



# LA GOVTECH, NOUVELLE FRONTIÈRE DE LA SOUVERAINETÉ NUMÉRIQUE

Clément TONON

Novembre 2020



L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

Les opinions exprimées dans ce texte n'engagent que la responsabilité de l'auteur.

ISBN : 979-10-373-0246-5

© Tous droits réservés, Ifri, 2020

**Comment citer cette publication :**

Clément Tonon, « La GovTech, nouvelle frontière de la souveraineté numérique »,  
*Études de l'Ifri*, Ifri, novembre 2020.

**Ifri**

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : [accueil@ifri.org](mailto:accueil@ifri.org)

**Site internet :** [ifri.org](http://ifri.org)



# Auteur

Diplômé de l'École des hautes études commerciales (HEC) et de l'École nationale d'administration (ENA), **Clément Tonon** est haut fonctionnaire.

Il est co-auteur de l'étude de l'Ifri intitulée « L'Europe : sujet ou objet de la géopolitique des données ? » parue en juillet 2018<sup>1</sup> et de l'article intitulé « Le futur d'une ellipse. Le vain débat français de politique étrangère » paru dans la revue *Hérodote* en 2018<sup>2</sup>.

---

1. T. Gomart, J. Nocetti et C. Tonon, « L'Europe : sujet ou objet de la géopolitique des données ? », *Études de l'Ifri*, Ifri, juillet 2018.

2. T. Gomart et C. Tonon, « Le futur d'une ellipse. Le vain débat français de politique étrangère », *Hérodote*, vol. 170, n° 3, 2018.



# Résumé

La crise sanitaire du COVID-19 a servi de catalyseur à l'émergence accélérée des GovTech, entendues comme l'irruption d'entreprises et de solutions innovantes dans la conception et l'exécution des services publics. Elle a également mis en lumière des problématiques et tensions nouvelles, ressortant notamment des « narratifs » de gestion de crise reposant sur un usage extensif des technologies provenant de l'Asie du Sud-Est. Plus largement, la crise sanitaire a démontré l'importance stratégique de trois secteurs particuliers de la GovTech, porteurs d'enjeux forts et générateurs de lignes de fractures nouvelles à explorer : le secteur de la e-santé, le développement des *smart cities* et la e-éducation.

L'État français dispose d'une architecture institutionnelle robuste en matière numérique mais souffre de limites structurelles remettant en question sa capacité à développer une véritable politique industrielle en matière de GovTech, permettant l'émergence d'écosystèmes nationaux et européens à l'instar de la Base industrielle et technologique de Défense (BITD) dans le domaine militaire. Plus généralement, l'émergence non coordonnée de la GovTech européenne soulève la problématique politique de l'apparition de nouvelles lignes de fracture internes à l'Union européenne (UE), mises en exergue lors de la crise du COVID-19 avec le développement d'applications de traçage en ordre dispersé. La carence européenne en matière de vision industrielle du secteur et l'absence de format politique de concertation sur le sujet pourraient conduire à faire de l'Europe un terrain privilégié de déploiement des acteurs de la GovTech chinoise ou américaine, bénéficiant du soutien et de l'expérience acquise auprès d'entités domestiques puissantes et faisant partie intégrante d'une stratégie industrielle de souveraineté cohérente et offensive.

Le développement des GovTech interroge fortement notre rapport à l'État et plus largement aux valeurs véhiculées par la technologie. En ce sens, le défi industriel et géopolitique lancé à l'Europe par les grandes puissances technologiques chinoise et américaine dépasse la simple dimension économique : elle menace désormais la capacité de l'Europe à définir son propre imaginaire, à conserver sa liberté de décision démocratique et à maintenir son autonomie stratégique en toutes circonstances.



# Abstract

The COVID-19 crisis has been a catalyst for a surge in the GovTech market, while triggering a debate around the use of new technologies in the public health response to the pandemic. More broadly, the sanitary crisis has shed a new light on the strategic importance of some domains relevant to GovTech such as HealthTech, smart cities and EdTech.

The French State has developed a comprehensive policy of government digitization but still suffers from a lack of investment in the GovTech sector: so far, it has been unable to nurture a GovTech ecosystem comparable to the French defense technological and industrial base.

At the European level, the rise of GovTech solutions could deepen existing divides between member states, as shown by the uncoordinated development of tracking apps by European countries during the crisis. In the long run, the lack of European industrial and political strategy focusing on GovTech could turn Europe into battleground for Chinese and American actors, which benefit from governmental support at home and abroad.

The rise of GovTech companies challenges deeply rooted ideas on the meaning of the public sector and the role of the State. It underlines how technology can affect the values and core principles of democratic societies. In that sense, the growing technological competition between the US, China and Europe means much more than economic rivalry: it is a real threat to European democracy and strategic autonomy.



# Sommaire

<b>INTRODUCTION .....</b>	<b>11</b>
<b>ENJEUX SECTORIELS DE LA GOVTECH : E-SANTÉ, ÉDUCATION NUMÉRIQUE ET DÉVELOPPEMENT DES <i>SMART CITIES</i>.....</b>	<b>17</b>
Les technologies de santé.....	17
Éducation numérique .....	20
Les <i>smart cities</i> .....	22
<b>MAÎTRISER LE DÉVELOPPEMENT DES GOVTECH : EXEMPLES DE STRATÉGIES NATIONALES .....</b>	<b>25</b>
Singapour .....	25
Royaume-Uni .....	26
Estonie.....	27
États-Unis.....	29
Chine.....	30
<b>LA GOVTECH EN FRANCE : ASSOCIER ÉTAT STRATÈGE ET ÉTAT PLATEFORME .....</b>	<b>33</b>
<b>L'UNION EUROPÉENNE FACE AUX GOVTECH : VERS UNE PRISE DE CONSCIENCE DE LA « COMMISSION GÉOPOLITIQUE » ? .....</b>	<b>39</b>
<b>CONCLUSION .....</b>	<b>43</b>



# Introduction

Entendue largement comme « l'utilisation et l'achat de solutions technologiques innovantes par un acteur public<sup>3</sup> », la GovTech (contraction de « government technology ») serait, pour ses promoteurs, porteuse d'opportunités afin d'améliorer le fonctionnement de l'État et de créer des services publics plus adaptés et plus efficaces pour les citoyens.

Sur le plan international, la généalogie de la notion peut être retracée à partir de trois dynamiques distinctes : d'une part, l'émergence du concept d'e-gouvernement, visant à numériser l'administration pour améliorer le rapport coût/efficacité des services publics, a été suscitée depuis le début des années 2000 par les institutions internationales comme l'Organisation de coopération et de développement économiques (OCDE), le Fonds monétaire international (FMI) et la Banque mondiale<sup>4</sup> dans une logique d'efficacité de l'action publique autour du concept d'« État plateforme<sup>5</sup> ». D'autre part, la CivicTech constitue un écosystème spécifique d'entreprises ayant connu une forte croissance au début des années 2010, autour du thème d'une plus grande transparence de l'action publique et une régénération des processus démocratiques par la technologie, logique endossée par le « Partenariat pour un gouvernement ouvert » lancé aux Nations unies par huit pays en 2011. Enfin, la doxa la plus récente en matière de GovTech est notamment produite par les fonds d'investissement et grands cabinets de conseil en stratégie d'entreprise anglo-saxons, qui se proposent de rassembler les problématiques communes des *start-ups* investissant les domaines traditionnellement réservés à l'action publique.

Ainsi entendu, le marché global des GovTech (qui recouvre plusieurs segments thématiques comme la HealthTech dans la santé, l'EdTech dans l'éducation, la sécurité et la défense...) est aujourd'hui estimé à environ

---

3. R. Berger/PUBLIC, « GovTech en France : état des lieux et perspectives », novembre 2019.

4. L'OCDE a mis en place un programme autour du gouvernement numérique établissant le « OECD Open, Useful and Re-Usable Data Index » centré sur les politiques d'*open data* (la France se classe 2<sup>e</sup> de l'édition 2019, derrière la Corée du Sud). La Banque mondiale a lancé en 2019 un programme baptisé GovTech Global Partnership afin d'améliorer la gouvernance dans les pays en développement.

5. Dans son texte de 2011, « Government as a Platform », le chercheur Tim O'Reilly définit l'État plateforme comme la « réorganisation du travail du gouvernement autour d'un réseau d'API (Application Programming Interface) et de composants partagés, de standards ouverts et de jeux de données canoniques, afin que les fonctionnaires, les entreprises et d'autres acteurs puissent offrir au public des services radicalement meilleurs, plus sûrs, efficaces et responsables ».

400 milliards de dollars, avec une croissance rapide de 15 % par an qui devrait le porter à environ 1 000 milliards de dollars en 2025<sup>6</sup>. La plupart des études sur la question illustrent le décrochage européen par rapport aux acteurs américains et, de plus en plus, chinois — l'Europe ne représenterait que 5 % des contrats GovTech, contre 67 % pour les États-Unis et 7 % pour la Chine en phase de rattrapage accéléré<sup>7</sup> — tout en soulignant le potentiel d'un marché encore trop fragmenté entre des États membres aux cultures administratives diverses<sup>8</sup>. Au sein du marché européen, estimé à environ 22 milliards d'euros<sup>9</sup>, c'est le Royaume-Uni qui fait figure de leader en matière de déploiement de la GovTech, faisant écho à une stratégie précoce et cohérente de la part des autorités (cf. infra) : le gouvernement britannique serait à l'origine de 42 % des contrats technologiques « Business-to-Government » (B2G) en Europe (loin devant la France figurant en deuxième position à 11 % et la Suède à 8 %).

La crise sanitaire du COVID-19 a servi de catalyseur à l'émergence accélérée des GovTech et mis en lumière des problématiques et tensions nouvelles, ressortant notamment des « narratifs » de gestion de crise issus d'Asie du Sud-Est, reposant sur un usage extensif des nouvelles technologies. Le développement d'applications de traçage en Europe a également fait émerger les paradoxes et impensés européens autour du concept de souveraineté numérique. Plus largement, la crise sanitaire a démontré l'importance stratégique de trois secteurs particuliers, porteurs d'enjeux forts et générateurs de lignes de fractures nouvelles à explorer : le secteur de la e-santé, le développement des *smart cities* et la e-éducation<sup>10</sup>. L'objectif de la première partie de cette étude est d'analyser les enjeux géopolitiques générés par l'explosion de ces segments au sein d'un « triangle stratégique » composé de l'Europe, des États-Unis et de la Chine.

Derrière le label GovTech émerge un phénomène lourd de conséquences, inédit dans l'histoire politique occidentale : le partage du monopole de l'État dans l'exécution voire la conception des fonctions publiques essentielles et plus encore des missions régaliennes (santé publique, défense, gestion des frontières...), ainsi que l'apparition de phénomènes d'effet cliquet et de dépendance à l'égard d'une poignée

---

6. N. Ismail, « GovTech to Hit \$1 Trillion by 2025 », *Information Age*, [www.information-age.com](http://www.information-age.com).

7. Accenture, « Transforming Public Service with AI. A GovTech Ecosystem Approach », 2019, [www.accenture.com](http://www.accenture.com).

8. PUBLIC, « Why Europe Will Lead the GovTech Revolution », 18 octobre 2019, [www.public.io](http://www.public.io).

9. Accenture, *op. cit.*

10. Pour ce qui est de la France, le rapport R. Berger/PUBLIC, « GovTech en France : état des lieux et perspectives » précité démontre qu'avant même la crise sanitaire, les trois secteurs les plus dynamiques en matière de levée de fonds entre 2012 et 2019 étaient : la HealthTech (678,7 millions d'euros levés), la ville intelligente/nouvelles mobilités (204 millions d'euros levés) et la EdTech (194,1 millions d'euros levés).

d'acteurs privés susceptible de remettre en question sa liberté d'action et de peser sur ses choix de long terme. Il conduit également à interroger, dans un univers d'*open data*, l'hybridation de la gestion des données publiques, au double sens des données à caractère personnel collectées dans l'exercice d'un service public et des données produites par l'administration dans son propre fonctionnement, y compris les plus sensibles. Dans le monde post-COVID, la question des données de santé et des données scolaires, archétypales de cette hybridation, appellent une réflexion renouvelée sur les modes de collecte, traitement, stockage et régulation dans un cadre européen, alors que des géants monopolistiques de la e-santé et de la e-éducation émergent de part et d'autre du Pacifique.

Avec le plan d'action européen pour l'e-gouvernement 2016-2020 et la déclaration de Tallinn, l'Union européenne (UE) a semblé entrer dans le sujet des GovTech *via* un double axe d'harmonisation du marché intérieur et de protection des droits des citoyens. Or, la fragmentation du marché européen, sa relative modestie malgré son dynamisme<sup>11</sup> et l'absence de vision industrielle ou politique de la question pourrait conduire à faire de l'Europe un terrain privilégié de déploiement des acteurs de la GovTech chinoise ou américaine, bénéficiant du soutien et de l'expérience acquise auprès d'entités domestiques puissantes (États fédéral et fédérés, municipalités dynamiques aux États-Unis, État central et provinces chinoises), mais aussi d'autres pays asiatiques comme Singapour ou la Corée du Sud. Ces États ont souvent inclus la GovTech comme composante d'une stratégie industrielle de souveraineté cohérente et offensive. L'objet de la deuxième partie de la présente étude est d'observer les stratégies mises en place par plusieurs pays avancés dans ce domaine – Singapour, le Royaume-Uni, l'Estonie, la Chine, les États-Unis – afin de maîtriser la numérisation de l'action publique et d'en faire, selon des modalités différentes, un vecteur d'influence.

La troisième partie de cette étude est consacrée à la réponse française et européenne à l'émergence des GovTech. L'État français dispose d'une architecture institutionnelle robuste en matière numérique mais souffre de limites capacitaires pour conduire une véritable politique industrielle en matière de GovTech, permettant l'émergence d'écosystèmes nationaux et européens à l'instar de la Base industrielle et technologique de Défense (BITD) dans le domaine militaire. Plus généralement, l'émergence non coordonnée de la GovTech européenne soulève la problématique politique

---

11. Les pays nordiques Danemark (1<sup>er</sup>), Finlande (4<sup>e</sup>) Suède (6<sup>e</sup>), ainsi que l'Estonie (3<sup>e</sup>) et les Pays-Bas (10<sup>e</sup>) se classent dans les 10 premières nations du 2020 « E-Government Index » des Nations unies. Le Royaume-Uni se maintient à la 7<sup>e</sup> place et la France perd dix places par rapport à 2018 et se classe 19<sup>e</sup>. L'Allemagne, accusant un retard relatif en matière de marché des GovTech et de gouvernement numérique, arrive à la 25<sup>e</sup> place.

de l'apparition de nouvelles lignes de fracture internes à l'UE, mises en exergue lors de la crise du COVID-19 avec le développement d'applications de traçage en ordre dispersé. La carence européenne en matière de vision industrielle de la GovTech et l'absence de format politique de concertation sur le sujet créent un risque de moyen terme sur la capacité des Européens à maintenir leur autonomie stratégique, conserver leur liberté de décision démocratique et capter la création de valeur dans des secteurs que l'on pensait jusque-là non délocalisables, comme l'éducation ou la santé.

Elle pose également une série de questions sur la construction européenne en tant que telle. Premièrement, la fragmentation des écosystèmes GovTech nationaux et l'absence de réel marché unique numérique peuvent conduire à augmenter le coût de la mutualisation des politiques partagées par les États membres, en rendant plus difficile la convergence d'outils et de données potentiellement incompatibles (c'est l'enjeu de l'« interopérabilité » prônée par la Commission européenne), tout en accroissant sensiblement les enjeux de compétition industrielle sous-tendant leur négociation. Deuxièmement, l'immixtion d'entreprises privées au cœur de politiques régaliennes peut induire la contamination de pans encore inconnus de la coopération entre États européens par des logiques opportunistes d'allégeances et de jeux de puissance instrumentalisés par des acteurs étrangers, aujourd'hui observables essentiellement en matière de technologies traditionnelles de défense et de souveraineté<sup>12</sup>. Enfin, méconnaître ou sous-estimer le sujet pourrait conduire les pays européens à prendre un retard important dans un nouveau grand jeu diplomatique tiré par l'internationalisation des entreprises de la GovTech, tant celles-ci sont porteuses de valeurs, de normes et de standards technologiques, mais aussi potentiellement créatrices de relations politiques denses et durables comparables à celles tissées dans le cadre des exportations d'armements<sup>13</sup>.

Cette étude s'achève sur une réflexion sur l'impact des GovTech sur la démocratie et plus largement le modèle culturel européen : un gouvernement numérique non maîtrisé est en effet susceptible de subir une influence fonctionnelle, c'est-à-dire échappant au débat démocratique, de

---

12. Sans évoquer la question de la 5G et de Huawei, faisant l'objet d'un rapport de force explicite de la part des États-Unis, le mouvement politico-médiatique qui a conduit un grand nombre de gouvernements européens à retenir le protocole conçu par Apple et Google pour développer leur application de traçage pose la question des nouvelles formes de pressions à l'œuvre sur les gouvernements démocratiques d'Europe en matière de choix technologiques.

13. La coopération franco-vietnamienne en matière d'identité numérique et de cybersécurité mérite d'être étudiée dans cette optique. Le développement de ce type de coopération pourrait susciter un débat administratif sur l'opportunité de la nomination d'« attachés numériques » sur le modèle des attachés de défense, chargés de piloter la relation bilatérale et de servir de lien avec l'écosystème GovTech national.

la part d'acteurs potentiellement vecteurs de conceptions distinctes du service public, de la citoyenneté et des droits individuels (c'est tout l'enjeu de l'internationalisation de la *safe city* à la chinoise, cf. infra). D'autre part, les nouvelles technologies de gouvernement induisent mécaniquement une mise en tension du ressort démocratique. Celui-ci se trouve en effet déstabilisé par l'irruption d'acteurs technologiques faisant primer le narratif de l'efficacité sur l'équilibre complexe au cœur de la notion « d'intérêt général » traditionnellement garantie par l'État et son administration. Cette tension a été illustrée de façon flagrante par le débat européen autour des applications de traçage dans le cadre de la crise du COVID-19. Enfin, les GovTech permettent d'éclairer d'un jour nouveau la notion de « souveraineté numérique » en proposant une vision réticulaire de celle-ci, fondée sur la maîtrise de points névralgiques, de « technologies clés », ainsi que des principes comme la réversibilité, la transparence et l'ouverture visant à maintenir, en toute occasion et en dernier ressort, la liberté de choix et de décision de la puissance publique.



# Enjeux sectoriels de la GovTech : e-santé, éducation numérique et développement des *smart cities*

## Les technologies de santé

La crise sanitaire a mis en valeur le caractère stratégique des technologies de santé et de l'usage des données médicales des individus, tout en illustrant les différences d'approche entre l'Europe, les États-Unis et la Chine. Avec le Règlement général sur la protection des données (RGPD), l'Europe dispose d'un cadre extrêmement protecteur pour les données de santé, qualifiées de « sensibles » et faisant l'objet d'un régime spécifique<sup>14</sup>. Toutefois, la qualité des bases de données des États-providence européens (la France dispose d'une des bases de données de santé les plus complètes du monde<sup>15</sup>) suscite les convoitises d'acteurs internationaux et tranche avec un retard relatif en matière de gouvernance et de développement de la e-santé<sup>16</sup>.

En France, si la loi du 26 janvier 2016 de modernisation de notre système de santé a permis de consolider la gouvernance des données de santé, celle-ci est encore en construction autour de la notion d'État plateforme, appelant une clarification des rôles entre l'État et les industriels du secteur qui mettra plusieurs années à se stabiliser. Une Direction du numérique en santé a ainsi été rattachée au cabinet du ministre de la Santé en 2019 avec pour mission de piloter la feuille de route ministérielle du numérique en santé jusqu'en 2022 et d'assurer la tutelle de l'Agence du numérique en santé en charge de l'établissement de référentiels, du développement de l'interopérabilité des bases, mais également des enjeux éthiques et de cybersécurité. Le projet phare de *Health Data Hub*, accéléré durant la crise sanitaire, a néanmoins mis en évidence trois vulnérabilités majeures de l'approche française et

---

14. Article 9 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

15. Entretien avec un haut fonctionnaire réalisé par l'auteur en septembre 2020.

16. Sur la problématique de la e-santé en France et en Europe, voir le récent rapport de l'Institut Montaigne, « E-santé : augmentons la dose », publié en juin 2020, [www.institutmontaigne.org](http://www.institutmontaigne.org).

européenne des technologies de santé : l'absence de doctrine claire et la fragilité des garde-fous interministériels face à une initiative aux conséquences médiatiques et opérationnelles sous-estimées, dans un tempo bouleversé par la crise sanitaire<sup>17</sup> ; la difficulté de faire émerger une alternative aux acteurs du *cloud* américains pour assurer un niveau de service (notamment sur les applications *Platform as a service* ou *PaaS*) conforme aux cahiers des charges exigeants de la puissance publique et les réticences de celle-ci à préférer une approche incrémentale s'appuyant sur des acteurs nationaux ou européens moins avancés ; les failles du modèle normatif européen fondé sur le RGPD face à la carence industrielle du continent et sa dépendance à l'égard d'acteurs soumis au *Cloud Act* américain<sup>18</sup> ou à d'autres dispositions réglementaires intrusives<sup>19</sup>.

Sauf *aggiornamento* régulateur sur le modèle européen<sup>20</sup>, les États-Unis semblent se diriger vers un modèle assumé de sous-traitance de l'exploitation des données de santé aux grandes entreprises technologiques (GAFAM et entreprises spécialisées). Les révélations autour du « projet Nightingale », contrat secret entre Google Cloud et le géant Ascension (réseau catholique de quelque 2 600 hôpitaux et cliniques) qui concernait fin 2019 le transfert de données de santé de près de 50 millions d'Américains pour nourrir des applications d'intelligence artificielle<sup>21</sup>, ont néanmoins suscité un débat public important autour de la question de la protection des données de santé. La prochaine bataille juridique et

---

17. Ayant conduit à une procédure d'achat accélérée par le biais de la centrale d'achat public UGAP plutôt que *via* un appel d'offres européen, posant la question plus générale du type de marché adapté au déploiement des GovTech.

18. L'invalidation le 16 juillet 2020 par la Cour de Justice de l'Union européenne (CJUE) du *Privacy Shield*, encadrant les transferts de données personnelles entre l'Union européenne et les États-Unis, constitue en ce sens une nouvelle étape du bras de fer normatif transatlantique (voir J. Martinez, « Invalidation du Privacy Shield par la CJUE et les grands défis de Shrems II », *Lexbase Hebdo édition affaire*, septembre 2020). Dans son mémoire en observation transmis au Conseil d'État sur la question du *Health Data Hub*, daté du 8 octobre, la Commission nationale de l'informatique et des libertés (CNIL) tire les conséquences de ce nouveau contexte : « La Commission en tire pour conséquence que le souhait qu'elle avait émis dans son avis du 20 avril 2020 repose désormais sur une obligation légale, l'arrêt Schrems II devant conduire selon elle, pour le cas des données de santé et en particulier dans leur centralisation, à soustraire ces données à la possibilité d'une communication aux services de renseignement [...] ». Dans son audition du 8 octobre 2020 devant la Commission d'enquête du Sénat sur la gestion de la crise sanitaire, Cédric O a par conséquent déclaré « travailler au transfert du *Health Data Hub* sur des plateformes françaises ou européennes ».

19. Notamment l'article 702 du *Foreign Intelligence Surveillance Act* et le décret présidentiel n° 12333.

20. Ce point constitue l'un des enjeux de l'élection présidentielle américaine de novembre 2020, le ticket du candidat démocrate Joe Biden, la sénatrice Kamala Harris, ayant déposé l'année dernière une proposition de loi ambitieuse de réforme du *Health Insurance Portability and Accountability Act* (HIPAA), la loi fédérale sur la sécurité sociale. Ce texte de 1996, plusieurs fois amendé, traite de façon incomplète les dernières possibilités technologiques en matière de traitement des données de santé, notamment celles permises par l'internet des objets.

21. R. Copeland, « Google's "Project Nightingale" Gathers Personal Health Data on Millions of Americans », *The Wall Street Journal*, 11 novembre 2019.

politique concernera la capacité des individus à vendre en temps réel à des acteurs monopolistiques leurs données extraites par les objets connectés. Dans cette optique, l'administration Trump n'a pas fait mystère de son désir d'encourager l'interopérabilité des bases de données de santé et la collecte de données en vie réelle afin de faciliter le développement du secteur numérique.

Dans sa gestion de la crise sanitaire, la Maison-Blanche a encouragé le positionnement des entreprises technologiques proches du pouvoir pour constituer une base de données concurrente de celle des Centers for Disease Control, en principe uniques destinataires des remontées des hôpitaux du pays. C'est Palantir Technology, dont le président Peter Thiel est un soutien historique du président, qui a été choisi pour constituer ce système national, baptisé « HHS Protect », sur la base de plus de 200 jeux de données issues des trois quarts des 8 000 hôpitaux du pays. Donald Trump a réaffirmé publiquement à plusieurs reprises son enthousiasme sur les avancées permises par la e-santé et promis des réformes normatives et budgétaires à l'issue de la crise. Les entreprises spécialisées américaines, notamment les GAFAM, sont d'ores et déjà engagées dans un effort massif d'investissement dans l'Intelligence artificielle (IA) en santé, avec pour horizon 2030, année estimée de maturité des principales applications : ils représenteraient près des trois quarts des investissements dans le secteur (73,3 %), suivis par la Chine (14,8 %), le Royaume-Uni (3,8 %) et Israël (2,5 %) <sup>22</sup>.

Le régime chinois a lancé depuis le milieu des années 2000 un développement à marche forcée de la e-santé, notamment dans le souci d'améliorer la couverture de vastes zones rurales, avec une mise à contribution importante des grands acteurs technologiques en appui des efforts des pouvoirs publics. Dans le cadre du plan « Healthy China 2030 », le gouvernement chinois encourage notamment la constitution de bases de données nationales face à un système fortement régionalisé. Le Conseil d'État chinois a publié en juin 2016 une directive interministérielle pour promouvoir et réglementer l'utilisation du *big data* dans le secteur de la santé, préconisant notamment un partage des ressources de données intersectorielles et interrégionales dans le pays. L'investissement massif — renforcé durant la crise du COVID-19 — d'Alibaba, Baidu, Tencent, Huawei et DiDi dans les technologies de santé, notamment d'analyse et de *big data*, renforce le caractère dual du système de santé chinois entre un secteur public peu performant et des acteurs privés détenteurs de masses critiques

---

22. Research and Markets, « Global Digital Health Outlook 2020 », octobre 2019.

de données pour se maintenir à la frontière technologique<sup>23</sup>. L'appétit en données du système chinois conduit en retour à un effort diplomatique important en matière de normalisation et de standards industriels<sup>24</sup> afin d'ouvrir l'accès à des marchés fortement régulés, comme en Europe. Pour ce faire, « la coopération vers une harmonisation des règles de protection des données est devenue l'un des principaux sujets de discussion des diplomates chinois dans les instances internationales<sup>25</sup> ».

## Éducation numérique

La crise sanitaire a mis en évidence l'importance de l'éducation numérique avec près de la moitié des étudiants dans le monde ayant eu recours à une forme d'enseignement à distance selon les chiffres de l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO). Ce phénomène consacre l'irruption inédite d'acteurs du numérique dans le développement cognitif de milliards d'individus, au sein d'un marché dynamique dont le taux de croissance annuel moyen post-COVID a été réévalué à 16-18 % par an par la plupart des cabinets d'analyse<sup>26</sup>. Il pourrait en outre constituer une future manifestation de la rivalité sino-américaine tant le marché semble se polariser autour d'acteurs issus de ces deux pays, qui représentent à eux deux 75 % des investissements dans l'EdTech, faisant craindre une marginalisation à moyen terme de l'UE. Le marché de l'EdTech en Europe, malgré son dynamisme, demeure en effet loin derrière celui des États-Unis et de la Chine, du fait de systèmes scolaires fragmentés et de la place importante des pouvoirs publics dans leur organisation. Londres demeure la place la plus dynamique avec un écosystème évalué à 3,4 milliards (Md) de dollars, loin devant Paris (1,9 Md) et Berlin (0,8 Md).

En France, le marché des services et des ressources dans l'EdTech était estimé à 89 millions d'euros en 2017 avec un potentiel à 156 millions en 2022<sup>27</sup>. Du côté des entreprises, le marché français apparaît fragmenté

---

23. Sur le modèle d'innovation des systèmes de santé post-COVID et leur exploitation par les acteurs chinois durant la crise, voir E. Grass, « Le Covid-19 va transformer radicalement nos systèmes de santé », *Les Échos*, mars 2020.

24. L'influence de la Chine dans certains organes internationaux de normalisation technique comme l'Organisation internationale de normalisation, la Commission électrotechnique internationale ou l'Union internationale des télécoms est bien documentée, notamment en France par les travaux de John Seaman. Voir par exemple : J. Seaman, « Normes et standards chinois, nouveau facteur de puissance. Une puissance technique conquérante », *RAMSES 2019. Les chocs du futur*, Paris, Ifri/Dunod, 2018. Le gouvernement chinois devrait publier avant la fin de l'année son plan stratégique « China Standards 2035 », axé sur les technologies à double usage civilo-militaire.

25. R. Creemers, « Comment la Chine projette de devenir une cyber-puissance », *Hérodote*, vol. 177-178, n° 2, 2020.

26. Voir par exemple : [www.holoniq.com](http://www.holoniq.com) et [www.prnewswire.com](http://www.prnewswire.com).

27. Deloitte Digital/Caisse des dépôts et consignations, « Le marché EdTech scolaire et parascolaire français (2018-2022) », juin 2018.

avec d'un côté quelques acteurs de taille moyenne (OpenClassrooms, Klaxoon...) et plusieurs dizaines de petites structures de moins de dix employés. Du côté des acheteurs, le secteur, fortement déconcentré, est caractérisé par une domination d'acteurs ayant une relative autonomie (écoles, collèges, lycée) pesant à eux seuls 95 % de l'achat de solutions numériques innovantes.

Si la loi du 8 juillet 2013 pour la refondation de l'École de la République instaure un service public du numérique éducatif, la polémique suscitée par le stockage de données scolaires — dont le statut juridique n'est pas particulièrement protégé par le RGPD — sur des serveurs d'Amazon Web Service en 2018, a conduit le ministère de l'Éducation nationale français à renforcer la supervision des nombreux applicatifs et dispositifs numériques<sup>28</sup>. La puissance publique s'est ainsi dotée d'une structure originale, le Gestionnaire d'accès aux ressources (GAR), dont la mission est d'assurer « un filtre sécurisant en contrôlant les données échangées avec les fournisseurs de ressources », d'un délégué à la protection des données (DPD) et d'un comité d'éthique et d'expertise en matière de données numériques, placé auprès du ministre de l'Éducation nationale en octobre 2019. Toutefois, les difficultés rencontrées par l'enseignement à distance en France durant la crise sanitaire ont conduit le ministre de l'Éducation nationale à annoncer la tenue d'états généraux du numérique pour l'éducation en novembre 2020. Pour la France comme pour les autres pays européens, où des acteurs sous-traitent à des sociétés d'intelligence artificielle américaines l'analyse des données émanant de cours en ligne<sup>29</sup>, l'enjeu est bien de faire émerger une industrie domestique allant du service au stockage, en passant par le traitement, soumis au RGPD et à des principes éthiques renforcés.

Les États-Unis demeurent les leaders mondiaux du secteur et se sont dotés dès 2010 d'un « National Educational Technology Plan » ayant pour ambition de faire des États-Unis la principale nation en matière d'enseignement numérique à horizon 2020<sup>30</sup>. Le pays dispose également de l'écosystème le plus dynamique du monde avec des géants spécialisés comme Coursera, alors que l'irruption des GAFAM dans le secteur des EdTech est désormais un fait accompli. Cette domination du marché mondial de l'éducation en ligne pourrait toutefois être remise en question à court terme par l'essor des acteurs chinois.

---

28. Voir les conclusions du rapport IGEN-IGAENR, « Données numériques à caractère personnel au sein de l'éducation nationale », février 2018, [www.education.gouv.fr](http://www.education.gouv.fr).

29. C. Authemayou, « Pour la CNIL, la France doit garder la souveraineté de ses données scolaires », *l'Étudiant EducPros*, 2017, [www.letudiant.fr](http://www.letudiant.fr).

30. Ainsi que l'affirmait Karen Cator, Directrice à l'Office of Educational Technology, lors de la présentation de la stratégie en 2010.

La Chine a investi massivement depuis le début des années 2000 dans le développement de la e-éducation<sup>31</sup>, laquelle a connu un essor sans précédent durant la crise sanitaire : plus de 200 millions d'élèves du primaire et du secondaire ont assisté à des cours en ligne durant la pandémie de COVID-19, et les cours privés en ligne de TAL Education, l'une des entreprises les plus importantes du secteur en Chine, ont été vus plus de 500 millions de fois durant les deux premières semaines suivant la rentrée des classes virtuelle<sup>32</sup>. La Chine affiche désormais de fortes ambitions en matière de e-éducation. Ces ambitions sont à la fois d'ordre idéologique de la part du Parti communiste chinois, qui mobilise des moyens technologiques de plus en plus sophistiqués au service d'un contrôle intégral des pensées, et d'ordre politique avec des gains escomptés dans la « compétition cognitive » en cours avec les États-Unis. Comme l'a déclaré le PDG de TAL Education lors de la prise de contrôle d'un acteur israélien en 2018, « l'éducation est une part importante de l'influence internationale de la Chine et nous aimerions en faire une façon de lier la Chine au monde ». Pour poursuivre ces ambitions, la Chine peut s'appuyer sur neuf « licornes » sur les vingt « licornes » mondiales de la EdTech (huit aux États-Unis, deux en Inde, une au Canada et aucune en Europe<sup>33</sup>) et un marché captif de 283 millions d'élèves en premier cycle, sans équivalent dans le monde.

## Les smart cities

Le développement des *smart cities*, « villes intelligentes », ou « hyperconnectées » a été mis en lumière d'une façon inédite par la crise sanitaire. Alors que jusqu'à présent l'utilisation des nouvelles technologies en milieu urbain était principalement envisagée en Europe et aux États-Unis dans une perspective d'urbanisme durable ou de lutte contre le terrorisme, c'est sur le plan sanitaire et du contrôle social que les diverses applications asiatiques ont fait l'objet d'avancées majeures. En outre, la question de la 5G et du découplage technologique entre les États-Unis et la Chine conduit à considérer de plus en plus la question des *smart cities* comme un enjeu profondément géopolitique, où se croisent de façon inédite dimensions politiques, sociales et industrielles<sup>34</sup>.

---

31. En 2018, la Chine aurait investi 4,5 milliards de dollars dans le numérique éducatif, contre 1,9 milliards de dollars pour les États-Unis. Voir à ce sujet M.-C. Levet, « Préserver notre souveraineté éducative », *The Digital New Deal*, novembre 2019.

32. D. Wei et J. Hong, « Parents Grapple with E-Learning as Chinese Schools Stay Shut », *Bloomberg*, février 2019, [www.bloomberg.com](http://www.bloomberg.com).

33. HolonIQ, « Global EdTech Unicorns », septembre 2020, [www.holoniq.com](http://www.holoniq.com).

34. Sur le sujet de la dimension géopolitique du déploiement des *smart cities*, voir A. Ekman, « La smart city chinoise. Nouvelle sphère d'influence ? », *Études de l'Ifri*, Ifri, décembre 2019.

Il est significatif de noter que le développement des premières *smart cities* en Chine a eu lieu à la suite de l'épidémie de SRAS (syndrome respiratoire aigu sévère) en 2003. En 2012, le 12<sup>e</sup> plan a accéléré ce mouvement entamé dix ans plus tôt et fait du développement de ces *smart cities* une priorité nationale au travers de plusieurs projets pilotes à Wuhan, Shenzhen, Tianjin ou encore Xi'an, tout en accélérant l'internationalisation du modèle chinois<sup>35</sup>. À la suite du déclenchement de l'épidémie de COVID-19, le régime a fait de la *smart city* à la chinoise un élément essentiel de son « narratif » de gestion de la crise sanitaire en mettant en valeur le déploiement de solutions innovantes et d'applications parfois inédites : drones connectés, reconnaissance faciale, développement de la technologie V2X (Vehicle-to-Everything) permettant aux véhicules d'interagir avec leur environnement au sein de *smart districts*, distribution des premières licences de taxis autonomes... Outre les BATX<sup>36</sup>, l'industrie de défense investit également dans la *smart city* à la chinoise qui se pense avant tout, dans le vocabulaire officiel comme dans les faits, en tant que *safe city*, « ville sûre ». Norinco et China Electronics Technology Group Corporation (CETC), deux conglomérats de défense, proposent par exemple la vente sur étagère d'infrastructures et de services pour une ville « sûre et intelligente ». Élément de sa propagande post-COVID, l'exportation de technologies de surveillance constitue ainsi un moyen pour le régime chinois de diffuser son modèle d'« autoritarisme numérique<sup>37</sup> », notamment dans les pays acheteurs d'Asie centrale, du Moyen-Orient et d'Afrique<sup>38</sup>.

L'Europe constitue un terrain privilégié de la confrontation sino-américaine sur le sujet des *smart cities* malgré la volonté des institutions communautaire de soutenir l'émergence de solutions proprement européennes<sup>39</sup> et la constitution de communautés nationales d'acteurs technologiques engagés dans le secteur<sup>40</sup>. Les États-Unis ont appelé leurs alliés à ne pas développer les réseaux 5G fondés sur la technologie de Huawei ainsi que les services inhérents à la *safe city* à la chinoise (dispositifs de surveillance et de vidéoprotection, nouvelles mobilités...).

---

35. Depuis 2013, 116 projets de *smart cities* incluant des entreprises chinoises auraient ainsi été approuvés dans plus de 70 pays. Voir sur ce sujet J. Kynge et N. Liu, « From AI to Facial Recognition: How China Is Setting the Rules in New Tech », *Financial Times*, octobre 2020.

36. Acronyme servant à qualifier Baidu, Alibaba, Tencent et Xiaomi, les *majors* technologiques chinoises.

37. A. Polyakova et C. Meserole, « Exporting Digital Authoritarianism: The Russian and Chinese Models », *Brookings Institution*, août 2019.

38. J. E. Hillman et M. McCalpin, « Watching Huawei's "Safe cities" », *CSIS Briefs*, novembre 2019, [www.csis.org](http://www.csis.org).

39. C'est le sens du European Innovation Partnership on Smart Cities and Communities soutenu par la Commission européenne. Plus d'information sur : <https://ec.europa.eu>.

40. Avec des acteurs comme Thales et Engie Ineo (Angers, Nice) ou encore Bouygues et Keolis (Dijon).

Renoncer à Huawei mettrait les Européens devant un choix : acheter sur étagère des solutions américaines développées par les GAFAM, ou développer une politique industrielle ambitieuse pour faire émerger une *smart city* à l'européenne, faisant écho aux valeurs de l'Europe, à son système politique et à sa conception des données personnelles. Si, comme l'affirme Alice Ekman, « la *smart city* émerge comme un terrain de compétition politique et géostratégique, opposant différentes sphères d'influence, dans un contexte de tensions prolongées entre la Chine et les États-Unis<sup>41</sup> », c'est, là aussi, la question d'une voie technologique européenne qui se pose avec une acuité accrue dans le monde post-COVID.

---

41. A. Ekman, « La *smart city* chinoise. Nouvelle sphère d'influence ? », *op. cit.*

# Maîtriser le développement des GovTech : exemples de stratégies nationales

Plusieurs pays ont développé des stratégies cohérentes de déploiement de la GovTech. En Asie, si la Corée du Sud et Taïwan font figure de pays avancés en la matière, c'est Singapour qui a initié dans les années 1980 un mouvement profond de numérisation de ses services publics, dont le pays a pu tirer les dividendes durant la crise sanitaire. En Europe, avec le Danemark et la France, ce sont le Royaume-Uni et l'Estonie qui proposent des modèles de e-gouvernement performants, malgré des échecs et des priorités divergentes. La Chine et les États-Unis, désormais engagés dans une guerre technologique, se sont lancés précocement dans l'internationalisation de leurs entreprises GovTech à l'appui de leurs stratégies d'influence respectives, ainsi que dans un déploiement domestique accéléré par la crise sanitaire.

## Singapour

Les efforts de la cité-État en matière de numérisation des services publics sont anciens. Dès les années 1980, le gouvernement a lancé le programme national d'informatisation (National Computerisation Programme) piloté par un Bureau national de l'informatisation, afin d'automatiser les procédures les plus simples et de constituer des bases de données publiques. La stratégie pluriannuelle pour un gouvernement numérique lancée en 2017 est fondée sur plusieurs piliers : une identité numérique pour tous, le e-paiement, les « moments de vie » (faciliter les démarches de la vie quotidienne), la mise en place de capteurs sur tout le territoire singapourien et les *smart cities*.

Singapour a mis en place dès 2016 une Agence de la GovTech disposant de plus de 2 500 agents. L'objectif de cette agence est de centraliser les compétences de l'État en matière de cybersécurité et de conduite de projets numériques (ce qui en ferait l'équivalent, en France, d'un regroupement de l'Agence nationale de la sécurité des systèmes d'information [ANSSI], de la Direction interministérielle du numérique [DINUM] et d'une partie de l'Institut national de recherche en sciences et technologies du numérique

[INRIA], cf. infra). Au-delà de la numérisation des services publics et d'un effort sur l'interopérabilité des bases et logiciels publics, l'Agence a lancé plusieurs programmes ambitieux en matière de *smart cities* (notamment la pose de milliers de senseurs dans l'espace public afin d'améliorer sa connaissance de l'environnement urbain). L'Agence s'est enfin dotée de bureaux à l'étranger, notamment en Californie, pour tenter de tirer profit des compétences de la diaspora singapourienne présente dans la Silicon Valley.

Dans le contexte de la pandémie de COVID-19, le gouvernement singapourien a mis en place un « narratif » au sujet de la gestion de crise qui repose largement sur l'efficacité de son modèle de gouvernement hyper-technologique et le succès de son application de traçage TraceTogether. Analysé en profondeur, ce récit repris par d'autres pays d'Asie du Sud-Est menacés par la montée en puissance de la Chine, comme Taïwan et la Corée du Sud, « vise à contrebalancer la propagande chinoise en mettant l'accent sur l'association possible entre société démocratique et *containment* technologique de la maladie<sup>42</sup> ». Cette « guerre des narratifs<sup>43</sup> » a d'autant plus de force dans le cas de Singapour qu'il constitue un retour de balancier dans l'influence mutuelle entre les deux pays, le modèle singapourien de Lee Kwan Yew ayant directement inspiré les réformes de Deng Xiaoping au tournant des années 1990. La question de l'usage des nouvelles technologies par les gouvernements d'Asie cristallise donc une nouvelle compétition intellectuelle et culturelle entre deux modèles de société façonnant les rapports de force dans l'espace indo-pacifique.

## Royaume-Uni

Le Royaume-Uni est l'un des pays européens les plus avancés en matière de gouvernement numérique, arrivant régulièrement dans le « top 5 » des sondages des Nations unies et de l'OCDE sur le e-gouvernement<sup>44</sup>. Dans le sillage du rapport fondateur « Directgov 2010 and Beyond: Revolution Not Evolution » rédigé par Martha Lane Fox, fondatrice de Lastminute.com, le pays a mis en place des dispositifs d'incitation originaux afin d'ouvrir ses marchés publics aux petites et moyennes entreprises (PME) innovantes (l'objectif affiché est de 33 % des marchés publics attribués à des PME) et s'est doté en mars 2011 d'un Government Digital Service (GDS) aux attributions larges.

Le GDS a ainsi piloté la mise en place de services tels que gov.uk verify (identité numérique) et gov.uk pay (paiement simplifié et sécurisé des

---

42. Entretien avec un haut fonctionnaire réalisé par l'auteur en juillet 2019.

43. *Ibid.*

44. Malgré un décrochage dans le classement 2019 de l'OCDE, avec une perte de 19 places depuis 2017 causée par une baisse du soutien du gouvernement à la réutilisation des données.

usagers), tout en supervisant l'ouverture d'activités régaliennes à des acteurs privés tels que la *start-up* CaseLines permettant aux tribunaux britanniques, dont la Cour suprême, d'automatiser la lecture et le tri de certains documents. Dans le sillage de la stratégie gouvernementale pour l'intelligence artificielle (« Artificial Intelligence Sector Deal », 2018), les ministères de la Culture et de l'Industrie ont en outre mis en place un Office for Artificial Intelligence chargé d'animer une communauté interministérielle autour de l'IA et d'incarner la position britannique à l'international sur les enjeux éthiques et normatifs afférents.

En 2017, le gouvernement a pris deux initiatives importantes afin d'accentuer son effort en matière d'administration numérique. D'une part, deux documents stratégiques ont permis d'établir une doctrine cohérente d'usage des nouvelles technologies par la puissance publique : la « Government Transformation Strategy 2017-2020 » et la « UK Digital Strategy ». Une nouvelle version de la « UK Digital Strategy » devrait être publiée à l'automne 2020 pour être adaptée au contexte post-COVID, au même titre qu'une nouvelle stratégie pour la gestion des données dont l'un des enjeux sera d'imaginer le régime de transfert avec l'UE qui sera retenu dans le cadre du Brexit. Cette dimension technologique du Brexit « démontre la perte pour l'Union européenne d'un acteur politique, industriel et sécuritaire majeur : industriel, avec la perte de Londres, première place de *start-up* innovantes en Europe ; politique, avec une nation ayant un agenda de souveraineté numérique proche de celui de la France ; et sécuritaire, avec un acteur majeur de la cybersécurité<sup>45</sup> ». La National Data Strategy, publiée le 9 septembre 2020, complète ce corpus stratégique et instaure une Data Standards Authority et un Government Data Quality Hub chargés de développer l'interopérabilité et l'exploitabilité des données entre départements ministériels. Enfin, le gouvernement britannique a souhaité créer les conditions financières pour développer le secteur en lançant le GovTech Catalyst Fund d'un montant de plus de 20 millions d'euros à investir dans des PME innovantes. L'objectif était de créer un effet de levier afin de mobiliser des fonds privés et de stimuler une activité de capital-risque déjà en forte croissance (+ 189 % en valeur de 2012 à 2016).

## Estonie

Dans le sillage de sa transition démocratique post-soviétique, l'Estonie a forgé son identité sur un modèle d'État plateforme original, grâce à un environnement porteur et à des programmes publics innovants déclinés

---

45. Entretien avec un haut fonctionnaire français réalisé par l'auteur en juillet 2020.

dans le « Digital Agenda 2020 for Estonia<sup>46</sup> ». Le modèle estonien repose ainsi sur la généralisation d'une e-identité combinant carte d'identité digitale et numéro d'identification – déclinée depuis 2014 en statut de e-résident permettant l'accès à certains droits et services pour des entreprises et particuliers étrangers – et un système de stockage et d'échange de données *open source* appelé X-Road permettant une interopérabilité totale entre près de 1 000 institutions publiques et privées. Le développement et la sécurité de X-Road sont supervisés par l'Autorité du système d'information de l'État (RIA) rattachée au ministère des Affaires économiques et des Communications.

L'identité numérique est progressivement devenue consubstantielle à la démocratie estonienne avec, en 2002, l'inscription dans la Constitution de l'accès à Internet comme droit des citoyens et, en 2005, l'organisation d'un vote numérique pour une élection nationale fondé sur une identification digitale. La numérisation de l'État estonien s'est également accompagnée d'un effort important des autorités pour assurer la réduction de la fracture digitale grâce à une politique de formation aux outils numériques dès le plus jeune âge et un accent sur la transparence des usages et des outils gouvernementaux, contribuant à bâtir une confiance forte des Estoniens dans leur forme de e-gouvernement. Kersti Kaljulaid, présidente de l'Estonie affirmait au sommet des GovTech en 2019 : « Aujourd'hui je ne comprends pas pourquoi des citoyens en arrivent à faire plus confiance à Google et Facebook qu'à leur gouvernement. Vous devez simplement démontrer que le digital est plus sécurisé que le papier et créer un cadre légal adapté pour que la technologie puisse servir toute la nation, et non pas seulement le petit nombre.<sup>47</sup> »

Après les cyberattaques de 2007 qui ont illustré les vulnérabilités de son modèle d'État plateforme, l'Estonie n'a eu de cesse de plaider auprès de ses partenaires de l'UE et de l'Organisation du traité de l'Atlantique nord (OTAN) pour un renforcement des capacités collectives de protection et d'offensive, tout en développant un écosystème national de « licornes » lui permettant d'assurer son autonomie technologique<sup>48</sup>. En matière de développement des GovTech, le modèle estonien mérite donc d'être étudié pour son caractère englobant, associant réforme de l'appareil d'État,

---

46. Sur ce sujet, lire le rapport d'A. Picron, « L'E-Estonie, modèle d'un État plateforme e-gouverné. L'exemple de la transformation totale d'un État grâce au numérique », Institut Sapiens, juillet 2018.

47. P. Berthoux, « GovTech : les États ont-ils dépassé le Proof-of-Concept ? », *Alliancy*, 15 novembre 2019.

48. Durant la crise sanitaire, l'Estonie a par exemple fait le choix de confier à un consortium de neuf entreprises nationales (Bytelogics, Cybernetica, Fujitsu Estonia, Guardtime, Icefire, Iglu, Mobi Lab, Mooncascade, Velvet) le développement d'une application de traçage décentralisée, compatible avec le protocole développé par Apple et Google.

réflexion stratégique et véritable transformation sociétale : « L'évolution de l'Estonie en tant que pays numérique [...] s'est faite de manière organique et continue, partant dans un premier temps de la transformation numérique des structures administratives du pays [...] pour ensuite, poussée par les attaques de 2007, se porter à la sécurisation des structures préexistantes, au développement d'un cadre légal renforcé dans les domaines civil et militaire, puis à la mise en place de nouvelles solutions pour faire évoluer les systèmes de concert avec le développement des nouvelles technologies<sup>49</sup>. »

## États-Unis

Le candidat Barack Obama avait fait de l'e-gouvernement l'un de ses thèmes de campagne et a conduit dès son premier jour en fonction<sup>50</sup> une politique de numérisation sans précédent dans l'histoire récente des États-Unis, portant tant sur l'accessibilité des services, la transparence des données (avec la création du site data.gov) que sur la participation des citoyens à la décision publique (plateforme challenge.gov). Le concept d'État plateforme, développé par Tim O'Reilly dans son essai « Government as a Platform » est en outre repris dès 2012 dans la feuille de route « Digital Government: Building a 21<sup>st</sup> Century Platform to Better Serve the American People ». Toutefois, l'échec du développement du site healthcare.gov en 2013<sup>51</sup> a conduit la Maison-Blanche à revoir le portage interne des projets numériques et à mettre en place en 2014 le United States Digital Service – maintenu par Donald Trump – consacrant un mode de fonctionnement inspiré de celui des équipes de développeurs de la Silicon Valley et entretenant une hybridation des méthodes et des personnels (la plupart des ingénieurs faisant la navette entre les GAFAM et le gouvernement fédéral).

Le gouvernement encourage également la constitution d'un écosystème GovTech dense grâce à un volume d'achat public sans équivalent facilement fléché sur les PME (*Buy American Act* et *Small Business Act*) de la part de l'État fédéral et de ses agences, mais aussi des États fédérés et de municipalités très dynamiques (Pittsburgh, Seattle, San Francisco...). La vitalité du secteur du capital-risque a également permis l'émergence d'acteurs dédiés comme le GovTech Fund qui a annoncé en

---

49. L. Ronzaud, « E-Estonie, le “nation-branding” numérique comme stratégie de rayonnement international », *Hérodote*, vol. 177-178, n° 2, 2020.

50. Dès le 21 janvier 2009, soit son premier jour de mandat, Barack Obama publie un mémo sur le e-gouvernement et la numérisation des services publics.

51. Pilier technique d'Obamacare, le site healthcare.gov a dysfonctionné à peine deux heures après sa mise en ligne du fait d'un nombre de connexions cinq fois supérieur à ce qui était attendu.

2018 la création d'une *joint-venture* de 450 millions d'euros avec le fonds européen Sunstone Technology Ventures afin d'investir dans des *start-ups* en Europe.

Les GovTech font en outre partie intégrante de la politique d'intelligence économique du pays, dans un contexte de rivalité technologique exacerbée avec la Chine. Le fonds d'investissement de la Central Intelligence Agency (CIA) créé en 1999, In-Q-Tel, investirait chaque année en moyenne 120 millions d'euros dans des *start-ups* du secteur de la sécurité et serait à l'origine du succès de Facebook, Google Earth (développé à l'origine par l'entreprise Keyhole) et de la croissance de Palantir Technology, qui a réalisé son introduction à la bourse de New York le 30 septembre 2020. De manière générale, les relations symbiotiques entre le complexe militaro-industriel et les grands acteurs du numérique américains, constante politique réaffirmée lors de la crise du COVID-19, « sont devenues telles que l'appareil de sécurité lie désormais explicitement sécurité nationale et capacité des GAFAM à se maintenir à la frontière technologique dans tous les domaines (stockage et traitement des données, mais aussi santé, information, environnement, *smart cities*...)»<sup>52</sup>, impliquant une « guerre technologique totale » aux équipementiers et géants du numérique chinois. Les États-Unis ont ainsi pour objectif « d'étendre à leurs alliés cette logique de bloc technologique, désormais pensée comme indissociable de l'alliance politique et militaire avec l'Amérique<sup>53</sup> ».

## Chine

Le développement des GovTech en Chine depuis le début des années 2000 est inséparable du basculement du régime vers un « capitalisme de surveillance » envahissant l'ensemble des domaines de la vie sociale. Le pays a défini les grandes lignes de sa politique de puissance dans le plan 2015-2025 « Made in China » et le 13<sup>e</sup> plan quinquennal 2016-2020, qui font des technologies de l'information et de l'IA des priorités de l'effort économique national. Tout en prévoyant le développement de capacités nationales dans l'ensemble des grands domaines stratégiques – le découplage sino-américain en matière de semi-conducteurs accélérant cette tendance –, ces plans consacrent une imbrication de plus en plus

---

52. Entretien avec un haut fonctionnaire spécialiste des questions de sécurité, réalisé par l'auteur en juillet 2019. C'est le sens de la Third Offset Strategy (TOS) du Pentagone, publié en 2015.

53. *Ibid.*

intime entre les BATX et l'appareil d'État chinois<sup>54</sup>, mise en lumière par la crise sanitaire.

Dans leur lutte contre l'épidémie de COVID-19, les autorités chinoises, centrales et locales, ont fait un usage extensif des nouvelles technologies. Celles-ci saturent désormais l'espace public, constituant un écosystème de surveillance de plus en plus interconnecté. La crise sanitaire a permis le déploiement de modes de traçage et de reconnaissance des individus, accélérant les efforts gouvernementaux pour combiner données de santé, géolocalisation mobile, reconnaissance faciale ou encore scannage thermique. Différents ministères ainsi que le conglomérat étatique de défense China Electronics Technology Group Corporation (CETC) ont développé une application de traçage, « Close Contact Detector », afin d'agrèger ces différents types de données pour détecter avec précision le déplacement des individus et prévenir les foyers potentiels. Les gouvernements locaux (provinces et municipalités) ont également mis en ligne leurs propres applications, accessibles sur les réseaux des grandes plateformes chinoises : Alipay (Alibaba), WeChat (Tencent) et Baidu<sup>55</sup>.

Pour Pékin, l'exportation de solutions GovTech dans le monde apparaît plus que jamais comme un outil stratégique d'influence. D'où l'importance de la « Route de la soie numérique » (Digital Silk Road), qui constitue le fer de lance de cette stratégie et devrait devenir encore plus déterminante dans le monde post-COVID. D'une part, l'attractivité du modèle chinois de gestion de la crise sanitaire, reposant sur l'usage de technologies de contrôle social, pourrait conduire à renforcer les demandes de coopération dans ce domaine<sup>56</sup>. D'autre part, le choc économique produit par le coronavirus pourrait durement toucher les capacités de la Chine à investir et à prêter à l'étranger dans le cadre des Nouvelles routes de la soie. Si ses capacités d'investissements dans des projets d'infrastructures lourds devaient être altérées, Pékin maintiendrait son intérêt pour les projets de télécommunication et le déploiement des GovTech, moins coûteux et de forte portée stratégique.

---

54. Cette imbrication est devenue telle qu'une politique publique de l'ampleur de l'identité numérique universelle souhaitée par le gouvernement serait portée par Alibaba et Tencent, [www.weforum.org](http://www.weforum.org).

55. Ces applications, nécessitant la fourniture des données biométriques, ont un fonctionnement similaire : l'algorithme attribue un code couleur (vert, jaune ou rouge), lisible via un QR code individuel, en fonction notamment de l'historique des mouvements de la personne et de son bilan de santé. Ce code détermine ensuite la mise en quarantaine pendant 14 ou 7 jours, ainsi que l'accès à certains secteurs ou services.

56. En Europe, le format 17+1, rassemblant 17 pays d'Europe centrale et orientale et la Chine pourrait constituer un vecteur privilégié de cette coopération. Avant même la crise sanitaire, la 4<sup>e</sup> conférence ministérielle sur l'innovation du format 17+1 d'octobre 2019 avait pour thème « la ville intelligente et la mobilité urbaine ». Voir A. Ekman et C. de Esperanza Picardo, « Towards Urban Decoupling? China's Smart City Ambitions at the Time of Covid 19 », *Institute for Security Studies*, mai 2020.



# La GovTech en France : associer État stratège et État plateforme

« Contrairement à ce qu'on pourrait penser, la digitalisation de l'État français est une histoire ancienne<sup>57</sup>. » Elle remonte au début des années 1960, avant même la lancée du premier Plan Calcul de 1966 à la suite du traumatisme suscité par le rachat, le 22 juillet 1964, du constructeur français d'ordinateurs Bull par le groupe américain General Electric. Le Plan Calcul prévoyait notamment la nomination d'un Délégué général à l'informatique placé sous l'autorité du Premier ministre, poste occupé par Robert Galley puis Maurice Allègre, tous deux chargés de définir les principales orientations face aux « problèmes posés par le développement d'une industrie nationale des ordinateurs<sup>58</sup> ». La délégation générale à l'informatique sera supprimée en 1975 à la suite de l'échec du projet européen « Unidata » visant la création d'un géant de l'ordinateur autour de la Compagnie internationale de l'informatique, Philips et Siemens.

Il faudra ensuite attendre le début des années 2000 pour que soient lancés les premiers programmes cohérents de numérisation de l'État : programme d'action gouvernemental pour la société de l'information (PAGSI) à l'origine du site service-public.fr en 2000, puis plan « ADELE » (Administration Électronique 2004-2007) en 2004. Ce dernier programme donnait le premier véritable cadre pluriannuel et coordonné au développement de l'administration électronique en France. En septembre 2014, la fonction d'administrateur général des données est créée pour concevoir une politique destinée aux données produites ou exploitées par les administrations, autour de trois axes principaux : la fourniture, la circulation et l'exploitation, afin d'améliorer l'efficacité de l'action publique dans une logique d'*open data*. Promulguée en octobre 2016, la loi pour une République numérique visait à « donner une longueur d'avance à la France dans le domaine du numérique en favorisant une politique d'ouverture des données et des connaissances<sup>59</sup> ». Enfin, le programme Action publique

---

57. Entretien avec un haut fonctionnaire réalisé par l'auteur en juillet 2019.

58. Relevé des décisions du Conseil restreint du 19 juillet 1966 consacré au développement des secteurs de pointe.

59. Exposé des motifs de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

2022, lancé le 13 octobre 2017, fixe comme objectif 100 % de services publics dématérialisés à horizon 2022. Il est décliné en une stratégie interministérielle de transformation numérique, tech.gouv 2019-2022, et des stratégies sectorielles comme le « Plan de transformation numérique-Défense Connect » d'avril 2018 pour le ministère des Armées<sup>60</sup>.

L'État s'est en outre doté de plusieurs organes de régulation, de contrôle et de portage de la politique publique de numérisation :

- L'Agence nationale des systèmes d'information (ANSSI), qui remplace depuis 2009 la Direction centrale de la sécurité des systèmes d'information, est un service à compétence nationale rattaché au Secrétariat général à la défense et à la sécurité nationale (SGDSN). L'ANSSI a une mission de défense des systèmes d'information de l'État, mais elle est aussi chargée d'une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale (OIV), notamment *via* ses procédures de certification de produits et de qualification des prestataires de services de confiance.
- En matière de transformation numérique, l'État s'est doté en 2019 d'une direction transversale, la Direction du numérique (DINUM, anciennement Direction interministérielle du numérique – DINSIC) dont le rôle est d'accompagner les ministères dans leur transformation numérique, de conseiller le gouvernement et de développer des solutions comme le réseau interministériel de l'État, l'identité numérique partagée (dont FranceConnect constitue la première étape) et l'*open data* de l'État (avec la mission Etalab et la plateforme data.gouv.fr), le tout dans une logique d'État plateforme (dont l'une des manifestations est le portail api.gouv.fr, permettant aux acteurs privés d'utiliser librement les bases de données publiques)<sup>61</sup>. Elle est également chargée de piloter la feuille de route tech.gouv 2019-2022 dont l'un des axes est la « maîtrise des systèmes d'information<sup>62</sup> ». Elle a enfin un rôle stratégique dans la supervision des grands projets technologiques des départements ministériels : son avis conforme doit être recherché par chaque administration sur les projets informatiques

---

60. Ces stratégies accompagnent une montée en puissance accélérée des projets liés à l'intelligence artificielle et au *big data* au sein des administrations depuis deux ans, comme le Health Data Hub déjà évoqué, mais aussi le Sport Data Hub, le projet « 3D » de la Direction générale des douanes et droits indirects (DGDDI) ou encore le projet « Artémis » du ministère des Armées.

61. Henri Verdier, DINSIC de 2015 à 2019, est le vulgarisateur en France du concept d'État plateforme avec son ouvrage co-écrit avec N. Colin, *L'Âge de la multitude, Entreprendre et gouverner après la révolution numérique*, Paris, Armand Colin, Paris, 2012 [2<sup>e</sup> éd. 2015].

62. La stratégie tech.gouv dispose notamment que « nous devons nous assurer de la maîtrise des systèmes d'information, des architectures, des logiciels et du patrimoine de données afin d'accroître l'autonomie numérique de l'État et sa sécurité. Renforcer cette maîtrise technologique concourt directement à préserver la souveraineté nationale. »

dont le montant est supérieur à 9 millions d'euros. Toutefois, le rôle de filtre de la DINUM se limite à une méthode d'analyse de la valeur (MAREVA) et ne constitue pas une appréciation en opportunité du projet en question. La DINUM n'a pu en outre empêcher la divergence des pratiques ministérielles, renforcée par la diversité et l'attrition globale des capacités de pilotage internes à chaque département.

- Enfin, l'INRIA, créée par le Plan calcul de 1966, a pour triple ambition de former un centre de recherche d'excellence sur l'algorithmique et le logiciel, d'animer un écosystème universitaire et entrepreneurial dense<sup>63</sup> et de constituer « le bras armé de l'État en matière de souveraineté numérique<sup>64</sup> ». Dans son plan stratégique à quatre ans, « Ambition INRIA 2023 », l'INRIA affirme ce dernier rôle en se posant en coordinateur du Plan IA tourné en priorité vers le secteur sécurité-défense, en partenariat avec l'ANSSI et l'agence de l'innovation de Défense (AID), tout en soulignant ses apports en matière de régulation numérique en lien avec la Direction générale des entreprises (DGE) de Bercy. De façon opérationnelle, l'INRIA a mis en place des structures conjointes avec la DINUM, dont le LabIA qui a pour objet de fournir un appui technique aux services de l'État sur les cas d'usage les plus difficiles<sup>65</sup>.

Malgré ces avancées, la structure administrative française peine à concevoir le sujet des GovTech comme un sujet stratégique en dehors, d'une part, du mouvement ancien de réforme et de numérisation de l'État et, d'autre part, du cadre fixé par le code des marchés publics. Plusieurs cas médiatisés<sup>66</sup>, de natures très différentes mais permettant de tirer quelques conclusions générales, ont cependant illustré « une certaine méconnaissance des enjeux numériques par une partie des élites administratives françaises mais également la fragmentation des structures et procédures de contrôle des projets technologiques de l'État<sup>67</sup> ». C'est bien la capacité de l'État à développer une véritable politique industrielle du numérique permettant l'émergence d'écosystèmes nationaux et européens tout en améliorant sa propre action qui est aujourd'hui en question et bute sur plusieurs facteurs structurels :

---

63. L'INRIA a notamment participé à la création de l'écosystème French Tech.

64. Contrat d'objectifs et de performance 2019-2023 entre l'État et l'INRIA, signé le 18 février 2020.

65. 21 administrations ont déjà pu bénéficier de l'expertise technique du LabIA, dont la Gendarmerie nationale ou le Conseil d'État.

66. Il s'agit notamment du contrat de la DGSI avec la société américaine Palantir, renouvelé en 2019, et de l'attribution à Microsoft Azure du contrat d'administration du Health Data Hub en juin 2020, récemment remise en question (cf. supra).

67. Entretien avec un haut responsable d'une entreprise du secteur des nouvelles technologies, réalisé par l'auteur en septembre 2020.

- Une tendance de fond à l'attrition des ressources humaines de l'État en matière de conduite de projets numériques, dans un contexte de compétition pour les talents et de rationalisation des choix budgétaires<sup>68</sup>, entraînant par ricochet le recours extensif à des sociétés de services du numérique (SS2I) avec une capacité de pilotage amoindrie et peu de capitalisation de connaissances par l'administration.
- En parallèle, une volonté de maintenir un niveau de contrôle élevé sur les spécifications de cahiers des charges entièrement définis par la puissance publique « dans un monde où l'innovation ne se pense plus comme la réponse univoque à une question technique mais appelle une connaissance fine des besoins pour y apporter une réponse sur-mesure le cas échéant évolutive<sup>69</sup> ». Cette tendance est parfois renforcée par la pression du temps politique, conduisant à préférer le recours à des solutions « clés en main » proposées par des acteurs américains ayant une connaissance historique de l'administration française et une avance technologique indéniable en termes de qualité et de variété des services proposés, notamment en matière d'applications dans le *cloud* (*PaaS*)<sup>70</sup>.
- La relative inadéquation du cadre des marchés publics au développement des GovTech, malgré les adaptations relatives aux marchés innovants issues du rapport Villani<sup>71</sup>.
- L'absence d'un acheteur expert de l'État, capable de conduire des programmes en matière de solutions numériques avec une vision industrielle et stratégique du secteur, animant un écosystème d'entreprises GovTech et harmonisant les doctrines d'emploi ministérielles. En cela, la Direction générale de l'Armement (DGA) pourrait constituer un « parallèle imparfait dans le domaine de l'industrie de défense<sup>72</sup> ». Le positionnement institutionnel de la DINUM, placée sous la tutelle de la ministre de la Transformation et de la Fonction publique, ne permet pas en outre « de développer son

---

68. Voir à ce sujet le Tome II du rapport public annuel 2020 de la Cour des comptes, « Le numérique au service de la transformation de l'action publique », février 2020.

69. Entretien avec un chef d'entreprise du secteur des nouvelles technologies, réalisé par l'auteur en août 2020.

70. « Les administrations sont ainsi prises dans une contradiction entre la stratégie IA et la stratégie *Cloud* visant à affirmer un objectif de souveraineté, qui est d'autant plus forte que leurs données sont considérées comme sensibles (santé, éducation, données fiscales...) ». Entretien avec Étienne Grass, vice-président exécutif de Capgemini Invent, réalisé par l'auteur en octobre 2020.

71. Décret n° 2018-1225 du 24 décembre 2018 portant diverses mesures relatives aux contrats de la commande publique.

72. Entretien avec un haut responsable d'une entreprise du secteur des nouvelles technologies, réalisé par l'auteur en septembre 2020.

ouverture sur l'international, ainsi que sur les sujets stratégiques et industriels<sup>73</sup> », ni d'animer une véritable communauté de travail interministérielle, « système d'intelligence collective de l'État », sur le sujet des données ou de l'IA.

- De façon plus générale, le manque de culture des managers publics sur les questions numériques, tant en matière de rudiments techniques que d'enjeux sécuritaires, stratégiques et industriels, à développer dès le cursus d'apprentissage au sein des grandes écoles du service public et au sein des démarches ministérielles de gestion prévisionnelle des ressources humaines (GPRH)<sup>74</sup>. Plus que le manque de compétences dures (*data engineers, data scientists...*), c'est bien le déficit de « product owners » aux échelons supérieurs et intermédiaires de l'État pour se saisir des nouveaux outils numériques qui handicape le développement de l'administration digitale, notamment en matière de politique publique de la donnée et de l'IA<sup>75</sup>.

Le développement d'un État plateforme « à la française », doté des outils stratégiques et de l'écosystème industriel national suffisant pour conserver la maîtrise de son ouverture progressive, est donc un enjeu majeur de souveraineté mais également un élément clé de la capacité de la France à peser sur le modèle européen en construction, dans un contexte post-Brexit : « Nous devons d'abord créer les conditions pour faire émerger des champions nationaux, tel que peut l'être une entreprise comme OVH. L'instrument réglementaire viendra dans un second temps. Et la question d'un projet à l'échelle européenne, tel que pourrait l'être Gaia-X, ne peut venir que dans un troisième temps, en s'appuyant sur les forces des États membres.<sup>76</sup> »

---

73. Entretien avec un haut fonctionnaire, réalisé par l'auteur en septembre 2020.

74. Gestion prévisionnelle des ressources humaines, sur le modèle des pratiques de l'administration britannique qui y a inclus précocement l'évolution des métiers de la fonction publique face au développement de l'IA.

75. Sur ces freins humains, culturels, juridiques et politiques, lire le rapport d'étape de la mission Bothorel sur la politique publique de la donnée en date du 8 octobre 2020, disponible sur [mission-open-data.fr](https://mission-open-data.fr).

76. Entretien avec Étienne Grass, vice-président exécutif de Capgemini Invent, réalisé par l'auteur en octobre 2020.



# L'Union européenne face aux GovTech : vers une prise de conscience de la « Commission géopolitique » ?

L'Union européenne envisage traditionnellement le sujet des GovTech *via* un double axe d'harmonisation du marché intérieur et de protection des droits des citoyens. La Commission Juncker a fait du marché unique du numérique un de ses principaux objectifs en favorisant notamment la libre circulation des données non personnelles au sein de l'UE, afin d'encourager l'innovation. La GovTech est perçue dans ce cadre comme un outil privilégié d'harmonisation du marché unique (notamment en mettant l'accent sur l'interopérabilité des services aux entreprises). Au sein de sa stratégie pour un marché unique numérique<sup>77</sup>, l'Union s'est ainsi dotée d'un plan d'action pour l'administration en ligne 2016-2020 intégrant les principes du numérique par défaut, du « demandez-le une fois », du caractère inclusif, de l'interopérabilité, de l'accessibilité, du caractère transfrontalier des services publics et de la sécurité. Les réflexions de la Commission ont abouti à la directive de 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (directive PSI<sup>78</sup>), adoptant une approche explicitement économique de la question de l'*open gov* afin d'encourager l'innovation par le secteur privé.

L'autre axe exploré par la Commission est celui du e-gouvernement comme vecteur de transparence et d'efficacité accrue pour les citoyens européens<sup>79</sup>. Les déclarations de Malmö (2009) et de Tallinn (2016) sur le e-gouvernement réaffirment ainsi les principes sous-jacents à l'utilisation du numérique dans les services publics pour les rendre plus « ouverts, efficaces et collaboratifs ».

---

77. Communication de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Stratégie pour un marché unique numérique en Europe », mai 2015, <https://eur-lex.europa.eu>.

78. Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

79. « D'ici à 2020, l'Union européenne devrait être dotée d'administrations et d'institutions publiques ouvertes, efficaces et inclusives, qui fourniront à tous les citoyens et entreprises de l'UE des services publics numériques de bout en bout conviviaux, personnalisés et sans frontières. »

En soulignant en janvier 2020 que « pour être un acteur géopolitique, il faut pouvoir être garant de sa souveraineté technologique », la Commission Von der Leyen a pour ambition de dépasser la simple réponse normative face au défi géopolitique et industriel lancé par les États-Unis et la Chine<sup>80</sup>. Sous l'impulsion du Commissaire au Marché intérieur Thierry Breton, la Commission européenne a présenté le 19 février 2020 sa stratégie en matière d'intelligence artificielle et de données, laquelle détaille son objectif de parvenir à faire émerger neuf espaces européens communs de données, dont l'un devra « favoriser des applications innovantes dans le domaine des technologies au service de l'administration (GovTech) ». Cette ambition industrielle s'accompagne d'un soutien de 10 milliards d'euros au projet franco-allemand d'infrastructure *cloud* de confiance Gaia-X, dont l'objectif est à la fois une meilleure maîtrise des données stockées en Europe mais également le développement de l'interopérabilité des données européennes à des fins d'applications industrielles<sup>81</sup>.

En matière de financement, l'émergence d'un écosystème GovTech innovant devrait passer au sein du nouveau cadre financier pluriannuel par la réorientation d'une partie des programmes Horizon 2020 vers un mode de financement plus adaptée à l'« innovation de rupture ». C'est dans cette optique que la France promeut la création d'une « Agence européenne d'innovation de rupture », entendue comme « un DARPA à l'européenne [...] car il est indispensable que l'Europe, sur l'intelligence artificielle, sur le véhicule autonome, sur la *blockchain* et toutes les innovations de rupture à venir, puisse se positionner en ayant une vraie politique commune de financement de ces avancées technologiques<sup>82</sup> ». Le Conseil européen du 2 octobre 2020, largement dédié à la question de la souveraineté numérique, a consacré ce basculement de la grammaire européenne<sup>83</sup>

---

80. Dans son discours sur l'état de l'Union du 16 septembre 2020, la présidente de la Commission a ainsi intégré les services publics numériques dans les trois priorités pour le futur « plan commun pour l'Europe numérique à horizon 2030 ». Tout en réaffirmant le risque pour l'Europe de devenir une « colonie numérique », elle a annoncé la mise en place d'une identité numérique sécurisée pour tous les citoyens européens et d'un effort de planification à mener : « Nous avons besoin d'un plan commun pour l'Europe numérique, avec des objectifs clairement définis pour 2030, notamment en matière de connectivité, de compétences et de services publics numériques. Nous devons aussi nous doter de principes clairs : le droit au respect de la vie privée et à la connectivité, la liberté d'expression, la libre circulation des données et la cybersécurité. »

81. Le ministre de l'Économie et des Finances français, Bruno Le Maire, expliquera ainsi lors de la conférence de presse de lancement de Gaia-X le 4 juin 2020 : « Pour développer une voiture autonome, vous avez besoin d'un grand nombre de données sur la sécurité routière. Le fait de pouvoir facilement échanger des données entre constructeurs européens grâce à une infrastructure compatible comme Gaia-X peut donc considérablement leur faciliter la tâche. »

82. Discours d'Emmanuel Macron lors du Sommet sur le numérique de Tallinn le 29 septembre 2017.

83. « Pour être souveraine sur le plan numérique, l'UE doit mettre en place un marché unique véritablement numérique, renforcer son aptitude à définir ses propres règles, à opérer des choix

et ajouté une pression politique sur la Commission européenne dont les progrès en la matière seront examinés par les chefs d'État et de gouvernement en mars 2021.

Si cette nouvelle ambition industrielle doit encore se concrétiser dans les faits, la crise sanitaire « a illustré les limites politiques » du projet de souveraineté numérique des Européens et l'incapacité de la Commission à donner une impulsion dans le développement d'une application de traçage unifiée, malgré un embryon de coordination technique à l'échelle de groupes de travail supervisés par la direction générale de la Santé et la publication de lignes directrices axées sur l'interopérabilité et à la protection des données personnelles<sup>84</sup>. L'inexistence d'un format de discussion sur les sujets numériques stratégiques permettant de débattre de l'opportunité d'alternatives à la solution Google-Apple, ainsi que le manque de culture du dialogue sur ces questions entre les États membres et la Commission, ont ainsi contribué à la divergence des pratiques et à l'incapacité des Européens à s'accorder sur une solution commune et interopérable<sup>85</sup>.

En l'absence d'un mécanisme de concertation entre les États membres et la Commission sur le sujet des GovTech, la crise a révélé le risque d'apparition de nouvelles lignes de fracture économiques et industrielles que leur déploiement non coordonné soulève pour l'Europe. Plus significativement, elle a révélé l'ambiguïté constitutive de la notion de souveraineté numérique en Europe<sup>86</sup>, dont le caractère incapacitant ne pourra être levé que dans le développement d'une culture stratégique commune dépassant désormais largement le spectre de l'outil militaire.

---

technologiques autonomes et à développer et déployer des capacités et des infrastructures numériques stratégiques. Au niveau international, l'UE tirera parti de ses instruments et de ses pouvoirs de réglementation pour contribuer à la définition de règles et de normes mondiales. » Conclusions du Conseil européen sur l'épidémie de COVID-19, la politique économique et les relations extérieures de l'Union européennes, le 2 octobre 2020.

84. Commission européenne, « Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19. Common EU Toolbox for Member States », avril 2020, <https://ec.europa.eu>.

85. Cédric O affirmera de manière assez significative lors de son audition du 8 octobre 2020 devant la commission d'enquête du Sénat sur la gestion de la crise sanitaire : « Pourquoi nous ne nous sommes pas coordonnés avec les autres pays européens ? Parce que nous avons un choix assez binaire : soit on choisissait de se coordonner et on n'avait plus qu'à appeler Apple et Google, soit on choisissait de ne pas se coordonner et on restait souverains. »

86. Sur l'ambiguïté de la notion de souveraineté numérique en Europe, lire l'article de D. Danet et A. Desforges, « Souveraineté et autonomie stratégique en Europe : du concept aux réalités géopolitiques », *Hérodote*, vol. 177-178, n° 2, 2020. On y trouve cette citation significative d'Angela Merkel lors du Forum de gouvernance de l'Internet en novembre 2019 : « Bien sûr, la souveraineté numérique est très importante. Mais il se peut que nous en soyons tous venus à comprendre quelque chose de différent, même si nous utilisons le même terme. »



# Conclusion

Le développement des GovTech interroge fortement notre rapport à l'État et plus largement aux valeurs véhiculées par la technologie : « Outre la bataille industrielle [...] se profile également une bataille culturelle qui tournera en grande partie autour de la question des données<sup>87</sup>. » La technologie, notamment lorsqu'elle touche aux missions régaliennes traditionnellement dévolues à la puissance publique comme la santé, l'éducation, l'urbanisme, la sécurité et la défense, n'est pas neutre : elle constitue une « grammaire qui détermine toutes les autres » et « formate le débat démocratique<sup>88</sup> ». Si le « numérique fonctionne physiquement sur la puissance de calcul, c'est également un vecteur de symboles et de représentations humaines et en ce sens, c'est un substrat profondément politique<sup>89</sup> ». Au temps de l'« État-entreprise<sup>90</sup> », plusieurs lignes de forces peuvent être identifiées pour cerner le potentiel de déstabilisation des GovTech, qui appellent à en développer une vision géopolitique alimentant l'action industrielle et politique.

Une ligne de force culturelle et symbolique d'abord. La GovTech ouvre la possibilité pour des acteurs potentiellement vecteurs de conceptions distinctes du service public, de la citoyenneté et des droits individuels, d'influencer par la technologie les modes de gouvernance et d'action publique d'un pays tiers. C'est tout l'enjeu de la « Route de la soie numérique » et des conceptions véhiculées par la *safe city* à la chinoise déjà évoquée. Cette guerre des récits est d'ores et déjà puissante entre le capitalisme de surveillance chinois et les démocraties hypertechnologiques d'Asie du Sud-Est. C'est également le nœud du défi lancé par les États-Unis à l'Europe sur la notion de protection de la vie privée et des données personnelles, dont le sens porté par le 4<sup>e</sup> amendement de la Constitution

---

87. Administrateur général des données, « La donnée comme infrastructure essentielle », Rapport au Premier ministre sur la donnée dans les administrations 2016-2017, *La Documentation française*, avril 2018.

88. Lors de son audition devant la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République du 27 mai 2020 sur l'application StopCovid, Cédric O affirmera : « Ce sont les réseaux sociaux, qui ancrent notre quotidien dans la culture et le droit anglo-saxons. Ce sont les moteurs de recherche, qui hiérarchisent notre accès à l'information et formatent notre débat démocratique. Ce sont enfin mille autres exemples qui témoignent de l'urgence d'inscrire le numérique au cœur du travail de nos institutions. Non pas comme une matière en soi mais comme une grammaire qui détermine toutes les autres. »

89. Entretien avec un haut fonctionnaire, réalisé par l'auteur en septembre 2020.

90. P. Musso, *Le Temps de l'État-Entreprise : Berlusconi, Trump, Macron*, Paris, Fayard, 2019.

américaine et appliqué par les acteurs de la Silicon Valley diffère largement de la philosophie européenne portée par le RGPD. Dans son discours de la Sorbonne en septembre 2017, Emmanuel Macron avait exprimé cette intuition d'une menace diffuse, par le numérique, planant sur la spécificité même de la civilisation européenne : « L'Europe a cet attachement unique à l'équilibre permanent entre la liberté, la solidarité et la sécurité, et c'est bien cela qui est en jeu dans la révolution numérique. [... C'est au fond] la capacité cognitive de la France et de l'Europe à façonner leur imaginaire qui est en jeu avec le numérique, pour ne pas dépendre de l'imaginaire des autres.<sup>91</sup> »

Une ligne de force démocratique ensuite. Par la GovTech, les démocraties occidentales sont déstabilisées par l'irruption dans l'action publique d'acteurs technologiques faisant primer le « narratif » de l'efficacité sur l'équilibre complexe au cœur de la notion d'intérêt général traditionnellement garantie par l'État et son administration. Durant la crise sanitaire, cette tension a été exprimée de façon flagrante par les appels au « pragmatisme » des défenseurs de la solution décentralisée proposée par Apple et Google, mettant en avant à la fois son efficacité présumée supérieure et les risques pour les libertés prétendument posés par une solution centralisée. Le fait que, dans une société démocratique, l'État dispose d'une légitimité supérieure aux géants privés du numérique pour superviser un système de traçage sanitaire, lui permettant de surcroît d'améliorer sa gestion de la crise au bénéfice de tous, n'a que peu pesé face à la crise de confiance démocratique traversée par les pays occidentaux<sup>92</sup>. En définitive, la crise sanitaire a révélé en creux l'absence d'espace de débat démocratique national et européen sur les sujets technologiques<sup>93</sup>, appelant à considérer désormais le numérique non comme un enjeu de méthode ou de procédure (la « démocratie numérique ») mais bien un objet de démocratie délibérative à part entière.

Une ligne de force en termes de pensée de la souveraineté, enfin. L'émergence des GovTech nous dit quelque chose du terme diffus et équivoque de « souveraineté numérique ». D'une part, elle souligne la persistance dans le domaine numérique de l'identité stratégique des nations, de leur plus ou moins grande appétence à « conserver leur liberté

---

91. Entretien avec un haut responsable d'une entreprise du secteur des nouvelles technologies, réalisé par l'auteur en septembre 2020.

92. Selon un sondage Accenture (2018) portant sur le Royaume-Uni, les États-Unis, l'Australie, Singapour, la France et l'Allemagne, seuls 31 % des citoyens ont confiance dans le gouvernement pour utiliser l'IA de façon éthique et responsable. Seuls 23 % estiment que des services publics fondés sur l'IA protègent mieux les données personnelles.

93. Le débat parlementaire sur l'application StopCovid faisant figure ici d'heureuse, bien que trop confidentielle, exception.

de décision et leur autonomie sous la contrainte<sup>94</sup> ». Durant la crise sanitaire, le Royaume-Uni est ainsi l'un des seuls gouvernements européens à avoir choisi comme la France de développer une application souveraine de traçage, avant de faire machine arrière pour des raisons techniques. Comme l'affirmait Cédric O lors du débat parlementaire sur StopCovid, cet alignement n'est pas une coïncidence : « Vingt-deux pays ont à ce jour choisi de développer une solution de protection des contacts qui s'appuie sur l'interface développée par Apple et Google. Vingt-deux pays, mais pas la France ni le Royaume-Uni qui, est-ce un hasard, sont aussi les deux seuls pays européens à disposer de leur propre appareil de dissuasion nucléaire – ce qui est finalement l'acmé de la souveraineté nationale. » Le pragmatisme allemand rallié à la solution des deux GAFAM pose ainsi la question de l'avenir de la coopération technologique européenne post-Brexit et d'une réflexion nécessaire entre la France et l'Allemagne sur les intérêts et choix sociétaux partagés en la matière.

D'autre part, en termes techniques, les GovTech nous permettent conceptuellement de dépasser la dialectique entre modèle fermé et modèle ouvert : elles nous entraînent vers une approche réticulaire ou « capacitaire<sup>95</sup> » de la souveraineté numérique, « où la maîtrise de points technologiques névralgiques est plus importante que de maîtriser toute la chaîne<sup>96</sup> ». La maîtrise de ces points névralgiques, de ces « technologies clés<sup>97</sup> », dont l'identification et la régulation devraient constituer une priorité de la puissance publique (« choisir quels combats on peut gagner et quels leviers de négociations ils autorisent »), permettra peut-être de décliner les principes directeurs d'une véritable politique industrielle plus que jamais nécessaire à l'Europe<sup>98</sup> et à la préservation de son identité.

---

94. Entretien avec un haut responsable d'une entreprise du secteur des nouvelles technologies, réalisé par l'auteur en septembre 2020.

95. Sur cette notion de « souveraineté capacitaire » telle qu'envisagée dans le cadre de la numérisation du ministère des Armées, lire le très complet article d'Arnaud Coustillère dans le numéro 2020/2 de la revue *Hérodote* intitulé « La transformation numérique du Ministère des Armées ».

96. Dans le cas de StopCovid, l'audition du 22 septembre 2020 de Bruno Sportisse, PDG de l'INRIA, devant la commission d'enquête du Sénat sur la gestion de la crise sanitaire, démontre que les systèmes d'exploitation des smartphones (notamment Android et iOS) constituent un tel « nœud technologique » dont la régulation pourrait améliorer la liberté d'action des différents acteurs publics et privés européens.

97. Dont la cryptographie et l'algorithmique constituent des éléments essentiels ainsi que la technologie des sondes de détection.

98. Les principes de réversibilité, de portabilité, d'ouverture, de transparence, d'interopérabilité...



Institut français  
des relations  
internationales