SciencesPo

CHAIRE DIGITAL, GOUVERNANCE ET SOUVERAINETÉ

LES ENSEIGNEMENTS DES PROJETS DE CLOUD SOUVERAIN POUR LA STRATÉGIE NUMÉRIQUE DE L'ÉTAT FRANÇAIS

Pierre NORO
Cofondateur de Pebble et chargé d'enseignement à Sciences Po

Executive summary

Depuis la fin des années 2000, l'industrie du *cloud computing* a connu une croissance rapide et ininterrompue. Le recours au *cloud computing* fait désormais partie intégrante de nos modes de vie et de production connectés, *a fortiori* dans le contexte pandémique actuel, qui encourage le recours au télétravail et à des moyens de divertissement et de sociabilité reposant sur des infrastructures *cloud*. Avec l'annonce, à l'été 2020, du lancement officiel de Gaia-X, le projet de bâtir un « *Cloud* souverain » a fait son retour sur le devant de la scène médiatique. Ce *policy brief* a pour but de définir le concept de *cloud* souverain, de poser une analyse systémique des politiques publiques françaises passées et actuelles en la matière et d'en tirer des enseignements concrets afin de profiter réellement du nouvel élan européen autour de la gouvernance des données et des services numériques. En voici les principales conclusions :

- Le recours aux services de *cloud computing* est essentiel à nos économies mais pose un problème de souveraineté numérique qui s'incarne dans trois dimensions complémentaires et interdépendantes : le droit, la sécurité et l'économie.

- Un *cloud* souverain devrait donc permettre à un utilisateur d'accéder de manière sécurisée et continue à des services dans le respect du droit qui lui est applicable, notamment en matière de protection des données, en préservant son indépendance. A l'échelle d'un État, s'ajoute à ces enjeux juridiques et géostratégiques l'impératif de développement d'une industrie capable de fournir de tels services, de maintenir leur accessibilité et d'en développer de nouveaux.

- En France, les projets de *cloud* souverains se sont principalement focalisés sur cette dimension économique tout en donnant lieu à des investissements sous-dimensionnés. Des discours idéologiques peu ancrés dans la réalité technique et industrielle du secteur ont généré une stratégie incohérente, déracinée de l'écosystème d'innovation national.

- L'absence de synchronisation entre les efforts de normalisation, de réglementation et la stratégie industrielle n'ont pas permis aux nouvelles solutions de *cloud* souverain

de répondre aux besoins émergents et déstructurés du secteur public. Ce manque de cohérence entre les discours en matière de *cloud* souverain et l'orientation de la commande publique persiste encore aujourd'hui.

- La *European Strategy for Data*, qui prévoit des investissements massifs pour des infrastructures de *cloud* européennes, et le projet de *Data Governance Act*, qui entend structurer les pratiques de partage de données notamment dans le secteur public, impriment une dynamique propice à l'élaboration de nouvelles initiatives de cloud souverain.

- Comme le montre l'initiative Gaia-X, la coopération entre les entreprises et institutions publiques issues de plusieurs États-Membres autour de valeurs fondamentales pour la souveraineté numérique (protection des données, transparence, utilisation de technologie *open source*, interopérabilité…) a le potentiel de générer de nombreuses opportunités économiques et de renforcer la compétitivité des acteurs européens face aux géants américains et chinois. Le succès de ces projets dépendra de leur capacité à construire une infrastructure commune répondant aux besoins des économies européennes tout en restant fidèle à ces valeurs, y compris dans leur gouvernance.

- Ces nouvelles initiatives de *cloud* souverain doivent tirer les enseignements des précédents échecs et s'appuyer sur des politiques industrielles et des investissements cohérents, favorisant le développement d'écosystèmes d'innovation où les entreprises peuvent collaborer, mutualiser des ressources et interfacer leurs solutions pour mieux répondre à la croissante demande européenne.

- A cet égard, la nouvelle stratégie annoncée en mai 2021 pose question. La nouvelle doctrine « Cloud au centre » et le label « Cloud de confiance » ont le potentiel d'accélérer l'adoption des services *cloud* dans le secteur public et dans l'économie française en général, mais la création d'un label permettant le recours à des technologies extra-européennes licenciées par des fournisseurs de services européens est insatisfaisante en matière de souveraineté et menace de créer une situation de dépendance économique dangereuse, pouvant aboutir à une perte de capacité industrielle et technologique pour l'écosystème français sur le long terme.

Introduction

Le 14 décembre 2020, une panne globale des services du Google Cloud Platform (GCP) a paralysé une partie de l'économie mondiale pendant près de deux heures. Face à l'impossibilité de s'authentifier et d'accéder aux services de Google (Gmail, Agenda, Drive, Docs, Meet, Calendar, Maps, Youtube…) mais aussi à de nombreux fournisseurs de services en ligne utilisant GCP comme infrastructure, comme par exemple Spotify, Snapchat ou encore Discord, de nombreuses entreprises ainsi que des établissements scolaires, universitaires, médicaux ayant recours à ces services se sont retrouvés incapables de fonctionner normalement. Cette dépendance était soudainement devenue tout aussi flagrante pour les individus utilisant ces services quotidiennement, pour des usages professionnels, sociaux ou récréatifs. Les utilisateurs dont les appareils domotiques sont contrôlés par Google Home ont même fait cette expérience de manière spectaculaire en étant, pour une partie de la journée, plongés dans le noir, inaptes à maîtriser leur espace privé, leur propre maison.

Les conséquences d'une panne de cette ampleur, quoique exceptionnelle, montre à quel point nos modes de vie, de consommation et de production connectés reposent sur l'utilisation de services de *cloud computing*. En dépit du développement vertigineux des capacités de calcul de nos *smartphones* et ordinateurs, nous avons de plus en plus recours à « l'informatique en nuage », c'est-à-dire à des services qui « délocalisent » les ressources informatiques (nécessaires au stockage et au traitement des données ainsi qu'aux opérations de calcul) et permettent nos usages en dehors de nos terminaux, grâce à des *data centers* capables de mobiliser de manière flexible, scalable et efficiente, des infrastructures bien supérieures à celles dont disposerait un utilisateur ordinaire (particulier ou entreprise).

Considérant ce rôle essentiel que joue le *cloud computing* dans nos économies, il n'est pas surprenant que l'accès au *cloud* soit rapidement devenu un enjeu de société dont s'est emparé l'État français. Depuis 2009, le projet du « *cloud* souverain » est devenu emblématique des politiques de l'État français en matière de souveraineté numérique. L'ambition de financer l'émergence d'un « géant du Web » national, a laissé place à Gaia-X, une plateforme européenne présentée le 4 juin 2020 par la France et l'Allemagne qui repose sur les acteurs de l'écosystème existant et s'intègre dans le nouveau cadre réglementaire européen du *Digital Single Market*, ainsi qu'à une nouvelle « Stratégie nationale pour le cloud », dévoilée le 17 mai 2021, qui veut étendre la notion de « cloud de confiance » aux solutions portées par des entreprises européennes reposant sur des technologies des

GAFAM sous licence. L'évolution des incarnations du projet de *cloud* souverain traduisent les échecs d'une stratégie industrielle française incohérente mais aussi la redéfinition de la notion de souveraineté numérique et de son champ d'application face aux impératifs économiques et aux discours mettant en scène l'urgence et le retard technologique.

1. Cloud et souveraineté numérique

Pour bien comprendre les enjeux du *cloud* souverain, il est nécessaire de revenir brièvement sur la définition et la croissance du *cloud computing*. C'est face à l'émergence de cette technologie, des usages innovants qu'elle facilite et des nouveaux leaders économiques qu'elle a couronnés que les décideurs publics ont élaboré le projet de *cloud* souverain en France. Ce concept de souveraineté numérique appliqué au *cloud* s'articule autour de trois impératifs de gouvernance, d'ordre juridique, sécuritaire et économique, qui sous-tendent les initiatives entreprises par des gouvernements successifs, dont nous dressons ici un rapide récapitulatif.

1.1. Le *cloud computing* infrastructure numérique essentielle de l'économie

L'expression *cloud computing* a aussi rapidement intégré notre langage courant que nos usages, sans pour autant qu'une définition unique ne fasse pleinement consensus (de Filippi, McCarthy, 2012). Le *National Institute of Standards and Technology* du *US Department of Commerce* définit le *cloud computing* comme un « modèle qui permet facilement l'accès à la demande, à un ensemble de ressources informatiques partagées, depuis n'importe quel endroit. »[1] Cette architecture est donc l'héritière des années 60 et de l'ère des *mainframes*, lorsque de nombreuses organisations qui ne pouvaient pas se procurer, opérer et entretenir des infrastructures informatiques suffisantes pour réaliser leurs calculs sollicitaient ces superordinateurs massifs et extrêmement coûteux, hébergés par quelques universités et entreprises dans le monde.

Malgré l'augmentation spectaculaire de la puissance des ordinateurs personnels, *smartphones* inclus, et la baisse de leurs coûts de production, qui ont progressivement rendu les outils informatiques accessibles au plus grand nombre dans les pays développés, le déploiement à grande échelle d'infrastructures réseau permettant d'accéder à internet à haut-débit a rendu possible le déplacement progressif de nos besoins grandissants en ressources de stockage et de calcul vers le *cloud*.

Le succès du *cloud* s'explique à la fois pour les avantages qu'il procure aux utilisateurs que pour les économies générées au niveau des fournisseurs. En effet, les services fondés sur le

[1] Traduction de l'auteur. Pour une définition plus détaillée, voir la notice du NIST (en anglais).

cloud permettent aux utilisateurs d'accéder facilement à distance à une quantité flexible et rapidement adaptable de ressources informatiques qui pourraient être coûteuses à acquérir et à administrer, surtout pour des usages temporaires, alors que les fournisseurs de service bénéficient de vastes économies d'échelle en mutualisant les équipements nécessaires au sein de *data centers* entièrement optimisés, assurant également la maintenance physique et informatique de ces équipements.

L'accès à ces ressources s'effectue selon trois modèles de services principaux :

- *Infrastructure-as-a-service* (IaaS), où l'utilisateur accède directement aux ressources informatiques (capacités de calcul, de stockage, réseau…) pour y déployer, sous son propre contrôle, ses propres applications et systèmes informatiques.
- *Platform-as-a-service* (PaaS), où l'utilisateur a accès à un ensemble d'outils et de services mis en place par le fournisseur afin de déployer des applications dans un environnement contrôlé.
- *Software-as-a-service* (SaaS), où l'utilisateur accède directement au service désiré hébergé par le fournisseur, via une simple interface, comme un navigateur web par exemple.

Les services de *cloud* se distinguent également par leurs modèles de déploiement. Alors que l'utilisation d'un *cloud* privé est souvent réservée uniquement aux membres de l'organisation qui le déploie, pour un usage interne, les *cloud* publics sont accessibles, gratuitement ou non, à n'importe quel utilisateur tandis que les *clouds* hybrides combinent des infrastructures de *cloud* publics et de *cloud* privés, dans un écosystème commun et souvent interopérable.

Si le *cloud computing* au sens actuel est devenu une tendance vraiment visible avec le lancement en 2006 *d'Amazon Web Services* (AWS),[2] la filiale *cloud* de la plateforme de commerce en ligne, les données précises quant à la croissance de ce marché divergent selon les sources et les méthodes de calcul. Dès 2009, Gartner estimait que les revenus liés au *cloud* public dépassaient les 56,3 milliards de dollars, pour 257,9 milliards en 2020 (41,6% de croissance annuelle en moyenne), pour les services de *cloud* uniquement, tandis que *Forrester Research* estime l'évolution du même marché de 6 à 300 milliards de dollars, entre 2008 et 2019. AWS continue de dominer cet immense secteur technologique avec un tiers du marché, aux côtés de concurrents américains tels que Microsoft, Google et IBM, mais également d'autres entreprises qui gagnent du terrain, notamment le chinois Alibaba.

Cette croissance est soutenue par l'évolution de nos usages numériques, le recours au *cloud* s'étant rapidement installé dans nos habitudes technologiques. Dès 2008, près de deux internautes sur trois avaient déjà eu recours au *cloud* (Horrigan, 2008).[3] Aujourd'hui, les services *cloud* sont tellement omniprésents qu'ils sont totalement intégrés à notre quotidien : services email en ligne, suites bureautiques collaboratives, stockage de photos haute-

[2] Même si une première version de la plateforme, alors loin de son modèle actuel, existait dès 2002.
[3] Selon une enquête publiée par le Pew Internet Project (Pew Resarch Center) en septembre 2008.

résolution, intelligences artificielles capables d'exécuter des commandes vocales ou accès instantané à des catalogues de contenus vidéo ou audio inimaginables jusqu'alors… Ces usages dépassent largement le champ individuel puisque de nombreuses entreprises, organisations et institutions reposent partiellement ou entièrement sur l'utilisation du *cloud*.

En ce sens, l'évolution de nos usages est à l'origine de la croissance des acteurs du *cloud computing*, tout autant que leur croissance a contribué, en retour, à l'évolution de nos usages : selon les rapports publiés par le cabinet d'études IDC depuis 2012, le volume de données stockées dans le monde a été multiplié plus de 40 fois, passant, entre 2006 et 2020, de 0,16 zettabytes (10^{21} bytes) à 6,8 ZB.[4]

1.2. Les principes fondamentaux de la souveraineté numérique appliquée au *cloud*

Si les avantages du recours au *cloud* sont évidents et expliquent l'ubiquité de ce modèle dans nos sociétés connectées, ils se réalisent au prix d'une centralisation accrue des données et à une perte de souveraineté sur celles-ci (de Filippi, McCarthy, 2012). D'une part, le transfert de nos données sur des serveurs hors du contrôle de l'utilisateur posent des problèmes de sécurité, de respect de la confidentialité mais soulève aussi la question des garanties offertes par le régime juridique applicable, *a fortiori* lorsque ces serveurs se trouvent à l'étranger ou bien sont la propriété d'une entreprise soumise à un régime juridique étranger. D'autre part, l'accès à des services externalisés parfois essentiels implique une forme de dépendance de l'utilisateur envers le fournisseur de service.

Considérant les risques techniques, les enjeux de sécurité et les problèmes juridiques, notamment en lien avec l'extraterritorialité du droit américain, l'adoption rapide du *cloud*, y compris dans les institutions publiques, a rapidement posé de multiples problèmes souvent rattachés à la question de la souveraineté numérique (Bômont, 2018).

Au regard de ces considérations se dessinent les trois dimensions fondamentales de la souveraineté numérique pour un État : le droit, la sécurité et l'économie.

- Le respect des droits des utilisateurs

Cette dimension s'incarne de deux manières. Elle implique logiquement que la localisation des données soit clairement identifiée et que, quel que soit le régime juridique applicable dans les lieux par lesquels les données et ressources de l'utilisateur transitent et dans lesquels elles sont stockées, les droits des utilisateurs sont respectés, notamment ceux qui leur sont garantis par la loi qui leur est applicable. Pour les utilisateurs européens, un service de *cloud* souverain devrait donc impérativement respecter les dispositions du Règlement

[4] D'après les données du « Global DataSphere program » mené par International Data Corporation.

Général sur la Protection des Données (RGPD),[5] ainsi que les éventuelles dispositions de droit national qui offriraient des protections supplémentaires. En cas d'incident ou d'infraction, l'utilisateur devrait également être en mesure de pouvoir saisir les tribunaux de l'Etat dans lequel il est établi.

D'autre part, l'utilisateur d'un service de *cloud* souverain ne devrait pas être soumis à l'extraterritorialité d'un régime juridique contrevenant aux protections prévues par le cadre juridique auquel il est initialement soumis. Cette dimension est cruciale pour le *cloud*, puisque la plupart des entreprises dominant le marché sont établies aux États-Unis et que plusieurs textes de lois fondent l'extraterritorialité du droit américain, notamment en matière de surveillance des données numériques. En effet, le Foreign Intelligence Surveillance Act (FISA) de 1978, autorise des procédures de surveillance électronique et de collecte de données initiées par les autorités exécutives, avec un mandat judiciaire dans le cadre d'opérations de contre-espionnage, y compris impliquant des citoyens ou résidents américains, et sans mandat judiciaire pour des besoins de renseignement à l'international, si les communications n'impliquent pas de citoyens ou de résidents américains, ni d'entités ou d'individus rattachés directement à un gouvernement étranger.

Avec les protections prévues par l'Electronic Communications Privacy Act (ECPA) et le Stored Communications Act (SCA) de 1986, le FISA constitue le cadre réglementaire concernant l'accès par les autorités américaines à des flux de communication et à des données stockées sur support électronique, notamment en matière d'opération de renseignement et de lutte contre la criminalité. Ce cadre a été considérablement amendé par le USA PATRIOT Act de 2001, dans un contexte post 11 septembre, pour permettre la collecte de données en cas de suspicion d'activité terroriste, puis, entre autres, par le Protect America Act de 2007 et le FISA Amendments Act (FAA) en 2008, qui ont étendu les possibilités d'opération de surveillance sans mandat concernant des entités en dehors du territoire américain.[6] Même si les révélations d'Edward Snowden, en 2013, ont prouvé la collaboration de certaines grandes entreprises du numérique avec l'État américain pour collecter massivement des données, sans prévenir les utilisateurs concernés, américains ou étrangers, dans des systèmes de collecte de données et surveillance de masse dépassant parfois le cadre légal prévu par le FISA et ses multiples amendements, le FISA a été réautorisé en 2017, bien que légèrement atténué par de nouveaux amendements replaçant certaines procédures sous le contrôle judiciaire.

Cet arsenal légal américain s'est encore vu renforcé par l'adoption du CLOUD Act,[7] en mars 2018. Modifiant le suranné SCA de 1986, il permet à la justice américaine d'exiger de toute entreprise établie sur le territoire américain et ses filiales (mêmes étrangères) fournissant

[5] General Data Protection Regulation 2016/679 (EU)
[6] Pour une revue plus en détail de l'extraterritorialité du droit américain antérieure au CLOUD Act et de ses conséquences pour les utilisateurs de *cloud*, voir l'article *Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad*, de Van Hoboken, Joris V. J., Arnbak, Axel and Van Eijk, Nico, Privacy Law Scholars Conference 2013
[7] Clarifying Lawful Overseas Use of Data Act 2018 (USA)

des services de communication électronique ou des services numériques à distance, la transmission des données de n'importe quel utilisateur, qu'importe qu'elles soient localisées, traitées ou qu'elles aient transité par les États-Unis ou qu'elles aient été toujours stockées dans des serveurs à l'étranger, sur la base d'un simple mandat émis par la justice. Le CLOUD Act permet aux entreprises de contester l'accès demandé si elles estiment qu'une telle procédure enfreindrait les lois de protection des données étrangères régissant l'individu ciblé, mais cette contestation peut être rejetée par un tribunal américain sans que l'individu ciblé ne soit jamais notifié. Enfin, le CLOUD Act permet au gouvernement américain d'établir des *executive agreements*, des accords bilatéraux avec des États étrangers répondant à certains standards de protection juridique et acceptant un ensemble de règles de minimisation de la collection des données, leur permettant ainsi de procéder sans plus de contrôle à des demandes d'accès similaires à celles prévues par le CLOUD Act auprès d'entreprises établies aux États-Unis et à leurs filiales.[8]

À travers l'exemple de l'extraterritorialité du droit américain, il apparait comme évident que ces deux aspects de la souveraineté d'un point de vue juridique, le respect des protections légales applicables à l'utilisateur, d'une part, et le non-accès des données par des tiers, y compris par des États, d'autre part, ne peuvent être résumés qu'à des enjeux de localisation des données, personnelles ou non, même si celles-ci sont traitées et stockées de manière intégrale et permanente dans la juridiction d'origine de leur propriétaire (Millard, 2015).[9] Un service de *cloud* souverain pourrait très bien avoir des infrastructures dans plusieurs juridictions tant qu'il n'expose ses utilisateurs qu'à des régimes juridiques offrant des garanties et des protections équivalentes ou supérieures à celle dont il bénéficie dans sa juridiction d'origine. Par exemple, l'article 45 du RGPD prévoit des « *adequacy decisions* », la Commission Européenne pouvant déterminer au cas par cas si un autre pays offre un niveau de protection des données similaire à celui en vigueur dans l'Union Européenne et autoriser, le cas échéant, des transferts de données internationaux sans autorisation spécifique.[10]

Il est d'ailleurs nécessaire de relever qu'une telle équivalence entre le régime juridique européen régissant la protection des données et celui des États-Unis n'existe pas, comme le souligne la Cour de Justice de l'Union Européenne (CJUE), dans son arrêt du 16 juillet 2020 invalidant le « Privacy Shield »,[11] l'accord de transfert de données entre les membres de l'Espace Économique Européen et les États-Unis (ce qui n'exclut pas toutefois les transferts relevant de clauses contractuelles standards).

[8] Pour l'instant, seul l'executive agreement liant les États-Unis et le Royaume-Uni est entré en vigueur, le 8 juillet 2020, après son adoption en octobre 2019.
[9] Comme le souligne Millard, la localisation des données est souvent invoquée par la sphère politique pour un ensemble de raisons, parfois peu pertinentes, qui ne se limitent pas à la protection des données.
[10] Les pays reconnus comme fournissant une protection équivalente par l'Union Européenne sont, pour le moment, Andorre, l'Argentine, le Canada, les Iles Féroé, Guernesey, Israël, l'Ile de Man, le Japon, la Nouvelle Zélande, la Suisse et l'Uruguay.
[11] *Data Protection Commissioner contre Facebook Ireland Ltd et Schrems (Schrems II)*, *2020* (CJUE), Aff. C-311/18

- La sécurité du service

La notion de souveraineté numérique implique la capacité de l'utilisateur à accéder de manière sécurisée au *cloud*. Cet impératif de sécurité s'applique évidemment à tous les services *cloud*, tous les fournisseurs affirmant garantir la sécurité, la confidentialité et l'intégrité des données utilisateur (non-accès par des tiers, non-utilisation…) ainsi que la résilience du service, dont l'accès est garanti et les contremesures en cas de panne ou d'attaque sont prévues par les plans de continuité d'activité (PCA).

Toutefois, dans le cadre de services essentiels ou qui requièrent la création, la transmission ou le stockage de données sensibles, c'est-à-dire lorsque l'utilisation du *cloud* est importante voire indispensable à l'utilisateur, privé ou public, et résulte en une situation de dépendance, le recours à un *cloud* souverain doit offrir un niveau de sécurité élevé voire maximal. Pour répondre à ces besoins de « souveraineté » aux sens technique et stratégique, un *cloud* souverain devrait donc satisfaire des impératifs de sécurité supérieurs à ceux des solutions commerciales conventionnelles. Les conséquences d'une éventuelle défaillance peuvent être si fortes qu'elles peuvent rendre la délégation complète de la sécurité du système inenvisageable, menant alors à l'internalisation partielle (recours à un prestataire mais déploiement des infrastructures « *on-premise* », chez le client) ou complète (déploiement d'une solution entièrement indépendante, en interne) d'un tel service.

C'est le cas, par exemple, de certains systèmes informatiques de l'État impliquant des données sensibles ou des fonctions stratégiques, identifiés par la doctrine d'utilisation de l'informatique en nuage par l'État de 2018 comme services de *cloud* interne ou de « cercle 1 »,[12] ce qui inclut notamment certains services du ministère de l'Intérieur et du ministère des Finances (respectivement les *clouds* Pi et NUBO)[13] ainsi que celui du Ministère des Armées français.[14] Au-delà de l'État, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) maintient une liste des Opérateurs de Services Essentiels (OSE) et des Opérateurs d'Importance Vitales (OIV), dont les Systèmes d'Information Essentiels (SIE) et les Systèmes d'Information d'Importance Vitales (SIIV) font l'objet d'audits et de règles de sécurité spécifiques puisque le moindre incident impliquant ces systèmes aurait « un effet disruptif important » sur les « activités sociétales ou économiques critiques » qu'ils soutiennent. Dans de telles circonstances, les solutions de *cloud* souverain doivent garantir

[12] Circulaire du 8 novembre 2018 relative à la doctrine d'utilisation de l'informatique en nuage par l'État dont nous reparlons plus bas.
[13] Pour plus de détails sur les infrastructures de *cloud* interne existantes, voir la page dédiée sur le site de la Direction Interministérielle du Numérique (DINUM).
[14] Pour le *cloud* du Ministère des Armées et ses enjeux spécifiques, voir l'interview de Clotilde Bômont pour la Chaire Digital, Gouvernance et Souveraineté dédiée à ce sujet.

la sauvegarde d'une forme d'indépendance pour leurs utilisateurs qui conservent les moyens de contrôle et de sécurisation des données et des services concernés, puisqu'ils restent responsables du maintien des activités reposant sur le *cloud*.

C'est donc dans cette dimension que s'incarne le potentiel caractère stratégique et géopolitique du *cloud* souverain, en tant qu'infrastructure numérique-clé pouvant supporter les services essentiels au bon fonctionnement d'un État et de son économie, qui ne peuvent pas être compromis sans conséquences graves, qu'ils soient liés à la défense, la gestion de données de santé ou celle des réseaux de transport ou d'énergie, entre autres. Outre les risques de défaillance, ces services essentiels représentent des cibles privilégiées pour des groupes cybercriminels qui n'hésitent pas à compromettre leur sécurité en infiltrant les outils *cloud* qu'ils emploient pour leur bon fonctionnement. L'exemple du hack de SolarWinds, révélé en décembre 2020, qui a touché les 33 000 clients publics et privés de leur logiciel Orion, dont plusieurs Départements du gouvernement américain ainsi que des réseaux de la National Nuclear Security Administration, est symptomatique à cet égard puisque les analystes de Microsoft estiment que le but des *hackers* était bien « d'accéder à des ressources en *cloud* et de réaliser des actions permettant d'exfiltrer des emails et de persister dans le *cloud*. »[15] Les retombées de cette cyberattaque, « la plus importante et la plus sophistiquée à ce jour » selon Brad Smith, président de Microsoft, sont difficiles à établir et resteront probablement pour partie classifiées, mais leur ampleur justifie une révision profonde de la stratégie technologique de l'État américain, notamment en matière de cloud, selon le Atlantic Council.[16]

De plus, les risques d'intelligence économique encourus par les entreprises nationales, notamment dans les secteurs innovants où la concurrence technologique et commerciale avec des acteurs étrangers est très forte, peuvent également justifier le recours à des offres de *cloud* souverain pour minimiser le risque de fuites de données représentant un avantage compétitif déterminant. Si ces risques sont réels pour certaines entreprises, la controverse autour de l'attribution par la Bpifrance de l'hébergement des attestations des Prêts Garantis par l'État, qui contiennent des informations critiques sur la santé de nombreuses entreprises françaises touchées par la crise du Covid, à Amazon Web Services souligne que ces enjeux de souveraineté peuvent s'étendre bien au-delà des entreprises prises individuellement et revêtir une dimension systémique.[17]

A cet égard, la souveraineté numérique aurait pour objectif de minimiser les risques d'attaques, de fuites de données mais aussi d'ingérence concernant ces services stratégiques reposant sur le *cloud*. Il existe cependant une tension entre cet impératif d'indépendance et la capacité à égaler les niveaux de ressources (matérielles, humaines, R&D), de redondance et de sécurité qu'offrent les entreprises dominant le secteur. Un *cloud*

[15] Voir l'article "Using Microsoft 365 Defender to protect against Solorigate" publié par la Microsoft 365 Defender Team, le 28 décembre 2020
[16] Voir le rapport "Broken trust: Lessons from Sunburst" publié par le Atlantic Council, le 29 avril 2021
[17] Voir l'article « Les partenariats entre Bpifrance et Amazon montrés du doigt » de Alexandre Picquard, *Le Monde*, 5 février 2021

indépendant, national mais insuffisamment sécurisé pourrait représenter un point de défaillance unique (*single point of failure*) posant un risque crucial pour la souveraineté d'un État et la santé de son économie.

- Le développement économique et industriel

La souveraineté numérique répond aussi à des enjeux économiques. L'ampleur du marché du *cloud* est considérable et les projets de *cloud* souverain soutiennent l'essor d'entreprises nationales afin, au minimum, de générer de l'activité économique en répondant à une partie de la demande sur le territoire, notamment la demande publique (sans quoi les institutions pouvant se voir forcées d'adapter leurs cahiers des charges en fonction de l'offre d'acteurs majeurs du marché venus de l'étranger), au mieux, de donner naissance à une entreprise potentiellement leader de son domaine, capable de capter de la valeur à l'international.

Cette dimension ne se limite toutefois pas à « prendre sa part du gâteau » mais aussi à mettre en place une politique vertueuse favorisant, par la commande ou l'investissement public dans le *cloud* souverain, le développement de capacités matérielles, logicielles et humaines à l'échelle nationale, ou régionale, dans le cas de l'Union Européenne notamment (Sarah Guillou, 2020). L'action publique peut également être le catalyseur de l'innovation dans des secteurs émergents, l'État endossant les risques liés à des investissements à fort potentiel que les entreprises sont réticentes à effectuer elles-mêmes (Mazzucato, 2013). En rendant l'écosystème plus compétitif, cette stimulation permet de réduire la dépendance envers des acteurs économiques extérieurs mais peut également entrer en tension avec le droit de la concurrence lorsqu'elle se traduit par des politiques relevant du protectionnisme ou du nationalisme économique.

Cet enjeu de développement économique, au cœur du projet de *cloud* souverain depuis ses débuts, est toujours capital en Europe : alors que le marché du *cloud* aurait triplé entre 2017 et 2020 pour atteindre 5,9 milliards d'euros, la part des fournisseurs européens a chuté de 26% à 16%, phagocytée par Amazon, Google et Microsoft représentant à eux trois les deux tiers du marché continental.[18]

Chacune de ces dimensions s'applique au cas du *cloud* souverain mais il est important de noter qu'elles sont complémentaires, cumulatives et interdépendantes, mais souvent inégalement appréhendées par les décideurs publics, que ce soit dans les discours ou dans les politiques mises en œuvre.

[18] Selon les données du Synergy Research Group, publiées le 14 janvier 2021.

1.3. Le projet de *cloud* souverain en France

En effet, en France, le projet de *cloud* souverain s'est en premier lieu incarné dans sa dimension économique et industrielle (Bômont, Cattaruzza, 2020). Dès janvier 2010, dans un discours sur le haut débit et de l'économie numérique, François Fillon, Premier Ministre, affirmait déjà que : « […] les Nord-Américains dominent ce marché, qui constitue pourtant un enjeu absolument majeur pour la compétitivité de nos économies, pour le développement durable et même, j'ose le dire, pour la souveraineté de nos pays. »

C'est avec cette prise de parole constatant la croissance rapide d'un marché émergent que commence le projet du *cloud* souverain en France, dont l'historique est dressé en détail dans un article disponible sur le site de la Chaire Digital, Gouvernance et Souveraineté. Seules les étapes marquantes sont reprises ici.

Après plusieurs mois de consultations et de discussions entre Orange, Thales et Dassault Systèmes, l'État met en chantier un partenariat public-privé dénommé « Projet Andromède », dont le financement doit être assuré par la 1ère vague des Programmes d'Investissement Avenir (PIA), à hauteur de 135 millions d'euros. Les divergences entre Orange et Dassault Systèmes viennent perturber la feuille de route du projet et ce sont donc deux « startups » qui sont annoncées en septembre 2012, financées chacune par des participations de 75 millions euros provenant du Fonds national de Sécurité Numérique, administré par la Caisse des Dépôts et des Consignations (CDC).

Fleur Pellerin, en tant que ministre déléguée à l'Economie numérique, présente donc Cloudwatt, portée par Orange et Thales, aux côtés de Numergy, résultat du rapprochement entre Bull et SFR, Dassault Systèmes ayant quitté cette nouvelle alliance face à la décision de financer deux projets simultanément. Elle souligne la concurrence entre ces deux « jeunes pousses » perchées sur les épaules de grands comptes comme un atout : « Le gouvernement a décidé de soutenir deux projets « cloud » de taille critique face à la concurrence nord-américaine. La volonté de l'État est de privilégier l'effet de levier plutôt que la concentration des efforts sur un seul projet. L'émulation ne peut apporter que des bénéfices. »

L'aventure ne fait pas long feu. Alors que le gouvernement suivant réaffirme son intérêt pour le *cloud* souverain l'année suivante, en l'incluant dans les « 34 plans de la Nouvelle France Industrielle » du Ministère de l'Économie, du Redressement productif et du Numérique, un premier changement d'orientation politique et stratégique s'opère. La valorisation de l'écosystème existant prend le dessus sur l'ambition du précédent gouvernement de biberonner un nouveau géant du numérique. Une nouvelle feuille de route est élaborée en juin 2014, associant cette fois Octave Klaba, directeur général d'OVH, et Thierry Breton, à l'époque PDG d'Atos (ex-Bull), alors que Cloudwatt et Numergy annoncent de premiers résultats très en-deçà des attentes. Andromède devait engranger près de 600 millions d'euro en 2015. En 2014, Numergy fait 100 fois moins tandis que Cloudwatt n'atteint pas les 2

millions de chiffre d'affaires, année durant laquelle celui d'AWS avoisinait les 4,6 milliards de dollars.[19]

L'État profite du rachat de toutes les parts des deux entreprises par Orange et SFR pour tourner la page en 2015. Même avec deux propriétaires uniques, ni Cloudwatt ni Numergy ne parviennent à trouver leur place sur le marché français, encore moins à l'étranger. Leurs maisons-mères mettent fin à leurs activités respectives en mars 2018 pour Numergy et en juillet 2019 pour Cloudwatt.

Entre temps, l'État aura tout de même étoffé ses politiques en faveur du *cloud* souverain. Le label franco-allemand pour les « *cloud* de confiance », fruit de la collaboration entre l'ANSSI et de la Bundesamt für Sicherheit in der Informationstechnikle (BSI), voit le jour en décembre 2016. Alors que la note d'information relative à l'informatique en nuage du 5 avril 2016[20] rappelait aux entités publiques que tout recours au *cloud* où les données ne seraient pas stockées et traitées en France était *de facto* illégal, la diffusion, le 8 novembre 2018, de la Circulaire du Cabinet du Premier Ministre relative à la doctrine d'utilisation de l'informatique en nuage par l'État établit enfin une doctrine générale quant à l'usage du *cloud* par les institutions publiques. Toujours ancrée dans la coopération franco-allemande, c'est désormais à l'échelle européenne que se joue l'avenir du *cloud* souverain.

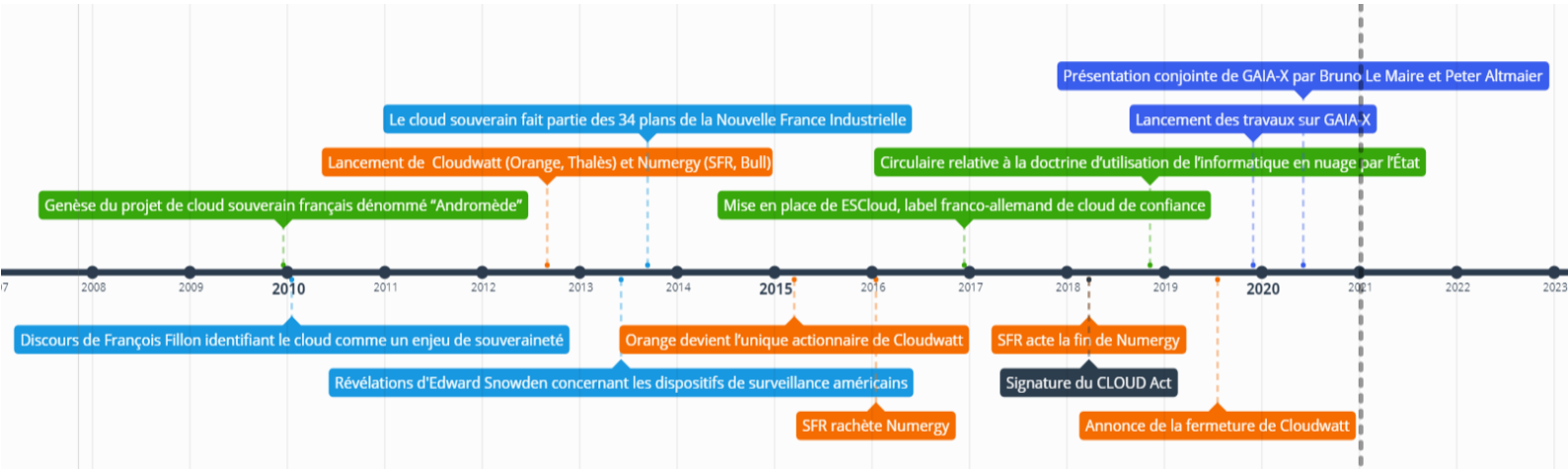

Figure 1 : Chronologie des projets de cloud souverain en France

[19] Sur ce sujet, l'article « Le cloud à la française, histoire d'un flop ? » de Delphine Cuny, paru dans *La Tribune* le 13 janvier 2015, présente un bon état des lieux des déconvenues des deux entreprises.
[20] Note d'information DGP/SIAF/2016/006 du 5 avril 2016 relative à l'informatique en nuage (*cloud computing*)

2. Les enseignements d'un échec : analyse systémique d'une politique d'innovation sous-dimensionnée et incohérente

Alors que les fins prématurées de Cloudwatt et de Numergy ont été largement commentées dans la presse, les limites du projet de *cloud* souverain porté par l'État français n'ont que rarement été analysées. Avant de se pencher sur les nouvelles initiatives au niveau européen, il est donc important de tirer les enseignements de l'échec de la stratégie industrielle envisagée et son application, le cloisonnement entre l'État et l'écosystème et le manque de coordination général entre les différentes politiques mises en œuvre.

2.1. Une stratégie industrielle incohérente

En focalisant son discours sur la dimension économique du *cloud* souverain, le gouvernement français a clairement affiché son ambition de donner naissance à un nouveau champion *ex nihilo*. Cet objectif, qualifié de « déraisonnable » par le rapport du Sénat intitulé « Le devoir de souveraineté numérique », déposé le 1er octobre 2019, révèle un manque de compréhension à la fois du marché du *cloud* mais également vis-à-vis de son modèle d'affaires.[21]

L'investissement initial de l'État était fondamentalement sous-dimensionné pour espérer concurrencer, même sur le seul marché français, les géants du numérique. L'État comptait sur les synergies avec les entreprises fondatrices de Cloudwatt et Numergy afin de réduire les coûts initiaux liés à leurs activités, tout particulièrement les *data centers* existants de Orange et de SFR. Les 150 millions d'euros promis au projet Andromède ne supportent néanmoins pas la comparaison avec les budgets des leaders du secteur, Amazon, Google, Microsoft, Oracle et IBM investissant tous, en 2013, entre 1 et 3 milliards de dollars en recherche et développement… par trimestre ![22]

Vouloir bâtir un géant du *cloud* est suffisamment difficile, diviser l'investissement initial, déjà maigre, entre deux entreprises se faisant concurrence a d'autant plus réduit les chances de succès du projet. Non seulement aucune d'entre elles ne pouvaient prétendre atteindre la « taille critique pour faire face à la concurrence, » mais ce dédoublement de l'investissement

[21] Rapport de M. Gérard Longuet au nom de la commission d'enquête sur la souveraineté numérique du Sénat, déposé le 1er octobre 2019
[22] Selon l'analyse de Rachel Stephens pour l'entreprise d'analyse Redmonk, en 2017, même si ces chiffres correspondent aux budgets de R&D totaux de ces entreprises, la spécialisation de Cloudwatt et Numergy ne pouvait pas suffire à rattraper l'avance compétitive de ses concurrents.

signifiait aussi que les parts de marché individuelles seraient proportionnellement restreintes, le marché pour des solutions de *cloud* souverain en France étant limité et immature.

Si la décision du gouvernement de mettre en concurrence Cloudwatt et Numergy aurait pu être vertueuse en termes d'innovation technologique et de placement commercial, au moins pour les clients, elle hypothéquait également les opportunités de réaliser des économies d'échelles conséquentes, qui sont au cœur du modèle d'affaires des leaders du marché, chaque entreprise devant développer ses propres technologies, exploiter ses propres *data centers* et autres infrastructures matérielles. S'inscrivant dans la tradition libriste française,[23] Cloudwatt et Numergy ont, par ailleurs, toutes les deux opté pour construire séparément leurs services sur OpenStack, dédiant une partie de leurs ressources à des contributions sur cette plateforme libre. Le choix de développer des outils fondés sur des technologies *open source* a probablement permis, à court terme, de bénéficier des travaux d'une communauté riche et active afin de lancer rapidement la conception de premiers services propriétaires, accessibles via des interfaces de programmation disponibles librement, mais a peut-être aussi participé à cette incapacité à construire un avantage compétitif substantiel sur le long terme.

2.2. Le cloisonnement entre l'État et l'écosystème

Outre la méconnaissance des décideurs publics vis-à-vis du marché du *cloud*, l'échec de la stratégie industrielle française s'explique également par le fort cloisonnement entre l'État et l'écosystème du *cloud* en France. En voulant s'appuyer sur des grands comptes habitués à traiter avec les institutions publiques, le Commissariat Général à l'Investissement (CGI) a fait passer les impératifs politiques devant les considérations économiques et surtout techniques. Les conflits entre les initiateurs du projet Andromède ont entraîné une genèse chaotique avec la création de deux consortia de fortune recomposés autour d'entreprises alliant expertise dans les télécoms et dans le secteur informatique, que le CGI n'a pas voulu départager.

Ce faisant, l'État a ignoré les entreprises innovantes déjà présentes dans le secteur du *cloud* en France, notamment Ikoula, Gandi et surtout OVH, déjà acteur majeur du marché français et européen en 2011 avec plus de 100 000 serveurs, qui s'apprêtait alors à lancer ses activités en Amérique du Nord. Alors que Cloudwatt et Numergy ne décollaient toujours pas en 2015, OVH devenait la première startup française à dépasser le milliard de dollar de valorisation, offrant à la France sa première « licorne », avant d'intégrer en 2019 le top 10 mondial des fournisseurs de *cloud* d'infrastructure (IaaS), avec 1% du marché global. En décidant de ne pas associer ces spécialistes bien implantés sur le marché, les initiateurs du projet Andromède se sont privés d'un vivier de talents foisonnant. Pire encore, en orientant

[23] L'ouvrage collectif *Histoires et cultures du Libre*, Sous la direction de Camille Paloque-Berges et Christophe Masutti, dresse un très beau panorama de la communauté du Libre en France.

les financements publics vers Cloudwatt et Numergy, l'État s'est mis à dos l'écosystème d'innovation français, voyant dans ce soutien public à deux nouveaux-venus portés par des entreprises déjà massives une forme de « concurrence déloyale », tout du moins jusqu'à ce que les espoirs de les voir se transformer en mastodontes écrasant les pionniers ne disparaissent.[24]

Prenant acte de cette erreur critique, le gouvernement décide donc de confier aux dirigeants d'OVH et d'Atos l'élaboration de la nouvelle feuille de route pour le *cloud computing* accompagnant les 34 Plans de la Nouvelle France Industrielle, invitant la plupart des acteurs de l'écosystème à la table de travail (Cegid, Talentsoft, Prestashop, CozyCloud, JoliCloud, Orange, Bull, Numergy, Cloudwatt et INRIA), dont les dix propositions soulignent les errances stratégiques, mais aussi l'incohérence de l'action publique concernant le *cloud* souverain.

2.3. Le manque de coordination dans l'action publique

Ce n'est effectivement pas un hasard si les trois premières mesures concernent la mise en place d'une labélisation et la stimulation de la commande publique, quitte à privilégier les solutions françaises dans les marchés publics. Les offres de *cloud* souverain ont du mal à se frayer un chemin dans un marché encore peu structuré, même en 2014. L'absence de prise en considération des dimensions d'ordre juridique et de sécurité du *cloud* souverain dans la stratégie de l'État français a même contribué à un positionnement commercial incohérent de Cloudwatt et de Numergy, en dépit de la présence de l'État, via la CDC, à leur capital.

Sans directive pour encadrer la commande publique, identifier des cas d'usage et orienter l'offre censée leur répondre, les institutions publiques n'ont que peu de raisons de se tourner vers Cloudwatt ou Numergy, tandis que celles-ci développent des solutions orientées vers le grand public, comme par exemple la « Cloudwatt Box », un espace de stockage en *cloud* souverain (car localisé en France) à destination des entreprises et même des particuliers, la solution étant relayée par Orange et faisant l'objet d'une large campagne marketing. Ce n'est que 2 ans après sa création que Cloudwatt « pivote » vers une offre IaaS plus complète.

Du côté de l'État, les marchés publics ne sont pas soumis à une politique homogène et les quelques entités prêtes à se lancer dans le déploiement de solutions innovantes ne peuvent principalement s'appuyer que sur les quelques clauses du cahier des clauses administratives générales – Techniques de l'Information et de la communication (CCAG-TIC). Ce texte de référence pour la formulation des marchés et la rédaction des contrats, adopté en septembre 2009 et qui ne sera que mis à jour douze ans plus tard, est évidemment très lacunaire en termes de clauses de protection des données personnelles et de cybersécurité, laissant les

[24] L'article « Cloud souverain : deux ans après, on fait le point » signé par la rédaction de NextImpact, le 25 septembre 2014, propose une remarquable analyse détaillée des tensions générées au sein de l'écosystème, et sur l'échec de Cloudwatt et Numergy en général.

acteurs publics quelque peu livrés à eux-mêmes. Il faut attendre décembre 2016 pour que l'ANSSI réponde aux vœux des entreprises derrière le « Plan Cloud », joignant ses forces avec son équivalent allemand pour lancer le label ESCloud et donner enfin une meilleure visibilité aux « *cloud* de confiance » certifiés en France, au sein du référentiel « SecNumCloud », et en Allemagne (BSI C5). Chaque entreprise labélisée doit obéir à « quinze règles techniques et organisationnelles qui visent à garantir le sérieux des initiatives nationales partenaires, le niveau de sécurité des solutions labélisées ainsi que le traitement et le stockage des données sur le territoire européen. »[25] Seule Outscale, la filiale *cloud* fondée par Dassaut Systèmes après avoir tourné le dos au projet Andromède, a reçu la qualification SecNumCloud pour ses offres en de cloud d'infrastructure, en décembre 2019, rejointe par OVH, le 24 décembre 2020.[26]

Si la note d'information relative à l'informatique en nuage du 5 avril 2016 limitait le champ des prestataires potentiels pour l'administration, elle a surtout refroidi les velléités d'adoption de services *cloud* en son sein.[27] Il a fallu encore attendre la Circulaire du 8 novembre 2018 relative à la doctrine d'utilisation de l'informatique en nuage par l'État pour structurer la commande publique en matière de *cloud*, identifiant cette fois les enjeux économiques, juridiques et plus particulièrement les enjeux stratégiques et de sécurité. Cette obligation dessine une organisation en trois « cercles » concentriques :

- Le « *cloud* interne », développé au sein de l'État sur une base OpenStack[28] et qui a pour vocation « d'accueillir des données, des traitements et des applications sensibles, et de répondre à des besoins régaliens d'infrastructures numériques répondant aux exigences d'internalisation des données et de sécurité des systèmes d'information » ;

- Le « *cloud* dédié », reposant sur une offre standard du marché adaptée pour les besoins de l'État et hébergée sur des infrastructures dédiées afin de garantir la pérennité d'accès aux données et solutions accueillies ;

- Le « *cloud* externe », correspondant aux offres « sur l'étagère » disponibles au grand public, garantissant un niveau minimum de sécurité, pour les usages peu sensibles.

Cette « stratégie hybride pour le *cloud computing* de l'État », qui s'applique également aux collectivités territoriales, fait cependant l'objet d'une gouvernance complexe, puisqu'elle est pilotée par le secrétariat d'État chargé du numérique, avec le support de la Direction Interministérielle du Numérique et du Système d'Information et de Communication (DINSIC,

[25] D'après le communiqué de presse de l'ANSSI
[26] Par souci d'exhaustivité, ajoutons que les solutions SaaS de Oodrive ont été les premières qualifiées SecNumCloud par l'ANSSI (la liste est accessible publiquement sur le site de l'Agence).
[27] La note d'information invite à « prévoir des clauses liées à la localisation, la sécurité, la confidentialité, la traçabilité, l'auditabilité, la portabilité et l'élimination des données du système », des critères pertinents mais impraticables alors que le label de l'ANSSI n'existait toujours pas et que les objectifs précis à établir dans les contrats étaient laissés à l'initiative des porteurs de projet.
[28] De ce fait, Cloudwatt et Numergy auront indirectement contribué à ces solutions de *cloud* interne.

devenue depuis la Dinum, direction interministérielle du numérique) et avec l'appui de l'ANSSI, les *cloud* interne et dédié devant être conformes au référentiel SecNumCloud. Elle pose également la question de la capacité de l'État à acquérir les compétences requises au développement des solutions ultra-sécurisées s'inscrivant dans le cercle du « *cloud* interne », les talents humains étant déjà drainés par l'attractivité des entreprises du secteur.

Toutefois, cette organisation de la demande publique, enfin coordonnée à la stratégie industrielle et aux politiques d'investissement initiées presque dix ans plus tôt, n'arrive que bien trop tard. Cloudwatt et Numergy avaient besoin de s'appuyer sur ces opportunités économiques dès leur lancement, afin de pouvoir entretenir un chiffre d'affaires conséquent dès leurs débuts, de se structurer autour de plusieurs commandes avec des attentes définies et d'envoyer un signal fort à tout le marché français et même européen. En laissant l'élan impulsé par les investissements publics s'essouffler avant d'établir une doctrine claire régissant l'utilisation du *cloud* dans le secteur public, l'État s'est privé de l'effet de levier que la demande publique aurait pu avoir sur le développement de ces deux entreprises et de l'écosystème français en général.

Du reste, même si les contours des besoins de l'État en matière de *cloud* souverain sont plus clairement définis, l'absence d'identification précise des cas d'usage appartenant à chacun des cercles rend l'application de cette doctrine toujours difficile. L'attribution de l'hébergement du Health Data Hub, officiellement opérationnel depuis le 1er décembre 2019, à Microsoft (sur ses serveurs aux Pays-Bas), avant que le gouvernement annonce, le 8 octobre 2020, le rapatriement de la plateforme de stockage de données médicales auprès de partenaires européens, suite à l'avis nuancé de la CNIL,[29] à la décision du Conseil d'État[30] et à l'invalidation de l'accord de transfert de données à caractère personnel « Privacy Shield » entre l'Union Européenne et les États-Unis, est d'ailleurs symptomatique de la persistante incohérence de la stratégie de l'État français en matière de *cloud* souverain.[31]

C'est justement dans un effort de rationalisation qu'est introduite la nouvelle « Stratégie nationale pour le cloud », le lundi 17 mai 2021, lors d'une conférence de presse tenue par Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance, Amélie de Montchalin, ministre de la Transformation et de la Fonction publiques, et Cédric O, secrétaire d'État chargé de la Transition numérique et des Communications électroniques,[32] puis, dans sa circulaire n°6282 parue le 5 juillet 2021, la doctrine d'utilisation de l'informatique en nuage

[29] Mémoire en observations *Conseil National du Logiciel Libre c/ Ministère des Solidarités et de la Santé* du 8 octobre 2020 (CNIL)
[30] Ordonnance *Association le Conseil National du Logiciel Libre et autre*s 13 octobre 2020 (Conseil d'État)
[31] On peut également noter, entre autres, les cas de l'hébergement des données liées aux prêts garantis par l'État (PGE) de la Bpifrance chez Amazon Web Services ou bien le partenariat entre le Ministère des Solidarités et de la Santé et l'entreprise Doctolib (aux côtés de Maiia et Keldoc) pour gérer la plateforme de rendez-vous de vaccination contre le Covid19 de Santé.fr alors que les données de Doctolib sont également hébergées chez AWS.
[32] Outre la conférence de presse, cette stratégie est également présentée dans un dossier de presse.

par l'État, cette fois intitulée « Cloud au centre ».[33] Articulées autour d'un nouveau label, celui de « Cloud de confiance », elles entendent toutes les deux s'appuyer sur le cadre offert par Gaia-X ainsi que l'élan industriel que cette initiative a généré pour accélérer l'adoption du cloud dans le secteur public, entraînant toute l'économie française avec lui, et ainsi « rattraper notre retard », comme l'affirmait le ministre de l'Économie lors de la conférence de presse, même au prix d'un positionnement stratégique qui remet à nouveau en question les ambitions de souveraineté numérique affichées.

3. De Gaia-X à la nouvelle stratégie nationale pour le cloud, l'impulsion d'une dynamique européenne, « pragmatique » et parfois paradoxale

Au niveau européen, une autre stratégie ambitieuse mais fondamentalement différente de celle entreprise en France autour des enjeux de souveraineté numérique s'est développée, avec notamment le projet de *Digital Single Market*, au centre du *Digital Agenda for Europe 2020* de la commission Junker, qui a conduit à l'adoption du RGPD le 27 avril 2016, transformant profondément les relations entre les utilisateurs et les fournisseurs de service *cloud* (Russo et al, 2018). C'est dans cette dynamique que s'inscrivent la *European Strategy for Data*, présentée par la commission von der Leyen, le futur *Data Governance Act* ainsi que l'initiative Gaia-X.

3.1. Un nouveau cadre réglementaire

Au cœur de la *European Strategy for Data*, présentée le 2 février 2020, se trouve le constat d'un marché européen du *cloud* victime de problèmes structurels mieux identifiés. Les grands acteurs étrangers, notamment américains, bénéficient du « *data advantage* », de l'accumulation d'un grand volume de données qui rend leurs clients captifs et leur donne un avantage compétitif pour répondre aux demandes émergentes sur un marché européen en développement (*lock-in effects*). La faible part de marché des acteurs européens pose alors, selon la Commission, un problème de souveraineté à travers la dépendance technique, stratégique et juridique. L'absence d'offre européenne compétitive empêche le marché de croître, que ce soit pour les entreprises (en moyenne, 26,2% des entreprises européennes ont recours à au moins un service *cloud* en 2018, la France est en retard, légèrement en-deçà de 20%) mais aussi de manière encore plus marquée dans le secteur public.[34]

[33] Circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État
[34] D'après « Cloud computing - statistics on the use by enterprises » (Eurostat, 2018)

Afin d'accélérer l'adoption de solution *cloud* européenne, la commission envisage d'investir dans un « projet à forte incidence relatif aux espaces européens des données et aux infrastructures en nuage fédérées. » Ce plan de co-investissement entre la Commission et les États-Membres, prévu pour 2022, serait doté d'un budget compris entre 4 et 6 milliards d'euros destiné à financer des architectures communes à l'espace européen, facilitant l'interopérabilité et la portabilité des données, ainsi que la conformité des services de *cloud* aux réglementations européennes. L'enjeu est donc de « décloisonner » le marché en facilitant la mobilité de la donnée, et donc celle des utilisateurs, entre différents fournisseurs, renforçant l'accès à des acteurs européens de moindre envergure qui ne demandent qu'à grandir.

Cette stratégie est agrémentée de lignes directrices afin de favoriser les bonnes pratiques et la convergence de l'écosystème vers un marché unique de la donnée, incarné par la future *European Alliance on Industrial Data and Cloud* et centré sur les droits des utilisateurs (suivant, pour partie, les principes FAIR data[35]). Outre le projet d'un recueil réglementaire pour l'auto-régulation du secteur, la stratégie prévoit également un nouveau Règlement sur la gouvernance européenne des données (également appelé « *European Data Governance Act* »), dont une première proposition a été présentée le 25 novembre 2020.[36]

Toujours dans le but d'encourager la formation et la croissance d'un espace européen de la donnée, cette proposition est axée sur le cadre entourant la gestion et le partage des données (*data sharing*), y compris dans le secteur public, et ambitionne de générer jusqu'à 11 milliards d'euros annuels en 2028 grâce au partage de données en Europe, réduisant les coûts et améliorant la performance des administrations et à travers plusieurs industries (transport, santé, agriculture, mobilités…).[37] Cette proposition introduit un ensemble de règles régissant la réutilisation de données issues des organismes publics, l'encadrement de l'activité des intermédiaires proposant des services de partage de données et l'enregistrement des organismes pouvant « réutiliser des données à des fins altruistes », c'est-à-dire non-lucratives et au service de l'intérêt général, comme la recherche par exemple.

Ce nouveau cadre renforce les restrictions concernant le transfert, le partage et la réutilisation des données détenues par des organismes du secteur public, tout particulièrement à caractère non-personnel, hors de l'Union Européenne, soumises à des conditions strictes de protection équivalente ou de décision judiciaire. Il est soutenu par un système de notifications et d'enregistrement pour les entreprises de partage de données, *data brokers* étrangers inclus, qui doivent désigner un représentant légal en Europe, articulé autour des autorités compétentes dans les États-membres et du nouvellement créé *European Data Innovation Board*, également chargé de faciliter la coopération des autorités,

[35] Wilkinson *et al.* The FAIR Guiding Principles for scientific data management and stewardship, Sci Data 3, 160018 (2016).
[36] Proposition de Règlement du Parlement Européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), 2020 (Commission Européenne)
[37] Selon l'étude d'impact SMART 2019/0024 commandée par la Commission.

de la commission et des entreprises afin de renforcer la standardisation et l'interopérabilité dans le marché européen de la donnée. Enfin, le projet de loi propose une séparation « structurelle » entre les services de partage de données et ceux ayant trait à leur hébergement, stockage et traitement.[38]

En posant les bases d'un nouveau système de gouvernance applicable au partage de la donnée, en limitant les transferts hors de l'Europe et en séparant les activités de partage et de traitement des données, le *Data Governance Act* est, sans évoquer directement la souveraineté dans son texte, une étape importante pour la stratégie numérique européenne, centrée sur l'interopérabilité et la compétitivité des acteurs européens du *cloud* et de la donnée.

3.2. Gaia-X, une approche ancrée dans l'écosystème

L'approche de Gaia-X partage les principes fondamentaux de la *European strategy for Data*. Cette initiative allemande a pris forme le 29 octobre 2019, sous l'impulsion d'industriels, d'universitaires et du Ministère des Affaires Économiques et de l'Énergie (BMWi), mettant l'écosystème au centre de sa vision.[39] Contrairement à la vision française, centralisée et étatique, Gaia-X s'inspire, dès ses débuts, de l'approche britannique, dont le service « G-Cloud » permet, depuis 2012, aux organismes publics d'accéder à une place de marché rassemblant des offres de service *cloud* provenant de fournisseurs agréés avec lequel l'État a conclu un accord-cadre. Gaia-X entend dès ses débuts aller plus loin, invitant tout l'écosystème à construire une architecture numérique européenne commune pour soutenir le Marché Digital Unique en suivant sept principes fondateurs, dont la souveraineté numérique :

1. Protection des données européennes
2. Ouverture et transparence
3. Authenticité et confiance
4. Souveraineté numérique et auto-détermination
5. Accès libre au marché et création de valeur en Europe
6. Modularité et interopérabilité
7. Facilité d'utilisation

En établissant un ensemble de règles et de standards techniques et juridiques, ancrés dans les bonnes pratiques industrielles et les réglementations européennes, et doté d'un réseau de ressources physiques, de « nœuds » tenus par les participants, Gaia-X a pour mission de donner corps à un écosystème de la donnée et des infrastructures *cloud* interconnectés,

[38] L'article 11, garantit, en effet, la neutralité des prestataires *data sharing*, exigeant la séparation des entités juridiques s'occupant du partage et du traitement de la donnée.
[39] Pour plus d'information sur la stratégie de *cloud* souverain en Allemagne, voir le rapport du BMWi de « The Standardisation Environment for Cloud Computing » (2012)

supportant la mise à disposition de « services fédérés », avec, en tout premier lieu, un catalogue des fournisseurs de service participant à Gaia-X à destination des administrations et du grand public. Ces fournisseurs respectant les principes et standards établis par Gaia-X et partageant des technologies *open source*, n'importe quel client pourra utiliser ce catalogue afin d'accéder à des solutions conformes au droit européen. Plutôt que d'avoir recours à l'un des leaders américains ou chinois, les utilisateurs pourront désormais combiner les offres interopérables de différents fournisseurs européens plus spécialisés et de moindre envergure.

En annonçant avec Peter Altmeier, son homologue allemand, lors d'une conférence de presse commune le 4 juin 2020, que la France se joignait à l'Allemagne pour le lancement officiel de Gaia-X, Bruno le Maire, Ministre de l'Économie, a renoué avec l'historique projet français de *cloud* souverain tout en adoptant un profond revirement de stratégie. Abandonnant définitivement l'objectif de faire émerger un géant français ou même européen, l'État Français soutient désormais une stratégie fondée sur la collaboration et l'auto-régulation de l'écosystème existant, promouvant la diversité d'offres compatibles entre elles et respectant les principes européens en matière de souveraineté numérique.

Cependant, l'approche pragmatique, industrielle et européenne de Gaia-X présente également des limites et des incohérences stratégiques. La gouvernance du projet est complexe. Piloté par une association internationale sans but lucratif de droit belge, fondée le 17 septembre 2020, Gaia-X est passée, entre juin et novembre, de 22 membres fondateurs (11 allemands et 11 français) à 180. La collaboration et l'alignement des intérêts entre des entreprises de taille très variée, certaines étant des PME, d'autres des groupes internationaux, est un véritable défi. Sa croissance rapide et immédiate, bien aidée par le soutien politique franco-allemand, valide l'intérêt de l'écosystème mais promet des débats difficiles pour la mise en œuvre d'une feuille de route déjà complexe, aux objectifs nombreux, pluridisciplinaires et intersectoriels, qui ne sont pas tous aussi clairement identifiés que la mise en place du catalogue de services prévu pour le premier trimestre 2021.

Peut-être plus inquiétant encore, les 180 entreprises annoncées en novembre proviennent de 18 pays, y compris 6 extra-européens. Amazon, Google, Microsoft, Oracle et Salesforce, toutes dotées d'un siège social en Europe, font désormais partie de Gaia-X. Les nouveaux arrivants incluent également des entreprises dont les noms sont rarement associés aux 7 principes prônés par le projet, avec notamment l'entrée de Palantir, société financée à ses débuts par In-Q-Tel, le fond d'investissement de la CIA,[40] et souvent pointée du doigt par les ONG de défense des libertés numériques, de la protection des données privées et même des droits de l'homme en général,[41] ainsi que les géants chinois Huawei et Alibaba.

[40] Sur les origines de Palantir et ses liens avec l'État américain, voir l'article d'Andy Greenberg pour Forbes (2013)
[41] Comme par exemple, et seulement en 2020, Privacy International et Amnesty International

Même si seules les entreprises dont le siège mondial se trouve en Europe peuvent siéger au conseil d'administration de l'association, l'ouverture de Gaia-X, dans les jours qui suivent son établissement officiel, pose déjà la question du respect de ses principes fondateurs. Ce choix traduit la pression exercée par les leaders du marché, même indirecte, puisque les utilisateurs pourraient ignorer le catalogue en cas d'absence de ces fournisseurs familiers.[42] Avec l'ouverture des portes de cette « infrastructure numérique souveraine et de confiance pour l'Europe », les initiateurs de Gaia-X espèrent peut-être conquérir graduellement des parts de marché, notamment sur des services spécifiques où l'expertise européenne est forte mais peu visible, les entreprises souffrant du manque d'interopérabilité et de portabilité des données.

Peut-être même envisagent-ils pour Gaia-X de participer au « *Brussels effect* », avec un destin similaire à celui du RGPD, dont les règles et principes se sont étendus et ont bénéficié aux utilisateurs par-delà des frontières européennes (Bradford, 2020). Il est trop tôt pour le dire. Toutefois, en l'absence de sanctions en cas de non-respect des principes au cœur du projet, il est difficile d'imaginer que ces acteurs non-européens qui dominent le marché et raflent la plupart des contrats, y compris ceux des États européens pour des usages qui sembleraient relever du *cloud* souverain, ne fassent plus que proposer des offres taillées « sur-mesure » pour s'insérer dans l'architecture de Gaia-X. Et si leur inclusion ne signe pas immédiatement l'arrêt de mort des sept principes fondateurs, elle fait assurément passer l'enjeu de valorisation des acteurs européens, qui devront limiter l'influence de ces compétiteurs, au second plan.

3.3. « Cloud au centre », un entre-deux qui sacrifie la souveraineté au nom du pragmatisme

Cette perméabilité envers les acteurs extra-européens déjà leaders dans le secteur du *cloud* se retrouve de manière encore plus marquée dans la nouvelle stratégie nationale pour le *cloud* présentée par le gouvernement français, le lundi 17 mai 2021. Cette stratégie s'inspire directement de Gaia-X. Elle fait la part belle aux entreprises (la conférence et le dossier de presse ont donné une place conséquente aux interventions de dirigeants d'entreprises manifestant l'urgence d'accélérer la transition des entreprises vers le *cloud*), présente une nouvelle vague de financements issus du 4ème Programme d'Investissement d'Avenir et de France Relance pour le renforcement de l'écosystème *cloud* en France et en Europe, y compris des financements directs pour les services de la plateforme Gaia-X, et elle lui emprunte même l'expression « *trusted cloud* » pour le nouveau label « Cloud de confiance » au cœur de son annonce. L'abandon du terme « *cloud* souverain » n'est d'ailleurs pas qu'un symbole, puisque ce nouveau label requiert l'obtention du visa SecNumCloud, reprenant donc les conditions de sécurité et de localisation européenne des données et de leur

[42] De manière similaire, G-Cloud avait progressivement accueilli AWS (2013) puis Google (2018), originellement exclus car les offres n'étaient pas « *government ready* ».

traitement qui faisaient déjà parties du référentiel de l'ANSSI, et impose également le « portage opérationnel et commercial de l'offre par une entité européenne, détenue par des acteurs européens. »

Le label Cloud de confiance a donc pour objectif d'identifier et de valoriser des offres permettant de protéger les données des clients et des utilisateurs contre l'extraterritorialité du droit américain, tout particulièrement des mesures du CLOUD act, même si ces solutions reposent sur des technologies et infrastructures logicielles américaines licenciées à des entreprises européennes qui en assurent la commercialisation, l'intégration, la maintenance et, évidemment, la localisation dans des *data centers* européens. Pour mieux rattraper le « retard » en matière d'adoption du *cloud* en France, ce nouveau label veut donc faciliter l'accès aux services qui se sont établis en tant que standards sur le marché mondial sans pour autant craindre l'extraterritorialité du droit américain ou, comme le déclare le Ministre de l'Économie : « conjuguer protection maximale et valorisation maximale des données. »

Outre l'annonce de ce nouveau label et des investissements français et européens, l'introduction d'une nouvelle doctrine pour l'utilisation du *cloud* dans le secteur public intitulée « cloud au centre » constitue l'un des piliers de cette stratégie. Présentée en détail dans la circulaire n°6282 du juillet 2021, cette doctrine établit une approche « *cloud* par défaut » pour tout nouveau projet numérique au sein de l'État. Elle reprend dans ses grandes lignes la précédente doctrine en distinguant les besoins du secteur public qui relèvent du recours aux *clouds* internes, désormais rationalisés autour des services de cloud du ministère de l'Intérieur (PI) et du ministère des Finances (NUBO), de ceux qui autorisent l'achat de solutions commerciales. Ces solutions, si elles impliquent des systèmes qui manipulent des données sensibles (données personnelles des citoyens français, relatives aux entreprises ou aux agents publics de l'État), devront impérativement faire l'objet d'une qualification SecNumCloud[43] et être « immunisé[es] contre toute réglementation extracommunautaire », ce qui semble bien correspondre au label « Cloud de confiance », même s'il n'est pas directement mentionné par la doctrine. Ces critères sont optionnels mais encouragés dans le cadre d'offres commerciales répondant à tous les besoins non-sensibles restants.

Le nouveau souffle insufflé par cette nouvelle stratégie ainsi que la doctrine qui l'accompagne ont été salués par une partie de l'écosystème comme un signal positif remettant la facilité d'utilisation et la valeur ajoutée des services, trop souvent négligées dans les précédents projets initiés par l'État en matière de *cloud*, au cœur de l'attention. Alors que les statistiques d'adoption du *cloud* en Europe indiquent que le marché continental possède une marge de progression significative, axer la nouvelle stratégie sur ces enjeux a pour ambition de réaliser la prévision de croissance du secteur dont la taille serait multipliée par 6, voire par 10, durant la prochaine décennie selon une étude de KPMG citée dans le

[43] Ou de son futur équivalent européen, le European Cybersecurity Certification Scheme for Cloud Service, dont une version de travail a été publiée en décembre 2020 par l'Agence Européenne pour la Cybersécurité (ENISA)

dossier de presse partagé par le gouvernement.[44] Des entreprises françaises ont d'ores-et-déjà noué des partenariats avec des GAFAM afin de distribuer leurs solutions sous licence, conformément aux critères du futur label Cloud de confiance. OVHcloud avait anticipé la nouvelle stratégie en signant dès novembre 2020 un partenariat de cette nature avec Google pour proposer des offres fondées sur Anthos, la solution de la figure de proue du groupe Alphabet, hébergée, exploitée et administrée depuis les infrastructures européennes du leader du *cloud* d'infrastructure français. [45] L'officialisation, quelques jours après la présentation de la stratégie gouvernementale, de la création de Bleu, une nouvelle société codétenue par Capgemini et Orange chargée de commercialiser les solutions Azure et Microsoft 365 sur un principe similaire, a été en retour applaudie par le Secrétaire d'État chargé du numérique.[46]

Néanmoins, la stratégie annoncée par le gouvernement ne correspond qu'à une définition très restreinte de la souveraineté numérique et ne répond qu'à l'un de ses trois aspects identifiés plus haut (cf. la partie 1.2. de ce papier), occasionnant logiquement une levée de boucliers de la part de parlementaires, d'experts et de dirigeants d'entreprise de l'écosystème du *cloud*, inquiets de ce que cette stratégie pourrait signifier sur le long terme pour la confidentialité des données impliquées, pour la sécurité des Opérateurs de Services Essentiels et d'Importance Vitales (OSE et OIV) qui opteraient pour ces offres et, plus généralement, pour l'avenir de la filière française et européenne.

D'une part, si le label récemment créé ajoute aux prérequis du référentiel SecNumCloud des mesures pour s'assurer que les données soient localisées et traitées en Europe par des entreprises européennes, sa capacité à empêcher toute expression de l'extraterritorialité du droit américain et à protéger ces données sur le long-terme est incertaine. Comme le note la sénatrice Catherine Morin Desailly, l'extraterritorialité du droit américain ne se limite pas au CLOUD Act et le recours à une solution sous licence américaine pourrait rendre possible une surveillance sous le régime du Foreign Intelligence Surveillance Act (FISA).[47]

D'autre part, la mise en œuvre de ce label et de la nouvelle doctrine ne sont que partiellement à la hauteur des enjeux économiques et géostratégiques de la souveraineté numérique appliquée au *cloud*. Certes, ce label devrait stimuler la demande publique et privée vers des fournisseurs de services *cloud* européens, mais il supprime une part importante de « l'avantage compétitif » promis aux entreprises françaises et européennes. Celles qui ont déjà massivement investi dans la recherche et le développement de technologies de *cloud* souveraines ou *open source* sont soudainement mises sur un pied

[44] Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030, rapport de KPMG pour Talan, InfraNum, OVHcloud et Linkt, Avril 2021
[45] « OVH se rapproche de Google Cloud pour lancer de nouvelles offres logicielles » Léna Corot, *L'Usine Digitale*, 10 novembre 2020
[46] « Capgemini et Orange créent un cloud souverain Azure et Microsoft 365 », Antoine Crochet-Damais, *Le Journal du Net (JDN)*, 27 mai 2020
[47] Question d'actualité au gouvernement n° 1875G de Mme Catherine Morin-Desailly, publiée dans le JO Sénat du 03/06/2021. La sénatrice a également pris position sur le sujet dans la presse, par exemple dans l'article « Doctrine "cloud" de l'Etat : le grand malaise » de Sylvain Rolland, *La Tribune*, 9 juin 2021.

d'égalité avec les solutions des géants mondiaux, qui jouissent de budgets sans commune mesure en matière de R&D, mais aussi de communication et de lobbying, si tant est qu'elles soient « packagées » par une entreprise au capital européen. Cette mise en concurrence directe, sans différenciation entre des offres qui fournissent des garanties fondamentalement divergentes, est un désaveu des politiques d'investissement publiques des dix dernières années ayant soutenu, au sein de l'écosystème européen, le développement de technologies de *cloud* innovantes et souveraines.

Perpétuant la constante tradition d'incohérence des politiques publiques et des stratégies industrielles en matière de numérique en France, ce label ne peut que, sur le long terme, diminuer la rentabilité des investissements en R&D des entreprises françaises et européennes qui ont tout intérêt à s'appuyer sur des solutions logicielles sous licence, dont les noms sont bien connus de leurs clients. En invitant à externaliser le développement de ces infrastructures logicielles du *cloud* et de se reposer sur les offres des géants américains et éventuellement chinois, ce label ne peut amener, sur le long terme, qu'à une perte de capacité de l'écosystème français et européen en matière d'innovation et de design de solution.[48]

Ce constat s'accompagne d'une conséquence logique sur le plan stratégique : la doctrine actuelle de « cloud au centre » créé une dépendance des entreprises et du secteur public, y compris pour des usages potentiellement sensibles et d'importance vitale pour la société (OSE et OIV), vis-à-vis de solutions créées par des entreprises étrangères. Comme le rappelle Yann Lechelle, PDG de Scaleway, l'une des entreprises majeures du paysage du *cloud* en France, la couche logicielle qui peut désormais être déléguée aux entreprises étrangères est « génératrice de la plus forte valeur ajoutée »[49] et c'est bien cette couche logicielle qui devrait être souveraine « par design » pour les activités sensibles. Puisqu'il autorise la conception du code source des solutions qu'il accrédite par des entreprises étrangères, le label « Cloud de confiance » confère des garanties insuffisantes en matière de sécurité et de protection des données. Le code source du programme licencié n'étant pas forcément pleinement auditable, des solutions pourtant labellisées « Cloud de confiance » pourraient exposer leurs utilisateurs à des risques par l'inclusion de « *backdoors* »[50] ou la mise en place de flux d'informations sensibles dissimulés.[51]

Même en écartant ces risques structurels, Yann Lechelle, Franck Spinelli, PDG d'Amarisoft et Jean-Paul Smets, PDG de Rapid.Space, rappellent dans une tribune commune que cette

[48] C'est de plus un « beau cadeau » que d'offrir des opportunités de marché supplémentaires à des entreprises connues pour leurs stratégies d'évitement fiscal et qui n'ont participé ni au financement des infrastructures *hardwares* (*data centers*…), ni à celui de la formation des professionnels amenés à intégrer ces solutions.
[49] *Doctrine "Cloud au centre" : un pas de géant pour la modernisation numérique de l'État… et des interrogations*, billet de Yann Lechelle sur le blog de Scaleway, 25 mai 2021
[50] Les *backdoors*, ou portes dérobées, sont des failles de sécurité laissées volontairement dans un programme par son auteur pour permettre un accès ultérieur relativement indétectable pour l'auteur ou un partenaire, comme, par exemple des services de renseignement.
[51] Tel que cité dans « "Cloud de confiance" : l'Etat a-t-il laissé entrer le loup américain dans la bergerie ? », Sylvain Rolland, *La Tribune*, 28 mai 2021

dépendance n'est pas sans conséquence.[52] Elle donne aux entreprises américaines qui ont déjà répondu à l'appel du pied du gouvernement un levier considérable pour n'importe quelle négociation commerciale. Au niveau international, elle confère un nouvel argument de poids à l'État américain qui peut agir directement sur l'économie nationale française via la mise en place de restrictions ou de taxes sur les exportations de logiciels ou même, en cas de fortes tensions diplomatiques ou économiques, en mettant dans la balance la suspension immédiate de ces licences.

[52] « Défense, cloud souverain : les PME au centre de notre indépendance », tribune de Franck Spinelli, Jean-Paul Smets et Yann Lechelle, *Les Echos*, 12 juillet 2021

Conclusion

Le *cloud* souverain est un projet emblématique de la souveraineté numérique pour l'État français, qui a inégalement appréhendé ses enjeux d'ordre juridique, économique et de sécurité. Les discours politiques, stratégies industrielles, politiques d'investissements et doctrines de commande publique successives, en dépit de leurs très nombreuses incohérences, ont eu le mérite d'avoir légitimé en France le concept, même imprécis, de *cloud* souverain et des besoins qui lui sont associés dans le secteur public et pour les entreprises assurant des services essentiels ou d'importance vitale pour la société et l'économie (Bourliataux-Lajoinie Stephane, David, 2018).

Marquée par les échecs liés aux tentatives de donner naissance, *ex nihilo*, à un champion capable de concurrencer les géants américains, la stratégie de l'État en matière de *cloud* souverain s'est métamorphosée tout au long des douze dernières années. Elle a évolué vers une approche plus résolument tournée vers l'écosystème industriel national, qui a mené à l'adhésion à une nouvelle vision européenne, fondée sur un cadre réglementaire en construction et sur le soutien au projet Gaia-X, un consortium d'entreprise où l'État joue un rôle de soutien, dont le choix de maintenir la porte ouverte aux entreprises extra-européennes semble surprenant mais a sans doute influencé la dernière doctrine gouvernementale « Cloud au centre » et la création d'un label « Cloud de confiance » qui interrogent tout autant. Sous prétexte de concilier l'accès aux offres de *cloud* standards sur le marché mondial et la « souveraineté des données »,[53] contournant, au moins à court terme, l'extraterritorialité du droit américain, ce nouveau label semble contredire les stratégies antérieures de souveraineté numérique en France, en oubliant ses aspects stratégiques et économiques, et en affaiblissant sur le long terme les acteurs de l'écosystème d'innovation français et européen.

Ces incohérences répétées, qui sont pour partie responsables de l'absence de résultats probants de la stratégie de *cloud* souverain en France, s'incarnent, tout particulièrement, dans l'écart observé entre les ambitions affichées par les discours politiques des gouvernements successifs et la réalité des actions mises en œuvre. Qu'elles relèvent des

[53] C'est Octave Klaba, le président et fondateur d'OVHcloud qui, répondant à une question interrogeant le partenariat entre son entreprise et Google vis-à-vis des ambitions qu'il affiche pour le développement de l'écosystème européen, essaye de faire la distinction entre la « souveraineté des données » pour laquelle « il « suffit » d'utiliser n'importe quel logiciel, y compris américain, et de l'opérer dans nos centres de données » et la « souveraineté technologique », soulignant la nécessité de développer des infrastructures *open source* permettant de « s'abstraire » des dépendances à ces briques logicielles. Les conséquences de la captation d'une partie de la valeur ajoutée par les géants américains sur la capacité à développer ces infrastructures libres ne sont, elles, pas évoquées. Voir « En Europe, il y a de quoi faire largement mieux que les Américains », J. Chauveau, D. Barroux, F. Debes, *Les Echos*, 18 juin 2021.

politiques publiques, des réglementations adoptées ou des choix en matière de commande publique, ces actions manquent systématiquement de l'envergure et de la coordination nécessaire à la construction, sur le long terme, d'infrastructures de *cloud* répondant aux enjeux de la souveraineté numérique, des capacités matérielles, logicielles et humaines qu'elles impliquent, et à l'enclenchement de boucles de rétroaction vertueuses à travers le secteur public et l'écosystème d'innovation français et européen.

En déplorant que « le retard européen dans la technologie du Cloud était trop grand », Cédric O, secrétaire d'État chargé du numérique, identifiait devant le Sénat, le 27 mai 2020, tout autant un symptôme de l'échec de la stratégie française qu'une raison motivant le choix de Microsoft pour héberger le Health Data Hub, un choix qui allait à l'encontre, à court et à long terme, de cette stratégie. En effet, il ne concordait alors ni avec la doctrine d'utilisation de l'informatique en nuage par l'État, ni avec l'ambition de développer un écosystème mature de *cloud* souverain, en France ou en Europe. En exploitant la rhétorique de « l'urgence technologique », cette décision laissait passer une nouvelle occasion de stimuler le développement des entreprises européennes et de s'assurer de la protection de données personnelles hautement sensibles. En revanche, elle contribuait directement à la dépendance du secteur public et des entreprises stratégiques envers les leaders américains du marché pour les besoins de services *cloud*. Quand bien même l'invalidation du Privacy Shield et l'indignation publique ont forcé à un revirement concernant l'hébergement du Health Data Hub, ce sont les mêmes arguments employés à l'attribution de ce marché, sans mise en concurrence,[54] ceux de « l'urgence », « du retard technologique » et de la nécessité d'accéder, sans plus attendre, sous peine de décrochage irrémédiable, « aux meilleurs services mondiaux », qui ont été utilisés à l'annonce de la nouvelle stratégie nationale pour le *cloud* afin de justifier le label « Cloud de confiance ». Cette rhétorique est la même que celle que Dominique Boullier nomme la « tyrannie du retard »[55] et qui exploite un impératif technologique, une nécessité économique et une injonction de progrès inéluctable pour « dépolitiser » et soustraire du débat public des prises de décision (souvent décorrélées de la réalité technique qu'elles invoquent) concernant des sujets stratégiques, comme par exemple les politiques de déploiement des réseaux 5G.[56]

La véritable urgence est donc d'enfin tirer les enseignements des échecs précédents, de dépasser ces discours qui instrumentalisent les motifs de l'urgence, du retard et du « fait » technologique soi-disant objectif, afin de mettre en place une véritable politique industrielle autour du *cloud* souverain, s'appuyant sur une stratégie de long-terme, cohérente et transparente, sur le nouveau cadre mis en place au sein de l'Union Européenne et sur une

[54] L'association Anticor a d'ailleurs saisi le Parquet National Financier le 26 mars 2021 concernant la potentielle attribution illégale de ce marché.
[55] Voir « Quelle 5G ? Pluralisme des stratégies de réseaux », Dominique Boullier, *AOC*, 2 octobre 2020
[56] Nul doute que cette rhétorique est influencée par les discours des géants du numériques, les GAFAM et Huawei formant le top 6 des entreprises du numérique avec les budgets de lobbying les plus importants au niveau européen (entre 3 et 6 millions d'euros en 2021) selon un rapport du Corporate Europe Observatory et de LobbyControl.

compréhension rigoureuse des enjeux de la souveraineté numérique ainsi que des besoins du secteur publique, des opérateurs de services essentiels et de l'écosystème d'innovation.

Recommandations

La migration du Health Data Hub vers des plateformes françaises ou européennes, à la suite de l'annulation du *Privacy Shield,* et l'implémentation de la nouvelle stratégie de l'État sont des opportunités à ne pas manquer pour réaligner l'action publique et la stratégie française du *cloud* souverain avec le nouvel élan européen.

Ce réalignement peut être opéré en procédant à :

- **La mise en place d'un label « Cloud souverain » réservé aux solutions *cloud* répondant aux critères du référentiel SecNumCloud, portées par des entreprises européennes, reposant sur des infrastructures logicielles propriétaires, licenciées par des entreprises européennes ou *open source*.** Ce label accessible aux offres d'entreprises déjà certifiées « Cloud de confiance » et répondant aux critères d'éligibilité ci-dessus serait requis pour tout système au sein du secteur public manipulant des données sensibles tel que défini par la doctrine « Cloud au centre » (paragraphe R9), ainsi que pour les systèmes sensibles d'organismes publics et privés identifiés par l'ANSSI et listés Opérateurs de Services Essentiels et Opérateurs d'Importance Vitale.

- **L'attribution du contrat du Health Data Hub à une ou plusieurs entreprises européennes** ayant obtenue la qualification SecNumCloud (ou équivalant européen) et participant activement au projet Gaia-X afin qu'il en devienne l'un des projets pilotes.

- **La mise en place d'un comité stratégique pour les usages du *cloud* et des données dans le secteur public** afin d'identifier les systèmes informatiques impliquant des données sensibles et d'évaluer, au cas par cas, les nouveaux cas d'usage requérant l'utilisation d'une offre de *cloud* interne, labellisée « Cloud de confiance » ou « Cloud souverain », dans la continuité de la doctrine « Cloud au centre » et de celle présentée par la circulaire du 8 novembre 2018 l'ayant précédée. Ce comité stratégique doit rassembler des

expertises **techniques, juridiques et opérationnelles**, avec par exemple, la participation de la Dinum, de la CNIL et de l'ANSSI.

- **L'élaboration de nouvelles directives en matière de commande publique concernant les fournisseurs de services *cloud* pour l'État afin de favoriser la concurrence et la compétitivité des acteurs français et européens.** Afin de réaligner les ambitions en matière de *cloud* souverain, les besoins réels du secteur public et les solutions disponibles sur le marché européen, il est nécessaire de faciliter le positionnement de plus petits acteurs, nationaux et européens, sur ces besoins. Le cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication (CCAG-IT), qui a bénéficié d'une mise à jour du 30 mars 2021, pourrait inclure davantage de clauses favorisant la transparence vis-à-vis de la localisation des données, le recours obligatoire à des solutions s'inscrivant dans le référentiel SecNumCloud pour des services publics essentiels identifiés par la doctrine ou le comité stratégique susmentionnés, ainsi que des dispositions permettant de diminuer l'emprise des entreprises dominant le secteur (*lock-in effect*) en renforçant, par exemple, les exigences de transparence des contrats et des cahiers des charges, en limitant les durées maximum des marchés et surtout en favorisant l'interopérabilité et la portabilité des données (seules les « données indispensables à l'exécution d'une mission de service public » sont pour l'instant couvertes par une clause de réutilisation).[57]

- **La production d'un rapport détaillé sur les besoins de l'État français en matière de *cloud* souverain,** et plus particulièrement sur les besoins émergents (*edge computing*, traitement du Big Data…).

- **La mise en œuvre d'une politique d'investissement plus ambitieuse**, articulée aux financements européens, **dans les entreprises nationales et européennes à même de répondre à ces besoins**. Cette politique d'investissement doit permettre à la fois la formation de nouveaux talents, la mise en place de projets de recherche et de développement à fort potentiel, notamment dans le développement de nouvelles technologies *cloud* (infrastructures logicielles, architecture de *cloud* décentralisées et chiffrées de

[57] Certaines des recommandations présentées par la coalition CISPE.cloud dans son rapport « 10 clés pour l'Acheteur Public de Cloud » restent tout-à-fait pertinentes après cette mise à jour.

bout-en-bout, *edge computing*…) et la construction d'infrastructures de dernière génération sur le territoire national et européen.

Bibliographie sélective

Clotilde Bômont. « Maîtriser le *cloud computing* pour assurer sa souveraineté », Stéphane Taillat éd., *La Cyberdéfense. Politique de l'espace numérique.* Armand Colin, 2018, pp. 91-97.

Clotilde Bômont, Amaël Cattaruzza. « Le *cloud computing* : de l'objet technique à l'enjeu géopolitique. Le cas de la France », *Hérodote*, vol. 177-178, no. 2-3, 2020, pp. 149-163.

Didier Danet, Amaël Cattaruzza. Cloud souverain et balkanisation du web : le cas des Etats-Unis, 2014.

Primavera de Filippi, Smari Mccarthy. "Cloud Computing: Centralization and Data Sovereignty". *European Journal of Law and Technology*, University of Warwick, 2012, 3 (2).

Bourliataux-Lajoinie, Stéphane & Mickael, David. « Analyse de la stratégie de légitimation d'un Cloud Souverain par l'Etat-le cas français », papier pour la conférence de l'Association Information & Management (AIM), Montréal, 2018.

Christopher Millard. "Forced Localization of Cloud Services: Is Privacy the Real Driver?", *IEEE Cloud Computing*, 2015.

Barbara Russo, Laura Valle, Guido Bonzagni, Davide Locatello, Marta Pancaldi, Davide Tosi. "Cloud Computing and the New EU General Data Protection Regulation," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 58-68, Nov./Dec. 2018.

Sarah Guillou. « La souveraineté numérique française passera par l'investissement dans les technologies numériques », Chaire Digital, Gouvernance et Souveraineté de Sciences Po Paris, Novembre 2020

Didier Danet, Amaël Cattaruzza. « Cloud souverain et balkanisation du web : le cas des Etats-Unis », Rapport pour le Ministère de la Défense, 2014.

Rapport de M. Gérard Longuet au nom de la commission d'enquête sur la souveraineté numérique du Sénat, « Le devoir de souveraineté numérique », 1 octobre 2019

Status report of Workstream 1 "User Ecosystems and Requirements", Gaia-X, "GAIA-X: A Pitch Towards Europe", Federal Ministry for Economic Affairs and Energy (BMWi), May 2020.

“GAIA-X: Technical Architecture”, Federal Ministry for Economic Affairs and Energy (BMWi), June 2020.

Au sujet de l'auteur :

Pierre NORO est le cofondateur de Pebble et chargé d'enseignement à Sciences Po. Après plusieurs années au sein de l'équipe Blockchain et Cryptoactifs de la Caisse des Dépôts et des Consignations, Pierre a collaboré avec plusieurs startups avant de revenir à Sciences Po en tant que coordinateur de la Chaire Digital, gouvernance et souveraineté et enseignant du cours Blockchain for Public Good.
En plus de son rôle au sein de l'équipe de chercheurs européens construisant Pebble, la première solution de vote électronique entièrement transparente et décentralisée, il participe depuis 2019 au développement de LabXchange, la plateforme d'éducation aux sciences en ligne hébergée par l'Université de Harvard et préside l'association d'innovation sociale BubbleBox.

Au sujet de la Chaire Digital, Gouvernance et Souveraineté :

La mission de la Chaire Digital, Gouvernance et Souveraineté de Sciences Po est de créer un écosystème unique pour rapprocher l'univers des entreprises technologiques du monde de la recherche académique, du monde politique, de la société civile, et des incubateurs de politiques publiques et de régulation du numérique. Ces relations nécessitent un écosystème de recherche, d'innovation et de formation qui soit pluridisciplinaire, international et en prise directe avec la sphère publique.

Portée par l'École d'Affaires Publiques, elle est résolument pluridisciplinaire pour penser de façon holistique les transformations économiques, juridiques, sociales ou encore institutionnelles entraînées par le numérique.

La Chaire Digital, Gouvernance et Souveraineté est dirigée par **Florence G'sell**, professeure de droit à l'Université de Lorraine, enseignante à l'École d'Affaires Publiques de Sciences Po. Elle bénéficie du précieux soutien de ses partenaires :