longtemps, perdu le match de l'Intelligence artificielle appliquée aux données personnelles et aux consommateurs. Les bases de données constituées par les très grandes entreprises américaines ou chinoises, exponentiellement grandissantes, font que l'écart s'accroît chaque jour. Il existe des domaines dans lesquels nous pouvons toutefois encore jouer, et même dans lesquels nous pouvons être parmi les meilleurs du monde. Cela concerne notamment les données industrielles et l'intelligence artificielle appliquée à certains secteurs du commerce interentreprises* (B to B)*, tels que les domaines de la santé, des transports, de l'environnement, de l'énergie, de la cybersécurité. Partout où le savoir-faire français est extrêmement fort, avec des très grandes entreprises françaises et des lacs de données à la bonne taille, nous sommes capables de créer des savoir-faire parmi les meilleurs du monde parce que nous avons l'une des meilleures écoles du monde en mathématiques et en informatique »* [(2)].

Il existe également **des marges de positionnement dans le domaine de l'Intelligence artificielle de confiance** comme l'a relevé le directeur général des entreprises M. Thomas Courbe : *« La deuxième orientation sur l'Intelligence artificielle porte sur l'Intelligence artificielle de confiance. Nous voyons bien que le numérique crée des sujets assez nouveaux dans la relation de confiance, à la fois pour les entreprises et pour les citoyens. Je crois qu'il s'agit de l'un des objets de votre mission. Nous avons engagé un grand défi d'innovation de rupture sur la manière dont on peut certifier les algorithmes d'Intelligence artificielle. Le but de cette certification est d'apporter un modèle de confiance, à la fois pour les entreprises et pour les citoyens. Il s'agirait d'une manière de garantir le fonctionnement de ces algorithmes. De notre point de vue, cela constitue aussi un élément de différenciation pour la production d'Intelligence artificielle en Europe, par rapport à d'autres acteurs moins sensibles à ces questions de priorités de confiance »* [(3)]. Ces possibilités doivent être pleinement exploitées.

---

[1] *Audition de Mme Stéphanie Combes, 18 février 2021.*

[2] *Audition de M. Cédric O, 22 décembre 2020.*

[3] *Audition de M. Thomas Courbe, 8 octobre 2020.*

Votre rapporteur observe que **plusieurs initiatives** ont été mises en œuvre au niveau national et européen par les pouvoirs publics pour soutenir un effort d'investissement élevé dans le domaine de l'Intelligence artificielle.

En France, d'abord, une stratégie nationale pour l'Intelligence artificielle, a été présentée par le Président de la République le 29 mars 2018, en prenant appui sur le rapport publié sur ce sujet par notre collègue, M. Cédric Villani. Cette stratégie fixe comme objectif de faire de la France l'un des pays leaders dans ce domaine. Elle s'articule autour de quatre axes concernant respectivement la nécessité de conforter, en France et en Europe, l'écosystème de l'IA (1), le besoin d'engager une politique volontaire d'ouverture des données (2), la volonté d'adapter le cadre réglementaire et financier national et européen sur cette technologie (3) et, enfin le souhait de traiter les enjeux politiques et éthiques de l'IA (4). Elle repose sur un effort d'investissement important de 1,5 milliard d'euros sur la période 2018-2022.

Cette stratégie nationale a permis et doit permettre à la France de renforcer sa capacité de calcul comme le montre la création du supercalculateur Jean ZAY pour GENCI (Grand équipement national de calcul intensif). M. Renaud Vedel a indiqué, en outre, que les autres initiatives de soutien aux technologies numériques allaient participer de cette dynamique IA. On peut citer, par exemple, « *le* cloud *d'État, la filière microélectronique dans le cadre d'un IPCE, projet commun européen, ou les travaux originaires d'Allemagne et désormais européanisés, de GAIA-X, offrant une filière européenne au calcul de haute performance* ». Selon M. Vedel, en outre, l'enjeu majeur des années à venir consistera à embrasser le développement de l'Internet des objets. Il estime en effet à 80 % la part de la puissance de calcul qui sera distribuée en périphérie » [(1)].

Au niveau européen, de nombreux travaux ont également été conduits, comme l'a rappelé Mme Lorena Boix-Alonso, directrice chargée de la stratégie et de la diffusion des politiques à la Direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne : « *Au niveau de l'Intelligence artificielle, comme vous l'avez mentionné, des travaux ont été faits. Nous avons créé un groupe de haut niveau pour développer des directives sur les principes éthiques de l'Intelligence artificielle. Ce travail sera pris en compte par la Commission européenne lorsque, l'année prochaine, nous proposerons un cadre réglementaire. Il est très important de trouver un équilibre avec nos valeurs et principes éthiques européens pour ne pas freiner l'innovation. La Commission cherche à garder cet équilibre et je pense que nous avons fait preuve par le passé de notre capacité à apporter des propositions réglementaires pour le maintenir. C'est d'ailleurs pour cette raison que nous sommes copiés par d'autres pays. L'année passée, nous avons proposé la première réglementation sur les plateformes, qui concernait d'autres domaines. Elle a été imitée par la Corée et le Japon. Compte tenu de l'impact que peut avoir l'Intelligence artificielle sur nos démocraties et nos droits fondamentaux, nous espérons pouvoir devenir un exemple*

[1] *Audition de M. Renaud Vedel, 6 mai 2021.*

au niveau international » [1]. Un cadre réglementaire spécifique dédié à l'intelligence artificielle a été présenté par la Commission européenne en 2021 (*infra*).

Enfin, à l'échelle internationale, la France et le Canada ont lancé en 2020 un partenariat mondial sur l'Intelligence artificielle (PMIA) dont l'objet est d'encourager le développement d'une Intelligence artificielle responsable fondée sur les principes du respect des droits de l'Homme, de l'inclusion, de la diversité, de l'innovation et de la croissance économique.

Votre rapporteur salue ces initiatives et souhaite formuler plusieurs remarques à ce sujet.

D'abord, **la crise sanitaire n'a eu qu'un impact limité sur la montée en puissance des instituts 3IA déployés en France dans le cadre de cette stratégie**. Il se réjouit donc de cette situation et souhaite insister sur la formation de nœuds de second rang au sein du maillage prévu sur le territoire national.

La crise sanitaire n'a pas non plus découragé l'investissement dans les start-up technologiques comme l'a précisé M. Renaud Vedel : « *La crise sanitaire a produit divers effets hétérogènes mais aussi bien dans le domaine du numérique que celui de l'IA plus spécifiquement, elle n'a pas été un obstacle majeur produisant un ralentissement. Par exemple, les importants investissements dans les start-up en France en attestent, avec cinq milliards de dollars investis en France, bien qu'il soit difficile d'isoler le sujet de l'IA des autres technologies du numérique. À l'échelle européenne, la position de la France est bonne, bien que Londres demeure de loin le principal centre de compétences. Pour autant, Paris constitue le premier écosystème en Union européenne* » [2]. **Le risque identifié de sous-investissement dans l'IA [3] ne s'est donc pas matérialisé**. L'action de soutien à la diffusion de l'IA dans l'économie, mise en œuvre par Bpifrance *via* le plan deeptech, ou encore grâce aux challenges d'IA, et aux Grands Défis prévus dans le cadre du programme d'investissements d'avenir est à la hauteur des enjeux.

Un point de vigilance demeure en revanche sur **le risque de fuite des talents puisque** « *du point de vue des profils rares, une compétition intense a lieu, incluant des acteurs puissants qui profitent de ce que d'autres rencontrent des difficultés conjoncturelles, pour recruter les ressources* ». Cette difficulté se retrouve dans la plupart des domaines à fort potentiel technologique. Sur ce sujet, M. Renaud Vedel a fait valoir qu'en réponse à la crise « *le plan de relance, dans son volet portant sur la recherche privée, permet la mise à disposition de chercheurs privés pour les laboratoires publics, avec une prise en charge de 80 % par l'État* » en ajoutant que l'État cherche en outre à protéger la génération des chercheurs en IA *« en offrant la*

---

[1] *Audition de Mme Lorena Boix-Alonso, 19 novembre 2020.*

[2] *Audition de M. Renaud Vedel, 6 mai 2021.*

[3] *Ainsi que l'a expliqué M. Renaud Vedel :* « Les systèmes d'IA étant encore des technologies en voie de maturation, les grands industriels, comme les *start-up* réalisant de la R&D, peuvent mener des arbitrages entre le court et le long terme, et ainsi juger que l'IA n'offre pas de retour sur investissement immédiat ».

possibilité d'un accueil temporaire dans les laboratoires publics pour des projets de recherche avec un contrat de travail qui, au bout de deux ans, sera pris en charge par une entreprise, ou entrera dans un financement de post-doctorat » [1].

Votre rapporteur souhaite également insister **sur le fait que la France et l'Europe disposent de beaucoup d'atouts pour réussir dans l'IA, au premier rang desquels comptent la quantité et la disponibilité de la donnée**. Il est, en ce sens, en parfait accord avec les propos tenus par M. Francesco Bonfiglio, directeur de l'initiative Gaia X, selon lequel « *grâce à son héritage industriel, à son modèle social, à son modèle environnemental, et dans la mesure où les données ne sont que les représentations de ces écosystèmes, l'Europe dispose des meilleures données au monde. Nous avons donc la possibilité d'entraîner la prochaine génération de* smart services *reposant sur l'Intelligence artificielle à partir de nos données européennes et de construire ainsi les algorithmes des sites de e-commerce permettant de créer le plus de valeur* » [(2)]. Il faut valoriser cet avantage en définissant un cadre réglementaire clair et propice à juste équilibre entre protection et valorisation des données. La définition du cadre technique de l'IA pourrait par ailleurs conduire utilement à la mise en place, au niveau européen d'un « *organisme d'évaluation de la performance de ces technologies, en opposition au NIST (National Institute of Standards and Technology), l'organisme américain de référence* » comme suggéré par M. Olivier Charlannes vice-président de la société IDEMIA [(3)].

Au-delà de l'enjeu économique, **l'Europe doit aussi affirmer fortement son modèle politique, en particulier sur l'Intelligence artificielle où les enjeux sont particulièrement sensibles.** Votre rapporteur salue donc les travaux engagés dans le cadre européen, qui ont conduit à la présentation d'un Règlement sur l'Intelligence artificielle, mais aussi dans le cadre national, la CNIL s'étant saisie à plusieurs reprises de ce sujet, en 2017 et en 2019 notamment. La question de la confiance affleure à cet égard et doit être traitée. Les efforts mis en œuvre ces dernières années en ce sens doivent donc se poursuivre et s'amplifier.

Enfin, votre rapporteur veut insister **sur la nécessité pour les administrations publiques de se saisir également de la révolution de l'Intelligence artificielle**. Les démarches de « *régulation par la data* » n'en sont en effet que le commencement. Il est possible de s'inspirer, à cette fin, des propos tenus par M. Marc Hansen, qui ont témoigné du dynamisme luxembourgeois sur ce point : « *En 2019, notre gouvernement a adopté une stratégie relative à l'Intelligence artificielle, soutenant le développement de l'Intelligence artificielle centrée sur l'humain. En 2020, une consultation publique à ce sujet nous a permis de comprendre comment les citoyens appréhendaient l'Intelligence artificielle, et d'identifier leurs besoins, leurs craintes et leurs attentes.* ***Nous avons lancé en interne un projet étatique baptisé « AI4GOV » et créé un comité interministériel pour nous occuper de ce sujet. Il s'agit d'encourager les ministères et les***

---

[1] *Audition de M. Renaud Vedel, 6 mai 2021.*

[2] *Audition de M. Francesco Bonfiglio, 22 avril 2021.*

[3] *Audition de M. Olivier Charlannes, 1er avril 2021.*

administrations à en faire usage par le soutien de projets concrets*. Le cadastre a par exemple soumis un projet de ce type, relatif à la topographie des terrains. Le comité interministériel assure un accompagnement technique, juridique et éthique »* [(1)]. Cette remarque vaut d'ailleurs également pour le déploiement de la *blockchain*, le Luxembourg ayant également lancé « *un projet de* blockchain *du secteur public permettant au gouvernement d'expérimenter et de développer de nouvelles applications réservées à l'administration, tout en prévoyant des interactions avec le secteur privé* », dont l'une des applications « *concerne les bourses d'études et vise à faciliter les échanges des étudiants avec les banques, dans les cas où ils souhaiteraient contracter un prêt pour financer leur formation ».*

3. L'informatique quantique

L'ordinateur quantique, une fois parvenu à maturité, devrait constituer une rupture technologique majeure, dont il est encore difficile, en toute objectivité, de définir l'ampleur exacte. Les auditions font apparaître un consensus autour du potentiel de rupture technologique que représente le calcul quantique, mais aussi des incertitudes sur la capacité à créer de façon effective un « *ordinateur quantique* ».

Du côté des acteurs privés, M. Laurent Degré, président directeur général de la société Cisco Systems France, a confirmé que le quantique va révolutionner « *les capacités de calcul et ouvrira des cas d'usage et des possibilités jamais connus* » en insistant sur la nécessité de ne « *pas rater ce virage* » [(2)]. Pour Mme Diane Dufoix-Garnier, directrice des affaires publiques d'IBM France, si les progrès de la recherche dans ce domaine sont rapides, le quantique reste encore « *un champ entier, qui n'en est encore qu'à ses prémices* » [(3)]. Cette interrogation sur la portée exacte de la révolution quantique était partagée par M. Fabrice Brégier, président de Palantir France, en ces termes : « *Des technologies de rupture sont parfois citées comme étant importantes dans le domaine de la cybersécurité. Nous pensons notamment à l'informatique quantique ; les ordinateurs quantiques parviendront-ils à casser les outils de chiffrement aujourd'hui utilisés pour protéger les données ? Beaucoup d'incertitudes demeurent sur le sujet.* A priori, *les algorithmes de chiffrement les plus avancés permettront de résister à des attaques quantiques, mais il faut continuer à investir et à utiliser dès maintenant les solutions de chiffrement les plus avancées pour prévoir cette nouvelle phase, qui peut intervenir d'ici cinq, dix ou quinze ans* » [(4)]. Il est donc difficile, en l'état, d'anticiper l'évolution des usages et des technologies à l'avenir, ce qui ne doit pas exclure, en revanche, la nécessité de ne pas rater ce virage. Cela implique, en particulier, selon Mme Diane Dufoix Garnier, à côté *« de l'investissement dans cette technologie (dans les ordinateurs, les simulateurs, etc.), [..] de constituer dès aujourd'hui des écosystèmes, par exemple avec de grandes entreprises françaises et des universités,*

---

[1] *Audition de M. Marc Hansen, 3 juin 2021.*

[2] *Audition de M. Laurent Degré, 6 mai 2021.*

[3] *Audition de Mme Diane Dufoix-Garnier, 9 mars 2021.*

[4] *Audition de M. Fabrice Brégier, 25 mars 2021.*

pour développer les algorithmes quantiques qui seront probablement au centre des usages de demain » [(1)].

Les pouvoirs publics se sont saisis assez récemment de cet enjeu tant en France qu'en Europe.

En France, une stratégie nationale d'accélération sur le quantique a été annoncée par le Président de la République le 21 janvier 2021**.** Pilotée par l'Agence nationale de la recherche (ANR), elle prévoit un investissement cumulé de l'État d'environ un milliard d'euros sur quatre ans, pour un engagement global public-privé de 1,8 milliard d'euros. Elle doit permettre à la France de disposer d'un élément « *de technologie essentiel pour la souveraineté numérique dans les prochaines années, pour des questions bien connues de performance mais aussi de sécurité. En effet, l'un des enjeux du calcul quantique sera la résilience des systèmes de cryptage et donc des systèmes de sécurité actuels* ».

Cette stratégie, qui prend notamment appui sur le rapport rendu par Mme Paula Fortezza, M. Jean-Paul Herteman et M. Iordanis Kerenidis intitulé « Quantique : le virage technologique que la France ne ratera pas », repose sur les sept piliers suivants :

– développer et diffuser l'usage des simulateurs et accélérateurs NISQ ;

– développer l'ordinateur quantique passant à l'échelle LSQ ;

– développer les technologies et applications des capteurs quantiques ;

– développer l'offre de cryptographie post-quantique ;

– développer les systèmes de communications quantiques ;

– développer une offre de technologies habilitantes compétitive ;

– de structurer l'écosystème de façon transversale.

Elle fixe plusieurs objectifs ambitieux pour la France, qui constituent des points d'étape au cours du processus de maturation de cette technologie. Cette stratégie doit ainsi permettre à la France de devenir le premier État à disposer d'un prototype complet d'ordinateur quantique généraliste de première génération dès 2023, de devenir un *leader* mondial dans la course à l'ordinateur quantique universel et d'être la première nation à disposer d'une filière complète productrice de Si28 industriels. Elle vise également à favoriser le développement les compétences et le capital humain nécessaire. Selon Mme Naomi Peres, secrétaire générale adjointe pour l'investissement, la France dispose en effet « *de toutes les compétences de haut niveau en matière quantique* », l'enjeu étant, contrairement à la cybersécurité, où il s'agit de ne pas perdre l'avance gagnée, « *d'abord d'investir*

[1] *Audition de Mme Diane Dufoix-Garnier, 9 mars 2021.*

dans l'amont, c'est-à-dire dans la recherche et le transfert technologique », le champ du quantique devant prendre « *sa pleine mesure d'ici cinq à dix ans* » [(1)].

Au niveau européen, Mme Lorena Boix-Alonso, directrice chargée de la stratégie et de la diffusion des politiques à la Direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne, a ainsi revendiqué l'ambition, pour l'Europe « *de mettre en place des infrastructures de communication ultra sécurisées qui utilisent des méthodes de cryptage quantique, et de progresser sur les supercalculateurs* » en soulignant l'intérêt, pour ce type d'investissement, de la coopération européenne : « *À titre d'exemple, les supercalculateurs occupent un rôle important dans le développement des vaccins et médicaments. Auparavant, comparer des molécules afin de confectionner un médicament prenait des années, mais le processus a été considérablement accéléré avec l'utilisation de ces machines. Pour autant, le coût d'un superordinateur est colossal. Dans cette optique, nous avons créé EuroHPC (European High Performance Computing Joint Undertaking - Entreprise commune européenne pour le calcul à haute performance), une entreprise commune aux pays européens. D'énormes projets peuvent ainsi participer favorablement à la souveraineté technologique que nous devons réaliser ensemble* » [(2)].

M. Benoît Darde, président de Syntec Numérique, partage cette analyse : face à la puissance financière des acteurs chinois et américains, seule une coopération à l'échelon européen peut avoir du sens sur des projets de cette ampleur : « *L'échelon européen nous semble également intéressant pour mobiliser des financements conséquents. Certains sujets d'un plan industriel et technologique européen requerront de très lourds financements. Ainsi, il est éclairant d'étudier les financements accordés dans d'autres régions du globe. Après avoir investi 250 millions de dollars dans le développement d'un ordinateur quantique, les États-Unis ont investi à nouveau 1,2 milliard de dollars sur les cinq prochaines années pour appuyer la capacité de développement de cette technologie. La Chine vient également d'investir près de 240 millions d'euros en la matière. Cela représente de très grands budgets. Nous devons utiliser l'échelon européen afin de définir des axes stratégiques et de dédier nos capacités financières à faire émerger le bon écosystème. Cela nous garantira ainsi d'être présents et d'être souverains dans cette technologie en Europe* » [(3)].

Le caractère récent des initiatives mises en œuvre et la complexité technique de ces sujets rendent difficiles l'évaluation des actions menées et la formulation de recommandations complémentaires. Aussi, votre rapporteur souhaite simplement partager différents points de vigilance émanant des auditions menées.

---

[1] *Audition de Mme Naomi Peres, 11 mars 2021.*

[2] *Audition de Mme Lorena Boix Alonso, 19 novembre 2020.*

[3] *Audition de M. Benoît Darde, 25 février 2021.*

Il convient de s'assurer, d'abord, de la bonne mise en exécution de cette stratégie et de l'adéquation entre les montants fixés et les objectifs à atteindre. Certains acteurs auditionnés ont en effet mis en avant l'existence d'un retard français dans ce domaine. C'est le sens des propos de M. Stéphane Volant, président du Club des directeurs de la sécurité et de la sûreté des entreprises (CDSE) : « *En m'intéressant ce matin aux statistiques, j'ai découvert que la Chine avait déposé l'année dernière 1 157 brevets en matière de quantique, que les USA en avaient déposé 363, la Grande-Bretagne 29, l'Allemagne 23 et la France 9. C'est dire notre retard, y compris sur ce sujet* » [(1)]. M Nicolas Brien, directeur de France Digitale, abondait d'ailleurs dans ce sens : « *Deutsche Telekom et South Korea Telecom sont en train d'investir des millions dans ce sujet et de déployer les premiers réseaux de télécommunications quantiques – alors que nos opérateurs français sont encore en train de déployer les pylônes 4G* » [(2)].

Si votre rapporteur ne partage pas complètement cette appréciation, **il relève néanmoins que cette dernière donne à voir le différentiel qui peut exister entre les écosystèmes européens et étrangers dans ce domaine.** Il faut donc mobiliser le maximum de financements pour être aussi ambitieux que possible sur ce segment technologique particulièrement critique.

Il est également nécessaire de **soutenir au maximum l'investissement dans les enjeux quantiques au niveau européen, dans le cadre des projets actuellement en cours.** La qualité de la coopération entre les acteurs économiques des différents États membres sera en effet décisive pour permettre à l'Europe de se positionner efficacement sur cette technologie.

Enfin, dans un domaine où la rupture technologique peut intervenir à tout moment, **votre rapporteur souhaite insister sur la nécessaire veille technologique que doivent effectuer les pouvoirs publics, ainsi que sur le rôle de protection vis-à-vis des entreprises technologiques nationales qui œuvrent dans ce domaine**.

4. Le *cloud*

La capacité de la France et de l'Europe à investir dans le *cloud* est une priorité au regard du caractère stratégique de cette technologie. La maîtrise de la donnée est en effet au cœur du processus d'innovation au sein de l'économie numérique. Au-delà de l'enjeu économique, le *cloud* revêt évidemment une dimension profondément politique à la fois en termes de protection des données, pour des raisons tenant à la fois au respect des droits fondamentaux et à la lutte contre l'espionnage industriel.

La situation actuelle est néanmoins celle d'une forte dépendance de l'Europe vis-à-vis des solutions proposées par des *hyperscalers* américains. Leur

---

[1] *Audition de Stéphane Volant, 11 février 2021.*

[2] *Audition de M. Nicolas Brien, 25 février 2021.*

taille critique rend en effet impossible ou presque une lutte « à armes égales ». En effet, lorsqu'Amazon *« avec AWS investit 22 milliards de dollars par an en recherche et développement. La France tout entière investit un peu plus de 60 milliards par an dans l'ensemble de sa recherche* » comme l'a rappelé le secrétaire d'État à la transition numérique, avant d'ajouter : « *d'après les chiffres de 2017, les Américains investissent chaque année 40 milliards de dollars dans l'IA, tandis que les grandes plateformes chinoises et le gouvernement chinois investissent chaque année 40 milliards d'euros. Les chiffres sont similaires en ce qui concerne le* cloud*. Les investissements des entreprises européennes dans ces deux domaines, qui sont absolument stratégiques pour notre souveraineté, ne dépassent pas 4 milliards d'euros* » [(1)].

La dépendance actuelle des acteurs publics et privés européens vis-à-vis des solutions de *cloud* américaines est profondément préjudiciable à la défense de la souveraineté numérique nationale et européenne. Les technologies numériques sont en effet profondément liées comme le rappelait également le secrétaire d'État à la transition numérique : *« la cybersécurité demande de l'Intelligence artificielle, de la maîtrise du* cloud*… Si nos acteurs ne sont pas parmi les meilleurs du monde dans l'Intelligence artificielle et la maîtrise du* cloud*, nous serons en retard en matière de cybersécurité* » [(2)]. Une absence de maîtrise d'un segment critique tend donc à créer des dépendances en chaîne dont il peut être difficile de sortir à court terme. Malgré le retard actuel de la France et de l'Europe sur le *cloud*, il convient toutefois d'être optimiste : il est encore possible de prendre position sur un certain nombre de segments à condition de mobiliser des investissements massifs et une volonté politique forte.

De ce point de vue, votre rapporteur considère que les pouvoirs publics ont compris le caractère critique de cette technologie et mis en œuvre un certain nombre d'initiatives positives, au niveau national et européen. En matière de technologies numériques critiques, ainsi que l'a rappelé M. Thomas Courbe, directeur général des entreprises, le *cloud* est également une priorité qui renvoie à l'enjeu de la maîtrise de la donnée : « *La quatrième priorité* [des pouvoirs publics pour assurer notre souveraineté numérique] *est le* cloud *et, plus généralement, la maîtrise de la donnée. Il s'agit d'une bataille difficile, face à des concurrents, notamment américains et chinois, très avancés. Il nous semble que des initiatives récentes permettront de consolider les acteurs européens et l'offre européenne de* cloud » [(3)].

M. Thomas Courbe a ensuite détaillé les trois axes principaux de travail pour une stratégie du *cloud* à la hauteur des enjeux, à savoir :

– *le soutien de l'initiative européenne GAIA-X*, d'initiative franco-allemande, dont l'objet est de « *répondre à un grand défaut des offres de* cloud *actuelles, en créant de l'interopérabilité et de la réversibilité. Aujourd'hui, dans la*

---

[1] *Audition de M. Cédric O, 22 octobre 2020.*

[2] *Audition de M. Cédric O, 22 octobre 2020.*

[3] *Audition de M. Thomas Courbe, 8 octobre 2020.*

plupart des solutions de cloud*, les clients – les entreprises notamment – sont en quelque sorte prisonniers de l'offre de* cloud *choisie. Les capacités à migrer d'une offre à une autre, donc à maintenir le pouvoir du client face aux autres offres de solutions sont assez réduites. L'un des enjeux de l'initiative GAIA-X est bien d'offrir un espace de marché, avec des solutions de* cloud *respectant un certain nombre de valeurs, en particulier ces valeurs d'interopérabilité et de réversibilité. Ces valeurs apporteront des garanties pour les clients de pouvoir faire évoluer leurs solutions au cours du temps. Nous pensons qu'il s'agira d'un élément assez différenciant. Il nous semble qu'il s'agit d'une place de marché sur laquelle des offres françaises et européennes de* cloud *pourront se développer et, peut-être, être mieux valorisées qu'aujourd'hui pour leurs clients* » ;

– *le développement des offres de cloud de confiance*, en raison des préoccupations légitimes des acteurs concernés pour *« la sécurité des données face à un certain nombre de législations étrangères et face aux doutes généraux sur la manière dont les données sont utilisées » ;*

– *le soutien du développement d'une offre la plus compétitive possible, pouvant rivaliser avec les autres offres, notamment américaines,* en précisant qu'il peut s'agir *« d'offres collaboratives, sur lesquels nous avons déjà une belle offre française restant à fédérer, ou de services d'Intelligence artificielle* ».

Le 17 mai 2021, le Gouvernement a présenté **une stratégie nationale pour le *cloud*** reprenant ces différentes priorités. Cette stratégie repose sur un constat simple : dans les années à venir, le *cloud* sera « *l'une des briques essentielles des innovations dans de nombreux secteurs* ». Il constitue, en outre, à court et moyen terme, un vecteur de croissance, le marché européen du *cloud* devant voir « *sa taille multipliée par 10 en dix ans* ». Dans ces conditions, et alors que le secteur du *cloud* devrait atteindre la taille de celui des communications électroniques en 2030, le Gouvernement entend **porter une stratégie ambitieuse dans ce domaine** autour des « *trois enjeux majeurs pour la France que sont « la transformation de nos entreprises et de nos administrations, la souveraineté numérique et la compétitivité économique* ».

Cette stratégie nationale se décline en conséquence selon les trois axes suivants :

– *la création d'un nouveau label « cloud de confiance »* qui doit permettre d'assurer « *le niveau de protection le plus élevé pour les données des Français* ». Ce label est une réponse aux attentes des acteurs publics et aux entreprises françaises, en particulier lorsqu'elles constituent des opérateurs d'importance vitale (OIV). Les solutions de *cloud* labellisées « de confiance » devront remplir plusieurs conditions : être conformes au référentiel technique SecNumCloud de l'ANSSI, reposer sur des infrastructures localisées en Europe et des systèmes opérés en Europe, et, enfin, assurer les portages opérationnel et commercial de l'offre par une entité européenne détenue par un acteur européen ;

– *une nouvelle politique « cloud au centre » pour la transformation numérique de l'État,* qui prévoit que le *cloud* doit désormais être la méthode d'hébergement par défaut pour les services numériques de l'État, pour tout nouveau produit numérique ainsi que pour les produits numériques connaissant une évolution substantielle. Les services numériques des administrations seront donc hébergés soit sur l'un des deux *cloud* interministériels internes de l'État, ou sur des offres *cloud* privées répondant à des exigences strictes de sécurité. Il est également prévu que les administrations mettent en place des plans de continuité d'activité en cas de difficulté ;

– *un investissement massif du programme d'investissements d'avenir n° 4 en soutien direct à des projets à forte valeur ajoutée dans le cadre du 4e programme d'investissements d'avenir et de France Relance*. Un PIEEC aura également pour objectif de développer une offre *cloud* européenne dans les domaines de rupture technologique, comme le *edge computing*.

Face à ces différentes initiatives, votre rapporteur formulera plusieurs remarques.

Il convient de saluer, d'abord, **la prise de conscience de l'importance du *cloud* et de la mise en œuvre d'une stratégie dédiée dans ce domaine**. La réduction de la dépendance de l'Europe vis-à-vis des solutions extra-européennes doit être un objectif affiché et réaffirmé fortement, afin de mobiliser aussi les acteurs du secteur privé en ce sens. **Sur ce point, les auditions ont donné à voir une vraie et forte attente de ces derniers vis-à-vis d'une offre de *cloud* de confiance, sur laquelle les acteurs européens peuvent être compétitifs de surcroît.** Lors de son audition, le CIGREF avait d'ailleurs détaillé ses attentes à ce sujet : un *cloud* « *de confiance* », terminologie privilégiée à celle de *cloud* souverain « *puisque toutes sortes de technologies peuvent se trouver dans un* cloud », qui doit être à la fois « *immune au droit extra-européen* », « *sécurisé* », et « *répondre à des besoins de réversibilité […], de portabilité des données* » et « *d'auditabilité de la solution* » [(1)]. L'approche défendue était donc celle d'un *cloud* pouvant « *héberger n'importe quel type de solution, mais en les protégeant suffisamment pour que nous soyons assurés, en utilisant ce* cloud*, de la relative immunité des données qui s'y trouvent* ». Il apparaît à votre rapporteur que ces messages ont été entendus au regard des éléments contenus dans la stratégie nationale pour le *cloud*.

Votre rapporteur souhaite également **saluer le soutien du PIA 4, dans le cadre du plan de relance, au développement des projets innovants en matière de *cloud***. Le PIA est un outil qui démontré son efficacité. Le lancement d'un PIEEC, de surcroît, montre que l'Europe a pris la mesure de l'ampleur du retard à rattraper, et se projette vers l'avant dans un domaine où elle peut encore s'imposer, c'est-à-dire le *edge computing*.

[1] *Audition de M. Henri d'Agrain, 18 mars 2021.*

***Proposition n° 56* :** Développer une offre *cloud* européenne respectant les valeurs du modèle européen.

Votre rapporteur est plus réservé, en revanche, sur l'état actuel de l'initiative Gaia X, dont il a souhaité que les représentants soient auditionnés. Au-delà des objectifs fixés dans ce cadre, qu'il ne peut que partager, il apparaît que la gouvernance actuelle n'est pas satisfaisante. S'il prend acte du fait que seul des acteurs européens peuvent être présents au conseil d'administration de Gaia X, il semble en revanche qu'au sein des comités techniques, on constate une écrasante majorité des acteurs américains, et un risque, en conséquence, de choisir des modalités techniques favorisant finalement les solutions américaines.

Votre rapporteur souhaite donc mettre un point de vigilance sur ce sujet : **l'ambition initiale de Gaia X d'affirmer une souveraineté numérique européenne doit être maintenue**. Un **effort de transparence** doit également être mis en œuvre pour veiller à limiter les tentatives d'orientation de ce projet vers des directions qui ne seraient pas conformes aux intérêts européens.

Proposition n° 57 : Garantir au sein de Gaia-X une gouvernance et une conduite de projets conformes aux ambitions exprimées par ses membres fondateurs afin d'éviter que cette initiative ne devienne un instrument au service de la croissance d'acteurs déjà dominants.

Il prend note, par ailleurs, avec intérêt, de la création cette semaine de **l'Alliance européenne EUCLIDIA** (European Cloud Industrial Alliance), qui regroupe 23 entreprises européennes indépendantes qui créent des technologies originales de cloud, dont une partie sont des acteurs du logiciel libre.

5. Les satellites

L'investissement dans le déploiement de constellations de satellites en orbite basse est également un enjeu décisif pour la souveraineté numérique de la France et de l'Europe. Comme l'a indiqué M. Rodolphe Belmer, directeur général d'Eutelsat, « *sur les aspects de souveraineté, de perturbation de notre secteur d'activité et de stratégie d'innovation, il faut à l'évidence reconnaître une profonde évolution de notre champ concurrentiel. (…) Le marché des opérateurs de télécommunications par satellites se déplace vers les enjeux de connectivité. Les dernières générations de satellites sont en mesure de connecter à l'Internet de haut débit et à des prix compétitifs, tant dans les pays émergents que dans les pays développés, de vastes segments de population qui ne l'étaient pas. Étendu, le marché qui s'ouvre répond à un besoin indéniable et d'une importance cruciale. Il suscite bien des convoitises* »[1].

Une nouvelle dynamique est en effet à l'œuvre dans ce domaine : le déploiement de constellations de satellites en orbite basse. Ces dernières reposent sur une approche différente de celle des satellites géostationnaires, comme le

[1] *Audition de M. Rodolphe Belmer, 6 avril 2021.*

résume M. Rodolphe Belmer : « *la technologie des constellations en orbite basse arrive progressivement à maturité. Elle repose sur une approche toute différente. Les satellites évoluent alors beaucoup plus près de la Terre et tournent autour d'elle. Dans ce cas, apporter un service constant suppose de couvrir l'orbite d'un nombre élevé de satellites. De flottes de quelques dizaines de gros satellites, nous passons à une logique de centaines, voire de milliers ou même de dizaines de milliers d'objets en orbite basse* ».

Ces constellations doivent permettre de fournir une connexion à Internet à moindre coût, en particulier dans les zones où la connectivité n'est pas satisfaisante (zones blanches). L'avantage de cette nouvelle technologie réside notamment dans la meilleure latence offerte au client. Ainsi que l'a précisé M. Rodolphe Belmer : « *recevoir un signal d'un satellite géostationnaire nécessite 0,4 seconde ; pour un satellite en orbite basse ou très basse, la communication devient quasiment instantanée, de l'ordre de 10 ou 14 millisecondes. Elle équivaut à celle de la fibre optique* ».

Le déploiement de constellations de satellites en orbite basse s'est accéléré ces derniers mois, dans un contexte où, par construction, « *les constellations en orbite basse n'excéderont pas un nombre fort restreint* [car] *quoiqu'elle puisse être amenée à évoluer encore, l'estimation la plus communément admise aujourd'hui prévoit un maximum de cinq ou six constellations. Au-delà, l'orbite atteindra son niveau de saturation* » [(1)]. La taille du spectre des fréquences utilisables est en effet limitée. À l'heure actuelle, plusieurs pays vont disposer à court terme d'une constellation de cette nature. Il s'agit en particulier d'acteurs nord-américains, « *dont SpaceX d'Elon Musk, Amazon de Jeff Bezos avec Project Kuiper et la société canadienne Telesat* », anglais, canadiens, et chinois.

Face à cette situation, votre rapporteur souhaite insister sur la nécessité, pour la France et l'Europe, de se positionner rapidement dans ce domaine.

Il prend acte de la prise en compte par l'initiative Gaia X du déploiement de ce type de constellations, comme l'a indiqué M. Pierre Gronlier, son directeur technique : « *La méga-constellation de fournisseurs d'Internet par satellite a été prise en compte dans GAIA-X à travers la notion d'*edge cloud*. Un satellite – tout comme une voiture, un train ou un bateau – peut être considéré comme une unité de calcul qui peut être fédérée. Dans ce contexte, disposer d'une bande passante plus importante et d'une moindre latence permettra de construire de nouveaux scénarios de cas d'usage. Par ailleurs, GAIA-X représentera une offre complémentaire en termes de régulation* » [(2)]. Il est en effet important de faire preuve d'anticipation des évolutions technologiques en cours.

Il souhaite saluer, en outre, le projet de déploiement d'une constellation européenne porté par le commissaire européen M. Thierry Breton. Il note

---

[1] *Audition de M. Rodolphe Belmer, 6 avril 2021.*

[2] *Audition de M. Pierre Gronlier, 22 avril 2021.*

néanmoins qu'il est indispensable que ce déploiement intervienne le plus rapidement possible pour ne pas être pris de vitesse, le cas échéant, par d'autres acteurs. Ainsi que l'a relevé M. Hervé Derrey, président-directeur général de Thales Alenia Space : « *l'enjeu tient désormais à la vitesse d'exécution. Nos concurrents américains font montre d'une célérité redoutable. Le service Starlink connaît actuellement sa phase dite de bêta-test. Sa commercialisation complète est annoncée dès la fin de l'année 2021* » [(1)].

Proposition n° 58 : Accélérer le déploiement d'une constellation européenne de satellites en orbite basse.

Enfin, votre rapporteur souhaite attirer la vigilance des pouvoirs publics sur les enjeux de sécurité afférents au déploiement de ces constellations.

IV. L'EUROPE : UN LEVIER INDISPENSABLE POUR RECONSTRUIRE PROGRESSIVEMENT DES ÉLÉMENTS DE SOUVERAINETÉ DANS LE MONDE NUMÉRIQUE

A. RELOCALISER LE NUMÉRIQUE EN EUROPE ET AMPLIFIER LES COOPÉRATIONS EXISTANTES DANS LES DOMAINES À FORT CONTENU TECHNOLOGIQUE

1. La relocalisation et le développement du *hardware* sur le sol européen

a. L'existence d'une dépendance européenne en matière de hardware

La mondialisation a conduit à la création de chaînes de valeur mondiales : les activités productives des entreprises sont en effet fragmentées, réalisées dans plusieurs lieux géographiques, de la conception du produit à sa livraison au consommateur. Cette fragmentation est source de gains économiques pour les entreprises, en raison de l'existence d'économies d'échelles et de différences de coût entre les facteurs de production selon les pays.

Dès lors, l'existence des chaînes de valeur mondiales augmente la concentration de la production pour certains intrants critiques, ce qui accroît les risques de rupture d'approvisionnement[(2)]. La dépendance globale de la France vis-à-vis de l'étranger du fait des chaînes de valeur est moins élevée que celle de l'Allemagne, mais reste supérieure à celle des États-Unis, puisque l'économie américaine est de grande taille et très tertiarisée. Si les interdépendances de la France sont avant tout européennes, elles augmentent néanmoins rapidement vis-à-vis du reste du monde, notamment de la Chine[(3)].

---

[1] Audition de M. Hervé Derrey, 6 avril 2021.

([2]) Note du conseil d'analyse économique (CAE) n° 46, Quelle stratégie de résilience dans la mondialisation ?, Xavier Jaravel et Isabelle Méjean, juillet 2018.

([3]) Ariell Reshef et Gianluca Santoni, Chaînes de valeur mondiales et dépendances de la production française, Lettre du centre d'études prospectives et d'informations internationales (CEPII), juin 2020.

Les interdépendances de la France et de l'Union européenne existent en particulier dans le domaine du numérique. Lors de son audition, M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique a ainsi relevé qu'« *aujourd'hui, particulièrement du fait de la pandémie, on a pu se rendre compte encore plus de notre dépendance technologique à des solutions et à des acteurs extra-européens* » (1). Si une conception fermée de la souveraineté, sans connectivité vis-à-vis d'acteurs établis hors du territoire de l'Union européenne paraît irréaliste et non souhaitable, une attention accrue doit néanmoins être portée à la dépendance technologique.

La reconstruction d'une souveraineté numérique nationale et européenne impose en effet une maîtrise de l'industrie du *hardware*. Les délocalisations successives des unités de production d'entreprises technologiques européennes vers l'Asie, en raison de l'ouverture des marchés et des faibles coûts de production, ont eu plusieurs effets. D'une part, les pays asiatiques ont rattrapé leur retard technologique mettant à mal la souveraineté numérique européenne, et, d'autre part, les pays européens ont souffert d'une perte de compétence, de maîtrise et de savoir-faire. Il est donc primordial de créer les conditions favorables à un retour des industries high-tech au sein de l'Union Européenne.

Proposition n° 59 : Encourager la localisation ou la relocalisation en Europe d'usines de production d'équipements numériques sur l'ensemble de la chaîne de valeur.

b. Les moyens de limiter la dépendance industrielle pour le hardware

i. Amplifier les efforts mis en œuvre dans le cadre des projets importants d'intérêt européen commun (PIEEC)

Des efforts ont été entrepris pour réduire la dépendance industrielle de la France et de l'Union européenne, avec le soutien d'acteurs privés. La direction générale des entreprises (DGE) a notamment lancé un appel à projets visant des projets de relocalisation de production de composants de microélectronique en France (2). Du côté des acteurs privés, l'entreprise Huawei a par exemple entamé des efforts de relocalisation de compétences en France en ouvrant cinq centres de recherche et développement (R&D) et un centre de recherche fondamentale déposant chaque année 50 brevets en France. Elle cherche à favoriser le « Made in France » et le « Made in Europe » en lançant la construction d'une usine en France pour la construction de matériel 2G, 3G, 4G et 5G (3).

Au niveau européen, les projets importants d'intérêt européen commun (PIIEC) constituent un levier performant pour favoriser le développement de compétences en Europe et la relocalisation des industries *high tech* dans un cadre coopératif.

(1) Audition de M. Bernard Benhamou, 20 octobre 2020.

(2) Audition de M. Thomas Courbe, 8 octobre 2020.

(3) Audition de Mme Linda Han, déléguée générale de Huawei France, 26 novembre 2020.

Comme l'a mentionné M. Thomas Courbe, directeur général des entreprises au ministère de l'Économie, des Finances et de la Relance, « *les PIEEC sont ces nouveaux cadres d'action européens dérogatoires des régimes habituels d'aide d'État, expérimentés sur les batteries par exemple. Dans le domaine des batteries, ils ont finalement montré que l'on pouvait réintroduire une industrie nouvelle pour l'Europe. Nous voulons appliquer ces régimes sur le* cloud *et sur la microélectronique dans les prochains mois avec la Commission européenne, notamment dans le cadre d'un dialogue approfondi avec l'Allemagne* » (1). Dans ce cadre, le Secrétariat général pour l'investissement (SGPI) participe activement à plusieurs PIIEC avec l'Allemagne ainsi qu'à un PIIEC réunissant quatre pays sur le sujet du *cloud* (2).

Votre rapporteur souhaite saluer le recours croissant aux PIEEC et inviter les pouvoirs publics à défendre un haut niveau d'ambition lors de leur mise en œuvre, tant en termes de financement que de calendrier.

Proposition n° 60 : Renforcer les moyens mis en œuvre dans le cadre des projets importants d'intérêt européen commun (PIEEC) et adopter à chaque reprise des calendriers ambitieux de déploiement.

ii. Défendre une stratégie de relocalisation de l'industrie du *hardware*

Lors de son audition, M. Thomas Courbe a relevé que « *la réponse de long terme est la souveraineté et la capacité à avoir la dépendance la plus faible possible par rapport à des acteurs non européens, dans nos productions et notamment dans le domaine du numérique en Europe* » (3).

Pour être efficace, la stratégie de relocalisation et de résilience doit identifier et cibler un nombre restreint d'intrants vulnérables. Ainsi, la relocalisation pourrait principalement cibler les **intrants vulnérables à la frontière technologique.** Le soutien à l'innovation pour produire sur le territoire national de manière compétitive peut ainsi être l'un des leviers du soutien à la relocalisation (4). Il importe ainsi de définir une liste d'intrants stratégiques vulnérables en matière numérique, pour **structurer une stratégie de résilience et définir quelles productions doivent être relocalisées sur le sol français et européen afin de favoriser la construction d'une souveraineté numérique.**

L'Europe doit par exemple continuer de faire preuve d'ambition en matière de semi-conducteurs. Selon M. Julien Nocetti, docteur en sciences politiques et chercheur associé à l'Institut français des relations internationales : « *les semi-*

1 Audition de M. Thomas Courbe, 8 octobre 2020.

(2) Audition de Mme Naomi Peres, secrétaire générale adjointe du secrétariat général pour l'investissement (SGPI), et de M. Clément Jakymiw, directeur adjoint du programme industries et services du secrétariat général pour l'investissement, 11 mars 2021.

3 Audition de M. Thomas Courbe, 8 octobre 2020.

(4) Note du conseil d'analyse économique (CAE) n° 46, Quelle stratégie de résilience dans la mondialisation ?, Xavier Jaravel et Isabelle Méjean, juillet 2018.

conducteurs sont aujourd'hui absolument fondamentaux et centraux dans ces ambitions de souveraineté numérique. Le sujet n'est pas nouveau, mais il s'est amplifié à mesure de notre dépendance accrue à ces composants, et à mesure que nous prenions conscience de la complexité des chaînes de valeur globales des semi-conducteurs. Nous dépendons d'acteurs américains pour leur conception et leur design, d'acteurs taïwanais pour la fonderie et leur production physique, mais aussi d'acteurs chinois, britanniques ou singapouriens pour d'autres volets de ces chaînes de valeur. Ces composants technologiques revêtent logiquement une dimension géopolitique extrêmement forte, ainsi qu'une dimension économique majeure au regard de leur prolifération et de l'industrie très globalisée qui les entoure. L'enjeu est également stratégique. En effet, si nous avons surtout tendance à aborder la dimension civile et commerciale de ces semi-conducteurs, qui innervent nos smartphones et autres produits informatiques, nous ne devons pas en oublier les enjeux critiques en termes de supériorité militaire pour les décennies à venir » (1).

En 2019, le marché des semi-conducteurs a représenté 440 milliards de dollars au niveau mondial. La moitié de ce marché est destinée à la production de PC, des smartphones et des mémoires. Les entreprises dominantes de ce marché sont Intel, Qualcomm, Broadcom ainsi que les trois fabricants de mémoires dynamiques dans le monde. L'Europe est quasiment absente de ce marché, les producteurs européens étant de plus petite taille, opérant avec un modèle d'entreprise *fabless* (soit sans usines situées sur le territoire de l'Union) et plutôt concentrés sur le secteur automobile (2). M. Thomas Courbe a mis en exergue l'importance stratégique que représente la production de semi-conducteurs : « *Nous voyons bien, suite à des déclarations récentes du gouvernement américain, que ce sujet fait l'objet d'une mobilisation internationale.* […]. *Suite à la crise, nous réfléchissons avec les Allemands et la Commission européenne à une accélération de ces soutiens à l'industrie de la microélectronique au niveau européen.* […]. *Dans le cadre de nos efforts sur la résilience de l'économie, et en particulier sur des projets de relocalisation, nous avons lancé un appel à projets, fin août, qui doit viser particulièrement des projets de relocalisation de production de composants de microélectronique en France* » (3).

iii. Limiter les prises de contrôle capitalistiques par des acteurs étrangers

En parallèle de la stratégie de relocalisation, la question du contrôle des entreprises produisant sur le sol européen est également essentielle pour la promotion d'une souveraineté numérique. Par exemple, dans le domaine des microprocesseurs et de l'Intelligence artificielle, la société britannique ARM a été rachetée par le géant américain Nvidia, pour une somme de 40 milliards de dollars. M. Thomas Courbe a qualifié ce rachat de « *très préoccupant* […] *En effet, nous ne*

(1) Audition de M. Julien Nocetti, 11 mars 2020.

(2) Audition de M. Thierry Tingaud, président du Comité stratégique de la filière Industrie électronique, 8 octobre 2020.

3 Audition de M. Thomas Courbe, 8 octobre 2020.

pouvons plus considérer qu'ARM répond à notre objectif de souveraineté numérique » [1]. Même dans l'hypothèse où les composants sont créés sur le sol européen, la souveraineté implique en effet un contrôle capitalistique des entreprises concernées.

Plusieurs réponses sont possibles, pour limiter les prises de contrôle capitalistiques des entreprises européennes par les acteurs établis en dehors du territoire de l'Union : la réglementation et l'intervention en fonds propres.

L'option de la réglementation doit permettre *a minima* de contrôler les investissements étrangers réalisés dans les entreprises du numérique à fort potentiel d'innovation. Si l'article 3 du TFUE prévoit que les investissements directs étrangers relèvent de la politique commerciale commune de l'Union, l'article 65 du même Traité stipule que les États membres peuvent « *adopter des procédures de déclaration des mouvements de capitaux à des fins d'information administrative ou statistique ou de prendre des mesures justifiées par des motifs liés à l'ordre public ou à la sécurité publique* ».

Ainsi, le Règlement 2019/452 du 19 mars 2019 [2] permet le contrôle des investissements étrangers : son article 4 détermine les facteurs susceptibles d'être pris en considération par les États membres ou la Commission pour déterminer si un investissement direct étranger est susceptible de porter atteinte à la sécurité ou à l'ordre public. Parmi ces éléments, figurent la présence d'infrastructures critiques, de technologies critiques, l'approvisionnement en intrants essentiels et l'accès à des informations sensibles. Les articles 6 et 7 prévoient la création d'un dispositif de coopération concernant les investissements directs étrangers, avec un système de notification à la Commission. La Commission peut émettre un avis, dont l'État membre doit tenir compte, dans sa décision d'acceptation ou de refus de l'investissement.

Selon M. Thomas Courbe « *ce Règlement est plutôt du ressort de l'échange d'informations que de celui d'un vrai contrôle de l'investissement lui-même. Il me semble que l'Europe doit encore progresser pour, idéalement, aboutir à un dispositif similaire au nôtre, permettant vraiment de contrôler l'investissement et éventuellement d'imposer des conditions à l'investisseur* » [3]. Ce Règlement pourrait ainsi être révisé, de manière à prévoir un rôle plus important de la Commission dans le processus d'acceptation des investissements étrangers dans les pépites technologiques européennes, qui ne se limiterait pas à un simple avis.

Les mesures de contrôle des investissements étrangers doivent, en outre, être mobilisées en parallèle des instruments de défense commerciale de l'Union européenne, qui permettent de lutter contre certaines pratiques commerciales

---

1 Audition de M. Thomas Courbe, 8 octobre 2020.

(2) Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union.

3 Audition de M. Thomas Courbe, 8 octobre 2020.

déloyales dans le respect du cadre juridique fixé par l'Organisation mondiale du commerce (OMC).

Proposition n° 61 : Renforcer le recours aux outils de défense économique de l'Union européenne et durcir, le cas échéant, le Règlement 2019/42 du 19 mars 2019 relatif au contrôle des investissements étrangers.

La seconde option repose sur l'intervention en fonds propres. Comme rappelé auparavant, l'objectif est, dans ce cas, de développer, à la fois au niveau français et européen, des acteurs capables de formuler des offres de rachat d'une entreprise donnée ou d'une *start-up*.

c. Le renforcement des moyens de coopération entre les acteurs du numérique par l'infléchissement des règles de concurrence

Afin de développer une véritable industrie du numérique européenne, en particulier du *hardware*, il est nécessaire d'inciter les entreprises à s'installer sur le sol européen. Dans les facteurs d'attractivité pour les entreprises, la facilitation des coopérations entre la puissance publique et les acteurs privés, d'une part, et entre acteurs privés, d'autre part, doit être améliorée. Or, selon M. Charles Thibout, chercheur associé à l'Institut de relations internationales et stratégiques (IRIS), « *nos totems – le libre-échange, la concurrence libre et non faussée, l'hygiène budgétaire – nous ont placé dans une position de faiblesse à l'égard des États-Unis et de la Chine qui ne se sont pas encombrés de telles restrictions juridico-économiques* » [(1)]. Les règles de concurrence limitent ainsi le rôle de l'État-stratège, notamment dans les secteurs à fort potentiel technologique.

En matière de coopération entre la puissance publique et les entreprises technologiques, l'article 107 du TFUE prohibe par exemple les aides d'État, limitant les moyens pour la puissance publique de soutenir les acteurs digitaux susceptibles de contribuer à la construction de la souveraineté numérique. Les PIIEC permettent une dérogation aux règles des aides d'État, mais leur champ d'application reste limité, notamment en raison des conditions strictes de leur qualification. Concernant les coopérations entre entreprises, l'article 101 du TFUE prohibe les ententes, limitant ainsi les échanges d'informations entre les différents acteurs.

Ces règles ont ainsi pour effet de limiter la croissance du tissu d'entreprises du numérique dans l'Union européenne, tout en étant à l'origine d'une concurrence déloyale de la part des acteurs étrangers qui ne sont pas soumis aux mêmes impératifs de concurrence. La construction d'une souveraineté numérique européenne implique ainsi l'intégration, au sein de la politique de concurrence de l'Union européenne, des enjeux de souveraineté numérique et d'autonomie stratégique de l'Union.

(1) Audition de M. Charles Thibout, 12 novembre 2020.

Proposition n° 62 : Intégrer, au sein de la politique de la concurrence de l'Union européenne, les enjeux de souveraineté numérique et d'autonomie stratégique de l'Union.

Il convient également de doter l'Union européenne d'une capacité d'anticipation et de veille sur les technologies numériques.

Proposition n° 63 : Doter l'Europe d'une capacité d'anticipation et de veille sur les technologies numériques.

2. La question de la localisation des données sur le sol européen

Outre le *hardware*, la souveraineté numérique européenne implique également la localisation du stockage et du traitement des données des utilisateurs sur le sol de l'Union. Selon M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique, « *Il est temps de mettre un terme à la naïveté, c'est-à-dire qu'il faudrait localiser les données en Europe (data sovereignty, data localization ou data residency). Les données des Européens doivent être traitées en Europe par des acteurs européens* » (1).

M. Olivier Micheli, président de Data 4, a rappelé que disposer de *data centers* localisés en France constitue une composante incontournable de la souveraineté numérique (2), pour au moins trois raisons. Premièrement, les applications que chacun utilise quotidiennement sont installées sur des serveurs, qui sont hébergés dans des *data centers* : leur maîtrise est donc essentielle, afin de ne pas dépendre d'un acteur tiers qui pourrait refuser l'accès aux données en cas de crise. Deuxièmement, la maîtrise de la qualité et de la continuité du service des *data centers* est essentielle pour l'accès aux données : la maîtrise d'un réseau électrique fiable et pérenne, comme le réseau français est incontournable pour l'atteinte d'une souveraineté numérique. Troisièmement, conserver les *data centers* en France permet d'y disposer d'un bon niveau de connaissances et de compétences.

L'arrêt *Schrems* II (3) de la Cour de Justice de l'Union européenne a invalidé en 2020 le *Privacy Shield* en matière de *cloud*. Le transfert de données entre les États-Unis et l'Europe n'est ainsi plus possible, en raison d'un niveau insuffisant de protection des données personnelles dans le cas de leur transfert à finalité commerciale vers le sol américain.

Cet arrêt peut avoir deux conséquences alternatives :

– *soit inciter les entreprises du numérique à ouvrir des data centers sur le sol européen*, de manière à y stocker et traiter les données, sans recourir à des transferts. Plusieurs acteurs auditionnés, français comme OVHcloud ou extra-

(1) Audition de M. Bernard Benhamou, 29 octobre 2020.

(2) Audition de M. Olivier Micheli, 4 mars 2021.

(3) CJUE, gr. Ch. 16 juillet 2020, aff. C-311/18 – Data Protection Commissioner c/ Facebook Ireland Ldt, Maximilian Schrems.

européens comme Microsoft et Huawei, ont fait part de leur intention d'investir dans l'ouverture de *data centers* sur le sol européen ;

– *soit inciter les pays tiers à renforcer leur niveau de protection des données personnelles*, de manière à rendre possible un transfert des données récoltées sur le territoire de l'Union européenne.

Votre rapporteur estime, comme indiqué précédemment, que cet arrêt plaide en faveur d'un effort de localisation maximale des données en Europe.

B. MOBILISER L'ÉCHELON EUROPÉEN AU SERVICE DE LA RÉGULATION DES GÉANTS DU NUMÉRIQUE

1. Un puissant besoin de régulation des activités des géants du numérique

Les activités des géants du numérique doivent mener à une actualisation des règles de droit et du cadre de la régulation digitale. La croissance des entreprises digitales et des réseaux sociaux a en effet conduit à des phénomènes de concentration et à des difficultés évidentes pour lutter contre les contenus illicites en ligne. En parallèle, le marché de la donnée est en plein essor : dans la compétition mondiale entre les entreprises évoluant dans le cyber espace, les acteurs européens ont besoin d'un cadre prévoyant le partage et la réutilisation de données, pour développer des applications innovantes dans des secteurs stratégiques.

Or, à l'heure actuelle, le droit de l'Union européenne ne permet pas de parvenir à une régulation suffisamment efficace des entreprises du numérique. Il est donc indispensable de forger un cadre juridique respectueux des valeurs européennes, vis-à-vis duquel les géants digitaux doivent se conformer.

En matière concurrentielle, les caractéristiques du numérique conduisent à une concentration naturelle des entreprises présentes sur le marché. Les facteurs d'explication de cette dynamique tiennent à l'existence d'économies d'échelle dans la production de produits ou services numériques, impliquant de forts coûts fixes, et d'effets de réseau dans la consommation de biens numériques, les consommateurs étant davantage attirés par une entreprise donnant accès à un large réseau, ce qui renforce d'autant sa position sur le marché [(1)]. La structuration actuelle des marchés numériques en témoigne (Google pour les moteurs de recherche, Facebook pour les réseaux sociaux par exemple).

L'entreprise dominante est alors en capacité d'ériger des barrières à l'entrée sur le marché, avec le contrôle par les plateformes des modalités d'accès et de référencement des utilisateurs professionnels de leur réseau. Les plateformes ont également la possibilité de collecter et d'exploiter un grand nombre de données générées par les utilisateurs, de manière à renforcer leur position dominante.

---

(1) Note du Conseil d'analyse économique, Plateformes numériques : réguler avant qu'il ne soit trop tard, n°60, Octobre 2020

Les régulateurs ont ainsi davantage de difficultés pour garantir un fonctionnement concurrentiel sur les marchés du numérique, appelant à une nouvelle action régulatrice de la part des pouvoirs publics.

En matière de régulation des contenus en ligne, la réglementation en vigueur repose sur la directive e-commerce du 8 juin 2000 (1). Or, depuis l'adoption de cette directive, de nouveaux services numériques ont vu le jour, contribuant aux transformations sociétales dans l'Union européenne. Les conditions pour la fourniture de services numériques dans le marché intérieur doivent donc garantir la sécurité en ligne, la protection des droits fondamentaux et la lutte contre la désinformation. Il est en effet fondamental que ce qui est illégal hors ligne soit également illégal en ligne. Le cadre juridique dessiné par la directive du 8 juin 2000 a donc vocation à évoluer.

En matière de données, aucun cadre européen ne permet de faciliter leur partage et leur réutilisation. Pourtant, l'économie de la donnée est un vecteur d'innovation et de croissance pour les entreprises et les États européens. En outre, la création d'un cadre spécifique pour l'échange des données doit permettre d'interdire les partages de données à caractère personnel ou non personnel non conformes aux valeurs de l'Union européenne, et de s'assurer de la transparence, de la sécurité et du caractère non discriminatoire des acteurs intervenant sur le marché de la donnée.

2. Plusieurs initiatives européennes doivent permettre une meilleure régulation de la concurrence, des contenus et de l'économie de la donnée

La Commission européenne a publié, le 15 décembre 2020, deux propositions de règlement pour réformer l'espace numérique européen, le *Digital Market Act* (DMA) et le *Digital Services Act* (DSA).

a. L'encadrement des gatekeepers *par le Digital Markets Act (DMA)*

Le Digital Markets Act (DMA) est une proposition de Règlement de la Commission européenne visant à instaurer un nouveau modèle de régulation du comportement concurrentiel des grandes plateformes sur le marché unique européen.

L'adoption de ce texte, qui pourrait aboutir sous la présidence française de l'Union européenne en 2022, devrait donc permettre une meilleure régulation concurrentielle des entreprises digitales, afin de prendre en compte les spécificités de l'économie numérique. L'adoption de cette proposition de Règlement doit contribuer à la construction d'une souveraineté numérique européenne. En outre, le DMA doit permettre aux citoyens de mieux maîtriser les informations sur le DSA.

---

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

Au-delà de l'Union européenne, le DMA entre en résonnance avec les positions américaines récentes en faveur de la régulation des géants du numérique, renforcées depuis l'élection de M. Joseph Biden en tant que président des États-Unis d'Amérique. Dès octobre 2020, le rapport de la sous-commission pour l'Antitrust de la commission des lois de la Chambre des représentants américaine proposait le démantèlement de certains groupes dont la position dominante représentait un risque sur le marché américain, et l'interdiction pour les entreprises digitales d'opérer sur des secteurs trop proches de leurs activités [(1)].

En lien avec les questions de concurrence et de compétitivité des entreprises du numérique, le président Joseph Biden a également proposé, au sein de l'OCDE, pour celles d'entre elles qui réalisent plus de 20 milliards de dollars de bénéfices par an, une exception à la règle de taxation des bénéfices dans le pays d'établissement. Ces dernières seraient imposées dans les pays où leurs biens et services sont réellement achetés : une centaine de compagnies serait concernée, dont les GAFA. Au niveau national, le Made in America Tax Plan prévoit de doubler le montant de la *Global Intangible Low Tax Income*, à 21 % [(2)].

(1) Judiciary Committee, subcommittee on Antitrust, Commercial and Administrative Law, Investigation of Competition in Digital Markets, 4 oct. 2020.

(2) IFRI, De la taxe numérique à l'imposition des multinationales – La révolution fiscale, 15 avril 2021.

Les points clés du Digital Markets Act (DMA)

Le Digital Markets Acts cible les entreprises considérées comme étant en capacité de contrôler l'accès au marché. On parle, à cet égard, de gatekeepers. Les plateformes sont considérées comme tel dès lors lorsqu'elles remplissent trois critères cumulatifs :

– Une position économique forte, avec une incidence significative sur le marché intérieur et une activité dans au moins trois États membres de l'Union européenne ;

– Une position d'intermédiation forte : l'entreprise relie une base d'utilisateurs importante à un grand nombre d'entreprises. Les seuils retenus pour déterminer la position d'intermédiation forte sont de 45 millions d'utilisateurs actifs par mois dans l'Union Européenne et de plus de 10 000 utilisateurs actifs professionnels lors de la dernière année d'exercice ;

– Une stabilité dans le temps, avec une position solide et durable sur le marché : la plateforme doit remplir les critères précédents sur la période couvrant les trois derniers exercices.

Le DMA soumet, en outre, ces contrôleurs d'accès au marché à des restrictions nouvelles et directement applicables :

– L'interdiction de connecter automatiquement l'utilisateur d'un de leurs services à d'autres services leur appartenant, sans recueil préalable du consentement ;

– L'interdiction de croiser les données personnelles des utilisateurs d'un de leurs services avec des données collectées par d'autres biais ;

– L'interdiction de contraindre un utilisateur à utiliser un service complémentaire pour accéder au service principal ;

– L'interdiction de restreindre les voies de recours des utilisateurs en cas de litige.

Les contrôleurs d'accès devront également informer systématiquement la Commission de tout projet de concentration impliquant un autre fournisseur de services numériques. Cette disposition vise à éviter les « acquisitions tueuses », mais le DMA ne prévoit pas de donner de pouvoirs supplémentaires à la Commission par rapport au contrôle classique des concentrations.

Le DMA prévoit en outre une liste d'obligations susceptibles d'être précisées par la Commission, dans le cadre d'un dialogue avec les contrôleurs d'accès et en fonction des services qu'ils proposent. Ces obligations, qui ne sont pas directement applicables et ne concerneront que certains contrôleurs d'accès, sont relatives à :

– La préservation des données générées par les utilisateurs professionnels auprès des contrôleurs d'accès ;

– La préservation de conditions concurrentielles équitables entre les contrôleurs d'accès et leurs utilisateurs professionnels, lorsqu'ils interviennent sur les mêmes marchés ;

– La liberté des utilisateurs professionnels de choisir leurs fournisseurs d'accès, d'installer ou de désinstaller des applications sans restrictions de services, grâce à la portabilité des données ;

– La préservation de conditions de concurrence équitables entre les contrôleurs d'accès et leurs partenaires commerciaux.

Le DMA renforce enfin les pouvoirs de la Commission en matière de contrôle des comportements anticoncurrentiels des plateformes sur le marché numérique. Il prévoit, en outre, un contrôle des obligations qu'il édicte, ainsi que des sanctions. La Commission peut désormais mener des enquêtes de marché pour deux motifs distincts : déterminer si un opérateur doit être ou non qualifié de contrôleur d'accès, et contrôler le respect par les contrôleurs d'accès de leurs obligations. Elle peut adopter une décision constatant la non-conformité du contrôleur d'accès avec ses obligations, et lui infliger une amende qui peut aller jusqu'à 10 % du chiffre d'affaires total réalisé lors de l'exercice précédent. En cas d'infraction systématique, elle peut également imposer des mesures coercitives comportementales ou structurelles, proportionnées à l'infraction.

Source : Digital Markets Act – auditions de la mission d'information

b. La régulation des contenus en ligne avec le Digital Services Act (DSA)

Le DSA, ou législation sur les services numériques, vise à renforcer le contrôle des contenus démocratiques.

Le DSA établit un nouveau cadre de régulation des contenus numériques, en complément de la législation existante. Il prévoit de compléter le droit européen de la régulation des contenus en ligne, qui repose actuellement sur la directive 2000/31/CE sur le commerce électronique du 8 juin 2000. La proposition de Règlement vise toutes les entreprises, quel que soit leur lieu d'établissement, qui offrent des services numériques aux personnes établies dans l'Union européenne.

L'ambition du DSA est double :

– *prendre en compte les évolutions survenues dans l'espace numérique,* notamment l'émergence de très grandes plateformes en ligne ou de nouveaux systèmes de publicité fondés sur des décisions algorithmiques complexes ;

– établir des *obligations claires et harmonisées dans toute l'Union Européenne* vis-à-vis des fournisseurs de services.

L'objectif de la Commission, soutenu par le Gouvernement français, est de parvenir à un accord entre le Parlement européen et le Conseil sur le DSA au premier semestre 2022.

Selon la Commission, en remédiant à la fragmentation juridique de la réglementation du numérique dans l'Union Européenne, le DSA pourrait aboutir à une augmentation du commerce numérique transfrontalier de 1 % à 1,8 %, soit l'équivalent d'une augmentation du chiffre d'affaires de 8,6 à 15,5 millions d'euros.

Les points clés du Digital Services Act (DSA)

Le Digital Services Act comporte plusieurs points clés qui doivent dessiner un cadre de régulation renouvelé pour les acteurs du numérique.

Il réaffirme, d'abord, les principes préexistants du droit de la régulation des prestataires de services en ligne. Les fournisseurs de services intermédiaires demeurent ainsi exonérés de responsabilité en cas de circulation, stockage ou d'un transmission d'un contenu illicite, à condition que leurs activités soient uniquement d'ordre technique vis-à-vis de ce contenu (principe du régime atténué de responsabilité). De même, ces prestataires ne sont pas soumis à une obligation générale de surveillance des contenus, la notion de « contenus illicites » n'est pas modifiée, et, enfin, la clause « marché intérieur », qui prévoit que les services de la société de l'information sont soumis à la législation de l'État membre dans lequel le prestataire est établi, n'est pas remise en cause.

Le DSA prévoit en revanche plusieurs nouveautés. Il crée en effet de nouvelles catégories juridiques parmi les acteurs du numérique :

– Les prestataires de services intermédiaires, qui comprennent l'ensemble des prestataires techniques intervenant dans l'espace numérique ;

– Les hébergeurs, qui offrent un service de stockage d'information fournie par un destinataire du service et à sa demande ;

– Les plateformes en ligne, qui constituent un type particulier d'hébergeur et qui, comme activité principale, stockent et diffusent des informations à la demande d'un destinataire du service ;

– Les grandes plateformes en ligne, caractérisées par un nombre d'utilisateurs mensuels moyens dans l'Union Européenne supérieur ou égal à 45 millions.

En lien avec ces différentes catégories d'acteurs, le DSA crée de nouvelles obligations, résumées dans un tableau en annexe, poursuivant deux objectifs principaux :

– La lutte contre les contenus et les pratiques illicites, avec l'obligation de coopération avec les autorités étatiques compétentes ou la mise en place de mécanismes permettant aux utilisateurs de signaler la présence de contenus ;

– Le renforcement des garanties offertes aux utilisateurs de services numériques, avec leur information sur les pratiques en matière de modération et le renforcement de l'obligation de transparence en matière de publicité.

Des obligations seront mises à la charge de l'ensemble de ces intermédiaires, mais des obligations plus sévères seront également mises à la charge des hébergeurs et des plateformes : les obligations varient selon les caractéristiques des prestataires de services numériques considérés. Par exemple, comme l'illustre le diagramme ci-dessous, les plateformes devront respecter les obligations pesant sur tous les prestataires de services intermédiaires, les obligations applicables uniquement aux hébergeurs, et les obligations supplémentaires destinées aux plateformes en ligne.

Le DSA prévoit enfin un contrôle du respect des obligations qu'il édicte, ainsi que des sanctions :

– Un coordinateur national des services numériques, chargé de la bonne exécution du Règlement, devra être désigné dans chaque État membre et disposera de pouvoirs d'enquête, de décision et de sanction ;

– Les sanctions applicables en cas de non-respect seront prévues par les droits nationaux : la sanction ne devra pas dépasser 6 % du chiffre d'affaire annuel de l'entreprise.

Source : Digital Services Act – auditions de la mission d'information

Le DSA doit permettre de renforcer la souveraineté numérique nationale et européenne de manière à ce que ce que les contenus illicites, ne respectant pas les valeurs des États membres et de l'Union européenne soient retirés dans un délai restreint après leur mise en ligne.

c. La création d'un marché unique des données avec le Digital Governance Act (DGA)

La Commission européenne a publié le 19 février 2020 sa stratégie en matière de données : le DGA est une proposition de Règlement présentée le 25 novembre 2020, dans la continuité de cette communication, qui doit s'articuler avec le DSA et le DMA. Le DGA a pour but de favoriser le partage de données, la création d'un espace européen de données, d'établir une relation de confiance avec les citoyens européens et de maintenir une relation étroite avec le RGPD.

Le DGA doit permettre à l'Union de s'adapter à l'augmentation sans précédent de la création et de l'utilisation de données numériques, liée au besoin des applications d'atteindre des performances toujours plus élevées. La Commission souhaite donc faire de l'Europe un lieu d'innovation et de croissance, en créant une économie de la donnée fondée sur la libre circulation et la réutilisation des données, incarnant une troisième voie, se différenciant des modèles américains et chinois.

Pour parvenir à cet objectif, l'Europe a besoin d'un cadre commun pour le partage des données au sein de l'Union européenne, qui remplace les normes actuelles, imposées par les grandes entreprises technologiques telles que les GAFAM.

L'objectif du DGA est donc de garantir la confiance en fournissant un cadre juridique européen de partage des données mais aussi de proposer une base technique, pour encourager la circulation des données entre entreprises ainsi qu'entre entreprises et administrations publiques.

La Commission donne une nouvelle définition large des données, définies comme « *toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, y compris sous forme d'enregistrement sonore, visuel ou audiovisuel.* »

Les points clés du Digital Governance Act (DGA)

Concernant les données détenues par les acteurs publics, le DGA propose la création d'un mécanisme de réutilisation de certaines catégories de données protégées du secteur public. Les organismes du secteur public devront être équipés sur le plan technique, afin que la protection des données, le respect de la vie privée et la confidentialité soient préservés, et les États membres devront mettre en place un point de contact unique pour aider les chercheurs et entreprises innovantes à sélectionner les données appropriées (1).

Le DGA doit également permettre d'accroître la confiance dans le partage de données à caractère personnel ou non personnel. Il définit en particulier les règles applicables à l'activité des prestataires de services de partage de données entre acteurs privés. Les intermédiaires devront satisfaire une obligation de neutralité et ne pourront pas utiliser les données pour leur propre compte.

Le DGA prévoit également de faciliter l'altruisme des données, soit les hypothèses dans lesquelles des entreprises privées sont amenées à partager leurs données avec des organisations à but non lucratif, afin de permettre le développement d'applications d'intérêt général. Les organisations à but non lucratif pourront s'inscrire sur un registre public en tant qu'« organisation altruiste en matière de données ».

Le texte prévoit enfin la création d'un comité européen de l'innovation dans le domaine de la donnée, qui sera un groupe d'experts formel chargé d'établir des bonnes pratiques à l'intention des autorités compétentes des États membres.

Source : Digital Governance Act – auditions de la mission d'information

Le DGA doit ainsi permettre à l'Union de rattraper son retard en matière d'économie de la donnée et d'élargir les possibilités de croissance pour les entreprises du numérique, tout en respectant les valeurs européennes en matière de confidentialité et de protection de la vie privée. Le DGA incarne ainsi un équilibre entre les deux piliers de la souveraineté numérique : la consolidation de l'écosystème européen des entreprises du digital et la régulation de leurs pratiques.

d. La proposition de Règlement sur l'Intelligence artificielle : maîtriser les risques sans entraver le développement technologique

La Commission a présenté le 21 avril 2021 une proposition législative afin d'encourager et d'encadrer le développement et le déploiement de l'Intelligence artificielle. Cette proposition vient parachever une réflexion menée depuis plusieurs années sur cette problématique et sur les enjeux associés, matérialisée par la publication d'une stratégie européenne en 2018 (2) et par la publication d'un livre blanc en février 2020 (3). La proposition repose sur deux axes : le soutien à l'innovation d'une part et le respect des droits fondamentaux de l'usager d'autre part. Cette approche duale qui vise, à la fois, à promouvoir le recours à l'Intelligence

(1) Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données, publiée par la Commission le 25 novembre 2020.

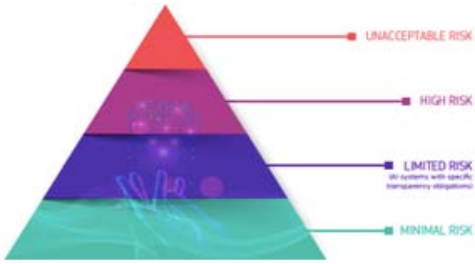
(2) Commission européenne, Communication « L'Intelligence artificielle pour l'Europe », COM (2018) 237 final.

(3) Commission européenne, Livre blanc « Intelligence artificielle, une approche européenne axée sur l'excellence et la confiance », COM (2020) 65 final.

artificielle, tout en tenant compte des risques associés, de façon proportionnée, est reprise par la Commission dans sa proposition de Règlement et constitue le fil conducteur de son action.

Les points clés de la proposition de Règlement sur l'Intelligence artificielle

Dans le cadre de sa proposition de règlement sur l'Intelligence artificielle, la Commission propose de différencier l'approche et l'intensité des obligations selon le niveau de risque créé par les différentes utilisations possibles de l'Intelligence artificielle. Elle distingue ainsi les utilisations qui créent un risque inacceptable pour les valeurs de l'Union (ces systèmes sont alors interdits), celles qui créent un risque élevé (systèmes soumis à des obligations renforcées), celles qui créent un risque faible et celles qui comportent un risque minime. La Commission propose d'encadrer les utilisations à haut risque, à l'aide d'obligations renforcées et de définir une liste de domaines d'utilisation interdits.



Infographie « catégorisation des risques » / Source : Commission européenne, europa.eu

La proposition de Règlement prévoit également des mesures pour encourager l'innovation, avec la mise en place des « bacs à sable » réglementaires, en vue de faciliter l'expérimentation de technologies innovantes pendant une durée limitée et sur la base d'un plan de test convenu avec les autorités compétentes.

Un comité européen de l'Intelligence artificielle sera également créé, ainsi qu'une base de données gérée par la Commission, pour les systèmes autonomes d'Intelligence artificielle à haut risque ayant des implications en matière de droits fondamentaux.

La proposition de Règlement s'accompagne enfin d'une actualisation du plan d'action coordonnée relatif à l'Intelligence artificielle mis au point par la Commission en 2018, afin de poursuivre quatre objectifs : la définition de conditions favorables au développement de l'Intelligence artificielle dans l'Union européenne (1); faire de l'Union européenne le lieu où l'excellence se développe, du laboratoire au marché (2); construire un leadership stratégique dans les secteurs à fort impact (3); veiller à ce que l'Intelligence artificielle soit au service des citoyens et de la société (4).

Pour atteindre ces objectifs, la Commission propose que l'Union européenne investisse dans l'Intelligence artificielle à hauteur d'un milliard d'euros par an par l'intermédiaire des programmes « Horizon Europe » et « Europe numérique » pour la période 2021-2027. L'objectif est d'augmenter le niveau global des financements publics et privés en Europe destinés à l'Intelligence artificielle à hauteur de 20 milliards d'euros par an d'ici à la fin de la décennie.

Source : Commission européenne – auditions de la mission d'information

Le Conseil européen des relations internationales, dans une étude du 21 juin 2021, a confirmé **l'importance d'une approche basée sur le risque**, en soulignant que « *l'Intelligence artificielle digne de confiance ou éthique est une priorité pour l'Union* ». L'étude présente cette technologique comme « *hautement géopolitique* ».

L'adoption rapide de ces différents textes (DSA, DMA, DGA, règlement sur l'Intelligence artificielle) est indispensable pour garantir la crédibilité de l'Union européenne vis-à-vis de son ambition de défendre sa souveraineté numérique. La question du numérique doit être, en conséquence placée, au cœur de la présidence française de l'Union européenne lors du premier semestre de l'année 2022.

Proposition n° 64 : Fixer un cap ambitieux d'adoption des différentes initiatives de régulation en cours (DSA, DMA, DGA), pour conserver une crédibilité maximale sur la capacité de l'Union européenne à adopter de façon souple et rapide une régulation du numérique.

Proposition n° 65 : Mettre le numérique au cœur de la présidence française de l'Union européenne au premier semestre de l'année 2022.

C. DÉFENDRE UN MODÈLE EUROPÉEN DU NUMÉRIQUE, FONDÉ SUR LES DROITS FONDAMENTAUX

1. Une volonté commune de tracer une troisième voie

L'intérêt des États membres pour la réduction des dépendances stratégiques, et pour un renforcement corrélatif de la souveraineté numérique européenne et nationale, est réel. Il s'illustre, par exemple, dans le choix effectué par certains de consacrer une part importante du plan national de relance au secteur numérique. En effet, le programme inédit de relance *NextGenerationEU* impose aux États membres de consacrer au moins 20 % du montant total des fonds à la digitalisation de l'économie. Toutefois, certains États ont prévu d'aller au-delà de ce seuil, à l'image de l'Espagne qui y consacre près de 30 % [(1)] et de l'Allemagne qui prévoit d'y consacrer près de 50 % des fonds reçus [(2)]. De même, le projet Gaia-X, impulsé par l'Allemagne, puis la France, démontre l'existence d'un intérêt commun et transfrontalier pour les problématiques numériques.

Une dynamique favorable au renforcement de la souveraineté numérique européenne semble ainsi engagée sous la double impulsion de la Commission et des États membres.

Pour l'Union européenne, l'objectif n'est pas de créer un modèle similaire à celui de la Chine ni à celui des États-Unis, mais bien de proposer une troisième voie, fondée sur des valeurs partagées. Comme l'a indiqué M. Frédéric Précioso, responsable scientifique « Intelligence artificielle » au sein de l'Agence nationale

(1) Gobierno de España, "Executive summary : Recovery, Transformation and Resilience Plan", 5 mai 2021.

(2) Federal ministry of Finance, "German recovery and resilience plan adopted", 27 mai 2021.

de la recherche (ANR), « *l'Europe est très active sur cette question de la souveraineté européenne, en particulier autour du numérique et de l'Intelligence artificielle. Elle se positionne comme une troisième voie par rapport à la Chine et aux États-Unis, avec une autre approche de la préservation de la confidentialité des données, de la vie privée* » (1). L'adoption du RGPD et le projet Gaïa-X s'inscrivent pleinement dans la construction de cette troisième voie, tout comme les différents projets européens devant favoriser la co-construction d'un Internet de la confiance.

2. L'existence persistante de modèles de souveraineté divergents

Si les États membres et les institutions européennes s'accordent sur la nécessité de réduire les dépendances stratégiques de l'Union européenne, les divergences terminologiques existantes illustrent toutefois la présence de modèles de souveraineté divers. Faire coexister ces différents modèles étatiques peut être complexe.

En effet, si la notion de « souveraineté » a été évoquée par Mme Ursula von der Leyen dans son discours sur l'État de l'Union (2), celle « d'autonomie stratégique », et même « d'autonomie stratégique ouverte » est préférée dans certains documents récents, comme celui actualisant la politique industrielle de l'Union européenne (3). Dans cette perspective, « la souveraineté » est entendue comme la liberté de choisir et de sélectionner ses dépendances, et de multiplier les fournisseurs d'un même composant. Cette acception rejoint d'ailleurs la définition de la souveraineté donnée par M. Arnaud Castaignet, directeur de la communication et des affaires publiques de Skeleton Technologies, et ancien directeur des relations publiques du programme estonien *e-residency* : *« La meilleure définition, à mon sens, de la souveraineté numérique assimile cette notion à la capacité d'effectuer des choix en tout liberté* […] *La coopération avec le reste du monde n'est pas écarter* a priori*, à condition d'en décider librement et en toute connaissance de cause* » (4).

Il est toutefois nécessaire de s'entendre sur le périmètre de cette coopération, et sur le choix des partenaires. Votre rapporteur soutient que ceux-ci peuvent différer selon les besoins stratégiques en cause et leurs sensibilités. Le degré d'ouverture doit varier selon les domaines considérés. Les partenariats commerciaux existants, ou les alliances militaires conclues, ne doivent pas freiner l'ambition de l'Union européenne dans ce domaine. À cet égard, votre rapporteur soutient pleinement l'initiative nationale consistant à doter la France d'un *cloud* entièrement souverain, garantissant un stockage des données très sensibles et critiques, totalement maîtrisé et sécurisé.

---

(1) Audition de M. Frédéric Précioso, 15 avril 2021.

(2) Commission européenne, « État de l'Union 2020 », p. 14.

(3) Commission européenne, « Updating the 2020 New Industrial Strategy : Building a stronger Single Market for Europe recovery », COM (2021) 350 final, 5 mai 2021.

(4) Audition de M. Arnaud Castaignet, 1er juin 2021.

Pour tracer cette troisième voie, les États membres de l'Union européenne, ainsi que leurs juridictions respectives, doivent s'entendre sur des valeurs partagées.

3. La nécessité de s'accorder sur des valeurs partagées et de les diffuser

Pour tracer une troisième voie et ainsi devenir une puissance influante sur la gouvernance d'Internet à l'échelon mondial, l'Europe doit prélablement s'accorder sur des valeurs partagées et les diffuser.

Les projets menés dans ce domaine peuvent utilement s'appuyer sur différents piliers : la réversibilité des choix effectués, la liberté pour les citoyens de disposer de leurs données, la sécurisation pleine et entière de ces dernières, l'affirmation d'un double principe de confiance et de transparence, la nécessaire prise en considération de l'empreinte environnementale des projets numériques.

À cet égard, votre rapporteur soutient pleinement les projets portés par M. Thierry Breton, qui s'inscrivent dans cette dynamique.

Comme l'a rappelé M. Arnaud Castaignet, la notion de transparence constitue la clé de voûte du système numérique estonien [(1)]. La transparence est en effet essentielle à l'établissement d'un système numérique européen et français de confiance et doit permettre aux citoyens de recouvrer un contrôle sur leurs données, afin de garantir leur intégrité. Pour favoriser la diffusion d'une telle approche, votre rapporteur propose de développer une culture de la transparence dans le cyberespace.

Il convient enfin de mieux défendre les intérêts français et européens au sein des instances de normalisation afin de peser au maximum sur les choix techniques opérés.

Proposition n° 66 : Investir davantage les instances internationales de régulation de l'Internet et de normalisation des technologies numériques, pour renforcer le poids de la représentation des intérêts français et européens dans le domaine du numérique.

([1]) Audition de M. Arnaud Castaignet, 1er juin 2021.

CONCLUSION

Les travaux menés depuis près d'un an conduisent votre rapporteur à une conclusion simple et forte : la construction d'une souveraineté numérique nationale et européenne doit être le fil rouge des décisions politiques mises en œuvre dans la décennie à venir. Il s'agit en effet d'un impératif absolu.

Sans cette boussole, le risque est grand de voir les capacités d'action des individus, des entreprises et des États se réduire progressivement, faute de maîtriser le « nouveau monde » numérique, alors que de nouveaux acteurs, publics et privés, se sont emparés de leviers d'influence pour servir leurs propres intérêts. Le cadre européen doit être considéré, à cet égard, de façon pragmatique : il est le niveau d'efficience à mobiliser au service de la vision du numérique que portent ses États membres et de la défense des intérêts numériques européens.

Votre rapporteur souhaite également porter un second message : au-delà de son caractère diffus, la souveraineté numérique est un sujet très concret. Chacun doit donc se saisir de cette question à son échelle. Il s'agit, par exemple, pour l'État de se prémunir des attaques informatiques d'ampleur et d'être capable de faire évoluer ses modes d'intervention, tout en conservant la maîtrise des processus utilisés.

Pour les entreprises en général, cet enjeu de souveraineté est une question de confiance vis-à-vis de leurs clients et de liberté dans leurs stratégies de croissance et de transformation. Quant aux acteurs technologiques nationaux, le soutien à leur apporter doit être une priorité, ce qui appelle un changement d'état d'esprit et de pratiques, notamment au sein de la commande publique.

Enfin, pour les citoyens, la souveraineté numérique prend la forme de la question de la confiance dans le numérique. Le recours à des usages numériques de plus en plus sophistiqués ne doit en effet pas conduire au moindre compromis vis-à-vis de la sécurité de leurs données. Elle concerne aussi, évidemment, leur liberté de choix en tant qu'électeurs, qui ne saurait être affectée par des tentatives d'influence étrangères, lors des moments clefs de la vie de la nation que sont les élections.

En définitive, une souveraineté numérique est possible, à condition de nous donner les moyens de nos ambitions et de faire preuve de pragmatisme. Si les points d'équilibre sont souvent difficiles à trouver, entre protection des données et innovation, préférence européenne et ouverture sur le monde, ou encore numérisation et inclusion, votre rapporteur est convaincu d'une chose : l'absence, dans ce domaine, pendant de nombreuses années, de ligne directrice et de stratégie de l'Europe, a été préjudiciable et explique en partie la situation actuelle de dépendance décrite au fil des pages du présent rapport.

Le récent « réveil européen », incontestable, doit désormais s'incarner dans des actes. De ce point de vue, les nombreuses initiatives lancées, tant sur le plan technologique que réglementaire, constituent des signaux positifs que la France doit soutenir de toutes ses forces, et porter, en première ligne, lorsqu'elle présidera l'Union européenne, au premier semestre de l'année 2022.

LISTE DES PROPOSITIONS

Proposition n° 1 : Créer un « comité numérique de crise » réunissant les opérateurs, les grands acteurs du numérique et les pouvoirs publics en cas de difficulté sur les réseaux numériques (page 40).

Proposition n° 2 : Renforcer les contrôles mis en œuvre par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) sur la qualité du déploiement des réseaux fixes (page 42).

Proposition n° 3 : Maintenir une exigence maximale de sécurité vis-à-vis des déploiements 5G.

Proposition n° 4 : Assurer un traitement rapide des demandes d'autorisation d'exploitation d'équipements 5G. Garantir également une transparence des critères de décision mis en œuvre dans ce cadre.

Proposition n° 5 : Renforcer les effectifs de la commission nationale de l'informatique et des libertés (CNIL) dans le cadre du projet de loi de finances pour 2022.

Proposition n° 6 : Simplifier le processus de sanction par la CNIL pour les dossiers de moyenne et de faible intensité, afin de renforcer sa capacité à prononcer les « mesures correctrices » prévues par le règlement général sur la protection des données (RGPD).

Proposition n° 7 : Intégrer de façon systématique au sein des arbitrages techniques des projets numériques les enjeux ayant trait à la souveraineté numérique, en particulier concernant la protection des données personnelles et la localisation des données en Europe.

Proposition n° 8 **:** Réaliser un état des lieux de l'arsenal juridique national permettant de s'opposer à la communication d'informations à une puissance étrangère et former les acteurs publics à ce type d'outils.

Proposition n° 9 : Actualiser et renforcer, le cas échéant, *la loi de blocage du 26 juillet 1968*, conformément aux recommandations formulées au sein du rapport « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » remis au Premier ministre par M. le député Raphaël Gauvain en 2019.

Proposition n° 10 : Accélérer le déploiement de l'identité numérique en France.

Proposition n° 11 : Engager une stratégie ambitieuse de montée en compétences au sein de l'État sur la gestion de projets numériques afin de ne pas répéter les erreurs du passé.

Proposition n° 12 : Renforcer le recrutement par contrat de droit privé de profils techniques, pour mener à bien les projets numériques de l'État et mettre en œuvre une stratégie de fidélisation pour les conserver au sein de la sphère publique.

Proposition n° 13 : Favoriser la circulation des compétences numériques au sein du secteur public.

Proposition n° 14 : Lancer une grande campagne de communication sur l'identité numérique.

Proposition n° 15 : Créer un guichet numérique unique d'accès de chaque citoyen à l'ensemble des services publics, lui permettant aussi d'être informé en temps réel de l'utilisation de ses données par l'administration.

Proposition n° 16 : Créer un numéro d'identification unique afin de mettre fin aux difficultés rencontrées par les administrations pour identifier les administrés et partager leurs informations de façon efficace.

Proposition n° 17 : Développer une culture de la transparence vis-à-vis des données utilisées par la puissance publique dans le cadre de ses interactions avec les citoyens.

Proposition n° 18 : Former aux compétences numériques dès le plus jeune âge et tout au long de la scolarité et de la vie professionnelle.

Proposition n° 19 : Former les citoyens aux gestes barrières face au risque cyber.

Proposition n° 20 : Développer l'apprentissage du code à l'école pour doter les élèves des fondamentaux de cet alphabet du monde numérique.

Proposition n° 21 : Développer la capacité des établissements scolaires à former les élèves aux enjeux de l'innovation et soutenir la création de projets numériques.

Proposition n° 22 : Proposer dans le cadre de la formation professionnelle des modules dédiés aux technologies numériques.

Proposition n° 23 : Poursuivre la dynamique de constitution d'un campus cyber.

Proposition n° 24 : Faire des instituts universitaires de technologie des centres d'excellence pour fournir à la France des techniciens numériques en nombre suffisant.

Proposition n° 25 : Accélérer le renforcement de l'offre de formation « *blockchain* » et soutenir la sensibilisation du monde professionnel au potentiel de cette technologie.

Proposition n° 26 : Privilégier, en matière de commande publique, le recours aux solutions d'acteurs technologiques français ou européens.

Proposition n° 27 : Exiger de l'Union des groupements d'achats publics (UGAP) des délais raisonnables dans le traitement des demandes de référencement des acteurs de l'offre numérique française (page 98).

Proposition n° 28 : Créer un guide d'information des acteurs publics sur les outils de la commande publique, afin d'encourager, notamment, la pratique de l'allotissement, le recours par les collectivités au « dialogue compétitif » en matière de numérique et l'usage de la mention « Spécial France », toutes mesures qui permettront de rendre plus systématique le recours aux acteurs français au sein de la commande publique.

Proposition n° 29 : Lancer une mission d'expertise sur les enjeux de souveraineté de la commande publique, afin d'identifier les leviers permettant de faire évoluer le cadre juridique actuel, en faveur de la prise en compte des enjeux de sécurité numérique, de gestion et de localisation des données en Europe.

Proposition n° 30 : Faire évoluer les pratiques et le cadre juridique de la commande publique :

Au niveau national :

– En intégrant le principe selon lequel l'hébergeur ne doit pas être soumis à des lois extra-européennes dans les normes de sécurité existantes (SecNumCloud, HDS, ISO 27001) ;

– En intégrant dans les clauses administratives générales des marchés (CCAG) des obligations liées à la localisation des données en Europe, sous peine de condamnation pénale des dirigeants du *cloud* ;

– En soutenant une « culture du risque » chez les acheteurs publics (sécurisation juridique) et en améliorant leur formation aux aspects extra-juridiques de la commande publique.

Au niveau européen :

– En mettant en place rapidement un *Small Business Act* ;

– En étendant à d'autres produits le régime de préférence communautaire existant dans les infrastructures ;

– En clarifiant l'article 25 de la directive européenne de 2014 pour identifier précisément les cas dans lesquels une offre d'un État tiers peut être écartée

Proposition n° 31 : Renforcer le soutien public à destination de la French Tech, pour encourager ses membres à « chasser en meute » (page 100).

Proposition n° 32 : Accélérer le développement du marché du capital-risque et l'harmonisation du marché des capitaux en Europe pour réduire le différentiel d'attractivité avec les États-Unis et éviter le départ de pépites européennes pour des raisons liées à la recherche de financements.

Proposition n° 33 : Encourager les entreprises françaises à développer des stratégies de captation de brevets, afin de leur permettre de résister aux pratiques agressives de leurs concurrents étrangers.

Proposition n° 34 : Augmenter les moyens financiers et les effectifs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour répondre à la croissance de la menace cyber (page 109).

Proposition n° 35 : Consentir un engagement financier inédit à destination des acteurs de la protection numérique au sens large, c'est-à-dire la plateforme Pharos, le groupement d'intérêt public Action contre la Cybermalveillance (ACYMA) et le parquet national cyber.

Proposition n° 36 : Labelliser les prestations de cybersécurité pour renforcer la visibilité des acteurs privés sur la qualité des offres disponibles sur le marché.

Proposition n° 37 : Systématiser la couverture du risque cyber dans les polices d'assurance.

Proposition n° 38 : Renforcer la sensibilisation des acteurs privés vis-à-vis du coût du risque cyber. Travailler également à l'amélioration des techniques de quantification de ce risque.

Proposition n° 39 : Veiller à ce que la trajectoire définie au sein de la loi de programmation militaire pluriannuelle soit en adéquation avec l'état de la menace et le niveau d'ambition porté par la France dans ce domaine.

Proposition n° 40 : Accélérer la mise à niveau des équipements numériques des collectivités territoriales et des structures de soins pour garantir leur résilience.

Proposition n° 41 : Appliquer une doctrine de l'autonomie technologique « maximale » en matière de renseignement et de cyberdéfense, en faisant du recours à des technologies extra-européennes une exception devant être motivée.

Proposition n° 42 : Accélérer la dynamique de constitution d'un écosystème français et européen d'entreprises « cybertech ».

Proposition n° 43 : Recruter davantage de profils techniques issus du secteur de la sécurité numérique, en rehaussant les rémunérations proposées et en adressant la question de la qualité de vie au travail.

Proposition n° *44* : Formaliser un « parcours public » cyber offrant des débouchés aux profils à haute valeur ajoutée recrutés par les acteurs de la chaîne de défense et de sécurité nationale.

Proposition n° 45 : Créer un ministère du numérique, doté d'une administration et de moyens propres, et chargé de porter les politiques numériques aux niveaux national, européen et international.

Proposition n° 46 : Mettre en place un briefing hebdomadaire du Président de la République sur les questions technologiques en s'inspirant du modèle américain.

Proposition n° 47 : Créer un document de politique transversale (DPT) dédié aux politiques publiques du numérique, en complétant en ce sens *l'article n° 128 de la loi n° 2005 – 1720 du 30 décembre 2005 de finances rectificative pour 2005*.

Proposition n° 48 : Renforcer le volet numérique des contrats de plan État-régions.

Proposition n° 49 : Accélérer la mise en œuvre d'une politique ambitieuse d'ouverture des données au sein des administrations publiques.

Proposition n° 50 : Créer un portail public rassemblant l'ensemble des offres numériques françaises disponibles.

Proposition n° 51 : Assurer un travail de veille pour intégrer dans la gestion des projets numériques les méthodes de travail et d'organisation les plus performantes.

Proposition n° 52 : Imposer au sein de l'administration le recours systématique au logiciel libre, en faisant de l'utilisation de solutions propriétaires une exception.

Proposition n° 53 : Imposer au sein de l'administration le recours systématique à des solutions numériques françaises, lorsque leur niveau de performance est satisfaisant pour les usages concernés.

Proposition n° 54 : Garantir en droit la force probante de la *blockchain* pour créer un cadre favorable au développement de cette technologie.

Proposition n° 55 : Lancer une réflexion sur la création d'un système de certification des blockchains conformément à la recommandation n° 7 du rapport IMT-CEA-INRIA « Les verrous technologiques des blockchains » publié en avril 2021.

Proposition n° 56 **:** Développer une offre *cloud* européenne respectant les valeurs du modèle européen.

Proposition n° 57 : Garantir au sein de Gaia-X une gouvernance et une conduite de projets conformes aux ambitions exprimées par ses membres fondateurs afin d'éviter que cette initiative ne devienne un instrument au service de la croissance d'acteurs déjà dominants.

Proposition n° 58 : Accélérer le déploiement d'une constellation européenne de satellites en orbite basse.

Proposition n° 59 : Encourager la localisation ou la relocalisation en Europe d'usines de production d'équipements numériques sur l'ensemble de la chaîne de valeur.

Proposition n° 60 : Renforcer les moyens mis en œuvre dans le cadre des projets importants d'intérêt européen commun (PIEEC) et adopter à chaque reprise des calendriers ambitieux de déploiement.

Proposition n° 61 : Renforcer le recours aux outils de défense économique de l'Union européenne et durcir, le cas échéant, le Règlement 2019/42 du 19 mars 2019 relatif au contrôle des investissements étrangers.

Proposition n° 62 : Intégrer, au sein de la politique de la concurrence de l'Union européenne, les enjeux de souveraineté numérique et d'autonomie stratégique de l'Union.

Proposition n° 63 : Doter l'Europe d'une capacité d'anticipation et de veille sur les

technologies numériques.

Proposition n° 64 : Fixer un cap ambitieux d'adoption des différentes initiatives de régulation en cours (DSA, DMA, DGA), pour conserver une crédibilité maximale sur la capacité de l'Union européenne à adopter de façon souple et rapide une régulation du numérique.

Proposition n° 65 : Mettre le numérique au cœur de la présidence française de l'Union européenne au premier semestre de l'année 2022.

Proposition n° 66 : Investir davantage les instances internationales de régulation de l'Internet et de normalisation des technologies numériques, pour renforcer le poids de la représentation des intérêts français et européens dans le domaine du numérique.

LISTE THÉMATIQUE DES PROPOSITIONS

I. CONSTRUIRE DANS LE TEMPS LONG UN CYBERESPACE FRANÇAIS ET EUROPÉEN SÛR ET FIABLE.

A. ASSURER LA CAPACITÉ DE RÉSILIENCE DE NOS INFRASTRUCTURES NUMÉRIQUES.

Proposition n° 1 : Créer un « comité numérique de crise » réunissant les opérateurs, les grands acteurs du numérique et les pouvoirs publics en cas de difficulté majeure sur les réseaux numériques (page 40).

Proposition n° 2 : Renforcer les contrôles mis en œuvre par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) sur la qualité du déploiement des réseaux fixes (page 42).

Proposition n° 3 : Maintenir une exigence maximale de sécurité vis-à-vis des déploiements 5G (page 43).

Proposition n° 4 : Assurer un traitement rapide des demandes d'autorisation d'exploitation d'équipements 5G et garantir une transparence des critères de décision mis en œuvre dans ce cadre (page 43).

B. PROMOUVOIR UNE CULTURE COLLECTIVE DE LA CYBERPROTECTION.

1. Entreprises.

Proposition n° 36 : Labelliser les prestations de cybersécurité pour renforcer la visibilité des acteurs privés sur la qualité des offres disponibles sur le marché (page 110).

Proposition n° 37 : Systématiser la couverture du risque cyber dans les polices d'assurance (page 111).

Proposition n° 38 : Renforcer la sensibilisation des acteurs privés vis-à-vis du coût du risque cyber. Travailler également à l'amélioration des techniques de quantification de ce risque (page 111).

2. État et acteurs publics.

Proposition n° 34 : Augmenter les moyens financiers et les effectifs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour répondre à la croissance de la menace cyber (page 109).

Proposition n° 35 : Consentir un engagement financier inédit à destination des acteurs de la protection numérique au sens large, c'est-à-dire la plateforme Pharos, le groupement d'intérêt public Action contre la Cybermalveillance (ACYMA) et le parquet national cyber (page 109).

Proposition n° 40 : Accélérer la mise à niveau des équipements numériques des collectivités territoriales et des structures de soins pour garantir leur résilience (page 120).

3. Citoyens – usagers du numérique.

***Proposition n° 19* :** Former les citoyens aux gestes barrières face au risque cyber (page 66).

C. CONSERVER DES CAPACITÉS DE CYBERDÉFENSE AUTONOMES.

Proposition n° 23 : Poursuivre la dynamique de constitution d'un campus cyber (page 77)

Proposition n° 39 : Veiller à ce que la trajectoire définie au sein de la loi de programmation militaire pluriannuelle soit en adéquation avec l'état de la menace et le niveau d'ambition porté par la France dans ce domaine (page 119).

Proposition n° 41 : Appliquer une doctrine de l'autonomie technologique maximale en matière de renseignement et de cyberdéfense, en faisant du recours à des technologies extra-européennes une exception devant être motivée (page 122).

Proposition n° 42 : Accélérer la dynamique de constitution d'un écosystème français et européen d'entreprises « cybertech » (page 123).

Proposition n° 43 : Recruter davantage de profils techniques issus du secteur de la sécurité numérique, en rehaussant les rémunérations proposées et en adressant la question de la qualité de vie au travail (page 124).

Proposition n° *44* : Formaliser un « parcours public » cyber offrant des débouchés aux profils à haute valeur ajoutée recrutés par les acteurs de la chaîne de défense et de sécurité nationale (page 124).

D. DÉFENDRE NOTRE PUISSANCE NORMATIVE NATIONALE ET EUROPÉENNE.

1. France.

Proposition n° 5 : Renforcer les effectifs de la commission nationale de l'informatique et des libertés (CNIL) dans le cadre du projet de loi de finances pour 2022 (page 47).

Proposition n° 6 : Simplifier le processus de sanction mise en œuvre par la commission nationale de l'informatique et des libertés au sein des dossiers de moyenne et de faible intensité afin de renforcer sa capacité à prononcer les « mesures correctrices » prévues par le règlement général sur la protection des données (page 47).

***Proposition n° 8* :** Réaliser un état des lieux de l'arsenal juridique national permettant de s'opposer à la communication d'informations à une puissance étrangère et former les acteurs publics à ce type d'outils (page 53).

Proposition n° 9 : Actualiser et renforcer, le cas échéant, *la loi de blocage du 26 juillet 1968*, conformément aux recommandations formulées au sein du rapport « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » remis au Premier ministre par M. le député Raphaël Gauvain en 2019 (page 53).

2. Union européenne.

Proposition n°64 : Fixer un cap ambitieux d'adoption des différentes initiatives de régulation en cours (DSA, DMA, DGA), pour conserver une crédibilité maximale sur la capacité de l'Union européenne à adopter de façon souple et rapide une régulation du numérique (page 178).

II. FAIRE DE L'UNION EUROPÉENNE UNE PUISSANCE NUMÉRIQUE AUTONOME ET INDÉPENDANTE

A. FAIRE DE L'EUROPE UN LEADER DES TECHNOLOGIES NUMÉRIQUES.

1. Tout faire pour « être dans la course » des technologies numériques.

Proposition n° 56 **:** Développer une offre cloud européenne respectant les valeurs du modèle européen (page 160).

Proposition n° 57 : Garantir au sein de Gaia-X une gouvernance et une conduite de projets conformes aux ambitions exprimées par ses membres fondateurs afin d'éviter que cette initiative ne devienne un instrument au service de la croissance d'acteurs déjà dominants (page 160).

Proposition n° 58 : Accélérer le déploiement d'une constellation européenne de satellites en orbite basse (page 162).

2. Assumer une ambition européenne forte en matière de numérique.

Proposition n° 59 : Encourager la localisation ou la relocalisation en Europe d'usines de production d'équipements numériques sur l'ensemble de la chaîne de valeur (page 163).

Proposition n° 60 : Renforcer les moyens mis en œuvre dans le cadre des projets importants d'intérêt européen commun (PIEEC) et adopter à chaque reprise des calendriers ambitieux de déploiement (page 164).

Proposition n° 63 : Doter l'Europe d'une capacité d'anticipation et de veille sur les technologies numériques (page 168).

3. Convertir l'Union européenne aux enjeux de souveraineté économique.

Proposition n° 61 : Renforcer le recours aux outils de défense économique de l'Union européenne et durcir, le cas échéant, le règlement 2019/42 du 19 mars 2019 relatif au contrôle des investissements étrangers (page 167).

Proposition n° 62 : Intégrer, au sein de la politique de la concurrence de l'Union européenne, les enjeux de souveraineté numérique et d'autonomie stratégique de l'Union (page 168).

B. SOUTENIR NOS ENTREPRISES TECHNOLOGIQUES ET DÉVELOPPER LES COMPÉTENCES NUMÉRIQUES DES CITOYENS

1. Créer les conditions de la croissance de notre écosystème « tech »

Proposition n° 25 : Accélérer le renforcement de l'offre de formation « blockchain » et soutenir la sensibilisation du monde professionnel au potentiel de cette technologie (page 79).

Proposition n° 31 : Renforcer le soutien public à destination de la French Tech, pour l'encourager à « chasser en meute » (page 100).

Proposition n° 32 : Accélérer le développement du marché du capital-risque et l'harmonisation du marché des capitaux en Europe pour réduire le différentiel d'attractivité avec les États-Unis pour éviter le départ de pépites européennes pour des raisons liées à la recherche de financements (page 102).

Proposition n° 33 : Encourager les entreprises françaises à développer des stratégies de captation de brevets, afin de leur permettre de résister aux pratiques agressives de leurs concurrents étrangers (page 104).

Proposition n° 54 : Garantir en droit la force probante de la *blockchain,* pour créer un cadre favorable au développement de cette technologie (page 145).

Proposition n° 55 : Lancer une réflexion sur la création d'un système de certification des blockchains conformément à la recommandation n° 7 du rapport IMT-CEA-INRIA « Les verrous technologiques des blockchains » publié en avril 2021 (page 146).

2. Développer les compétences numériques des citoyens français.

Proposition n° 18 : Former aux compétences numériques dès le plus jeune âge et tout au long de la scolarité et de la vie professionnelle (page 66).

Proposition n° 20 : Développer l'apprentissage du code à l'école pour doter les élèves des fondamentaux de cet alphabet du monde numérique (page 68).

Proposition n° 21 : Développer la capacité des établissements scolaires à former les élèves aux enjeux de l'innovation et soutenir la création de projets numériques (page 69).

Proposition n° 22 : Proposer dans le cadre de la formation professionnelle des modules dédiés aux technologies numériques (page 76).

Proposition n° 24 : Faire des instituts universitaires de technologie des centres d'excellence pour fournir à la France des techniciens numériques en nombre suffisant (page 78).

C. ASSUMER UNE AMBITION NUMÉRIQUE FORTE AU SEIN DE L'ACTION PUBLIQUE.

1. Défendre des politiques numériques ambitieuses et efficaces

Proposition n° 7 : Intégrer de façon systématique au sein des arbitrages techniques des projets numériques les enjeux ayant trait à la souveraineté numérique, en particulier concernant la protection des données personnelles et la localisation des données en Europe (page 50).

Proposition n° 45 : Créer un ministère du numérique, doté d'une administration et de moyens propres, et chargé de porter les politiques numériques aux niveaux national, européen et international (page 133).

Proposition n° 47 : Créer un document de politique transversale (DPT) dédié aux politiques publiques du numérique, en complétant en ce sens *l'article n° 128 de la loi n° 2005 – 1720 du 30 décembre 2005 de finances rectificative pour 2005* (page 134).

Proposition n°48 : Renforcer le volet numérique des contrats de plan État-régions (page 134).

2. Renforcer la compétence numérique de l'administration française

Proposition n° 11 : Engager une stratégie ambitieuse de montée en compétences au sein de l'État sur la gestion de projets numériques afin de ne pas répéter les erreurs du passé (page 59).

Proposition n° 12 : Renforcer le recrutement par contrat de droit privé de profils techniques, pour mener à bien les projets numériques de l'État et mettre en œuvre une stratégie de fidélisation pour les conserver au sein de la sphère publique (page 61).

Proposition n° 13 : Favoriser la circulation des compétences numériques au sein du secteur public (page 62).

Proposition n° 46 : Mettre en place un briefing hebdomadaire du Président de la République sur les questions technologiques, en s'inspirant du modèle américain (page 133).

Proposition n° 51 : Assurer un travail de veille pour intégrer dans la gestion des projets numériques les méthodes de travail et d'organisation les plus performantes (page 135).

3. Garantir l'exemplarité de l'État dans ses usages numériques

Proposition n° 17 : Développer une culture de la transparence vis-à-vis des données utilisées par la puissance publique dans le cadre de ses interactions avec les citoyens (page 65).

Proposition n° 49 : Accélérer la mise en œuvre d'une politique ambitieuse d'ouverture des données au sein des administrations publiques (page 135).

Proposition n° 50 : Créer un portail public rassemblant l'ensemble des offres numériques françaises disponibles (page 135).

Proposition n° 52 : Imposer au sein de l'administration le recours systématique à des solutions numériques françaises, lorsque leur niveau de performance est satisfaisant pour les usages concernés (page 138).

Proposition n° 53 : Imposer au sein de l'administration le recours systématique au logiciel libre, en faisant de l'utilisation de solutions propriétaires une exception (page 138).

4. Simplifier la vie des citoyens grâce au numérique

Proposition n° 10 : Accélérer le déploiement de l'identité numérique en France (page 59).

Proposition n° 14 : Lancer une grande campagne de communication sur l'identité numérique (page 62).

Proposition n° 15 : Créer un guichet numérique unique d'accès de chaque citoyen à l'ensemble des services publics, lui permettant aussi d'être informé en temps réel de l'utilisation de ses données par l'administration (page 63).

Proposition n° 16 : Créer un numéro d'identification unique afin de mettre fin aux difficultés rencontrées par les administrations pour identifier les administrés et partager leurs informations de façon efficace (page 65).

D. FAIRE DE LA COMMANDE PUBLIQUE UN VÉRITABLE LEVIER DE SOUVERAINETÉ.

1. Faire de nos entreprises « tech » le cœur de cible de la commande publique.

Proposition n° 26 : Privilégier, en matière de commande publique, le recours aux solutions d'acteurs technologiques français ou européens, et faire ainsi montre d'exemplarité (page 98).

Proposition n° 27 : Exiger de l'Union des groupements d'achats publics (UGAP) des délais raisonnables dans le traitement des demandes de référencement des acteurs de l'offre numérique française (page 98).

Proposition n° 28 : Créer un guide d'information des acteurs publics sur les outils de la commande publique, afin d'encourager, notamment, la pratique de l'allotissement, le recours par les collectivités au « dialogue compétitif » en matière de numérique et l'usage de la mention « Spécial France », toutes mesures qui permettront de rendre plus systématique le recours aux acteurs français au sein de la commande publique (page 98).

2. Faire évoluer, à moyen terme, le droit national et européen de la commande publique

Proposition n° 29 : Lancer une mission d'expertise sur les enjeux de souveraineté de la commande publique, afin d'identifier les leviers permettant de faire évoluer le cadre juridique actuel, en faveur de la prise en compte des enjeux de sécurité numérique, de gestion et de localisation des données en Europe (page 100).

Proposition n° 30 : Faire évoluer les pratiques et le cadre juridique de la commande publique :

Au niveau national :

– En intégrant le principe selon lequel l'hébergeur ne doit pas être soumis à des lois extra-européennes dans les normes de sécurité existantes (SecNumCloud, HDS, ISO 27001) ;

– En intégrant dans les clauses administratives générales des marchés (CCAG) des obligations liées à la localisation des données en Europe, sous peine de condamnation pénale des dirigeants du cloud ;

– En soutenant une « culture du risque » chez les acheteurs publics (sécurisation juridique) et en améliorant leur formation aux aspects extra-juridiques de la commande publique.

Au niveau européen :

– En mettant en place rapidement un *Small Business Act*.

– En étendant à d'autres produits le régime de préférence communautaire existant dans les infrastructures.

– En clarifiant l'article 25 de la directive européenne de 2014 pour identifier précisément les cas dans lesquels une offre d'un État tiers peut être écartée (page 100).

E. MIEUX DÉFENDRE LES INTÉRÊTS NUMÉRIQUES DE LA FRANCE ET DE L'UNION EUROPÉENNE AU NIVEAU INTERNATIONAL

Proposition n° 65 : Mettre le numérique au cœur de la présidence française de l'Union européenne au premier semestre de l'année 2022 (page 178).

Proposition n° 66 : Investir davantage les instances internationales de régulation de l'Internet et de normalisation des technologies numériques, pour renforcer le poids de la représentation des intérêts français et européens dans le domaine du numérique (page 180).

TRAVAUX DE LA MISSION D'INFORMATION

I. POINT D'ÉTAPE DES TRAVAUX AU 16 MARS 2021

M. le président Jean-Luc Warsmann. Notre mission d'information a tenu trente-sept auditions à ce jour. La note récapitulative de ces travaux vous est parvenue sous forme numérique et vous a été distribuée aujourd'hui sous format « papier ».

M. Philippe Latombe, rapporteur. La note distribuée récapitule de façon synthétique, mais exhaustive l'état des travaux de la mission d'information. Elle présente la synthèse des échanges au 16 mars 2021, après le rappel du cadre initial des travaux de la mission d'information, comprenant les grands thèmes et les principaux sujets à traiter lors des auditions.

Sept constats ressortent de ces échanges :

– Premier constat : la pluralité des définitions de la souveraineté numérique. Il importe de s'accorder sur la définition la plus exhaustive et la plus simple. Les définitions de la direction générale des entreprises (DGE) et de la direction interministérielle du numérique (DINUM) recouvrent le champ complet de la souveraineté numérique : la capacité d'établir des règles dans le domaine du numérique, de contrôler les impacts de ses usages et de disposer de l'autonomie sur les principales technologies numériques ainsi que la préservation de notre liberté de choix, la maîtrise des compétences numériques au sein de l'État et la réversibilité. En additionnant les deux conceptions, on obtient le champ exhaustif de la définition ;

– Deuxième constat : une indépendance industrielle et technologique de la France et de l'Europe à reconstruire, qu'il s'agisse de l'industrie électronique, des réseaux numériques, des logiciels et matériels, de l'Intelligence artificielle, cette dernière justifiant de tenir une série d'auditions ;

– Troisième constat : des acteurs publics qui recourent trop peu à des solutions souveraines, qu'il s'agisse de l'État ou des collectivités territoriales. Une attente particulière a été portée aux propositions ayant trait à la commande publique. Nombre d'interlocuteurs de la mission ont critiqué les règles de la commande publique, en raison de leur complexité, de leur rigidité, des règles appréhendées trop uniquement sous l'angle juridique et non comme cadre en vue d'obtenir des propositions de services ou des offres de marché ;

– Quatrième constat : des interrogations fortes à propos du *cloud* et des données personnelles, en particulier dans le domaine de la santé, les plus sensibles des données personnelles. La compréhension de cette particularité peut contribuer à l'appréhension d'autres données sensibles du domaine de l'État, comme celles de l'Éducation ou d'autres secteurs ;

– Cinquième constat : un pilotage perfectible des politiques numériques, la gestion interne des projets apparaissant trop « en silos », sans homogénéité, sans stratégie globale clairement affichée de la part de l'État, mais seulement en suivant des stratégies sujet par sujet ;

– Sixième constat : la nécessité de développer notre capital humain numérique : formation, emploi. Ce thème identifié par la mission d'information au début de ses travaux a suscité l'insistance des différents acteurs auditionnés et justifie d'y consacrer un cycle d'auditions (depuis l'Éducation nationale, les écoles et jusqu'à la formation professionnelle tout au long de la vie) ;

– Septième constat : un rôle-clé de l'Europe comme puissance normative, scientifique et économique. Cet angle d'approche a été systématiquement abordé dans les différentes auditions, qu'il s'agisse de ce qui est fait à l'échelon national ou de ce qui est fait à l'échelon européen. Le constat d'une puissance normative de l'Europe ayant émergé avec le Règlement général sur la protection des données (RGPD) est en train de se renforcer avec les trois *directives DSA (Data Services Act), DMA (Data Markets Act)* et *DGA (Data Governance Act)*.

Le tableau récapitule les propositions formulées par les acteurs auditionnés, en fonction des grands thèmes abordés. Par exemple :

– Revoir les conditions d'éligibilité aux appels à projets européens pour y intégrer une exigence de réciprocité avec les pays tiers dans les marchés publics. L'impact de l'Europe est manifeste à cet égard et justifie de présenter des propositions spécifiques. Lors de son audition, la commissaire européenne, Mme Mariya Gabriel, avait émis cette idée ;

– Promouvoir l'exemplarité de l'État en matière de commande publique, non dans le seul domaine de la santé, mais selon une approche systémique ;

– Réfléchir à la mise en place d'un *Buy European Act* équivalent du *Small Business Act* américain, en ce qui concerne les règles européennes de marchés publics. Cette demande a été exprimée par la presque totalité des intervenants ;

– Créer une agence européenne chargée de casser les monopoles en établissant des règles de séparation et d'interopérabilité, afin de passer d'un système centralisé à une véritable concurrence entre différentes entités. Cette proposition a été avancée par M. Sébastien Soriana, ancien président de l'autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). Elle l'a également été par plusieurs autres interlocuteurs ;

– Instituer un crédit d'impôt à la numérisation des entreprises – qu'il s'agisse d'un crédit d'impôt pour la numérisation ou d'un crédit d'impôt pour la cyber-sécurité – afin d'inciter les entreprises, notamment les PME et les TPE, à se numériser ;

– Faire de la souveraineté numérique un véritable projet politique : un cadre et une stratégie complète relevant de l'initiative politique ;

– S'inspirer de la gestion de l'innovation par la DARPA *(Defense Advanced Research Projects Agency)* aux États-Unis. Le constat a été régulièrement dressé de

l'absence d'un organisme éclairant la vision à moyen et long terme pour infléchir la stratégie. Ce thème sera abordé avec le Haut commissaire au Plan ;

– Reconnaitre un droit à l'erreur et accepter la prise de risque au sein de l'État, afin de favoriser le déploiement de solutions innovantes. Cette proposition rejoint le domaine des marchés publics. Le choix d'une solution américaine intégrée a l'avantage de permettre la passation d'un seul marché public, quand un allotissement impose la passation de plusieurs marchés, avec la nécessité de rendre les solutions interopérables, toutes choses qui nécessitent du temps, de l'expertise, les critiques à l'encontre de l'État fusant en cas de difficultés ;

– Développer la solidarité interétatique européenne *via* une coalition européenne pour peser au niveau mondial. Cette proposition a trait, plus globalement, à la gouvernance européenne. Les auditions de la semaine dernière, en ce qui concerne l'environnement géostratégique, ont mis en évidence des situations dans lesquelles des pays européens peuvent avoir envie de conduire une action propre, suivant des visions différentes, situations appelant un besoin de cohérence à développer ;

– Créer un ministère du numérique et le doter des moyens d'agir et créer une direction générale du numérique, pour faire en sorte que l'État ne fonctionne plus ministère par ministère, mais de façon globale, structurée et en cohérence. Un tel besoin a également été affirmé lors de plusieurs auditions ;

– Sensibiliser le public à la cybersécurité et aux enjeux d'autonomie stratégique ou de souveraineté numérique. Il existe un manque manifeste d'une telle culture chez les dirigeants d'entreprise ou de la part d'un certain nombre de décideurs. Ce besoin pourrait être également abordé sous l'angle de l'éducation, en termes de formation des futurs ingénieurs et décideurs, pour lesquels la cybersécurité et la souveraineté ne font pas partie des cursus suivis ;

– Créer un Internet de la confiance, c'est-à-dire un environnement numérique éthique, protecteur des données personnelles, et qui garantisse les conditions de la liberté et de l'autonomie. Ce thème est apparu lors de nombreuses auditions. Si la puissance des États-Unis est liée notamment aux GAFAM et à leurs solutions intégrées et la puissance de la Chine en relation avec sa centralisation étatique et sa vision particulière de l'Internet, l'Europe trouverait sa place en mettant ses valeurs au service de son Internet, lui permettant de construire un écosystème et son environnement. Il convient de mettre les valeurs européennes au cœur de la stratégie numérique, ce qui apportera une forme de souveraineté, en promouvant une « troisième voie », distincte de celle suivie par les Américains, très capitaliste et hégémonique, et de celle, très centralisée et marquée par le contrôle, suivie par les Chinois.

M. Philippe Gosselin. S'agissant du concept global des valeurs européennes, une difficulté tient à l'existence de quelques dissensions sur ces valeurs. Entre ce que proposent l'Irlande, les Pays-Bas ou les États membres ayant appartenu à l'ancien bloc de l'Est, il existe des différences, qui ne sont pas seulement liées à des questions d'attractivité fiscale ou d'implantation de sièges d'entreprises. Il existe une fracture entre la *common law* et le droit européen, droit

écrit, etc. Le concept de « valeurs européennes » est opératoire, mais lorsqu'on entre dans le détail, apparaissent des visions économiques, des visions de puissance, voire d'influence, y compris en termes de *soft power*. Une prise de conscience d'un bloc démocratique est nécessaire, selon un modèle différent du modèle anglo-saxon pur, mais qui soit aussi un modèle solvable de plusieurs centaines de millions de personnes, ce qui n'est pas le cas de tous les marchés, notamment du marché chinois, en progrès vertigineux toutefois, sa population médiane se comparant désormais à la nôtre, en termes de pouvoir d'achat.

M. Philippe Latombe, rapporteur. C'est la raison pour laquelle la proposition de développer la solidarité interétatique européenne *via* une coalition européenne pour peser au niveau mondial a du sens. Il existe des divergences – lesquelles apparaissent, s'agissant du *DSA* par exemple, quant aux contenus – en raison de valeurs ou de visions différentes entre pays européens. Sur le principe de base, l'accord se fait, des écarts apparaissent dans sa déclinaison.

Ces propositions mises en exergue n'ont volontairement pas été « retravaillées ».

Il est proposé de poursuivre le programme des auditions pendant les mois d'avril et mai, en retenant plusieurs thématiques :

– l'identité numérique, sans vouloir refaire le rapport de Mme Christine Hennion et de M. Jean-Michel Mis déjà intervenu sur ce thème, mais en envisageant, à partir de ce rapport, ce qui a déjà été engagé ou non et quelles actions sont nécessaires pour rejoindre la trajectoire initialement suggérée. Il ne s'agit pas de recommencer le débat sur l'identité numérique ;

– l'éducation et la formation aux compétences numériques. Ce thème a été abordé de façon quasi systématique, mais incidente, par les interlocuteurs de la mission. C'est l'indice d'une véritable question qu'il convient d'approfondir, depuis le primaire jusqu'à la formation continue des salariés ;

– les enjeux de la fiscalité du numérique et des monnaies virtuelles, dans ce cas également, sans vouloir recommencer les travaux déjà réalisés, mais en vue de faire un point de situation par rapport à la trajectoire qu'ils avaient proposée ;

– les technologies numériques, dans le même esprit, par exemple, pour déterminer où l'on en est aujourd'hui de la *blockchain*, notamment sa force probante en droit français ;

– le cyberespace, compte tenu des annonces de l'Union européenne sur l'envoi de constellations afin de rattraper le retard par rapport aux Américains et aux Chinois.

Il est également proposé des auditions complémentaires :

– le Conseil national du numérique, qui était en cours de renouvellement lors des débuts de nos travaux. Cette question de légitimité est aujourd'hui réglée ;

– le Haut commissaire au plan, audition devant être réalisée après avoir entendu le secrétariat général pour l'investissement, afin de disposer déjà d'une vision à moyen et long terme ;

– Bpifrance, pour ce qui a trait au plan de relance et à la numérisation ;

– la French tech ;

– le commissaire européen, M. Thierry Breton, qui a lancé un certain nombre de projets, sur la suite de ceux-ci ;

– l'union des entreprises du logiciel libre pour examiner la mise en œuvre des préconisations du rapport présenté par M. Éric Bothorel ;

– Eutelsat et Thales sur le cyberespace ;

– Yes We Hack, le gouvernement ayant décidé de recourir à des hackers éthiques, notamment pour tester la solidité et la robustesse de StopCovid au moment de sa création.

Différentes auditions sont proposées en relation avec le thème de l'éducation et de la formation, parmi lesquelles celle, importante, de la ministre de la transformation et de la fonction publiques.

En annexe, figure la récapitulation de l'ensemble des auditions tenues par la mission d'information à ce jour.

M. Philippe Gosselin. Ce point d'étape est complet, permet de repérer les grands axes d'actions et de hiérarchisation de celles-ci et témoigne d'une ambition pour une mobilisation sur un sujet qui est bien-là, clairement identifié, même s'il n'est pas totalement nouveau. La Covid conduit à poser un regard particulier à cet égard, ainsi que certaine plateforme de données de santé.

Cet allant et cet élan national français, qui doit être phénoménal, ambitieux, engageant, enthousiasmant, le nôtre, ne pourra néanmoins pas aboutir sans une ambition partagée en Europe.

Notre démarche doit s'inscrire dans la perspective d'un débouché vers une loi de programmation, ambitieuse en termes de moyens.

M. Jean-Michel Mis. Ce point d'étape était nécessaire, s'agissant d'une mission au champ aussi large. Les points examinés montrent que tous les thèmes sont traités. Les recommandations vont dans le bon sens. Le souhait d'un *Buy European Act* est pertinent. S'agissant de la commande publique, les difficultés mises en évidence tiennent au fait que le recours aux appels d'offres est appréhendé de façon différente selon les ministères. Dans ces domaines, il ne doit pas être question d'appels d'offres « classiques ». Il est indispensable de retenir désormais une approche faire de type *« Business to Government »*, la puissance publique devant aborder un certain nombre d'aspects technologiques. Il entre dans le rôle de la commande publique de pousser notre écosystème, sans se contenter de programmes de financement, comme les PIA. De nombreuses entreprises demandent d'abord de la commande, suivant un schéma classique, mais sain. Mais cela doit se faire à concurrence égale, toutes choses égales par ailleurs, sans défavoriser nos écosystèmes en pratiquant de façon exagérée le principe de précaution, ce qui aboutit à renforcer les positions de place au détriment de l'écosystème émergent. Il convient de trouver l'intelligence collective de défendre

nos écosystèmes, même lorsque les *start-up* n'ont pas cinq, dix ou vingt ans d'existence, sans être installées comme des acteurs internationaux.

Un pilier à placer au même niveau que la souveraineté numérique est la façon dont nous envisageons la cybersécurité, avec un certain nombre de thèmes relatifs à la défense-sécurité ou à la stratégie industrielle. Au-delà du pur numérique, en font partie nos capacités à gérer le foncier, les installations d'importance vitale. Cela suppose de revoir où en sont les textes européens, comme la directive *NIS* ou le RGPD et les évolutions qu'ils peuvent appeler.

Il serait utile que M. Clément Beaune puisse venir présenter la feuille de route de la future présidence française de l'Union européenne sur les enjeux de souveraineté et son regard sur les directives *DMA*, *DSA*, *NIS* et la refonte du RGPD.

L'audition de M. Guillaume Poupard permettra d'évoquer les cyberattaques. Quelques auditions complémentaires de sociétés gérant des SOQ, pratiquant la maintenance opérationnelle de sites seraient bienvenues, afin de voir la façon dont nos entreprises sont accompagnées dans le domaine de la cybersécurité et de la résilience, de même que, lorsque cela est nécessaire, de la restauration des données dans un cadre qui soit le plus souverain possible. Cela pose, par exemple, la question du rôle des opérateurs français et européens dans le fonctionnement de GAIA X. Lorsqu'on souhaite faire monter des acteurs en puissance, cela ne se conçoit qu'à l'état de l'art, la souveraineté n'ayant pas vocation à défendre des acteurs qui ne seraient pas à l'état de l'art.

En matière de concurrence, le contrôle et les sanctions appartiennent à la Commission européenne. Il n'est pas certain que la proposition, notamment celle suggérée par M. Sébastien Soriano, de créer une agence en vue de casser les monopoles soit réalisable.

Au-delà de la somme d'échanges intervenus ou à venir, il conviendrait que la mission dépasse les constats déjà établis pour trouver un angle pertinent afin de présenter des propositions audacieuses pouvant être soutenues de façon transpartisane.

M. Philippe Latombe, rapporteur. Le sens de ce point d'étape était d'abord d'identifier d'éventuels angles morts. Des auditions sont à venir, par exemple, en ce qui concerne la cybersécurité, la CNIL, l'ANSSI. Sa deuxième justification est de commencer à réfléchir à la façon de présenter les choses : les propositions pouvant être mises en avant et les angles de présentation du rapport.

M. Philippe Gosselin. Il faut réfléchir à un « atterrissage » sous forme d'une proposition de loi ayant une force transpartisane afin de prendre date pour l'avenir.

M. le président Jean-Luc Warsmann. Compte tenu du caractère à la fois national et européen, de ces questions, les propositions du rapport doivent porter sur ces deux aspects.

II. EXAMEN PAR LA MISSION D'INFORMATION

Au cours de sa séance du mardi 29 juin 2021, la mission d'information, s'est prononcée sur l'autorisation de publication du rapport de M. Philippe Latombe.

M. Philippe Latombe, rapporteur. Le 16 mars dernier, lorsque nous avions tenu un point d'étape de nos travaux, nous avions procédé à 37 auditions. Au total, nous aurons tenu 83 auditions pendant 104 heures.

D'abord, nos auditions supplémentaires ont consisté en plusieurs cycles thématiques sur l'éducation et la formation avec les représentants du ministère de l'Éducation nationale, du ministère de la Recherche, de l'Agence nationale de la recherche ainsi que sur certaines technologies comme l'Intelligence artificielle et la *blockchain.*

Ensuite, quelques auditions complémentaires nous ont permis d'entendre le Conseil national du numérique, Bpifrance, le Conseil national du logiciel libre, Eutelsat et Thales, GAIA X.

Enfin, nous avons pu entendre les ministres en charge du numérique dans trois pays européens : le Luxembourg, la Lituanie et l'Estonie.

De la liste de toutes les propositions qui figureront dans le rapport, j'ai extrait trente d'entre elles à titre de propositions clés autour de quatre axes.

Premier axe : garantir la résilience de nos infrastructures, j'y inclus ce qui a trait aux réponses qu'appelle la menace cyber. Se doter des moyens de faire face au risque cyber est le corollaire de toute démarche visant à passer au numérique ou à accroître son champ d'intervention.

Deuxième axe : se doter d'une base technologique nationale et européenne, sans laquelle la réaffirmation de notre souveraineté numérique relèvera du vœu pieu. Il ne suffit pas de prétendre monter sur le « ring » de la compétition technologique, encore faut-il s'en donner les moyens et être compétitifs dans la durée.

Troisième axe : mettre la souveraineté numérique au cœur de l'action publique. Un certain nombre de principes d'organisation doivent devenir les « intangibles » de la culture politico-administrative du numérique : la création du ministère du numérique doté d'une administration et de moyens propres, le recours de principe au logiciel libre et aux solutions numériques françaises à performance égale, l'entretien d'un vivier de compétences numériques propre au secteur public.

Dernier axe : mettre le citoyen au cœur des politiques numériques. De ce point de vue, la comparaison avec les choix d'organisation de la relation numérique entre l'administration et le citoyen qui ont été retenus au Luxembourg ou en Estonie suffit à montrer que des marges notables d'amélioration existent dans notre pays.

La question est autant juridique que technique, puisque la création, peut-être faut-il dire le tabou, d'un numéro d'identification unique en fait partie.

M. Pierre-Alain Raphan. Le travail considérable qui a été réalisé par le rapporteur fait bien le tour des questions en jeu. Il a vocation à constituer un document de référence. Les mesures proposées portent sur les sujets qui appellent effectivement une action. Il faut souhaiter qu'elles soient suivies d'effet de la part du gouvernement.

La mission d'information a ***autorisé*** *le dépôt du rapport et sa publication.*

LISTE DES PERSONNES AUDITIONNÉES

(par ordre chronologique)

Les comptes rendus des auditions sont consultables à l'adresse suivante : https://urlz.fr/g3Jl

Jeudi 1er octobre 2020

– Mme Mariya Gabriel, commissaire européenne

Jeudi 8 octobre 2020

– Comité stratégique de filière Industrie électronique (CSF Industrie électronique)

M. Thierry Tingaud, président
M. Guillaume Adaam, délégué
Mme Virginie Hoel, professeur des universités

– M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance

M. Mathieu Weill, chef du service de l'économie numérique

Jeudi 15 octobre 2020

– M. Henri Verdier, ambassadeur pour le numérique

Jeudi 22 octobre 2020

– M. Cédric O, secrétaire d'État auprès du ministre de l'économie, des finances et de la relance et de la ministre de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques

Jeudi 29 octobre

– Mme Geneviève Boucher, présidente du Forum Atena

– M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique

Jeudi 5 novembre 2020

– M. Stéphane Séjourné, député européen, rapporteur sur un cadre d'aspects éthiques en matière d'Intelligence artificielle, de robotique et de technologie connexes

Jeudi 12 novembre 2020

– M. Charles Thibout, chercheur associé à l'Institut de relations internationales et stratégiques (IRIS) et chercheur au Centre européen de sociologie et de science politiques (CNRS, EHESS, Paris 1)

Jeudi 19 novembre 2020

– Mme Lorena Boix Alonso, directrice chargée de la stratégie et de la diffusion des politiques à la direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne

– M. Werner Stengg, membre du cabinet de Mme Margrethe Vestager, vice-présidente exécutive de la Commission européenne, sur « une Europe adaptée à l'ère du numérique »

Jeudi 26 novembre 2020

– Fédération française des Télécoms et groupe de télécommunications Iliad

M. Olivier Riffard, directeur des affaires juridiques de la Fédération française des Télécoms
M. Anthony Colombani, directeur corporate de Bouygues Telecom
Mme Claire Perset, secrétaire générale adjointe de SFR
Mme Ombeline Bartin, responsable des relations institutionnelles de Free mobile

– Sociétés de télécommunications Ericsson, Huawei et Nokia

M. Viktor Arvidsson, directeur des activités relations institutionnelles, innovation et stratégie d'Ericsson
M. Minggang Zhang, directeur général adjoint de Huawei France
Mme Linda Han, déléguée générale de Huawei France
M. Jean-Christophe Aubry, responsable des affaires publiques de Huawei France
M. Marc Charrière, directeur des affaires publiques de Nokia

Jeudi 3 décembre 2020

– Comité stratégique de filières « Infrastructures numériques »

M. Jacques de Heere, vice-président du comité stratégique et président du groupe industriel ACOME
M. Michel Cobot, délégué permanent du comité stratégique
M. Aubin Bernard, chargé de mission à la Fédération InfraNUm

Mme Marie-Thérèse Blanot, Syndicat professionnel des fabricants de fils et câbles électriques et de communication (SYCABEL)
M. Jugwal Doyen, Fédération française des Télécoms

Jeudi 10 décembre 2020

– Table ronde « Collectivités territoriales »

M. Artel Turpin, délégué général de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA)
Mme Valérie Nouvel, vice-présidente du département de la Manche,
Mme Ann-Gaëlle Werner-Bernard, conseillère parlementaire de l'Assemblée des départements de France (ADF)
M. Guilhem Denizot, conseiller « Innovation » de l'ADF
M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France

– Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)

M. Sébastien Soriano, président
M. Jean Cattan, conseiller

Jeudi 17 décembre 2020

– France Brevets

M. Didier Patry, directeur général
M. Guillaume Ménage, directeur-adjoint
M. Vincent Puyplat, directeu-adjoint
Mme Anne-Sophie Sebire, directrice juridique
Mme Audrey Lenne, directeur conseil du cabinet Rivington

– Compagnie lyonnaise d'études et de services en systèmes électroniques (CLESSE)

M. Denis Psomiades, président-directeur général

Jeudi 14 janvier 2021

– Table ronde « Entreprises »

M. Yoann Kassianides, délégué génréral de l'ACN
Mme Louise Bautista, représentant M. Mathieu Iasia, directeur général de TheGreenBow
M. Arthur Bataille, président de Silicom, fondateur de Seela
M. Jacques de la Rivière, président et cofondateur de Gatewatcher
M. Sébastien Garnault, fondateur de la CyberTaskForce et de Paris Cyber Week, président de Garnault et Associés

– Table ronde « Organisations patronales »

Confédération des petites et moyennes entreprises (CPME)

M. Alain Assouline, co-président de la commission « Innovation et économie numérique »

Mouvement des entreprises de taille intermédiaire (METI)

M. Alain Conrard, président de la commission digitale, directeur général de Prodware Group
Mme Florence Naillat, adjointe au délégué général
M. Alexandre Bonis, responsable des affaires publiques
M. Sylvain Rouri, directeur des ventes d'OVHcloud

Mouvement des entreprises de France (MEDEF)

M. Laurent Giovachini, président du comité « Souveraienté et sécurité économique », président de Syntec et directeur général adjoint de Sopra Steria
M. Christian Poyau, co-président de la commission « Mutations technologiques & iimpacts sociétaux », co-fondateur et président-directeur général de Micropole
Mme Maxence Demerlé, directrice du numérique
Mme Stéphanie Tison, directrice-adjointe à l'international au pôle économique
Mme Fadoua Qachri, chargée de mission à la direction des affaires publiques
Mme Clémentine Furigo, chargée de mission senior à la direction juridique

Jeudi 21 janvier 1921

– Union des groupements d'achats publics (UGAP)

M. Edward Jossa, président
Mme Pierrette Vidal, directrice commerciale secteur public
M. Michel Ferrand, directeur avant-vente de Specialist Computer Company France (SCC France)

– Direction interministérielle du numérique et direction des achats de l'État

M. Nadi Bou Hanna, directeur interministériel du numérique
M. Michel Grévoul, directeur des achats de l'État

Jeudi 28 janvier 2021

– Table ronde sur la commande publique

Pr Stéphane de la Rosa, professeur de droit public à l'Université de Paris-Est Créteil
Me Thierry Dal Farra, avocat associé du cabinet UGGC Avocats
M. François Benchendikh, maître de conférences en droit public à Science Po Lille

– Direction des affaires juridiques (ministère de l'économie, des finances et de la relance)

Mme Laure Bédier, conseiller d'État, directrice, agent judiciaire de l'État

M. Benoît Dingremont, administrateur civil, sous-directeur en charge de la commande publique

Mardi 9 février 2021

– Table ronde sur le *cloud* et la protection des données

Mme Servane Augier, directrice générale déléguée de 3DS OUTSCALE
M. Michel Paulin, directeur général d'OVHcloud
Mme Karine Picard, directrice générale d'Oracle France

Jeudi 11 février 2021

– Table ronde sur le *cloud* et la protection des données

M. Jean-Noël de Galzain, président d'HEXATRUST
M. Stéphane Volant, président du Club des directeurs de la sécurité et de la sûreté des entreprises (CDSE)
Pr Florence G'Sell, professeure de droit à l'Université de Lorraine

Jeudi 18 février 2021

– Groupement d'intérêt public Plateforme nationale d'accès aux données de santé (*Health Data Hub*)

Mme Stéphanie Combes, directrice

– Groupement de coopération sanitaire des hôpitaux universitaires de Grand Ouest et plateforme de données hospitalières Ouest Data Hub

Mme Laurence Jay-Passot, déléguée générale
Pr Marc Cuggia, professeur des universités-praticien hospitalier au centre hospitalier universitaire (CHU) de Rennes

– Association InterHop

M. Adrien Parrot, médecin-ingénieur, président
Me Juliette Alibert, avocate, membre

Jeudi 25 février 2021

– Syntec Numérique

M. Benoît Darde, administrateur

– France Digitale

M. Nicolas Brien, directeur général

Jeudi 4 mars 2021

– Direction des systèmes d'information de l'Assistance publique – Hôpitaux de Paris (AP-HP)

Dr Laurent Treluyer, directeur
Mme Hélène Coulonjou, directrice déléguée auprès du directeur
Mme Elisa Salamanca, responsable du département Web, Innovation, Données

– M. Dominique Pon, responsable ministériel du numérique en santé

– M. Olivier Micheli, président de DATA4

Mardi 9 mars 2021

– IBM

Mme Diane Dufoix-Garnier, directrice des affaires publiques
M. Michel Gesquiere, responsable des ventes

– Caisse nationale d'assurance maladie (CNAM)

M. Claude Gissot, inspecteur général de l'INSEE, directeur de la stratégie, des études et des statistiques (DSES)
Mme Stéphanie Naux, directrice de mission au cabinet du DSES

Jeudi 11 mars 2021

– Secrétariat général pour l'investissement (SGPI)

Mme Naomi Peres, secrétaire générale adjointe
M. Clément Jakymiw, directeur-adjoint du programme « Industries et services »

– Pr Thibault Douville, professeur des universités, directeur du master Droit du numérique à l'Université de Caen Normandie

– M. Julien Nocetti, docteur en sciences politiques, chercheur associé à l'institut français des relations internationales (Ifri) et enseignant –chercheur en relations internationales et études stratégiques aux Écoles de Saint-Cyr Coëtquidan

Jeudi 18 mars 2021

– Amazon Web services (AwS)

M. Julien Groues, directeur général
M. Stéphan Hadinger, directeur technique

– Google France

M. Olivier Esper, chargé des relations institutionnelles
M. Fenitra Ravelomanantsoa, responsable des affaires publiques

– Institut national de recherche en sciences et technologie du numérique (Inria)

M. Bruno Sportisse, président-directeur général

– Club informatique des grandes entreprises

M. Jean-Claude Laroche, vice-président
M. Henri d'Agrain, délégué général

Jeudi 25 mars

– Commission nationale de l'informatique et des libertés (CNIL)

M. Gwendal Le Grand, secrétaire général adjoint

– Agence nationale de sécurité des systèmes d'information (ANSSI)

M. Guillaume Poupard, directeur général
(Cette audition qui est tenue à huis clos n'a pas fait l'objet d'un compte rendu)

– Palantir France

M. Fabrice Brégier, président
M. Olivier Tesquet, journaliste spécialisé dans les questions numériques à Télérama
M. Olivier Laurelli, cofondateur de Reflets.info

Mardi 30 mars 2021

– M. Éric Baissus, président-directeur général de Kalray

– Fédération française de la Cybersécurité (FFC)

M. David Ofer, président

Jeudi 1er avril 2021

– Audition commune sur les titres d'identité sécurisés et l'identité numérique

M. Pierre Lelièvre, vice-président de la société IDEMIA
M. Olivier Charlannes, vice-président de la société IDEMIA
M. Cosimo Prete, président fondateur de la société Crime Science Technology

– Audition commune sur les titres d'identité sécurisés et l'identité numérique

Mme Valérie Peneau, inspectrice générale de l'administration, directrice du programme interministériel France Identité numérique (FIN)
Mme Anne-Gaëlle Baudouin-Clerc, préfète, directrice de l'agence nationale des titres sécurisés (ANTS)

Mardi 6 avril 2021

– Audition commune sur les constellations de satellites

M. Rodolphe Belmer, directeur général d'Eutelsat
M. Hervé Derrey, président-directeur général de Thales Alenia Space

– Audition commune sur les titres d'identité sécurisés et l'identité numérique

Mme Coralie Héritier, responsable des identités numériques, dirigeante d'IDnomic, groupe Atos
M. Romain Galesne-Fontaine, directeur des relations institutionnelles d'IN Groupe
M. Yann Haguet, vice-président exécutif « Identité numérique », copilote du groupe de travail 3Identité numérique » au sein du comité stratégique de filière des industries de sécurité

– Groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA)

M. Jérôme Notin, directeur général

– Yes We Hack

M. Guillaume Vassault-Houlière, président-directeur général et coordinateur
Mme Rayna Stamboliyska, vice-présidente en charge des affaires publiques et institutionnelles

Mardi 13 avril 2021

– Mission Campus Cyber

M. Michel Van Den Berghe, président

– M. Arnaud Dechoux, responsable des affaires publiques « Europe » de la société Kaspersky

– Cisco Systems France

M. Laurent degré, président-directeur général
M. Bruno Bernard, directeur des affaires publiques

Jeudi 15 avril 2021

– Direction générale des entreprises (ministère de l'économie, des finances et de la relance)

Mme Bénédicte Roullier, cheffe du pôle « Transformation numérique des TPE/PME »
M. Aurélien Palix, sous-directeur des réseaux et des usages numériques

– M. Paul-François Fournier, directeur exécutif en charge de l'innovation de Bpifrance

– Agence nationale de la recherche (ANR)

Mme Martine Garnier, responsable du département « Numérique et mathématiques appliquées »
M. Frédéric Precioso, responsable scientifique « Intelligence artificielle »

Mardi 20 avril 2021

– Confédération française de l'encadrement-confédération générale des cadres (CFE-CGC)

Mme Raphaëlle Bertholon, secrétaire nationale à l'économie, l'industrie, le logement et le numérique
M. Nicolas Blanc, délégué national au numérique

Jeudi 22 avril 2021

– Fédération française des professionnels de la *blockchain* (FFPB)

M. Rémy Ozcan, président

– UNIRIS

M. Sébastien Dupont, président et co-fondateur
M. le général d'armée Grégoire de Saint-Quentin, président du cabinet de conseil Petra advisors et ancien conseiller du gouvernement pour la défense

– Association internationale sans but lucratif GAIA-X

M. Francesco Bonfiglio, directeur général
M. Pierre Gronlier, directeur des technologies

Mardi 27 avril 2021

– Association pour le développement des actifs numériques (ADAN)

M. Simon Polrot, président
Mme Faustine Fleuret, directrice stratégique et relations institutionnelles

– Me Nathalie Chiche, avocate au Barreau de Paris, déléguée à la protection des données, rapporteure de l'étude du Conseil économique, social et environnemental « Internet : pour une gouvernance ouverte et équitable »

Jeudi 29 avril 2021

– Task Force Blockchain (ministère de l'économie, des finances et de la relance)

Mme Liliane Dedryver, directrice de projets « Technologies et solutions numériques émergentes » du service de l'économie numérique à la direction générale des entreprises
Mme Pauline Faucon, adjointe au responsable du pôle « Affaires internationales, coordination européenne et enjeux technologiques du secteur financier à la direction générale du Trésor
M. Thimothée Huré, bureau « Épargne et marché financier » (FinEnt 1) à la direction générale du Trésor
M. Clément Robert, bureau « Services bancaires et moyens de paiement » (BancFin4) à la direction générale du Trésor

Mardi 4 mai 2021

– Direction générale de l'Enseignement scolaire (ministère de l'Éducation nationale)

M. Édouard Geffray, conseiller d'État, directeur général
M. Jean-Marc Merriaux, inspecteur général de l'Éducation nationale, directeur du numérique pour l'éducation

Jeudi 6 mai 2021

– Stratégie nationale pour l'Intelligence artificielle

M. Renaud Vedel, préfet, coordonnateur
M. Julien Chiaroni, directeur du « Grand défi sur l'IA de confiance »

– Conseil national du numérique

Mme Françoise Mercadal-Delasalles, co-présidente
M. Gilles Babinet, co-président

Jeudi 20 mai 2021

– Direction du renseignement militaire (ministère des armées)

M. le général de corps aérien Jean-François Ferlet, directeur du renseignement militaire
M. le lieutenant-colonel Thibaud de Warren

(Cette audition qui s'est tenue à huis clos n'a pas fait l'objet d'un compte rendu)

Vendredi 21 mai 2021

– Commandement de la cyberdéfense (COMCYBER) (état-major des armées) (ministère des armées)

M. le général de division aérienne Didier Tisseyre, officier général commandant de la cyberdéfense
ASC Sébastien Bombal, chef du pôle Stratégie

(Cette audition qui s'est tenue à huis clos n'a pas fait l'objet d'un compte rendu)

Mardi 25 mai 2021

– **Direction de l'enseignement supérieur et de l'insertion professionnelle (ministère de l'enseignement supérieur et de la recherche)**

M. Mehdi Gharsallah, conseiller stratégique pour le numérique auprès de la directrice générale de l'enseignement supérieur et de l'insertion professionnelle

– M. Jean-Luc Sauron, professeur associé à l'université de Paris-Dauphine

– Groupe La Poste

M. Olivier Vallet, président-directeur général de Docaposte, membre du comité de direction de la branche Numérique
M. Gabriel de Brosses, directeur de la Cybersécurité

Jeudi 27 mai 2021

– Microsoft France

Mme Corinne Caillaud, directrice des affaires extérieures, publiques et juridiques, membre du comité exécutif
M. Jean-Renaud Roy, directeur des affaires institutionnelles

Mardi 1er juin 2021

– M. Arnaud Castaignet, directeur de la communication et des affaires publiques de Skeleton Technologies, ancien directeur des relations publiques du programme e-Residency du gouvernement estonien

– Conseil national du logiciel libre (CNLL)

M. Stéfane Fermigier, co-président

Mercredi 2 juin 2021

– Direction générale de la sécurité extérieure (DGSE) (ministère des armées)

M. Patrick Pailloux, directeur technique
M. Julien Barnu, conseiller

(Cette audition qui s'est tenue à huis clos n'a pas fait l'objet d'un compte rendu)

Jeudi 3 juin 2021

– M. Marc Hansen, ministre délégué à la digitalisation du gouvernement du Grand-Duché du Luxembourg

Vendredi 4 juin 2021

– Direction générale de la sécurité intérieure (DGSI) (ministère de l'intérieur)

M. Nicolas Lerner, administrateur civil hors classe, directeur des services actifs de la police nationale, directeur général de la sécurité intérieure

(Cette audition qui s'est tenue à huis clos n'a pas fait l'objet d'un compte rendu)

Mardi 8 juin 2021

– M. Margiris Abukevicius, vice-ministre de la défense nationale de la République de Lituanie

Mercredi 9 juin 2021

– **M. Andrès Sutt,** ministre du commerce et des technologies de l'information de la République d'Estonie