Rapport de la Fondation Concorde

Décembre 2021

Construire un Cloud de confiance pour l'État

Enjeux autour de la migration des données publiques vers le Cloud

FONDATION CONCORDE

Le Think Tank
dédié à la **compétitivité**,
la **croissance** et **l'emploi**

Sommaire

Rapport réalisé par Nicolas Sironneau et Jean-Benoit Arvis

Nicolas Sironneau - Expert Numérique Nicolas travaille en conseil en stratégie, notamment dans le domaine des nouvelles technologies, après des études à Sciences Po, au MIT et à la Bocconi. Il est notamment co-auteur de rapports sur la 5G ou les cas d'usage de la Blockchain pour la Fondation Concorde

Jean-Benoit Arvis - Expert Numérique. Jean-Benoît travaille en conseil en stratégie après des études à HEC Paris et à l'université Bocconi de Milan. Il est notamment co-auteur d'un rapport sur les cas d'usage de la Blockchain pour la Fondation Concorde

Introduction

Un enjeu fondamental

En décembre 2020 a été découverte une attaque informatique massive contre le gouvernement fédéral américain, baptisée *SolarWinds*, du nom de l'entreprise dont le logiciel fut piraté et utilisé pour accéder aux systèmes de l'État fédéral. Pendant neuf mois, des intrus ont eu accès aux systèmes informatiques des départements du Trésor, du commerce et de l'énergie sans être détectés, leur permettant d'exfiltrer des données sensibles. Un an après, l'affaire continue d'agiter les États-Unis comme le reste du monde, **faisant revenir au premier plan l'enjeu de la cybersécurité dans le secteur public.** En France, les attaques sont pour l'instant moins spectaculaires, mais néanmoins inquiétantes. L'hôpital de Dax a été attaqué le 9 février 2021 par un programme dit de rançongiciel, qui a crypté les données de l'établissement en exigeant un paiement pour les restituer[1]. La structure fut obligée de revenir à un mode de fonctionnement papier pour assurer la continuité des opérations. Un tel scénario, à plus grande échelle, est de plus en plus redouté par les décideurs du public et des grandes entreprises.

Ces attaques interviennent dans un contexte de pression toujours plus forte pour la digitalisation des services publics. Une tendance accentuée par la pandémie actuelle puisque de nombreux services publics ne peuvent plus désormais être dispensés qu'en ligne. De la Nouvelle-Écosse à l'Australie en passant par l'Estonie, les gouvernements redoublent d'inventivité pour accélérer leur transition digitale[2]. La France n'est pas en reste puisque la digitalisation des services publics est un des grands chantiers du quinquennat du président Macron[3].

Aucune thématique ne symbolise mieux ces deux mouvements opposés que le Cloud, à la fois pierre angulaire de cette « digitalisation » tant recherchée et en même temps objet de controverses sur la sécurité et la souveraineté des données. Le Cloud est un paradigme dans lequel le stockage des données, les logiciels, les fonctions de calcul et tout ou partie des fonctions d'un data center sont hébergées et/ou entretenues par un prestataire externe[4]. Le Cloud est une réponse technique à l'augmentation exponentielle des volumes de données

[1] Le Monde (2021), « Touché par une cyberattaque "massive", l'hôpital de Dax veut poursuivre les soins coûte que coûte », Mayer, Claire, 12 février 2021

[2] KPMG (2020), "Digital is not the future; it is today: Digital transformation in the public sector", https://home.kpmg/xx/en/home/industries/government-public-sector/the-new-reality-for-government/digital-is-not-the-future-it-is-today.html [dernier accès le 30/01/2021]

[3] La Tribune (2017), « Numérique : les grands chantiers du président Macron », Sylvain Rolland, 17 mai 2017

[4] Dodd, Annabel Z. (2019), The Essential Guide to Telecommunications, Sixth Edition, p. 47

informatiques traitées aujourd'hui, et s'appuie sur une explosion des débits internet. Déjà largement plébiscité par le secteur privé, le Cloud l'est aussi de plus en plus par les États. Son principal atout est **celui de la flexibilité** : l'accès aux services Cloud, effectué via une simple connexion internet, peut se faire partout, ce qui favorise à la fois le travail flexible et la collaboration pour les utilisateurs. Mais la flexibilité du Cloud consiste aussi et surtout en une capacité de stockage et de calcul modulable, et une facturation à l'usage qui permet le développement rapide de nouveaux usages tout en optimisant les coûts d'infrastructures.

L'État français, dans une circulaire de novembre 2018, a annoncé son intention d'**accélérer le transfert des données et des applications des administrations publiques sur le Cloud.** Ceci est la deuxième tentative de lancement d'une politique de Cloud étatique en France, venant compléter un premier chantier lancé en 2012 sous l'appellation de « Cloud souverain ». Face à un déploiement jugé encore trop lent, l'État décide début 2021 de mettre les bouchées doubles et annonce une **nouvelle doctrine de Cloud le 17 mai 2021.** Celle-ci reçoit un fort écho médiatique, du fait du rôle accordé à des prestataires de services Cloud américains.

Le débat autour du Cloud tourne autour de trois éléments. D'abord, le Cloud représente un accélérateur majeur de la digitalisation des services publics. Au Royaume-Uni par exemple, la politique de Cloud a été définie dès 2010[5]. L'utilisation du Cloud par de nombreux départements du gouvernement de Sa Majesté a permis, parmi d'autres cas d'usage, de réduire de 40 % les coûts du bureau de l'immigration du *Home Office*[6], ou encore de permettre au gouvernement du Pays de Galles d'adopter une politique de travail flexible (*smart working*) pour ses fonctionnaires en faisant passer ses applications et données sur le Cloud[7]. Fort de ces succès, le *Home Office* continue d'accélérer sa transition vers le Cloud avec, en mars 2021, le transfert de certaines fonctions : RH, paie, finance et assistance client pour les 35 000 collaborateurs du ministère, ces fonctions étant hébergées sur une solution *Oracle Cloud*[8].

Cependant, deuxième élément, même si les solides capacités de cybersécurité de l'État français offrent une certaine garantie, **l'adoption du Cloud par les pouvoirs publics ne peut faire l'impasse sur les nouveaux risques** de sécurité liés à la technologie, et les mesures prises pour assurer une confiance dans son usage.

Mais le troisième, et le plus important des éléments du débat autour de l'adoption du Cloud par les services publics, est celui de la souveraineté des données. Qu'un État souve-

[5] Cisco (2017), "How to adopt Cloud for digital government success", 2017
[6] Gov.uk (2021), "Cloud guide for the public sector", 8 février 2021, https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector [dernier accès le 27 février 2021]
[7] Gov.uk (2021), "How the Welsh government migrated their technology to the Cloud", 27 mars 2020 https://www.gov.uk/government/case-studies/how-the-welsh-government-migrated-their-technology-to-the-cloud [dernier accès le 27 février 2021]
[8] Oracle (2021), "Home Office leads the way as UK Government transfers crucial services to Oracle Cloud", 23 mars 2021 https://www.oracle.com/uk/news/announcement/home-office-with-oracle-cloud-2021-03-23.html [dernier accès le 17 avril 2021]

rain garde la maîtrise de ses données semble une évidence. Pourtant, dans un monde où les fournisseurs Cloud sont pour l'essentiel des entreprises non-européennes, comment faire émerger le « Cloud de confiance » proposé par le ministre de l'Économie et des Finances Bruno Le Maire en 2019[9], tout en se reposant sur les technologies les plus récentes ?

Ce rapport cherche à **retracer brièvement l'historique de l'effort de l'État français pour migrer vers le Cloud (I)** - tant dans son aspect rationnel que dans son contexte politique - avant **d'analyser plus en détails les enjeux et implications de son utilisation (II)** - en termes de risques mais aussi en termes de souveraineté.

[9] Les Échos (2019), « La France cherche son "Cloud de confiance" », Dèbes, Florian, 14 octobre 2019, Paris

Quel Cloud pour l'État français ?

A. Rappel sur le fonctionnement du Cloud

I. Qu'est-ce que le Cloud ?

Aujourd'hui, le Cloud devient un outil incontournable pour toutes les organisations, publiques et privées. Fondamentalement, le Cloud est un **moyen d'organiser les ressources informatiques** en déplaçant le stockage des données et des applications sur un serveur qui n'appartient pas à l'utilisateur mais à un tiers. Le Cloud vient réduire la dépendance à la fois aux disques durs des appareils individuels, mais permet également aux organisations de ne pas avoir à gérer elles-mêmes leurs infrastructures, notamment d'éventuels *data centers*. Pour faire simple, le Cloud est comme un ensemble de *data centers* mutualisés entre un grand nombre d'utilisateurs, et accessibles via une connexion internet.

On distingue traditionnellement le **Cloud public** où les serveurs sont partagés entre clients, et le **Cloud privé** où le client a accès à un serveur dédié[10]. La distinction entre les deux est encore généralement vraie aujourd'hui, même si d'un fournisseur à l'autre les appellations commerciales et les définitions précises varient considérablement.

En fait, tous les Clouds **partagent certaines caractéristiques communes :**

• Tous les Clouds gèrent et allouent des capacités de calcul sur un réseau et une infrastructure ;

• Des interfaces de programmation d'application, plus communément appelées *API*, sont un élément récurrent bien que les *API* proposées par les différents Clouds restent différents ;

• Enfin ces Clouds possèdent des plateformes de gestion[11]

Sur la base de ce socle commun, on différencie trois principales sous-catégories de Clouds commercialisées aujourd'hui, chacune offrant une proposition de valeur spécifique, en fonction du niveau de sensibilité des données et des attentes des clients en matière de sécurité, de personnalisation des accès et de la gestion des opérations d'administration :

1. Le **Cloud public** correspond aux offres de Cloud « standard » disponibles sur le marché. Les données sont hébergées dans des infrastructures mutualisées construites par une entreprise privée pour servir la majorité de ses clients *(data center)*. Dans ce modèle, le fournisseur prend à sa charge la maintenance, les mises à jour, et la gestion de la sécurité des données. Elles n'exigent aucun investissement en infrastructures physiques de la part du client, elles sont simples à mettre en œuvre et très utiles pour héberger les données peu sensibles, les projets pilotes et les expérimentations.

[10] Dodd, Annabel Z. (2019), The Essential Guide to Telecommunications, Sixth Edition, p. 49

[11] Red Hat (2021), « Cloud Computing - Cloud Public, Privé et Hybride, Quelles différences ? », https://www.redhat.com/fr/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud [dernier accès le 21 mars 2021]

2. Les **Clouds dédiés (ou communautaires)** offrent un espace de stockage individualisé et peuvent répondre à des certifications supplémentaires. Pour des raisons de sécurité, ils sont souvent directement installés au sein du *data center* du client, derrière son pare-feu, mais peuvent également être installés en colocation. En fonction de la taille du client, les coûts de construction de l'infrastructure dédiée peuvent être entièrement assumés par le fournisseur sur fonds propres, en contrepartie d'un engagement de dépenses minimales sur une période déterminée, ou réparties avec le client. Les tarifs sont généralement comparables à ceux du Cloud public. Ces offres sont utiles lorsqu'une organisation ou un gouvernement a décidé de s'engager dans la migration et l'exploitation d'un Cloud à grande échelle. Elles sont adaptées à certains marchés réglementés (Banques, Assurance, Énergie, etc.) et aux agences gouvernementales et du renseignement.

3. Enfin, les **Clouds privés (ou contrôlés)** sont construits pour un client unique afin de répondre à ses spécifications en matière de sécurité et d'habilitation. Historiquement, il s'agit de Clouds privés personnalisés, pour lesquels le client supporte l'intégralité des coûts de construction et d'exploitation de l'environnement. Cependant, certains fournisseurs proposent à présent des variantes de leurs offres commerciales construites et exploitées selon les spécifications des clients. Dans ce modèle, ils prennent à leur charge l'intégralité de l'investissement en contrepartie d'un engagement sur plusieurs années. Ces solutions - principalement destinées aux gouvernements et agences de renseignement - s'adaptent aux besoins spécifiques des États en matière de souveraineté numérique, notamment l'architecture et la cybersécurité (déconnexion d'internet, connexion au réseau interministériel, habilitation du personnel gérant la maintenance, contrôle et certification des infrastructures, contrôle des flux entrant et sortant, etc.). Elles permettent aux administrations de construire un Cloud sur-mesure et souverain tout en faisant appel aux meilleures technologies proposées sur le Cloud Public, et sans avoir à investir elles-mêmes dans des infrastructures coûteuses.

Le secteur du Cloud connaît une croissance massive. Les revenus du secteur du seul Cloud public, c'est à dire l'implémentation « classique » avec partage des serveurs entre plusieurs utilisateurs, devraient atteindre 210 milliards d'euros en 2020 selon Gartner[12]. Ceci alors qu'en 2017, il représentait autour de 130 milliards d'euros[13]. Ce marché a donc **vu sa taille augmenter en moyenne de 19 % chaque année depuis trois ans.** Toujours selon Gartner, d'ici 2022 la valeur du Cloud public devrait encore croître pour dépasser les 300 milliards d'euros, soit 40 % plus qu'en 2020, et 2,3x plus qu'en 2017.

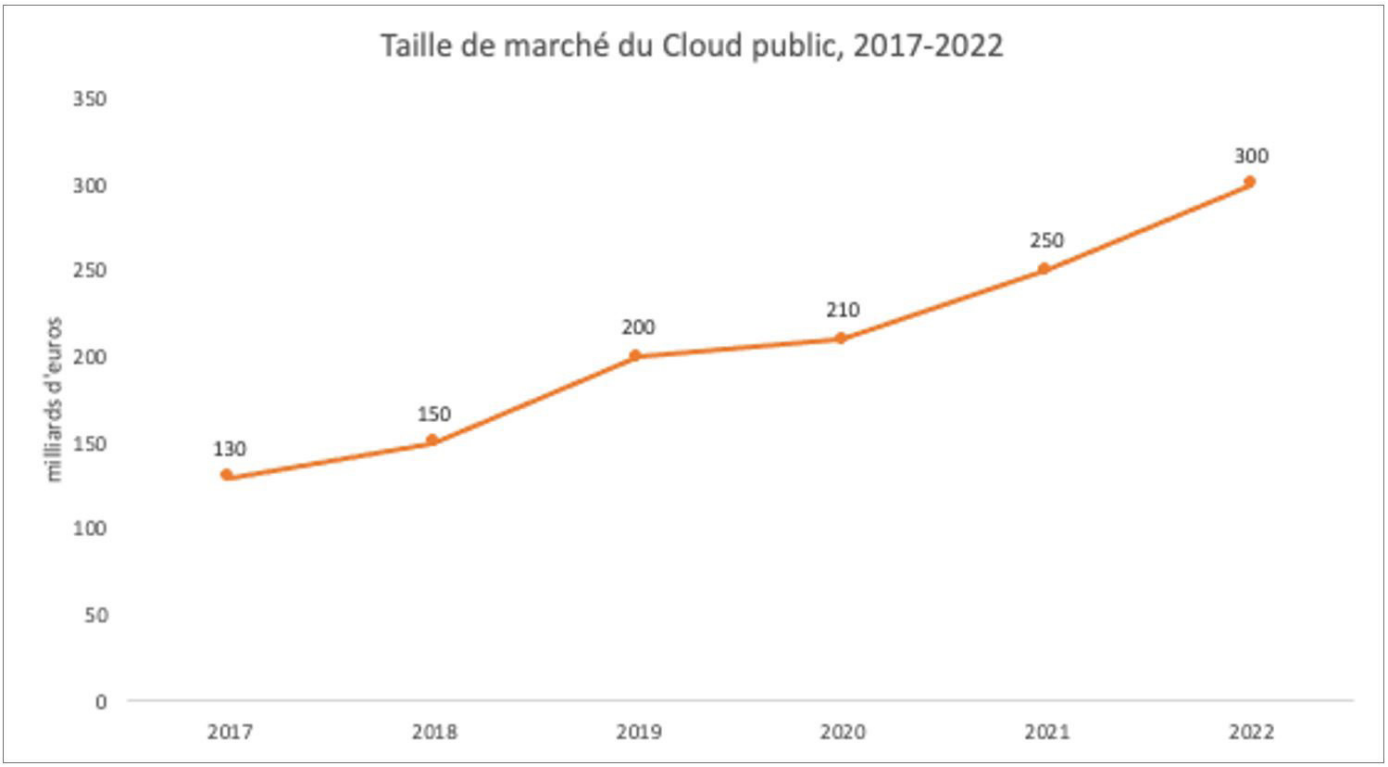
Le seul marché du Cloud européen (toutes implémentations confondues) a connu une croissance de 27 % par an entre 2017 et 2019, pour atteindre 53 milliards d'euros en 2020, d'après une récente étude publiée par *KPMG*[14]. Ce marché devrait encore croître pour atteindre 300 à 500 milliards d'euros en 2027-2030, toujours selon la même étude.

[12] Gartner (2020), "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.6% in 2020", 23 juillet 2020 https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020 [dernier accès 30 janvier 2021]

[13] Gartner (2016), "Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach $204 Billion in 2016", 25 janvier 2016 https://www.gartner.com/en/newsroom/press-releases/2016-01-25-gartner-says-worldwide-public-cloud-services-market-is-forecast-to-reach-204-billion-in-2016 [dernier accès 7 mai 2021]

[14] KPMG (2021), « Le Cloud européen », 4 mai 2021, https://home.kpmg/fr/fr/home/media/press-releases/2021/05/cloud-europeen-marche-enjeux-economiques.html [dernier accès le mai 2021]

Schéma 1.1 : La croissance du marché mondial du Cloud public



Le principal critère utilisé pour définir un Cloud est celui du **modèle d'utilisation.**

Le Cloud - contrairement au modèle qu'il vient remplacer - ne nécessite aucun nouvel investissement en infrastructures pour le client final. Le service est facturé à la consommation, en fonction de l'usage réel du client. Il existe trois modèles principaux : l'IaaS, le SaaS et le PaaS.

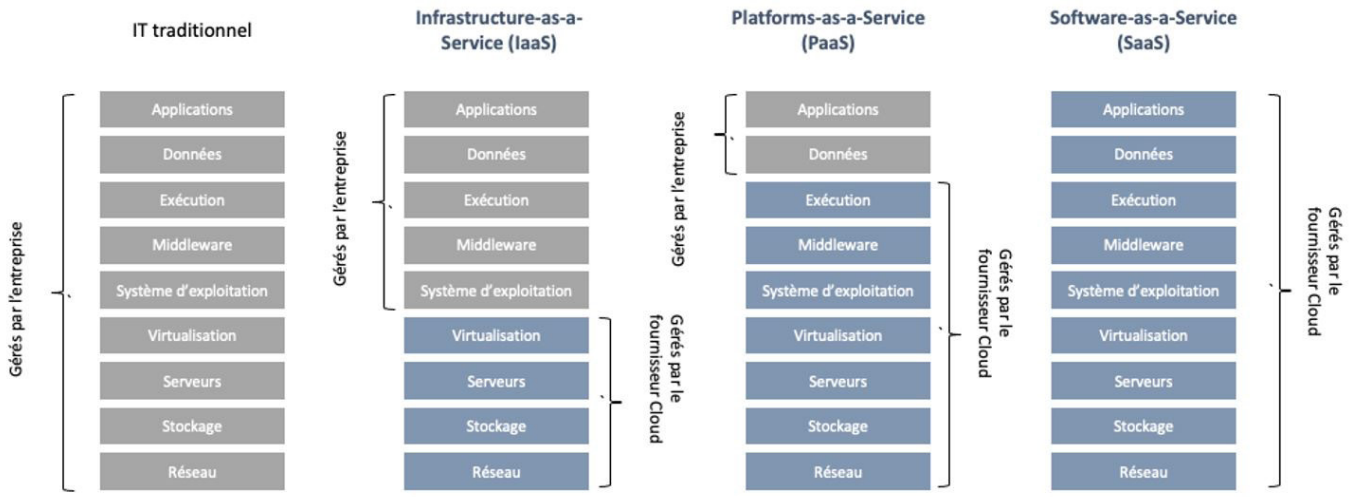
L'IaaS, ou *Infrastructure-as-a-Service*, permet au client de bénéficier de la puissance de calcul et des capacités de stockage des serveurs, mais laisse au client le choix des OS, des applications et des utilisations finales. Le fournisseur de Cloud se charge uniquement de l'infrastructure, donc des serveurs, du réseau, de la virtualisation et du stockage des données.

Le SaaS, *Software-as-a-Service*, longtemps symbolisé par l'américain *Salesforce*, consiste en un fournisseur qui développe sur le Cloud des applications métier (ERP, HCM, etc.) qui peuvent ensuite être librement consultées et utilisées par le client.

Le PaaS, ou *Platform-as-a-Service* est entre les deux : le fournisseur met à disposition ses serveurs Cloud et offre en complément certaines technologies (type système d'exploitation, base de données) permettant de développer des applications[15].

[15] Dodd, Annabel Z. (2019), The Essential Guide to Telecommunications, Sixth Edition, p. 31

Schéma 1.2 : La division des responsabilités entre IaaS, PaaS et SaaS



II. L'éventail des fournisseurs Cloud

À l'échelle mondiale, le marché du Cloud est dominé par des acteurs américains : *Amazon Web Services* (AWS) avait plus de 32 % du marché fin 2020[16] [17], suivi par *Microsoft Azure* avec 20 %. On peut y ajouter *Google*, *IBM* et *Oracle* qui possèdent chacun moins de 10 % du marché mondial. Le plus grand fournisseur non-américain est le chinois *Alibaba*, avec une part du marché mondial en 2020 de 5 %, légèrement devant *IBM*, ce qui en fait le 4e acteur mondial.

En France, ces grands acteurs sont également prépondérants mais **partagent le marché avec plusieurs entreprises tricolores de premiers plans.** Les deux principaux acteurs du Cloud français sont *OVHcloud*, basé à Roubaix et *Dassault Systèmes* avec sa solution *3DS Outscale*, les deux entreprises ayant reçu l'accréditation de sécurité *SecNumCloud* de l'ANSSI[18] pour leurs solutions de Cloud privé[19]. À ces acteurs hexagonaux, on peut ajouter *Orange Business Services* et *Scaleway* sur l'IaaS, et *Oodrive*, spécialisée sur les offres SaaS.

III. L'intérêt pour l'État : Le Cloud pour quoi faire ?

Si, comme le rappelle l'entrepreneur Tariq Krim, faire appel au Cloud c'est prendre le risque d'utiliser *« l'ordinateur de quelqu'un d'autre »*[20], la forte augmentation de son utilisation repose sur plusieurs avantages concrets :

• Un **coût compétitif** pour les utilisateurs, avec une tarification basée sur l'utilisation effective du service (le fameux *pay-as-you-go*) à comparer avec

[16] Synergy Research Group (2021), "Cloud market ends 2020 on a high while Microsoft continues to Gain Ground on Amazon", 2 février 2021

[17] Le chiffre ne prend en compte que les marchés de l'IaaS, du PaaS et de l'hébergement de Clouds privés ; le SaaS est donc exclu

[18] L'ANSSI est l'Agence nationale de la sécurité des systèmes informatiques, agence sous tutelle du Premier ministre et qui a la charge de veiller à la sécurité de l'infrastructure informatique de l'État français

[19] L'Usine Digitale (2019), « Le Cloud de Dassault Systèmes labellisé Cloud de confiance par l'ANSSI », Vitard, Alice, 4 décembre 2019 https://www.usine-digitale.fr/article/le-cloud-de-dassault-systemes-labellise-cloud-de-confiance-par-l-anssi.N910209 [dernier accès 27 février 2021]

[20] Krim (2021), « Lettre à ceux qui veulent faire tourner la France sur l'ordinateur de quelqu'un d'autre », Tariq Krim, 14 juillet 2021

des amortissements importants pour un *data center* en propre.

• Une **flexibilité de service,** avec la possibilité d'augmenter rapidement le stockage et la puissance de calcul utilisée, et donc de s'adapter rapidement aux besoins des clients. Si une entité - entreprise ou État - souhaite par exemple tester un nouveau produit ou une nouvelle application, elle peut faire appel de manière temporaire à une capacité de calcul accrue.

• Une **simplicité d'usage** pour le client, celui-ci ne gérant plus directement le maintien opérationnel des infrastructures et des applications (opérations d'administration, maintenances et mises à jour).

• Une **garantie de sécurité**, les fournisseurs de Cloud possédant des capacités de cyber-protection bien supérieures à ce que peut allouer une entreprise ou entité non spécialisée. En 2017, *Microsoft*, parmi les rares entreprises à publier des chiffres sur le sujet, annonçait un budget annuel de 1 milliard de dollars par an pour des activités de recherche et de développement en cybersécurité[21].

• Une **accessibilité** du service qui passe par internet plutôt que par un réseau privé. Ceci permet à la fois d'augmenter le nombre d'utilisateurs mais aussi de permettre des connexions distantes (par exemple pour le télétravail).

Ces avantages peuvent se résumer de manière assez simple pour l'État. Du côté des DSI[22] des différents ministères et autres administrations, l'utilisation d'une infrastructure Cloud de type IaaS ou PaaS **permet aux équipes de se focaliser sur la fourniture des services**, et non plus sur l'environnement de programmation et la gestion physique du *data center*. Du point de vue des fonctionnaires et des citoyens, cela doit se traduire par un développement plus rapide de nouvelles applications et une plus grande flexibilité d'utilisation des services existants. De plus, pour des applications à diffusion très large (traitement de texte, logiciels de RH et de paie, etc.), le recours à des applications commerciales de type SaaS peut permettre à l'État d'allouer des ressources à des tâches à plus forte valeur ajoutée (développement des applications les plus spécifiques et les plus critiques). Un autre avantage à mentionner est que les compétences « Clouds » sont valorisables de la même manière partout : quelqu'un qui a appris à utiliser un système dans le privé pourra facilement mettre en application ces connaissances dans l'administration. Cela **facilite énormément le recrutement et la montée en compétences des équipes.**

B. L'histoire mouvementée du Cloud étatique

I. L'ébauche d'une stratégie de Cloud à la française

À l'aube de l'envol du Cloud au début des années 2010, l'État français entame une réflexion sur celui-ci. Sous le quinquennat du président Sarkozy, plusieurs éléments motivent une prise de conscience des décideurs :

• Le désir de faire de la France un acteur industriel précurseur sur le Cloud et de bénéficier des retombées économiques

• La crainte de voir des acteurs américains dominer une innovation appelée à devenir la norme de stockage de données, pour les entreprises en Europe comme dans le reste du monde

• Le désir de s'appuyer sur le Cloud pour accélérer la digitalisation des services publics

[21] Reuters (2017), "Microsoft to continue to invest over $1 billion a year on cybersecurity", Cohen, Tova, 26 janvier 2017

[22] Direction des Services Informatiques

Ceci aboutit au lancement du projet Andromède en 2011, visant à créer un géant français du Cloud en rassemblant des acteurs de pointe, avec en premier lieu *Orange* et *Dassault Systèmes*[23]. À l'origine, ce projet vise à fournir au secteur privé et public une alternative aux offres des géants américains. Si l'État prévoit initialement d'allouer un montant de 150 millions d'euros à un consortium mené par *Orange* et *Dassault Systèmes*, les désaccords entre les deux parties aboutissent à l'émergence de deux projets, chacun recevant 75 millions d'euros. Du côté de *Dassault Systèmes*, on verra émerger *Numergy*, qui deviendra finalement filiale de *SFR* et *Bull*[24]. Du côté d'*Orange*, c'est *Cloudwatt* qui fait son apparition avec un catalogue de services destiné à la fois à l'État et aux entreprises.

Le développement de ce « Cloud souverain » a été pensé en parallèle d'une politique plus large de mutualisation et de rationalisation de l'infrastructure informatique de l'État. Ces programmes, menés par la Direction Interministérielle du numérique et du système d'information et de communication (DINSIC), comportent à l'époque plusieurs volets liés au stockage des données :

- Le Projet TCI (Transformation des Centres Informatiques), lancé en 2013 avec pour but de réduire le nombre de *data centers* utilisés par des agences de l'État, pour passer de 120 en 2012 à 20 en 2022[25]
- La fourniture de solutions de Cloud externes pour les administrations
- La constitution, en parallèle, de Clouds internes pour quatre ministères

Ces deux derniers points sont le socle d'une stratégie de Cloud qualifiée « d'hybride », car associant des approches différentes. La première approche est l'utilisation d'un Cloud externe, dont l'achat est réalisé par le Service des Achats de l'État (SAE) auprès d'*Orange Business Services* (OBS)[26]. Destinée aux applications et données à sensibilité moindre, cette offre est lancée en 2015[27]. Avec l'intégration de *Cloudwatt* dans *OBS* en 2015, la transformation numérique de l'État rejoint le projet Andromède. *OBS* exprime en effet le souhait de faire de *Cloudwatt* la base d'une offre de Cloud souverain à destination des institutionnels[28].

La deuxième approche dans cette stratégie est le soutien au développement par certains ministères de leurs propres Clouds. Le Programme Investissements d'Avenir (PIA) de la Caisse des Dépôts de l'État a permis de financer plusieurs projets de Clouds internes des ministères de type IaaS et basés sur les logiciels *OpenStack*[29] :

- Le ministère de l'Agriculture et de l'Alimentation et le ministère de la Transition écologique et solidaire ont travaillé au développement d'*OSHIMAE*, sur la base d'un budget autour de 40 millions d'euros[30]. *OSHIMAE* en particulier héberge depuis

[23] Noro, Pierre (2020), « Le Cloud souverain est de retour : généalogie d'une ambition emblématique de la souveraineté numérique en France », 20 juillet 2020, SciencesPo chaire Digital, Gouvernance et Souveraineté https://www.sciencespo.fr/public/chaire-numerique/2020/07/20/cloud-souverain-genealogie-ambition-emblematique-souverainete-numerique/ [dernier accès le 3 mars 2021]
[24] Les Échos, « Une page se tourne pour le cloud souverain français », Florian Debès, 1er août 2019
[25] Bilan DINSIC 2017-2018
[26] Jerôme Martin, Jerôme de Badereau, « Le Cloud, plus que jamais un élément majeur de la transformation numérique de l'État », BearingPoint, 2017 https://www.bearingpoint.com/fr-fr/blogs/blog-secteur-public/le-cloud-plus-que-jamais-un-élément-majeur-de-la-transformation-numérique-de-létat/
[27] "Le Cloud, plus que jamais un élément majeur de la transformation numérique de l'État", BearingPoint
[28] Orange Business Services (2017), « Orange Business Services lance en France son nouveau cloud public et renforce son offre mondiale de services », 5 juin 2017, https://www.orange-business.com/fr/presse/orange-business-services-lance-en-france-son-nouveau-cloud-public-et-renforce-son-offre [dernier accès le 7 mars 2021]
[29] BearingPoint (2020), « Le Cloud, plus que jamais un élément majeur de la transformation numérique de l'État »,
[30] Le Monde de L'informatique (2018), « Les grands projets IT de l'État dérapent », Filippone, Dominique, 27 mars 2018

janvier 2019 l'application Géoportail de l'Institut Géographique National, ce qui représente une des réussites les plus importantes à date de cette stratégie de Cloud

• Le ministère de l'Intérieur a développé *CloudPI*, déplaçant par exemple des services comme la gestion des demandes d'asile et des permis de conduire sur cette solution Cloud

• Enfin, le ministère de l'Économie et des Finances a également développé son Cloud, appelé *NUBO Cloud*

L'objectif de ces Clouds ministériels était de fournir des solutions à la fois pour les ministères eux-mêmes, mais aussi pour les autres administrations de l'État.

Néanmoins, cette stratégie de Cloud hybride n'a pas entraîné l'adoption espérée par les stratèges numériques de l'État. Les administrations publiques n'avaient que peu l'habitude du travail avec des prestataires privés, et n'ont pas adopté les solutions proposées aux niveaux attendus. D'après nos interviews auprès des administrations publiques, le problème principal était celui d'un manque d'acculturation et de maturité sur le sujet : les DSI et les administrations n'étaient pas prêtes à l'époque pour le Cloud. Résultat : **en 2018, seules 60 applications de l'État étaient stockées sur le Cloud**[31]**.** De plus, la solution de type IaaS retenue exigeait un fort investissement pour maintenir l'environnement de programmation. Enfin, pour ce qui est de l'utilisation des Clouds ministériels par d'autres administrations de l'État, deux problèmes supplémentaires se sont posés : l'épineuse question de la facturation interministérielle et la réticence de certains ministères à faire héberger leurs applications chez leurs confrères.

Avec du recul, l'erreur « philosophique » de l'État français sur toute cette période aura été de favoriser l'aspect l'infrastructure, alors que la valeur dans le Cloud se déportait sur les logiciels. En effet, comme le rappelle Tariq Krim[32], les GAFAM eux-mêmes ne possèdent pas leurs *data centers*, car *« la question est ce qu'on fait tourner sur les machines »* plutôt que les machines elles-mêmes.

II. 2018 : Une relance de la stratégie Cloud

En 2018 est publiée une nouvelle doctrine de modernisation de l'État, dont un des chantiers principaux est celui du Cloud. En effet, le 3 juillet 2018, le secrétaire d'État chargé du numérique de l'époque, Mounir Mahjoubi, annonce la stratégie du gouvernement pour développer l'utilisation du Cloud par les administrations, les établissements publics et les collectivités territoriales sur une échelle de 3 ans. En clair, l'État français souhaite que ses administrations stockent leurs données et leurs applications sur le Cloud. Pour cela, il va mettre en place une offre de type IaaS organisée en trois couches différentes[33] :

• Le **Cloud interne** pour les applications les plus sensibles, qui sera hébergé entièrement par l'État et accessible via un portail interministériel. Ce Cloud interne est également appelé **Cercle I.**

• Le **Cloud dédié** pour les données et applications à sensibilité moindre, qui sera hébergé par des prestataires externes mais sous la supervision de l'ANSSI. Ce Cloud est appelé aussi **Cercle II** et concerne essentiellement des données du

[31] Journal du Net (2019) « OVH et Dassault Systèmes prêts à contribuer à un nouveau Cloud souverain », 7 octobre 2019, Antoine Crochet-Damais https://www.journaldunet.com/solutions/cloud-computing/1446589-ovh-et-dassault-systemes-prets-a-contribuer-a-un-nouveau-cloud-souverain/

[32] Entretien avec Tariq Krim, 24 septembre 2021

[33] Numerique.gouv.fr (2018), « Le gouvernement annonce sa nouvelle stratégie en matière de Cloud », 3 juillet 2018, communiqué officiel https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-en-matiere-de-cloud/

ministère de l'Intérieur et de la défense.

• La troisième sera un **Cloud externe** pour les données et applications les moins sensibles se basant sur des offres de Cloud public de prestataires externes. Parmi les données contenues sur ce Cloud, aussi appelé **Cercle III**, on trouvera notamment des données de fonctionnement des collectivités locales (e.g., entretien des espaces verts, nettoyage public, etc.). Le Cercle III concerne, à long terme, la vaste majorité des données et applications que l'État souhaiterait voir transférées sur le Cloud.

Derrière ces changements de paradigme, on distingue **plusieurs changements de principes.** Les objectifs de 2012 sont réaffirmés : le développement rapide de nouvelles applications pour les services publics, l'amélioration du travail en mobile et l'optimisation des coûts.

Les compétences de programmation existant déjà dans le secteur public, l'utilisation du Cloud en IaaS permet d'offrir un environnement de programmation ou la mise en place d'applications est beaucoup plus aisée et plus rapide. Par exemple, pour tester une nouvelle application, l'État peut rapidement commander plus de puissance de calcul via des Clouds pour une durée de temps limitée avec une facturation basée sur le temps d'utilisation (en l'occurrence, une facturation à la seconde).

Parmi les objectifs annoncés pour cette nouvelle politique : atteindre 200 applications publiques sur le Cloud en 2022 et 25 % d'effectifs outillés pour le travail en mobile (contre 60 et 5 % en 2018 respectivement)[34].

Autre changement de doctrine majeur : **les appels d'offres n'incluent pas de préférence nationale.** C'est un bouleversement par rapport au « Cloud souverain » initialement annoncé en 2012. Ce changement de cap est dicté par une réalité décevante : les fournisseurs de Cloud nationaux que l'État voulait déployer, *CloudWatt* et *Numergy*, n'ont remporté l'adhésion ni des administrations ni du secteur privé. Ce qui se traduit par la fermeture de ces deux services, *Cloudwatt* ayant fermé le 1er février 2020[35]. Même s'il reste des acteurs nationaux, comme *OVHcloud*, *3DS Outscale* ou encore *Dassault Systèmes*, le gouvernement Macron a considéré qu'il serait difficile de se passer entièrement d'acteurs de nationalité étrangère pour construire un Cloud étatique. La notion de « Cloud souverain » a donc progressivement disparu dans le discours officiel, au profit d'un « Cloud de confiance ».

[34] Journal du Net (2019) « OVH et Dassault Systèmes prêts à contribuer à un nouveau Cloud souverain », 7 octobre 2019, Antoine Crochet-Damais
https://www.journaldunet.com/solutions/cloud-computing/1446589-ovh-et-dassault-systemes-prets-a-contribuer-a-un-nouveau-cloud-souverain/

[35] Les Échos, « Une page se tourne pour le cloud souverain français », Florian Debès, 1er août 2019

Tableau 1.1. Récapitulatif des déploiements Cloud de l'État tels que prévus en novembre 2018[36]

Implémentation Cloud	Type de donnée ou de services	Organisme responsable	Date de livraison
Cercle I (Cloud interne de l'État)	Données et applications les plus sensibles à garder à l'intérieur de l'État	Ministère de l'Économie et des Finances[37]	2019 avec finalisation en 2020
Cercle II (aussi appelé Cloud dédié et Cloud partenarial)	Données à caractère intermédiaire (essentiellement ministère des Armées et ministère de l'Intérieur)	Ministère des Armées, Direction Interministérielle du numérique (DINUM[38])	N/A
Cercle III (Cloud externe - basse sensibilité des données)	Données de fonctionnement de certaines administrations, offre de services pour les administrations de l'État	État avec Capgemini en charge d'intégrer les services de stockage et les applications proposées par 8 fournisseurs de Cloud public	Début 2021
Architecture Cloud européenne (Gaia-X)	Architecture et normes pour des services de Cloud européens	Consortium Gaia-X de plus de 200 entreprises et administrations, encadré par la coopération gouvernementale franco-allemande	Premiers services disponibles en 2021
Déploiement d'applications diverses (codées par l'État ou bien fournies en SaaS)	Exemples d'applications codées par l'État : • Messagerie instantanée de l'État (Tchap) • Service de vidéoconférence (Jitsu), Exemple de SaaS : service de gestion des rendez-vous de vaccination dans le cadre de la lutte contre la COVID-19 (Doctolib)	DINUM	2020

[36] Tech.gouv.fr, « Accélérer la transformation numérique du service public : Stratégie et Feuille de Route 2019-2021 », 2019, https://www.numerique.gouv.fr/uploads/TECH-GOUV_2019-2021.pdf [dernier accès le 27 février 2021]

[37] Tech.gouv.fr, « Accélérer la transformation numérique du service public : Stratégie et Feuille de Route 2019-2021 », 2019, https://www.numerique.gouv.fr/uploads/TECH-GOUV_2019-2021.pdf [dernier accès le 27 février 2021]

[38] La DINSIC est devenue en 2019 la Direction Interministérielle du Numérique (DINUM)

À ces trois couches, on peut ajouter le projet Gaia-X, officialisé en juin 2020[39]. Celui-ci correspond néanmoins davantage à la volonté de créer des normes communes, en définissant une architecture multicloud et un cahier des charges de sécurité, qu'à la création d'un nouveau Cloud. Il s'agit en pratique d'un projet de « Méta-Cloud » qui vise à rendre interopérables les différentes offres développées par les participants du projet. Ces offres sont d'origine à la fois européennes et extra-européennes, comme les Chinois *Alibaba Cloud* et *Haier Cosmo IoT Ecosystem Technology* ou les Américains *AWS, Google Cloud* ou *Azure*.

Le Cercle III, contenant les données les moins sensibles (comme les données de fonctionnement des services publics des collectivités territoriales) **est devenu opérationnel fin janvier 2021.** Pour mettre en place ce Cercle III, l'État français a mandaté *Capgemini* - à la suite d'un appel d'offres - afin de consolider les offres commerciales de 9 fournisseurs différents, dont *AWS*, *Oracle* et *OVHcloud*. *Capgemini* fournit un catalogue de ces services Cloud et un portail d'accès unique pour le provisionnement par les administrations, en coopération avec l'Union des groupements d'achat publics (UGAP). Pour favoriser l'adoption, l'État a souhaité rendre l'offre commercialement intéressante, avec notamment la possibilité pour les administrations de provisionner rapidement de la puissance de calcul supplémentaire et de régulariser a posteriori les contrats.

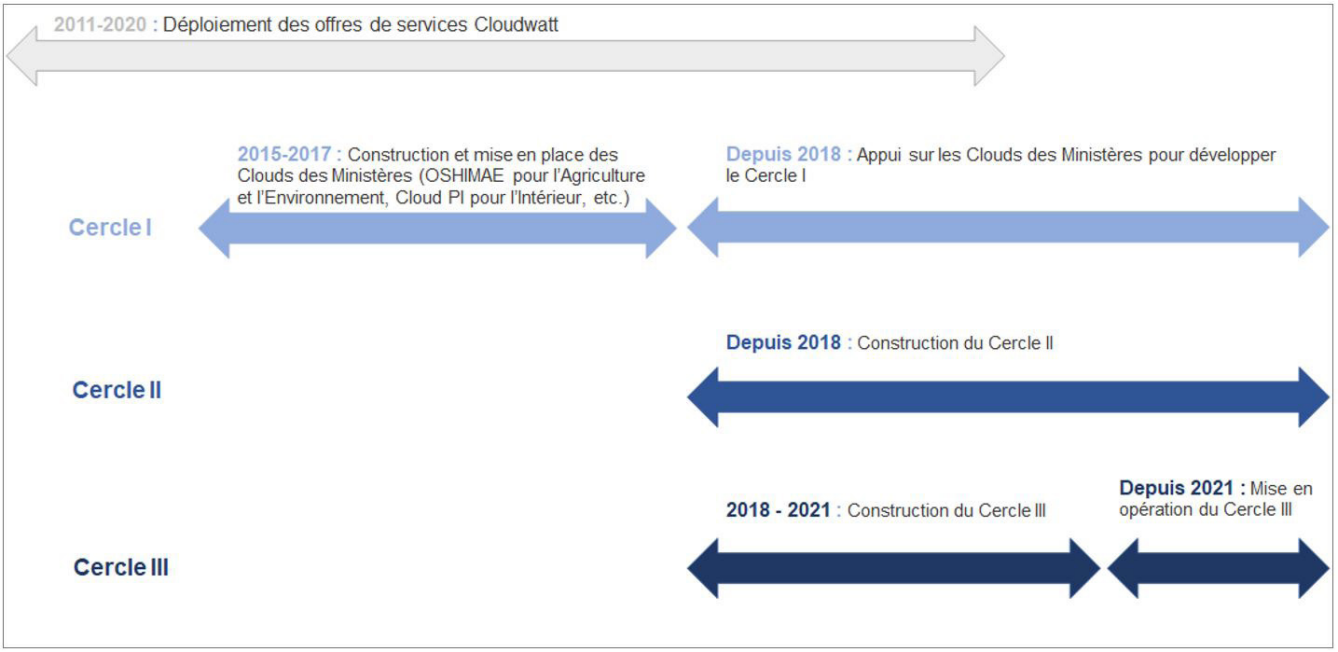
Le Cercle I, lui, s'appuie sur les Clouds développés par les ministères entre 2015 et 2017, notamment celui de Bercy. À ce stade, **l'État ne prévoit pas de s'appuyer sur des prestataires externes pour les services d'infrastructure du Cercle I.**

Le Cercle II était prévu dans la continuité du Cercle III, mais devait contenir des données plus sensibles, essentiellement du ministère de l'Intérieur et du ministère de la Défense. Pour ce faire, l'État songeait à s'appuyer uniquement sur des fournisseurs qualifiés *SecNumCloud* par l'ANSSI. Ce qui aurait amené potentiellement l'État à se baser sur un nombre d'acteurs réduit par rapport au Cercle III, puisque, en ce qui concerne l'IaaS, seuls deux acteurs (*Outscale et OVHcloud*) ont été jusqu'ici accrédités. La disparition du Cercle II est néanmoins actée au mois de mai 2021[40].

[39] Ministère de l'Économie (2020), « Concrétisation du Projet "Gaia-X", une infrastructure européenne de données », 4 juin 2020 https://www.economie.gouv.fr/concretisation-projet-gaia-x-infrastructure-europeenne-donnees [dernier accès le 16 mars 2021]

[40] Ministère de la Transformation et de la Fonction Publiques, « Doctrine "Cloud au centre de l'État" »

Schéma 2 : la mise en place des différents cercles dans le temps, tels que prévus en novembre 2018



Parmi les services Cloud déployés avec succès par l'État, on peut citer la Caisse Nationale des Allocations Familiales (CNAF) qui a dématérialisé 100 % de la gestion de la Prime d'Activité sur le Cloud d'*Oracle* avec l'ambition d'améliorer les calculs des allocations, réduire les délais de traitement et se diriger vers le « zéro papier »[41]. De même, lors de la crise de la COVID-19, confrontée à une hausse massive des demandes d'indemnités de chômage partiel, l'Agence de services et de paiements de l'État (ASP) a eu recours au Cloud privé d'*Oracle* pour répondre à la hausse des demandes. Plusieurs millions de demandes ont ainsi pu être traitées en quelques jours[42]. Depuis l'introduction du Cercle III en janvier 2021, plusieurs nouvelles applications ont également été lancées avec succès, en particulier la nouvelle application de visioconférence du ministère de l'Éducation nationale.

III. La nouvelle doctrine Cloud du 17 mai 2021 : point de rupture ou maintien du cap ?

Le 17 mai 2021, la stratégie Cloud de l'État français prend un nouveau tournant avec la publication d'une nouvelle feuille de route[43].

Il s'agit désormais **d'aller au-delà de l'infrastructure et de publier une doctrine de l'État pour le PaaS et le SaaS,** afin de garantir une augmentation de l'utilisation du Cloud par les administrations. Cette dimension SaaS / PaaS est baptisée « Cloud pour les utilisateurs », par opposition au « Cloud pour les équipes informatiques » qui recouvre l'IaaS.

[41] Oracle (2020), « La CNAF dématérialise la Prime d'Activité sur le Cloud Oracle : 11 millions de simulations pour près de 2 millions de bénéficiaires sur trois mois » https://blogs.oracle.com/oracle-france/la-cnaf-dematerialise-la-prime-d-activite-sur-le-cloud-oracle

[42] Acteurs Publics (2020), « Cloud et transition numérique », Carassou, Justine, 3 juillet 2020 https://www.acteurspublics.fr/web-tv/emissions/acteurs-publics-solutions/cloud-et-transition-numerique [dernier accès le 27 février 2021]

[43] numérique.fr (2021), « Stratégie nationale pour le Cloud : Dossier de presse », 17 mai 2021

Cette nouvelle stratégie s'articule en trois points :

• La **mise en service du label « Cloud de confiance »,** qui permet d'émettre des permis, ou licences, autorisant les acteurs certifiés, qu'ils soient européens ou extra-européens, à proposer des services PaaS et SaaS en direction des administrations publiques. S'adaptant à cette nouvelle doctrine, *Orange* et *Capgemini* ont annoncé le 27 mai leur projet de lancer ensemble une nouvelle société, *Bleu*, qui fournira directement les services Cloud aux administrations publiques[44]. *Bleu* commercialisera les services PaaS et SaaS *Microsoft Azure*, permettant ainsi au géant américain de desservir le marché des administrations françaises.
• La **politique vis-à-vis de l'IaaS**, lancée en novembre 2018, est **maintenue et rebaptisée « Cloud au centre »**, en écho aux politiques *Cloud first* adoptées par le Royaume-Uni et l'Australie, l'idée étant que les administrations sont fortement incitées à choisir en priorité le Cloud plutôt que les *data centers* traditionnels.
• Le troisième pilier de cette nouvelle doctrine est un **renforcement du soutien aux projets Cloud jugés stratégiques**, et notamment le projet paneuropéen Gaia-X.

L'ensemble de l'offre IaaS pour les administrations (Cercle I, II et III) est refondue sous le nom de « Cloud pour les équipes informatiques ». Derrière ce changement sémantique, l'offre IaaS de l'État français est refondue avec la disparition du Cercle II. Cette offre IaaS s'articule désormais en deux volets[45] :

• Le « Cloud interne de l'État » remplaçant le Cercle I et s'appuyant désormais sur deux Clouds internes : celui de l'Intérieur et celui de Bercy
• Le « Cloud commercial » remplaçant le Cercle III et concernant les offres destinées au reste des administrations non couvertes par le cloud interne

Avec le coup d'accélérateur que représente la publication de cette nouvelle doctrine, il est imaginable que d'autres prestations sociales, dont le RSA, soient délocalisées vers le Cloud pour renforcer leur capacité de traitement et leur efficacité. Ces exemples rappellent l'argument principal autour du déploiement d'un Cloud public : la rapidité de la mise en service de nouvelles applications, grâce à la modularité de la puissance de calcul mise à disposition en évitant l'obsolescence et en minimisant l'entretien nécessaire des applications hébergées sur le Cloud.

En adoptant l'utilisation du Cloud, l'État français suit donc la trajectoire de nombre de ses entreprises. Entre le déploiement Cloud d'un État et d'une entreprise, les objectifs recherchés sont souvent les mêmes : agilité dans le développement d'applications, déchargement des responsabilités et maîtrise des coûts. Pourtant, alors que les acteurs du privé valorisent le fait de ne pas devoir mettre en place leurs propres actions de cybersécurité et d'obtenir des économies de coûts, pour l'État qui manie à la fois les données de tous les citoyens et des données de défense nationale, **il est impossible de se dispenser d'une prise en compte accrue des questions de sécurité.**

[44] Orange (2021), « Capgemini et Orange annoncent le projet de créer « Bleu », une société qui fournira un « Cloud de Confiance » en France », 27 mai 2021

[45] Ministère de la Transformation et de la Fonction Publiques, « Doctrine "Cloud au centre de l'État" »

Cloud et Sécurité : quels enjeux pour quelles responsabilités ?

A. Quels sont les risques liés à l'utilisation du Cloud ?

Comme évoqué en introduction, les cyberattaques (qu'elles concernent ou non le Cloud) ne cessent d'augmenter en nombre et en intensité. Entre janvier et avril 2020, en conséquence du confinement lié à la COVID-19, celles-ci ont augmenté de 630 %[46]. Ainsi, même si les avantages des solutions Cloud pour l'État français semblent clairs, il convient en priorité de s'assurer que ces outils répondent à ce défi de sécurité.

3 grands types de risques peuvent ainsi être distingués :

- **Les risques physiques** via le *data center* ;
- **Les risques numériques** via une intrusion dans le système d'administration ;
- **Les risques humains,** via une erreur de manipulation et/ou de configuration de l'outil de la part des utilisateurs.

Risques physiques :

Une intrusion physique malveillante, ou une inadvertance au sein d'un *data center* peut entraîner la destruction de serveurs, le démarrage d'incendies, ou encore le vol de matériel contenant des données. Ce type de menaces qui pèsent sur l'équipement informatique, englobe également les risques liés à l'environnement.

Beaucoup de ces menaces sont généralement contrôlées par des fonctionnalités intégrées. Par exemple, les systèmes d'onduleurs contrôlent la qualité de l'alimentation, la charge et l'état des batteries au sein du *data center* ; les distributeurs d'alimentation contrôlent les charges des circuits ; les unités de refroidissement surveillent les températures d'entrée, de sortie et l'état du filtre ; les systèmes d'extinction incendies vérifient la présence de fumée et de chaleur[47]. Ces contrôles suivent des protocoles souvent pilotés par des systèmes logiciels qui regroupent, consignent, interprètent et affichent les informations.

Face au risque de destruction et/ou de compromission des serveurs, la majorité des grands fournisseurs de Cloud disposent de sauvegardes (appelées « *Disaster recovery* »). Ces infrastructures de secours sont généralement installées à plusieurs centaines de kilomètres du serveur principal et permettent de garantir une continuité des opérations - sans interruption - et la sécurité des données, même lorsque l'infrastructure principale est entièrement détruite.

[46] Rapport McAfee (2021)

[47] Livre Blanc 102 Schneider Electric - Contrôle des menaces physiques dans les datacenters

Zoom

Les Certifications : comment apporter de la lisibilité

De l'extérieur, il n'est pas toujours évident pour un client d'avoir de la visibilité sur le niveau de risque physique des *data centers* d'un fournisseur de Cloud potentiel. **Une des manières de corriger cette asymétrie d'information est le recours à des certifications externes.**

Une des certifications les plus reconnues est celle du *Uptime Institute* qui classe les centres de données en quatre niveaux correspondant à des critères de maintenance, d'alimentation, de refroidissement et de capacité de détection des pannes[48]. À titre d'exemple, le niveau de redondance d'un *data center* est un des éléments pris en compte dans cette catégorisation.

Autre source d'informations importante, les certifications SOC (*Service Organization Control)* permettent de garantir qu'une infrastructure a été évaluée dans le cadre d'un audit.[49]

- SOC 1 : Auto-certification du fournisseur, avec valeur informative limitée
- SOC 2 de type 1 : Analyse théorique des contrôles de sécurité
- SOC 2 de type 2 : Audit réalisé pour valider cette analyse théorique
- SOC 3 : Certification correspondant à l'obtention d'un papier certifiant

Si ces certifications ne sont qu'un des éléments permettant d'éclairer la décision de l'État, et ont nécessairement un impact sur le coût total d'un service, elles n'en demeurent pas moins une garantie que ce dernier doit prendre en compte.

Risques numériques :

La première catégorie de menaces numériques est celle liée au piratage informatique. Dans un article de 2019, Loïc Guézo, Stratégiste Cybersécurité à *Trend Micro* explique que plus de **59 000 entreprises en Europe ont déjà signalé des vols de données aux instances de contrôle RGPD**[50]. Face à cette montée des risques, les serveurs doivent être équipés d'antivirus, de firewall, ou de solutions visant à limiter la possibilité d'attaques (*type Denial of Service (DoS)* - c'est à dire des attaques qui visent à surcharger un serveur en multipliant les demandes d'accès).

[48] Site internet Uptime Institute
[49] https://www.itgovernance.eu/fr-fr/audits-et-rapports-soc-fr
[50] DC Magazine (2019), Sécuriser les datacenter d'aujourd'hui : comment protéger les investissements digitaux ?

Zoom

L'Intelligence artificielle au service de la cyberdéfense

Les progrès technologiques et la pénétration des techniques d'intelligence artificielle dans la cyberdéfense ont progressivement permis de complémenter la protection et l'étanchéité du Cloud. Que cela soit en développant les capacités de détection des menaces (A) ou en améliorant la protection du Cloud (B), l'IA apporte un soutien significatif à la prévention des risques.

A. Détecter avant d'être impacté : L'IA au service de la détection

• Traiter et analyser les données de connexion

Le flux de données traité sur les Clouds est en constante augmentation. Avec le phénomène COVID, et son impact sur le télétravail, cette tendance s'accélère avec aujourd'hui des milliards de points d'entrée ou de localisation d'utilisation Cloud. Les volumes de données concernés sont ainsi gigantesques et ne peuvent pas être traités manuellement. **Le premier intérêt de l'IA est tout simplement de rendre possible la gestion de ces flux.**

Une des manières classiques de traiter cette problématique est d'utiliser un SIEM (*Security Information and Event Management*) récupérant les logs utilisateur et mettant en place des règles. Avec l'IA, les fournisseurs de Cloud sont en mesure de mettre en place une *baseline utilisateur* (c'est-à-dire une modélisation des comportements habituels) qui permet d'identifier facilement les menaces et de les bloquer automatiquement.

• La sonde de détection

Tout l'enjeu d'une technologie de détection est d'intercepter de potentielles anomalies dans les flux de données vers et depuis le *data center*.

Les sondes de détection sont des *hubs* sur lesquels sont branchés plusieurs ports Ethernet. Une fois connectées au système, ces sondes peuvent **analyser les paquets-réseau à leur portée, à la manière d'une caméra de surveillance.** Par exemple, si l'intranet d'une entreprise est relié à l'extérieur, déployer une sonde entre les deux parties peut permettre de repérer un trafic inhabituel, des fuites de paquets de données non autorisées, ou remarquer un décalage de plusieurs secondes indiquant qu'un individu essaie de télécharger un virus à l'intérieur du système.

L'intérêt d'un tel système, par rapport à un *firewall* classique, est sa facilité de prise en main par le client. Cette technologie est également prisée car elle **permet des opérations d'autopsie.** À l'image d'une caméra qui capture des images, ce type de technologies peut retenir des flux de données et rejouer des scénarios ou reconstituer des attaques. L'utilisation du *Machine Learning* permet ensuite

de mieux comprendre les événements passés, et d'anticiper les menaces à venir pour s'y préparer de manière optimale.

Des acteurs comme *Thalès* avec *Cybels Sensors* ou *Gatewatcher* avec *TrackWatch* dont les sondes sont homologuées par l'ANSSI[51] permettent de traiter toutes ces données. Il existe de nombreux types de sondes. Elles peuvent varier en termes de périmètres, d'acteurs, de couches, mais également en termes de capacités ou de débits.

B. Apprendre pour se renforcer : L'IA au service de la protection

• Les technologies de remédiation

« C'est bien utile de détecter une attaque ou une menace, mais si je ne suis pas capable de la traiter, cela n'est pas très utile » - *EMEA Cloud Security* et *System Management BDM* chez *Oracle*.

Une technologie de détection seule n'est pas suffisante. C'est pour cette raison que les fournisseurs Cloud offrent également des solutions pour remédier à ces failles, comme *Cloud Guard* d'*Oracle*.

Prenons l'exemple de l'attaque ayant mené au vol des bases de données d'*Uber* - et de 57 millions d'utilisateurs[52]. Cette fuite de données avait été rendue possible par la présence de données sur un segment « public » du Cloud, c'est-à-dire accessible à tous, ce qui avait facilement été capté par des *crawlers* (des logiciels parcourant le web pour analyser le contenu de documents de manière organisée dans un index).

Si une technologie de détection avait permis de remarquer cette erreur, **une solution de remédiation aurait permis d'édicter de nouvelles règles automatiquement pour la rectifier et prévenir la menace.**

Cette dimension auto correctrice de l'IA est également à l'œuvre dans les bases de données autonomes. Composée d'un *data warehouse* et d'un traitement de transactions, la base de données autonomes utilise l'IA pour fournir une automatisation de bout en bout des fonctions *business* (performance, gestions des changements, etc.) mais aussi de la sécurité.
• Tout d'abord une base de données autonome **fonctionne par pilotage automatique**, que cela soit pour les processus de gestion ou de surveillance. Des administrateurs restent nécessaires uniquement pour les tâches administratives (comme la manière dont les applications se connectent à la base de données).

[51] https://www.ssi.gouv.fr/administration/protection-des-oiv/la-cybersecurite-en-action/liste-des-systemes-de-detection-et-des-prestataires-de-detection-prevue-a-larticle-r1332-41-9-du-code-de-la-defense/

[52] Uber : les données de 57 millions d'utilisateurs ont été piratées fin 2016, Le Figaro, le 22 novembre 2017

• Elle se sécurise automatiquement. Au-delà d'une adaptation régulière aux menaces potentielles, l'automatisation des tâches permet, selon *Oracle* - qui développe ce produit - d'éviter les interruptions de service *« une base de données autonomes pouvant nécessiter moins de 2,5 minutes d'interruption de service par mois »*[53].

À cela s'ajoutent les risques liés à la connexion internet utilisée pour accéder de manière distante aux données ou aux applications sur le Cloud. **En effet, la vulnérabilité d'un Cloud est proportionnelle au nombre d'individus qui y accèdent**[54], multipliant les portes d'entrées possibles pour des incidents.

Avec le Cloud, les risques physiques et numériques ne sont plus de la responsabilité du client, mais sont à la charge du fournisseur de service Cloud. Ces risques incluent notamment les risques liés aux *« insiders »,* c'est-à-dire des employés du fournisseur qui peuvent accéder aux données ou aux applications contenues sur celui-ci de manière non justifiée. Cela requiert une capacité de contrôle supplémentaire pour l'entité responsable de la gestion de l'infrastructure à la fois technique, mais à laquelle s'ajoute un sujet sur les accords de confidentialité auxquels sont soumis les employés du fournisseur.

Néanmoins les risques liés aux connexions à distance sont à gérer par le client. Ce risque étant proportionnel au nombre de connexions il peut être l'un des plus critiques. Ceci explique que dans de grandes entreprises, l'accès aux applications et aux données stockées sur le Cloud requiert une authentification multi-facteurs et/ou l'obligation de passer par un VPN pour accéder aux opérations d'administration. De plus, les clients des solutions Cloud louent parfois des applications de sécurité à des entreprises comme *Amazon*, *Alert Logic* ou *Threat Stack* afin d'évaluer le trafic sur leurs Clouds et de repérer des accès ou des comportements suspects[55].

Un autre risque provient du fait que les serveurs de Cloud Public hébergent souvent les données de plusieurs utilisateurs en même temps via une technologie de virtualisation, entraînant potentiellement **une confusion ou un risque d'intrusion dans les données d'un autre client hébergé sur le même serveur.** Dans ce contexte, il devient indispensable d'assurer et de contrôler l'étanchéité des données entre elles. Évidemment, de tels risques intrinsèquement liés au Cloud public, apparaissent moins pertinents pour un État et de grandes entreprises ayant davantage recours à des Clouds privés ou à des serveurs isolés et réservés à l'intérieur de leur propre *data center*.

En termes de risques numériques, la responsabilité dans la préparation et la limitation des dangers est partagée entre fournisseurs et clients. **Le propriétaire des données - dans notre situation l'État - ne peut en aucun cas se passer de mesures de sécurité** spécifiques en plus du service fournisseur.

S'il faut toujours auditer les politiques de cybersécurité de son fournisseur de services, les risques sur le Cloud sont souvent liés à des problèmes

[53] Oracle (2021), "What is an autonomous database?"
[54] Dodd, Annabel Z. (2019), The Essential Guide to Telecommunications, Sixth Edition, p. 55
[55] Dodd, Annabel Z. (2019), The Essential Guide to Telecommunications, Sixth Edition, p. 55

d'accès aux données ou de compliance qui doivent être traités en amont. 90 % des problèmes de sécurité dans le Cloud sont imputables à l'erreur humaine[56]. Par exemple, le fait de sauvegarder un document avec une adresse IP *(Internet Protocol)* publique plutôt que privée.

Des risques numériques amplifiés par un contexte global de cyberguerre

Un monde de grandes puissances aux capacités impressionnantes

En 2011, la révélation des cyberattaques contre les installations de *Natanz* en Iran, jugées centrales pour le programme nucléaire de ce pays, font la démonstration des capacités américaines et israéliennes. Depuis, de nombreuses autres attaques sont survenues, parmi lesquelles on citera *NotPetya* et *WannaCry,* toutes deux survenues en 2017 et soupçonnées d'avoir été orchestrées par des États. À cela s'ajoute la très médiatique attaque de l'année 2020, réalisée contre plusieurs départements d'État américains via les logiciels de l'entreprise *SolarWinds*. Le secrétaire d'État américain de l'époque Mike Pompeo avait attribué cette offensive à la Russie, renforçant un contexte déjà tendu. Ce paysage d'États concurrents est également complexifié par l'action de groupes criminels parfois étroitement liés aux États : c'est le cas par exemple de *WannaCry*, attaque initiée par le *Lazarus Group* lié à la Corée du Nord.

Nous assistons donc à une guerre déjà bien engagée. Des attaques régulières ont en particulier lieu contre des cibles françaises et européennes. Récemment, ce sont les équipes de chercheurs travaillant sur des traitements COVID-19 qui ont été ciblées au Royaume-Uni[57] et en Espagne, et qui auraient respectivement été menées par des hackers russes et chinois[58]. Pour donner un ordre de grandeur, le général Sanders de l'armée britannique, dans une interview au *Financial Times*, évoque une moyenne de 60 attaques quotidiennes contre des installations militaires au Royaume-Uni pour lesquelles une riposte est nécessaire[59].

Un risque limité par des capacités défensives française éprouvées

En France, les prérogatives de cybersécurité sont réparties entre plusieurs agences et ministères. La principale est l'ANSSI, l'Agence nationale de la sécurité des systèmes d'Information, agence dépendante du cabinet du Premier Ministre et chargée de la surveillance des systèmes de l'État ainsi que de la lutte directe en cas d'attaque contre ces mêmes systèmes. L'ANSSI est particulièrement reconnue à l'international pour ses capacités en termes de détection, étant également à l'origine de campagnes d'information importantes sur ce type de problématiques. L'armée française, au travers du *ComCyber*, qui réunit les fonctions de cybersécurité des branches de l'armée, défend ses propres systèmes. Enfin, le ministère de l'Intérieur et la Gendarmerie Nationale ont également leurs forces de cybersécurité.

[56] Interview avec Régis Louis, VP Cloud Oracle, vendredi 15 janvier 2021
[57] AFP, Le Parisien, Vaccin contre le coronavirus : des hackers russes accusés de cibler les recherches britanniques, 16 juillet 2020
[58] El País, Hackers chinos robaron información de la vacuna española para la Covid, 18 septembre 2020
[59] Financial Times (2020), "Top general lifts lid on Britain's cyber attack capability", Warrell, Helen, 25 septembre 2020,

Ce maillage permet à la France d'afficher la sixième place dans le classement *NCPI* du *Harvard Belfer Center*, qui hiérarchise les pays par leur capacité cyber. Mais en regardant uniquement les capacités défensives, la France arrive à la deuxième place mondiale !

Parallèlement à ce savoir-faire défensif, la France est également en développement de capacités cyber-offensives. L'État a notamment détaillé, en 2018, la notion de Lutte Informatique Offensive définie comme « l'ensemble des actions entreprises dans le cyberespace produisant des effets à l'encontre d'un système adverse, pour en altérer la disponibilité ou la confidentialité des données[60] ». Selon Nathan Cook, *Chief Technology Officer* pour l'offre *National Security d'Oracle* et ancien responsable dans les services de cybersécurité australiens, **la France peut être appelée à jouer un rôle majeur sur ces questions au sein de l'OTAN.**

Avec néanmoins des questions qui restent en suspens

Car si l'État français s'appuie aujourd'hui sur de solides compétences dans ce domaine, plusieurs interrogations persistent.

- Comment recruter de nouvelles ressources compétentes, et en nombre suffisant pour répondre en continu aux nouvelles menaces qui se dessinent ?
- Comment doit être établi le partage des responsabilités entre les différents acteurs (et notamment du renforcement de la coopération européenne) ?
- Comment assurer une coopération entre alliés sur les questions de cybersécurité qui reste aujourd'hui compliquée, malgré la signature d'un engagement de l'OTAN en 2016 et la création de l'ENISA, l'Agence européenne de cybersécurité basée à Athènes ?
- Quel doit être le rôle de la doctrine offensive dans une perspective de défense ?

[60] Doctrine Militaire de Lutte Informatique Offensive (LIO) - ComCyber, ministère des Armées

Interview

Avec Nathan Cook, le 25 janvier 2021
Nathan Cook a fait carrière au département de la Défense australien avant de rejoindre Oracle, dont il est aujourd'hui Chief Technology Officer (CTO) pour les clients Sécurité & Défense nationale.

Quel est votre avis sur la récente attaque SolarWinds ?

« Souvent, les gouvernements prennent des décisions sur la technologie sans réellement prendre en compte les implications [...] en termes des risques et d'acteurs hostiles. Le vrai coût de la sécurité n'est pas visible au premier abord, et des décisions sont souvent prises rapidement. Une mauvaise connaissance du marché et une mauvaise définition du périmètre peuvent amplifier un problème [...]. Beaucoup de gouvernements verront la sécurité comme quelque chose uniquement fournie par des logiciels, alors qu'une imbrication étroite de la sécurité des appareils et des logiciels est nécessaire. Sécuriser les appareils rajoute un niveau de protection en plus, qui réduit les surfaces attaquables [...]. De mon expérience, c'est un des motifs pour lesquels les clients du renseignement et de la défense s'intéressent à notre approche [d'Oracle] pour créer un Cloud déjà hautement sécurisé et ensuite fournir des services « Cloud native ».

La migration des gouvernements vers le Cloud leur permettra de s'appuyer sur la cybersécurité imbriquée dans ces solutions, de sécuriser l'approvisionnement de leurs logiciels et appareils et de s'appuyer sur l'Intelligence artificielle et le Machine Learning pour détecter les intrusions, notamment via des analyses du comportement des utilisateurs. Le Cloud permet une identification des intrusions beaucoup plus rapide et rend plus difficile la tâche de l'adversaire en donnant l'avantage au défenseur. Mais les États doivent accepter de s'appuyer sur les acteurs privés ; il y a bien plus d'expertise en matière de cybersécurité dans le privé que dans le secteur public à cause de la taille et de l'envergure des problèmes auxquels font face les entreprises. De plus, la demande du marché pour ce type d'expertise et les salaires attractifs proposés par les hyperscalers font que les États ont du mal à recruter les profils les plus qualifiés. Privé et public ont un rôle conjoint à jouer pour protéger et sécuriser le cyberespace des acteurs malveillants, et protéger les citoyens.»

Quelles sont les principales technologies utilisées en cyberdéfense ?

« Beaucoup de technologies imbriquées utilisées pour la cyberdéfense sont en train d'être intégrées par défaut dans les solutions commerciales de Cloud. Les fournisseurs ont un intérêt extrêmement fort à protéger leurs clients - leur marque et réputation sont tout aussi importantes que la sécurité des données qu'ils hébergent. De plus, le Cloud offre la possibilité d'exploiter l'IA, le Machine Learning, l'analyse spatiale et graphique, de l'analytique Big Data..., ce que beaucoup dans la défense et la cybersécurité appellent des technologies émergentes, mais qui sont en fait utilisées dans le privé depuis de nombreuses années. Ces technologies sont puissantes au vu de la croissance exponentielle des données. Ces éléments représentent un véritable changement de paradigme pour les

cyber-analystes. Fournir de la sécurité supplémentaire est également devenu beaucoup plus facile à travers les plateformes intégrées et la possibilité de s'appuyer sur des vendeurs spécialisés (e.g. les marketplaces Cloud). Cette imbrication serrée permet de renforcer la sécurité des données tout en offrant aux clients une plateforme ouverte.

Les gouvernements à l'avenir vont se rendre compte qu'ils peuvent prendre l'avantage sur leurs adversaires en utilisant le Cloud, surtout dans le cas du Cloud de seconde génération avec son architecture "zero trust".»

Comment répondez-vous à l'affirmation, selon laquelle, le Cloud Act est un blocage majeur pour travailler avec des entreprises ayant des activités aux États-Unis ?

« Il y a des moyens techniques pour les gouvernements d'adresser leurs inquiétudes vis-à-vis du Cloud Act. Pour avoir été à leur place, je comprends leurs inquiétudes, mais [...] il existe des solutions qui permettent de réduire drastiquement le risque, notamment le contrôle des clés de chiffrement pour s'assurer que le vendeur n'a pas accès à vos données. Le chiffrement des données de bout-en-bout permet de garder la main sur ses données, et de les protéger - y compris vis-à-vis de son fournisseur et des lois extraterritoriales.

Par ailleurs, il y a désormais sur le marché des modèles de sécurité pour assurer la souveraineté des données des Gouvernements dans le Cloud. Quelques bonnes pratiques peuvent être prises en compte, comme l'installation de l'infrastructure dans un data center gouvernemental. Oracle a par exemple des offres dédiées, les National Security Regions, qui sont construites directement dans le pays hôte et opérées par des citoyens accrédités par l'État. Ceci signifie que ces employés sont soumis à la législation nationale du pays hôte pour lequel ils travaillent. Si quelqu'un essayait de partager des données sans autorisation avec des tiers, cela pourrait être considéré comme du travail à la solde d'une puissance étrangère et pourrait entraîner des accusations criminelles et/ou d'espionnage.

Enfin, le Cloud Act n'est pas conçu pour l'espionnage, et les gouvernements de tout acabit ont des outils offensifs bien plus sophistiqués pour ce type d'activités illégales. Imaginer que les autorités américaines utiliseront cet outil juridique pour voler des secrets industriels est un faux débat - et évite de soulever la vraie question : quelle est la résilience de son infrastructure à une cyber attaque ? »

Quelles recommandations feriez-vous au gouvernement français pour lisser le processus de passage sur le Cloud ?

« Le gouvernement français peut faire plusieurs choses
• Tester le Cloud public avec des données peu sensibles, ce qui pourrait aider à convaincre les administrations, ainsi que valider les architectures de sécurité et la conception de l'ensemble.
• Définir une stratégie de données faisant référence à la sensibilité de la donnée, le développement

d'un modèle basé sur les risques, avec de la donnée non-sensible qui peut être stockée dans un Cloud public, et différents contrôles de sécurité pour les niveaux de données les plus sensibles.
• Pour les niveaux de données les plus sensibles, sonder le marché pour comprendre les différentes offres proposées par les fournisseurs - qu'ils soient européens ou non-européens. Contrairement à ce qu'on pense, il y a une grande variété de solutions et d'architectures.
• Définir une stratégie Cloud. Quand on discute de la transformation Cloud, il ne devrait pas y avoir simple transfert de l'existant sans référence à une stratégie plus globale.
• Commencer à réfléchir à l'allocation des responsabilités entre entités et agences gouvernementales.
• Ne pas réinventer la roue. Les géants de la Tech ont investi des centaines de milliards de dollars pour proposer des services performants. Les États ne pourront jamais concurrencer la qualité de ces services. Le mieux est de s'appuyer sur le marché et d'innover en ayant recours à des solutions sécurisées existantes pour accélérer la digitalisation des services publics. Vouloir tout faire soi-même dès le départ signifie que les erreurs et les leçons du passé ne seront pas retenues, ce qui facilitera la tâche des adversaires.
• Concernant la sécurité, l'humain est toujours le point faible, et c'est toujours ce qu'essayent d'exploiter les agences de renseignement étrangères. L'infrastructure Cloud des fournisseurs est généralement très bien sécurisée, mais les clients doivent aussi s'impliquer fortement. Fournir de la sécurité n'est pas qu'une question de réseaux, mais aussi une question de cryptage, de sécurité des bases de données et gestion des identités et des accès. De plus, les clients doivent savoir dans quels écosystèmes les vendeurs Clouds opèrent. Par exemple, Oracle est en train de réduire sa présence en Chine et vous ne trouverez pas de data center Cloud Oracle dans le pays. Il y a un risque à faire affaire avec la Chine car c'est un pays avec l'intention d'exploiter et de comprendre le Cloud pour des objectifs cyber-offensifs. En évitant de placer des Clouds dans des régions à haut risque, nous essayons délibérément d'améliorer notre posture de sécurité et la protection de nos clients.
*• **Enfin, il devrait y avoir une vraie culture d'entraînement et de conscience vis-à-vis des cyber-risques.** Ceci n'est souvent pas vu comme un facteur de risque pour l'État et les entreprises, mais cela devrait l'être.»*

Risques humains :

Au-delà de la mise en place de systèmes de surveillance poussés ou de technologies qui s'améliorent au cours du temps, il est clair que le facteur humain est clé dans la mise en place de systèmes de prévention viables. Dans son baromètre de la cybersécurité des entreprises, le Club des experts de la sécurité de l'information et du numérique (CESIN) a mis en avant l'erreur humaine comme principales causes d'intrusion[61]. Le phishing est cité à 79 % au sein du baromètre, suivi par la fraude au président[62] (47 %). Dans le cadre des cyber-risques identifiés par les dirigeants d'entreprise, 43 % évoquent les négligences ou erreurs de manipulation de salariés ou encore 38 % l'utilisation d'applications non approuvées[63].

[61] 5e Édition du baromètre annuel du CESIN, CESIN et OpinionWay, le 24 janvier 2020
[62] Il s'agit d'un acteur malveillant qui usurpe l'identité d'un supérieur pour obtenir un virement financier
[63] Cyber-Attaques : L'erreur humaine pointée du doigt, Hans & Associées, le 30 janvier 2020

Il existe ainsi un problème de culture cyber, dans l'État comme dans les entreprises. La prévention et la formation, permettant à tous de comprendre les risques de l'utilisation de tels outils est un des leviers d'action les plus importants.

Les mesures de cybersécurité sont souvent contraignantes sur un plan humain, la tentation de ne pas prendre toutes les précautions possibles - à l'image d'une double authentification - pouvant accroître la fragilité aux attaques.

L'ergonomie de l'offre technologique devient alors clé : avoir une technologie performante est important, mais s'assurer que les acteurs amenés à la manipuler ne fassent pas d'erreur est encore plus indispensable.

Mais si le fournisseur de services ou de technologies possède une grande part de responsabilité, celle du client est fondamentale pour prévenir tout risque majeur.

B. La répartition de la responsabilité dans le Cloud : le client au centre du jeu

Le modèle de responsabilité partagée, défini par AWS, distingue la sécurité du Cloud - responsabilité du fournisseur - de la responsabilité dans le Cloud - qui est l'affaire de l'utilisateur[64].

Le gestionnaire, que ce soit un fournisseur de Cloud Public ou un client en Cloud privé, doit ainsi apporter **les garanties suivantes :**

• Un contrôle strict des accès et des privilèges utilisateurs ;
• Un audit strict et une compréhension forte des méthodes de sécurité et de la localisation des *data centers* ;
• Un système de cryptage hermétique et fiable ;
• Un système de sauvegarde (hors-ligne ou dans un « *Disaster Recovery* ») pour les catégories de données les plus sensibles, ou dont la perte serait la plus dommageable pour l'administration.

À ces « indispensables » viennent de plus en plus souvent s'adosser des solutions permettant au client d'être à proximité de ses données, par exemple des solutions de Cloud dédiées, proposant d'installer l'infrastructure dans le *data center* du client – tout en profitant de toutes les technologies et performances du Cloud public.

Une fois ces garanties apportées, **c'est bien l'utilisateur final, et non l'infrastructure Cloud, qui est le maillon critique de la sécurité.** C'est ce que Gartner annonçait en 2019 en introduisant le paradigme SASE (*Secure Access Service Edge*). Les équipes des grands fournisseurs l'ont bien compris et ont renforcé les efforts de sécurité dans cette direction. Aujourd'hui, les mesures de sécurité sont de plus en plus critiques sur le Edge, ou les « points d'accès » virtuels du Cloud.

Le Cloud pose effectivement des nouveaux défis de sécurité avec la multiplication des applications Cloud, les connexions à distance (en-dehors des sites de l'entreprise) et les volumes des flux de données entre le Cloud et les bureaux (plus importantes qu'avec un *data center* traditionnel situé dans l'entreprise). Gartner prévoit que, d'ici 2024, au moins 40 % des entreprises auront adopté des éléments de l'architecture SASE vs 1 % en 2018.

En définitive, la sécurité du Cloud dépend en premier lieu des mesures prises par l'État pour

[64] AWS website, the Shared Responsibility Model

protéger les accès. C'est aussi l'occasion de rappeler que le principal risque cyber auquel font face les organisations n'est pas forcément l'introduction « par la force brute » dans leurs systèmes, mais le vol ou l'utilisation illégale des accès du personnel. La capacité à anticiper et à contrôler les personnes ayant accès aux données de l'État est donc essentielle.

Interview

Extrait - Avec Damien Rilliard, le 12 mars 2021
Damien Rilliard est EMEA Cloud Security & System Management BDM chez Oracle

Que pensez-vous du Cloud Act ?

« […] Il y a beaucoup d'a priori sur ce sujet, notamment qu'il permettrait aux États-Unis d'accéder à n'importe quelles données hébergées chez un fournisseur ayant des activités aux États-Unis : en réalité le Cloud Act apporte simplement un cadre juridique qui - sinon - n'existerait pas et cette loi ne change en rien le niveau de risques pour les entreprises : les gens mal intentionnés ne passent par des lois ou des processus juridiques internationaux pour voler des données confidentielles. Par ailleurs, je rappelle que le Cloud Act est strictement limité aux investigations pénales, comme le terrorisme ou la pédopornographie, et ceci dans un strict contrôle judiciaire. Il ne permet en aucun cas d'accéder librement, et sans discernement, à toutes les données stockées sur les serveurs d'un fournisseur – et les fournisseurs peuvent contester toutes demandes considérées comme abusives ou ne respectant pas les réglementations nationales. Contrairement à ce qu'on pense, les fournisseurs ne sont pas non plus obligés de déchiffrer les données, le chiffrement est donc une arme sans faille contre toutes formes d'extra-territorialité du droit américain, surtout si les clés sont détenues par le client ou un tiers de confiance.»

Quelle technologie utilisez-vous pour la détection des menaces ?

« Nous avons recours à des technologies de pointe sur l'ensemble de nos infrastructures qui donnent en temps réel des informations sur les menaces principales, et permettent de les stopper en temps réel le cas échéant. C'est le cas notamment avec les DoS (Denial of Service attacks) : les fournisseurs doivent eux-mêmes les identifier pour les intercepter et éviter toute interférence sur leurs solutions. Mais ces dernières sont difficiles à anticiper car cela impliquerait d'arrêter le trafic internet mondial. Nous appelons ça de la "threat awareness". Pour avoir des informations sur les cybermenaces tout le monde utilise des sondes réseaux. Elles permettent 1) de comprendre et 2) de prévenir certaines attaques.

*En plus de la partie détection, **il existe tout un portefeuille de solutions** qui ont recours à l'intelligence artificielle et au machine learning (type Oracle Autonomous Database). Ces technologies permettent à nos solutions de détecter automatiquement les menaces et de s'auto-sécuriser.*

À côté de ça, il ne faut pas sous-estimer les risques physiques *: parfois les clients oublient de regarder le niveau de classification des data centers de leurs fournisseurs, c'est-à-dire le niveau de sécurité des infrastructures physiques, le nombre de redondances et le nombre de data centers concernés. Pourtant il s'agit d'un élément très important.* ***Le niveau de classification est clé pour cela*** *- le plus connu est celui du Uptime Institute, qui va du niveau 1 au niveau 4. Plus vous avez de la redondance par exemple, mieux c'est. Mais évidemment, le niveau 4 n'a pas le même prix que le niveau 1.*

Un autre classement intéressant est lié à la totalité des audits et contrôles qu'un fournisseur de cloud a subi. Il peut s'agir d'une certification de type SOC [Service Organization Controls, qui correspond au niveau de détail de l'audit réalisé], avec les applications de la ICPA aux États-Unis, ou type ISO. Par exemple, un SOC 2 Type 2 signifie qu'un auditeur est venu vérifier les mesures de sécurité prises.»

Il y a-t-il d'autres technologies mettant en œuvre de l'intelligence artificielle ?

« Il y a 4 ans nous avons racheté Palerra, une start-up qui est très en pointe sur ces technologies (CAS-B). Ce que rend possible le machine learning c'est de traiter un gros volume de données liées à l'utilisation du Cloud. Concrètement, le ML permet de traiter des milliards de data points que les capacités humaines ne permettent pas de traiter manuellement.

Aujourd'hui la meilleure manière de traiter une menace en temps réel est d'utiliser un Security Information and Event Management pour récupérer les logs utilisateurs, et faire des règles en fonction de leurs habitudes. Le gros problème est alors celui des faux positifs – l'"accuracy". Si vous devez traiter beaucoup de fausses alertes, vous vous retrouvez facilement submergé, vous ne pouvez pas tout gérer et vous risquez de louper la vraie menace. Grâce à l'IA, on est parvenus à diminuer les faux positifs. Nous sommes, par exemple, capables de créer un profil par utilisateur en définissant une baseline. Si une personne commence à avoir une utilisation très différente de son habitude, il y a un risque que cela soit anormal.

Avec cette solution on fait l'analyse à l'intérieur de l'application. Par exemple, au sein d'un ERP, on peut remarquer qu'il y a systématiquement des modifications des salaires de l'entreprise.

1) Si l'entreprise a l'habitude de ce type de changement – rien n'est signalé.
2) Si ce n'est pas le cas, il y a une alerte.

Une fois que l'on a détecté une menace, il faut agir. Chez Oracle, une façon de « boucler la boucle » a été trouvée avec Cloud Access Security Broker – que l'on appelle Cloud Guard – qui permet de bloquer automatiquement les menaces identifiées.

Enfin ***le travail de renseignement est très important****. Les attaques entre États et les attaques de cybercriminels sont différentes et il faut savoir les distinguer, comprendre les différents groupes, leurs liens, leurs activités, ou leurs spécificités. Nous avons des équipes dédiées en Threat Intelligence*

avec leurs propres outils très spécifiques.
Comme vous pouvez le voir – les technologies capables d'utiliser au mieux l'IA sont nombreuses.»

Quelle est la répartition des responsabilités entre client et fournisseur ?

« C'est une très bonne question : la répartition est extrêmement bien délimitée mais cette délimitation est malheureusement trop méconnue. Cela s'appelle le Shared Responsibility Model inventé par Amazon et tous les services Cloud de l'univers ont ce même modèle, pour répartir de manière très précise la responsabilité dans le cadre d'une attaque.

Ce qu'il y a de moins clair, c'est le partage qui dépend du service. Cet aspect-là est donc contractuellement établi, service par service. Entre le IaaS, et le SaaS, la responsabilité entre le fournisseur et le client sera très différente. Plus on remonte la chaîne de valeur du Cloud (par exemple recours aux Applications SaaS, plus le fournisseur a de responsabilités).

Aujourd'hui les États sont dans une guerre avec beaucoup de participants. La question de la sécurisation des serveurs n'est donc pas neutre, et cette responsabilité du côté fournisseur doit aller jusqu'à la supply chain. Ce n'est pas quelque chose que le fournisseur peut prendre à la légère.

Le client, quant à lui, a toujours la responsabilité des personnes à qui il donne accès à son Cloud (la gestion des utilisateurs), mais aussi le choix de la donnée concernée. Il est important de garder à l'esprit que l'on ne peut pas vous voler une base de données que vous ne possédez pas. Lorsque l'on fait des projets DLP (préventions des fuites de données) c'est pour éviter ce type de risques, mais cela n'est pas toujours évident pour toutes les entreprises.

Autre distinction importante à faire : la catégorisation de la donnée est souvent différente de la réalité de la donnée. Par exemple, des éléments peuvent être classifiés comme très confidentiels – après avoir été présentés dans des réunions de haut niveau – mais s'avèrent en même temps être des données publiques.

Les niveaux maximums de protections sont par définition plus coûteux, et savoir faire la distinction entre les niveaux de sensibilité, c'est-à-dire donner la bonne catégorie au bon type de données, est une source d'efficacité à garder en tête.»

Quels arguments donneriez-vous à des acteurs s'inquiétant d'un fournisseur d'origine américaine pour s'occuper de données sensibles de l'État ?

« La transparence et la visibilité sont les principaux éléments que je mettrais en avant. Aujourd'hui la majeure partie des entreprises qui vont dans le Cloud - quel que soit le fournisseur – manque de visibilité. Le temps moyen de détection d'une attaque par une entreprise est de plusieurs mois. Une

grande entreprise comme Marriott s'est, par exemple, fait voler les passeports de sa clientèle ayant séjourné dans leurs bâtiments depuis 2014 - et ces derniers ont mis 5 ans à s'en rendre compte.

Pour avoir cette confiance il nous paraît important que le Cloud provider donne de la visibilité sur ce qui se passe. Par exemple, chez nous, un client peut décider de faire du « penetration testing » pour tester la robustesse de nos infrastructures. Nous avons aussi des offres dédiées - incluant toute l'offre du Cloud public Oracle - mais installées directement chez nos clients, dans leur data center et avec leurs critères de sécurité. Cette offre permet de répondre aux attentes de certains États ou secteurs d'activité souhaitant créer des « Clouds souverains ».

Ce n'est pas la nationalité du fournisseur qui compte mais ses capacités cyber. De plus, il faut garder en tête que le Cloud Act ne concerne pas que les entreprises américaines, mais aussi toutes les entreprises ayant des opérations aux États-Unis, soit la très grande majorité des fournisseurs européens.»

C. Les questions de sécurité, frein pour le passage au Cloud ?

En définitive, les questions de sécurité ne devraient pas être perçues comme un frein à l'adoption du Cloud par l'État. D'abord, parce que les risques ne sont pas fondamentalement différents par rapport à une organisation traditionnelle avec des *data centers*. Le seul risque « nouveau » est potentiellement dans la connexion internet qui relie le *data center* au reste du monde, mais celui-ci est facile à maîtriser via des mesures de sécurité classiques. Et ensuite, parce que l'État français possède une capacité de cyberdéfense importante et a largement les moyens d'offrir une sécurité conséquente.

Le risque n'est pas dans la technologie mais bien plus dans la bonne décomposition des responsabilités de sécurité entre les fournisseurs Cloud et les organisations. Néanmoins, derrière les risques, et surtout les risques numériques, se dessinent des **craintes vis-à-vis du contrôle des données**. Le défi de garder ce contrôle - dans le privé - est particulièrement accru puisque les données sur le Cloud **sont souvent « répliquées » dans d'autres juridictions,** ou les lois sur la protection et la sécurité des données ne sont plus les mêmes.

L'enjeu autour de la maîtrise des données a été rappelé récemment par la polémique sur les données récupérées et stockées par IQVIA. IQVIA, spécialiste américain des données de santé, récupère, auprès de presque 14 000 pharmaciens sur le territoire national, des informations sur les transactions effectuées par des particuliers[65], ce qui est réalisé le plus souvent sans le consentement de ces mêmes clients lors de leur passage en pharmacie[66]. IQVIA est alors libre d'utiliser ces données notamment pour des études de marché ou pour d'autres usages. Les échos autour de cette affaire montrent qu'il existe un autre défi pour l'État dans son passage au Cloud, celui de **maintenir la souveraineté des données.**

[65] Franceinfo (2021), « Cash investigation » : on vous résume la polémique autour d'IQVIA et des données personnelles de santé », 20 mai 2021

[66] Krim (2021), « Lettre à ceux qui veulent faire tourner la France sur l'ordinateur de quelqu'un d'autre », Tariq Krim, 14 juillet 2021

Souveraineté : comment concilier dépendance aux acteurs étrangers et maîtrise des données publiques ?

A. Le « Cloud de confiance », des exigences de souveraineté fortes

La disparition de *Cloudwatt* et *Numergy*, les deux pousses françaises du Cloud nées à la suite du projet Andromède, a été un tournant majeur. **Les décideurs politiques ont peu à peu abandonné l'idée d'un « Cloud souverain »** - dont les fournisseurs seraient forcément des entreprises nationales - **en faveur d'un « Cloud de confiance »** autorisant l'utilisation de fournisseurs étrangers sous conditions de garanties de sécurité suffisantes.

C'est en effet « un contrôle absolu » sur ses données[67] que doit garantir ce « Cloud de confiance » avec notamment :

• Une **réversibilité**, c'est-à-dire la possibilité de sortir facilement du Cloud les données et applications qui y sont contenues. Cette dimension permet une liberté dans l'extraction des données du Cloud, à la suite par exemple d'une attaque, d'un dysfonctionnement ou simplement d'un changement de la politique de l'État.
• Une **garantie de sécurité supplémentaire** par rapport à celles déjà mises en place par le *Cloud Provider*, par exemple en exigeant des fournisseurs qu'ils obtiennent la qualification *SecNumCloud* de l'ANSSI.
• Un engagement fort des fournisseurs sur la **confidentialité des données et des applications**, notion retenant particulièrement l'attention des décideurs publics.

Le fournisseur de confiance est donc avant tout celui qui chiffre complètement les données contenues sur le Cloud, et **chez qui seul le client possède la clé de déchiffrement**. Mais le fait de proposer un stockage réversible, ultra-sécurisé et chiffré n'est qu'une première étape.

Avec la publication de la nouvelle doctrine du Cloud le 17 mai 2021, le « Cloud de confiance » est redéfini par le ministre de l'Économie et des Finances Bruno Le Maire, comme s'appuyant sur deux piliers[68] :

• Un premier pilier qui est celui de la protection technique et juridique des administrations et entreprises utilisant ce service.
• Un deuxième pilier qui est l'accès aux meilleurs services Cloud du marché, ce qui est un moyen de justifier le recours aux acteurs américains.

Avec la définition de cette nouvelle doctrine de Cloud, qu'en est-il de ces garanties ?

[67] Entretien avec un dirigeant commercial d'un grand acteur du Cloud en France
[68] Texte intégral de la déclaration de Mr. Bruno Le Maire, ministre de l'Économie, des finances et de la relance, sur la stratégie nationale du Cloud, à Paris le 17 mai 2021, viepublique.fr, https://www.vie-publique.fr/discours/280312-bruno-le-maire-17052021-strategie-nationale-du-cloud [dernier accès le 5 décembre 2021]

B. Quel impact des lois sur notre souveraineté du Cloud ?

I. Le Cloud Act : Une loi fortement médiatisée et source d'inquiétudes sur la souveraineté

Les polémiques autour du sujet du Cloud d'État tournent donc autour du problème de la souveraineté, avec, en arrière-plan, le Cloud Act. Le Cloud Act, de son nom complet *Clarifying Lawful Overseas Use of Data Act* ("loi clarifiant les cas d'usages licites d'utilisation de données étrangères") est une loi américaine datant du 23 mars 2018. Cette dernière précise que **toute entreprise soumise à la législation américaine et offrant des services Cloud doit**, en cas de soupçons avérés de crimes majeurs et sous validation d'un « juge indépendant », **transmettre les données hébergées dans leurs serveurs au Département de la Justice américain** - que ce soient des serveurs aux États-Unis ou à l'étranger.

Cette loi a déclenché une levée de boucliers en dehors des États-Unis. Elle est largement interprétée comme une source de risque vis-à-vis de l'utilisation des fournisseurs de Clouds américains, à qui un juge fédéral pourrait demander l'exfiltration de données vers les États-Unis. Bien que son applicabilité fasse encore débat, elle ne concerne d'ailleurs a priori pas seulement les entreprises américaines mais l'ensemble des fournisseurs Cloud opérant sur le territoire américain, même français[69].

Ce qui inquiète, ce sont les intentions cachées derrière cette régulation[70]. En 2019, un rapport du Sénat français indiquait la possibilité d'un contournement du processus judiciaire habituel et d'un champ d'application potentiellement très large de la loi, qui pourrait ainsi être utilisé pour dissimuler de l'espionnage industriel[71].

Que penser alors de ce Cloud Act ? En réalité, **l'applicabilité de celui-ci n'est pas encore pleinement déterminée**. Même pour les premiers concernés, les géants américains, l'application de cette loi n'est pas claire. Un responsable d'un de ces acteurs nous confie ainsi que **« les départements légaux sont en pleine ébullition »**, précisant qu'une centaine de personnes travaillent en ce moment-même pour comprendre l'impact sur les clients étrangers.

Le cœur de ce puzzle juridique est de savoir s'il est possible de « compartimenter » les filiales nationales, afin d'éviter que l'ensemble ne soit soumis au Cloud Act. Les représentants d'IBM France ont ainsi affirmé, le 9 mars 2021 devant l'Assemblée nationale qu'«*aucun serveur* d'IBM France *n'est soumis au Cloud Act*[72].»

II. Le Cloud Act, ou l'arbre qui cache la forêt ?

Quel est l'impact du Cloud Act pour le Cloud étatique français ? Malgré les craintes exprimées dernièrement dans les médias et par certains décideurs, nous pensons que le vrai risque posé par le Cloud Act est beaucoup plus nuancé :

[69] Décision du Conseil d'État, Alinéa 27 (Juin 2020) : https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-plateforme-health-data-hub

[70] Sénat français, « Le devoir de souveraineté numérique », http://www.senat.fr/rap/r19-007-1/r19-007-13.html [dernier accès le 27 février 2021]

[71] Ibid

[72] Assemblée nationale (2021), « Bâtir et promouvoir une souveraineté numérique nationale et européenne : auditions diverses », 9 mars 2021 https://videos.assemblee-nationale.fr/video.10443891_604736b51feb0.batir-et-promouvoir-une-souverainete-numerique-nationale-et-europeenne--auditions-diverses-9-mars-2021 [dernier accès le 16 mars 2021]

• **Tout d'abord, le Cloud Act ne doit pas, en théorie, permettre aux États-Unis d'accéder librement à toutes les données stockées sur les serveurs des fournisseurs.** Le champ d'application prévu est, d'après le Département de la Justice américain, limité aux investigations pénales, et ceci dans un strict cadre de contrôle judiciaire[73]. En pratique, le Cloud Act n'est donc pas prévu pour exfiltrer massivement des données mais doit cibler le plus possible ses demandes.

• **Par ailleurs, l'obtention par les autorités américaines des clés privées permettant de décrypter les données contenues sur le Cloud n'est pas garantie par la régulation.** Les fournisseurs ne sont pas dans l'obligation de fournir les clés, ni d'aider à les déchiffrer. Si les clés sont détenues par un tiers de confiance, ou simplement par le client final, les données restent illisibles et inutilisables. Pour Nathan Cook, « *le chiffrement des données de bout-en-bout permet de garder la main sur ses données, et de les protéger, y compris vis-à-vis de son fournisseur et des lois extraterritoriales*[74] ». La justice américaine pourrait toujours décider de déchiffrer les clés de sécurité, par exemple en faisant appel à des hackers indépendants, même si les algorithmes utilisés en pratique n'ont pas encore de preuve de leur faisabilité.

• **Puis, un fournisseur peut également refuser de transmettre les données au Département de la Justice américain**. En 2016 - soit 2 ans avant la mise en place du Cloud Act - Apple a ainsi décidé de ne pas aider le FBI à contourner les mesures de sécurité d'un iPhone ayant appartenu à des terroristes. L'entreprise déclarait craindre que ce contournement ponctuel ne compromette la sécurité de tous les autres smartphones de la marque[75]. Plus récemment - et plus directement lié au Cloud Act - certaines entreprises, comme Microsoft France, ont promis « une stratégie de mobilisation contentieuse » contre les éventuelles demandes au nom de la loi, afin de protéger leurs clients européens[76].

• Ensuite, **cette loi apporte un cadre juridique à quelque chose qui était déjà possible préalablement**. Indépendamment des obligations relatives au Cloud Act, les données stockées par les opérateurs peuvent d'ores et déjà être demandées dans le cadre d'autres accords transatlantiques existants comme le Mutual Legal Assistance Treaty (MLAT). De même, la plupart des pays de l'UE ont adopté des lois similaires permettant aux autorités judiciaires d'accéder aux données stockées par des opérateurs étrangers.

• Enfin, comme le rappelle Nathan Cook, l'État américain, à travers son agence de renseignement - la NSA - **dispose de programmes ou d'outils bien moins contraignants que le Cloud Act pour espionner des pays étrangers**. La NSA n'a par exemple pas besoin de l'autorisation d'un juge américain pour espionner des ressortissants d'un autre pays[77], certaines pratiques avec des acteurs télécoms ayant notamment déjà été révélées[78].

[73] Département de la justice américain (2018), "FAQs about the CLOUD Act", https://www.justice.gov/dag/page/file/1153466/download [dernier accès le 21 juin 2021]
[74] Interview avec Nathan Cook, le 25 janvier 2021
[75] Los Angeles Times (2016), "FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now", Rubin, Joel, Queally, James, and Paresh, Dave, 28 mars 2016 https://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html [dernier accès le 1 mars 2021]
[76] Sénat français, « Le devoir de souveraineté numérique », http://www.senat.fr/rap/r19-007-1/r19-007-13.html [dernier accès le 27 février 2021]
[77] CBS (2013), "NSA speaks out on Snowden, spying", John Miller, 15 décembre 2013, https://www.cbsnews.com/news/nsa-speaks-out-on-snowden-spying/ [dernier accès le 27 février 2021]
[78] 01Net (2018), Comment l'opérateur américain AT&T aide la NSA à espionner les communications du monde entier, Amélie Charnay, 27 juin 2018

Le Cloud Act ne rend donc pas plus vulnérables les Français et les européens à une saisie de leurs données par le gouvernement américain que ce qu'ils sont déjà. L'existence des capacités de collection de données américaines préexistent à l'établissement de ce cadre juridique - comme le montrent les derniers épisodes d'espionnage révélés de la NSA contre les Européens[79]. Un des problèmes majeurs vient de la loi FISA de 1978[80] (*Federal Intelligence Surveillance Act*, "loi sur la surveillance par le renseignement fédéral"). En autorisant de manière large la surveillance des citoyens étrangers, cette régulation rend possible la collecte de données étrangères sans préavis.

La loi FISA est à l'origine de l'annulation par la Cour de justice européenne le 16 juillet 2020 du dispositif *Privacy Shield* ('bouclier de confidentialité') qui encadrait le transfert de données entre l'UE et les États-Unis. La cour a jugé que le dispositif n'offrait pas de garantie suffisante, notamment eu égard à cette loi FISA, et qu'il était donc devenu illégal pour les entreprises européennes de transférer certaines catégories de données vers les États-Unis.

De plus, les lois américaines ne sont pas les seules lois de renseignement étrangères créant des zones d'incertitude. La loi chinoise sur le renseignement de 2017 exige aussi que les entreprises nationales coopèrent avec le gouvernement dans le partage de données, avec une application territoriale qui reste assez floue. En Russie, la loi antiterroriste de 2016, dite « loi *Yarovaya* », oblige les entreprises à aider l'État à décoder certaines données, et celui-ci n'hésite pas à demander les clés de chiffrage[81].

Les dispositions qui mettent potentiellement à risque les données européennes existaient donc avant le Cloud Act. Mais la crispation engendrée par le sujet, illustre **l'importance de donner des réponses claires aux craintes en matière de protection des données.**

[79] FranceInfo (2021) Espionnage des Européens par les États-Unis : « Pour la NSA, l'Europe, c'est open bar », affirme un spécialiste, 31 mai 2021

[80] Entretien avec la sénatrice Catherine Morin-Desailly, 22 juillet 2021

[81] Reuters (2019), "Russia's Yandex resists pressure to share encryption keys with the state", 19 juin 2019, https://www.reuters.com/article/us-yandex-privacy-idUSKCN1T51JY [dernier accès le 18 avril 2021

Interview

Extrait - Avec Tariq Krim le 24 septembre 2021

Présent en tant que correspondant dans la Silicon Valley à la fin des années 90 au moment de l'essor d'internet, Tariq Krim est également entrepreneur numérique, ayant notamment crée Netvibes et Jolicloud. Il a également été pendant trois ans vice-président du Conseil National du Numérique. Il s'est notamment exprimé publiquement sur la doctrine du Cloud de l'État du 17 mai 2021 dans son livre « Lettre à ceux qui voudraient faire tourner la France sur l'ordinateur de quelqu'un d'autre ».

1. Comment doit-on définir la souveraineté des données ? Quelle est votre définition d'un Cloud souverain ?

« Il existe plusieurs typologies de souveraineté numérique. La souveraineté totale, atteinte par exemple avec le Minitel, veut dire que 100 % des composants sont fabriqués en France. Mais aujourd'hui on achète énormément de technologies pour des raisons de coût et de rationalisation, et on a considéré également que les informaticiens étaient une source de coûts. Ce qui explique l'achat aux firmes étrangères et le recours massif aux SS2I. Toutefois, si l'informatique est déportée chez des entreprises françaises comme Atos ou Capgemini, elle reste souveraine. Mais on a commencé à intégrer des technologies non contrôlées par des acteurs nationaux.

La souveraineté totale est difficile à mettre en place car on n'a pas le contrôle sur toute la chaîne de valeur. La souveraineté des données est un renoncement à la souveraineté numérique totale : on met les données sur l'ordinateur de quelqu'un d'autre mais on se protège légalement. Mais on accepte le risque qu'une écoute ou une analyse soit faite sur n'importe quelle partie de la chaîne.

Deux types de risque apparaissent avec cette souveraineté des données : 1) Le risque juridique ; on peut interdire à telle ou telle société de faire commerce de nos données. Mais ces entreprises peuvent faire du « reverse engineering », même sur la base de la metadata et rendre caduque la protection juridique. Par exemple si vous êtes hébergé chez Amazon, Amazon peut déduire beaucoup de choses sur la base de vos usages, par exemple si vous êtes en croissance ou pas. 2) La question du risque étatique. Entre deux entreprises, il est possible de gérer le risque contractuellement. Mais pour une entreprise face à un État, on n'est plus dans la même logique juridique.»

2. Est-ce que le Cloud Act représente une menace selon vous ? Quelles autres lois posent un problème ?

« Ce qu'il faut comprendre c'est que chaque région du monde (US, Chine, Europe) dispose de lois d'écoute. La principale loi américaine, la loi FISA, date des années 1970. Le Cloud Act est une clarification de celle-ci, à la suite d'un refus de Microsoft de partager au gouvernement américain des information stockées en Irlande. Le problème de ces lois (y compris les lois chinoises) c'est que derrière la justification du renseignement, on fait mine de ne pas voir que l'on s'en sert pour de l'espionnage industriel.

Mais ce problème existe aussi entre les entreprises, par exemple Amazon Web Services héberge Netflix alors que Netflix concurrence directement Amazon Prime. De même, Intel, Apple et Microsoft se concurrencent tout en travaillant ensemble. L'analyse des métadonnées permet d'avoir autant d'informations que l'analyse des données elle-même, donc même si peu de données sont transférées, il y a un risque autour de la propriété intellectuelle.

Par ailleurs, dans le cadre du Cloud Act, l'éditeur de logiciel n'a pas le droit de prévenir la personne écoutée. Encore une fois, beaucoup de choses sont faites dans le cadre du renseignement et chaque État mène sa politique comme il l'entend. Le cas le plus connu dans lequel il y a des soupçons d'utilisation du Cloud Act reste la controverse autour de la vente d'Alstom.»

3. Est-ce que selon vous un Cloud avec connexion internet surveillée et gérée par des équipes accréditées est un moyen de concilier la souveraineté et les contrats avec des entreprises étrangères ?

« J'ai toujours cru que les entreprises internationales gardent une forte loyauté envers leur pays d'origine. Dans le cas des lois extraterritoriales, on étend la juridiction et la méthodologie d'analyse en dehors de l'endroit où on est légalement autorisé à le faire. Je n'ai pas de vision particulière sur le fait ou non que les acteurs étrangers respectent les lois européennes ; je suppose qu'en général ils les respectent. Mais si les lois américaines les obligent à faire quelque chose, ils le feront car les contrats des entreprises avec le gouvernement américain sont gigantesques par rapport à tous leurs contrats en Europe. Ces acteurs américains respectent aussi la loi française, mais entre une préférence américaine et européenne, du fait de la nationalité des dirigeants, les États-Unis auront toujours la préemption.

Pour en venir à la question, je ne crois pas à ce modèle [de coupure de la connexion internet] qu'on essaie de mettre en place avec Bleu [la coentreprise entre Capgemini, Orange et Microsoft]. La question juridique reste importante entre savoir s'il s'agit d'un État ou d'une entreprise. Mais on voit apparaître une deuxième chose, quelque chose d'intéressant qu'on a entendu ou dit au sujet du Privacy Shield (qui a été refusé en partie car il ne respectait pas le RGPD), c'est qu'un vide juridique apparaît. On découvre que beaucoup d'acteurs se retrouvent potentiellement dans une logique d'insécurité juridique.»

4. Dans votre livre, vous mentionnez que l'Allemagne et la France sont les pays européens les plus avancés sur le Cloud. Quels sont les exemples de cette avance ?

On a la chance d'avoir en France et en Allemagne des entreprises leaders sur les infrastructures physiques. Les GAFAM – et c'est finalement peu connu - ne possèdent pas leurs data centers afin de réduire leur exposition. Il y a une logique de se focaliser essentiellement sur la question des logiciels et non des infrastructures. Construire un immeuble, tout le monde sait le faire, mais construire un hôtel à forte valeur ajoutée c'est un autre savoir-faire. Les data centers ne coûtent rien (quelques dizaines de millions d'euros), mais contiennent des millions d'euros de machines qui génèrent des milliards de

revenus par l'hébergement de données.
Ce que l'État français n'a pas compris lors de la première phase d'implémentation du Cloud de l'État, c'est que le logiciel est essentiel.

Ce qui n'est pas en open source, et ce qui n'est pas disponible avec une seule entreprise française, c'est le logiciel qui offre des fonctions intégrées. Les entreprises françaises ont le même scope qu'un Amazon ou qu'un Microsoft, mais ces derniers acteurs ont été capables de tout intégrer dans une seule offre. En France il faut faire un assemblage car 3-4 entreprises différentes existent pour chaque fonctionnalité. Aux États-Unis, tout est offert clé en main. De plus, la commande publique américaine est importante et représente un levier important pour le développement des entreprises de Cloud locales. En France on n'est pas en mesure de faire les investissements ou d'avoir les cahiers des charges techniques qui aideraient le développement de nouvelles entreprises.

Mais il faut décider aujourd'hui : aide-t-on ces entreprises ? Ou doit-on les abandonner et les laisser dans une situation de sous-investissement chronique ?

Il y a finalement trois moyens de faire de la concurrence aux hyperscalers :

1/ Offres intégrées des entreprises françaises et européennes
2/ Orientation de la commande publique vers les acteurs nationaux et européens
3/ Développement d'un modèle d'utilisation spécifique à l'État français. Il est difficile d'avoir de la réversibilité dans le modèle de Cloud actuel. Le modèle des américains n'est pas le seul modèle, le modèle du « super-big » ne peut pas toujours fonctionner. Il y a une autre problématique, au-delà d'encourager les acteurs à travailler ensemble, qui est de faire diverger le développement du Cloud européen. Il faut faire un « leap of faith » et proposer des choses que d'autres acteurs ne proposent pas. Blablacar, par exemple, marche bien en France mais très mal aux États-Unis, dans le Cloud on aura la même chose, on n'a pas forcément les mêmes besoins en France qu'aux États-Unis.»

5. Avez-vous des exemples de savoir-faire français dans le Cloud ?

« Ils [les acteurs français] ont tous des fonctionnalités qui fonctionnent bien. On est excellents dans le serveur dédié. Cela dit attention à la volonté de benchmarker des choses qui ne doivent pas l'être. Sur les produits de base (data lake, etc.), qui constituent 95 % du marché, tous les acteurs français sont capables de répondre.»

6. Pensez-vous que ce soit utile de définir plus clairement les critères d'étanchéité que l'ANSSI peut exiger entre filiales françaises et maisons-mères internationales des fournisseurs Cloud, au-delà des licences ?

« Ces critères sont déjà en pratique définis, sachant que beaucoup de choses sont de l'ordre du confidentiel. Après, l'ANSSI n'est pas un acteur juridique mais un acteur en charge de la sécurité. Histori-

quement, c'est une agence de cryptologie, ça n'a rien à voir avec un organisme comme la CNIL par exemple. C'est un acteur de défense nationale, pas une agence de régulation donc est-ce réellement leur prérogative de définir ces critères ?»

7. Est-il utile de mieux responsabiliser les administrations vis-à-vis des enjeux de souveraineté ?

« Il est important de responsabiliser les administrations mais l'accent doit être mis sur la responsabilisation technique et les risques juridiques. Par exemple on peut repenser au Health Data Hub, on va rentrer dans une logique de plus en plus judiciaire où les choix vous impliquent, vous et le fournisseur ; la politique des 10 prochaines années dans le numérique, c'est le droit. Ce qui se voit d'ailleurs avec la montée en puissance du champ d'études de l'antitrust, notamment aux États-Unis. Cela dit, la logique de l'utilisation de moyens juridiques par les Américains contre les GAFAM est différente, les Américains veulent éviter la disparition de pans entiers de l'économie traditionnelle (les magasins de type Sears, Barnes & Noble, etc.) au profit du numérique.»

8. Pensez-vous qu'il est important que l'État développe un plan de maîtrise des compétences essentielles ?

« On a un vrai problème en France, on ne sait pas mettre en avant le talent technique. Si vous regardez, tous les Product managers de Google sont des développeurs. Mais dans le public les décideurs souvent ne sont pas techniciens, ce qui fait qu'ils n'ont pas toujours les mêmes réflexes que les ingénieurs.»

9. Vous avez mentionné dans votre livre le rôle du « CTO de l'État ». De quoi s'agirait-il précisément ?

« Cela fait dix ans que j'en parle. Aux États-Unis, Barack Obama a nommé 3 CTOs à son époque. Le roll-out de l'agile et la conduite du changement correspondent plus à une logique de DSI, une logique d'exécution qui correspond à la mission de la DINUM. Mais il faut également une vision stratégique, ce qui est le rôle du CTO. Il a un rôle et stratégique, et géopolitique. Ce qui est désolant quand on regarde les décisions prises récemment, c'est qu'il y a peu d'anticipation et beaucoup de réaction, on ne réagit qu'au Cloud Act en 2021 alors qu'il existe depuis trois ans. Il nous manque une vision stratégique dans tous les grands domaines, ainsi qu'une doctrine qui devrait être apolitique. Même sur le numérique les débats sont politisés (la gauche parle d'open source, la droite parle de Big Data) alors qu'il faudrait dépolitiser ces choses-là. Aux États-Unis, sous Bush, Obama et même Trump, la position vis-à-vis des grandes entreprises de technologie américaine n'a jamais changé, hormis la demande de Trump de sortir Amazon des contrats gouvernementaux du fait de son inimitié avec Jeff Bezos. Ainsi, le rôle du CTO est de mettre en place une doctrine, d'être apolitique. Le CTO doit voyager, comprendre les "uses cases" de la technologie et être en lien avec les grandes universités pour rester au fait des évolutions.»

10. Faut-il intégrer, au sein du plan de déploiement du Cloud de l'État, un certain nombre de créneaux réservés pour la commande aux acteurs nationaux et européens ?

« Il y a eu un mécanisme d'exclusion des petits acteurs avec la nouvelle doctrine [du 17 Mai 2021] alors qu'il aurait fallu un modèle qui leur donne un coup de pouce. Il aurait aussi fallu regarder les fournisseurs dans leur globalité : une entreprise qui ne paie pas tous ses impôts ne devrait simplement pas être autorisée à participer à ces appels d'offres.

On est face à un paradoxe : l'État investisseur finance l'innovation et fait grandir les entreprises mais l'État acheteur n'achète pas leurs produits.
Cependant, c'est l'occasion de développer des projets européens qui ne vont pas dans la même direction que les projets américains. Si l'on prend un autre domaine, le spatial, Ariane, par exemple, est un projet européen qui n'avait rien à voir avec les projets américains, Si l'État doit financer la R&D, il ne faut pas que ce soit pour faire la même chose qu'Amazon deux ans plus tard. Par exemple les Chinois ont fait le Cloud différemment, tandis que la base de données la plus puissante en termes d'analyse de données est Clickhouse, développé par le fournisseur russe Yandex, repris par beaucoup d'entreprises américaines ensuite (LinkedIn, etc.).»

11. Faut-il clarifier au niveau européen les ambitions en matière technologique et notamment de Cloud ?

« Développer le numérique, c'est mettre de la R&D sur le logiciel. La bataille aujourd'hui est la bataille du logiciel. Beaucoup de petits logiciels apparaissent en France (e.g., Snowflake), mais face au manque de soutien les fondateurs ont tendance à s'exiler aux États-Unis. En France, on investit dans l'applicatif (e.g., Doctolib) mais pas dans le logiciel qu'il y a derrière. Sur les machines, on est les meilleurs au monde avec OVH. C'est quelque chose que l'on sait faire, OVH gère des data centers partout, mais la question est ce qu'on fait tourner sur les machines. La vraie bataille n'est pas celle du Cloud, c'est celle du logiciel.»

III. Quels leviers pour faire advenir un Cloud compatible avec la souveraineté des données ?

La question de la souveraineté se résume ainsi au problème suivant : « *jusqu'à quel niveau de sensibilité doit-on confier les données à des acteurs localisés à l'étranger ou soumis à des lois étrangères et, pour les données les plus sensibles, y-a-t-il des solutions techniques permettant de se protéger des lois extra territoriales ?* »

Face aux implications encore incertaines de ces législations étrangères, l'État français a ainsi plusieurs options.

• (1) La première est tout simplement de ne **faire confiance qu'aux acteurs nationaux**, par exemple identifiés via la qualification *SecNumCloud*, en s'interdisant le recours aux acteurs transnationaux par précaution. Ceci impliquerait aussi d'exclure tout acteur national éventuellement soumis à des lois étrangères potentiellement contraignantes. Cependant faire émerger des acteurs nationaux n'est pas facile, et c'est l'échec de la première génération d'entreprises du Cloud français (*Cloudwatt*, *Numergy*) qui a motivé le changement de discours de l'État français pour aller vers le « Cloud national stratégique » ou le « Cloud de confiance ».

• (2) Une **ouverture quasi-totale aux fournisseurs étrangers** avec néanmoins certaines « zones sensibles » (défense, intérieur) qui ne seraient pas accessibles. Cette position considère qu'il faut privilégier uniquement les critères de décision commerciaux (prix, qualité de service), et se rapproche en pratique de celle adoptée par l'État le 17 mai 2021.

• (3) Le choix intermédiaire consiste à **ouvrir le marché à certains acteurs non nationaux de manière contrôlée**, à travers soit un contrôle plus fort (par la publication en open source notamment) ou une compartimentation très stricte. Le but serait d'ouvrir la porte à des acteurs opérant simultanément en France et aux États-Unis, permettant d'accéder à un catalogue d'offres plus important, tout en prenant en compte les contraintes induites par les lois de renseignement étrangères.

De plus en plus de voix s'élèvent, dans la sphère publique aujourd'hui, pour demander que la doctrine Cloud du 17 mai 2021 soit amendée, pour exercer justement plus de contrôle sur les fournisseurs de Cloud. La sénatrice Catherine Morin-Desailly rappelle que *« avec le Cloud de confiance, on instaure la théorie selon laquelle on pourrait contractualiser avec ces acteurs américains [...] au moment même où la Commission européenne a diligenté une enquête sur le recours aux sociétés extra-européennes, il y a donc une contradiction forte entre action de l'État français avec la théorie qui est développée au niveau européen* [82]. »

[82] Entretien avec la sénatrice Catherine Morin-Desailly, 22 juillet 2021

Zoom

Le système des licences, un frein au développement d'acteurs nationaux du Cloud ?

Au sein de l'annonce de doctrine du Cloud du 17 mai 2021, une mesure particulièrement significative est prise sur les dimensions PaaS et SaaS : celle de la mise en place de licences.

« Ce mécanisme de licences met les données des Français et des entreprises françaises à l'abri de la législation américaine du CLOUD Act », explique Cédric O, Secrétaire d'État chargé de la Transition numérique et des Communications électroniques. Une entreprise américaine pourrait ainsi ne plus être soumise au Cloud Act en étant revendue et entièrement gérée par un opérateur européen comme *OVHcloud*, *Outscale* ou encore *Scaleway*.

Ce mécanisme permet de distendre le lien entre d'un côté, les géants de type *Azure*, *AWS* et *Oracle* et de l'autre côté, les clients finaux des administrations publiques. Cette proposition s'inspire du partenariat entre *Google* et *OVHcloud* qualifié par un acteur proche de l'accord de « meilleur des deux mondes.»

« Quand Google a choisi de déraciner sa solution Anthos de son Cloud pour le mettre sur la plateforme OVH, cela a permis d'assurer à la fois la qualité de service d'Anthos avec la souveraineté d'OVH Cloud. […] Avec ce type de partenariat, on se rapproche de la promesse originelle d'une technologie où les choses sont claires, maximisées, sans enfermer les gens » – Directeur des ventes d'une entreprise du secteur.

Des cas similaires existent à l'étranger. En Chine, *Salesforce* est vendu, hébergé et géré par *Alibaba* - annonçant en décembre dernier une offre "Hyperforce" pour que ses clients puissent héberger les données applicatives sur le Cloud de leur choix.
Cette décision semble donc aller vers une plus grande réversibilité de l'offre, et une plus grande souplesse du dispositif et du choix d'acteurs.

Pourtant, le système des licences est également critiqué et accusé d'être porteur de risques. Parmi ceux-ci, on peut distinguer :

• L'incertitude autour de la **propriété intellectuelle.** Plusieurs questions clés se posent : Quel sera le partage de celle-ci entre les éventuels acteurs étrangers et les firmes françaises avec lesquelles ces entreprises travaillent ? Celle-ci sera-t-elle purement à l'avantage des géants de la technologie américains ? Il n'y a pas encore de certitude sur ces différents points laissant planer le doute pour des acteurs nationaux qui nous rappellent être « nettement plus contraints avec ce type de licences qu'en-dehors de ce système ».

• La question des **contrats de licence**. En effet, ces contrats peuvent-ils prendre fin unilatéralement si les fournisseurs de service le décident, ce qui exposerait potentiellement l'administration à des difficultés de fonctionnement ? Si ce risque existe effectivement dans la théorie, il convient néanmoins de rappeler qu'une licence, contrairement à un abonnement, ne devient pas automatiquement inutilisable pour motif de rupture de contrat.

• Mais la plus grosse critique vis-à-vis de la nouvelle doctrine de Cloud, qui est relayée notamment par la sénatrice Catherine Morin-Desailly, l'entrepreneur Tariq Krim, et d'autres acteurs nationaux, est qu'elle entraverait **le développement de l'écosystème du Cloud français**. En effet, les détracteurs du système des licences estiment que le risque est de cantonner des acteurs français tels qu'*OVHcloud* ou *Scaleway* à un pur service d'hébergement (IaaS), alors que la valeur dans le Cloud aujourd'hui est créée avant tout par la fourniture de logiciels. Fourniture de logiciels qui, avec le système des licences, reviendrait presque exclusivement à des acteurs étrangers. Ces détracteurs estiment donc qu'au moins une partie de la commande publique de PaaS et de SaaS devrait être réservée à des acteurs nationaux afin d'assurer le développement d'une filière nationale compétitive.

« Il faut bien comprendre que les obligations Sec Num Cloud sont extrêmement restrictives. On parle en général de 2 ans, de 20 agréments, qui coûtent à chaque fois près de 50 000€ à acquérir, à travers les différentes mises à niveau. Vous comprenez bien que cela est fortement dissuasif pour une petite entreprise française. Elle doit dépenser du temps et de l'argent, pour – peut-être – atteindre le même niveau de confiance que des géants comme Azure ou Amazon. Cela est forcément dangereux pour notre écosystème » – CEO d'un fournisseur de Cloud.

Pour le président du Medef, Geoffroy Roux de Bézieux, ce système des licences n'est pas incompatible avec le développement d'acteurs nationaux : *« Il ne faut pas renoncer à avoir des entreprises françaises. En attendant, le système de licence est une bonne solution […] Il y a eu cet accord entre OVH et Google, mais il y en aura d'autres*[83] *»*. Il convient néanmoins de garder en tête ces différents risques et d'y répondre au mieux, afin de s'assurer l'existence d'un tissu fort d'entreprises françaises et européennes.

Un débat important surgit donc quant à l'avenir du Cloud étatique français : **pour les applications et données à caractère sensible mais pas suffisamment pour être hébergées sur le Cloud interne de l'État, comment valider ou non l'accès de fournisseurs étrangers ?** Le Ministère de la Défense anglais a par exemple mis en place une suite de services Cloud - pour accélérer sa propre transformation digitale - selon un modèle **de « niveau de confiance**[84] **»**. Ce modèle considère que s'il est possible de contrôler toutes les entrées et sorties d'un data center, et de faire en sorte que tout le personnel soit doté d'une accréditation de sécurité nationale, il est envisageable d'intégrer des prestataires étrangers dans des environnements de données critiques (voir encadré ci-dessous).

[83] Présentation de la stratégie nationale pour le cloud – 17 mai 2021 - Transcript (Economie.gouv)

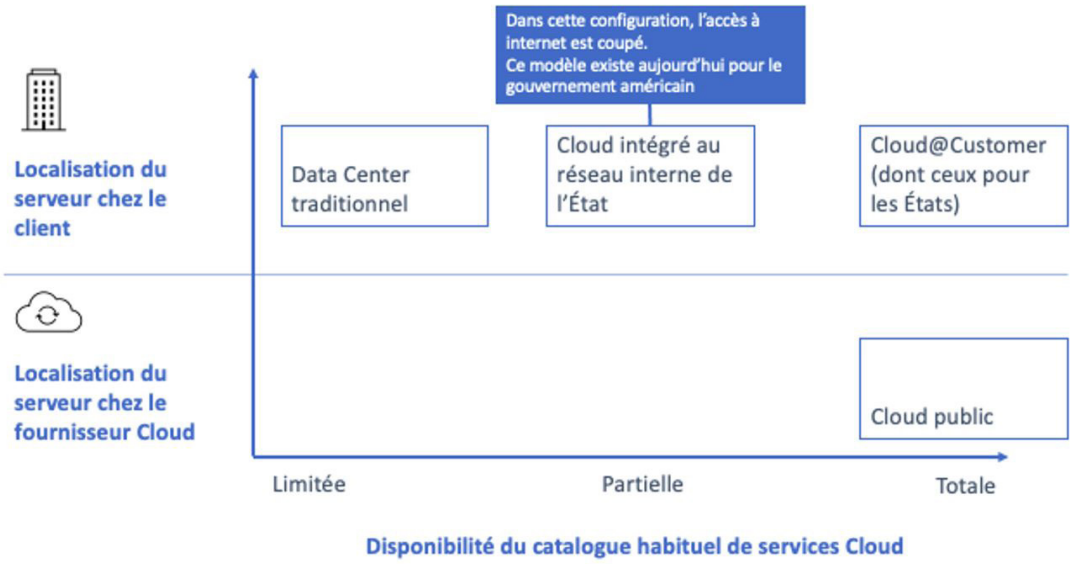
[84] Oracle.com (2020), "The Ministry of Defence Selects Oracle Cloud Infrastructure for Improved Agility and Speed of its Digital Transformation", 23 septembre 2020, https://www.oracle.com/uk/news/announcement/defence-selects-oracle-cloud-infrastructure-2020-09-23.html [dernier accès le 21 mars 2021]

Zoom

Zoom : quelles solutions pour les États les fournisseurs Cloud proposent-ils ?

Prendre une décision implique de passer en revue le spectre d'options disponibles pour l'État, allant d'un Cloud 100 % interne à diverses offres existantes des fournisseurs américains spécifiquement destinées aux gouvernements.

Schéma 3.1 Localisation et disponibilité de services Cloud : les alternatives



Comme dans le schéma ci-dessus, on peut distinguer :

• Les **systèmes traditionnels**, avec des centres de données appartenant à l'État français. C'est le modèle actuel (qui est également celui du système bancaire) mais dont les limites sont éprouvées aujourd'hui.
• Le **Cloud@customer** qui sera mis en place pour le Cercle III. Ce service, analogue à celui utilisé par la plupart des grandes entreprises, est proposé par la plupart des grands fournisseurs (*AWS*, *Oracle*, *Azure*, *OVHcloud*, etc.).
• Pour les données et applications les plus sensibles, il est possible de mettre en place **un Cloud coupé d'internet et intégré avec le réseau interne de l'État.**

Concernant ces deux dernières options de manière plus précise :
• Le Cloud@customer consistera en des **espaces physiques séparés au sein des data centers**. Ceci permet d'avoir sur site des équipes de l'opérateur Cloud qui seront chargées d'assurer la disponibilité des services accessibles sur le Cloud régulier, mais ceux-ci sont logés dans une salle différente avec

des accès restreints par rapport aux collaborateurs de l'État. La solution *Dedicated Regions* d'*Oracle* a l'avantage d'offrir des services identiques au Cloud Public (une cinquantaine au total). Cette solution est déployée notamment par les gouvernements du Royaume-Uni, d'Australie et d'Oman. *AWS* propose un concurrent, *Outposts*[85]. Ces solutions ont pour intérêt de localiser physiquement le Cloud chez le client, ce qui facilite les opérations nécessitant une faible latence, tout en permettant au client de bénéficier aussi de services disponibles également sur le Cloud. Dans ces espaces physiques séparés, les équipes du fournisseur Cloud se chargent de la maintenance et de la gestion du cycle de vie de l'infrastructure, tandis que les équipes client peuvent se consacrer pleinement au développement de nouvelles applications, en s'appuyant sur une suite de produits et de services complets.

• Il est possible de pousser encore plus loin cette logique des **espaces physiques séparés en se passant d'une connexion internet**. Par exemple, *Oracle* déploie un *National Security Region* ("région de sécurité nationale") aux États-Unis pour le compte du *Department of Defense*. Ce système est proche de celui des espaces physiques séparés mais les flux entrants et sortants sont filtrés par une zone tampon « *Air-Gap* » gérée par le client. Par ailleurs, les infrastructures sont connectées, non pas à internet, mais aux réseaux sécurisés du gouvernement américain.

Le fait de limiter l'accès des fournisseurs étrangers pour certaines fonctions du Cloud étatique français pose néanmoins une question importante : comment s'assurer que la France dispose d'acteurs capables de répondre à cette demande ? C'est bien là l'argument principal mis en avant par le gouvernement français, notamment Cédric O quand il a affirmé, en juillet 2020, qu'aucun acteur français n'était en mesure d'offrir des prestations comparables à celle de Microsoft, pour construire un répertoire national de données de santé (le fameux *Health Data Hub*)[86]. La mise en place d'un contrôle plus étroit sur les données de l'État français n'est donc pas indépendante de l'entretien d'un écosystème national performant d'entreprises du Cloud.

[85] Aws.com, Page de présentation AWS Outposts, https://aws.amazon.com/fr/outposts/ [dernier accès le 27 février 2021]

[86] Entretien avec la sénatrice Catherine Morin-Desailly, 22 juillet 2021

Conclusion : comment avancer sereinement vers le passage des données publiques sur le Cloud ?

La première conclusion à tirer de ce tour d'horizon est que **la migration des données sur le Cloud doit s'insérer dans une stratégie d'ensemble pour le numérique de l'État.** Le passage sur le Cloud n'est pas plus indépendant de la question de la numérisation des services publics que des questions de cybersécurité. Elle n'est pas non plus indépendante de la question du stockage des données des Opérateurs d'Importance Vitale (OIV) et des Opérateurs de Services Essentiels (OSE). La question de la stratégie Cloud est donc partie intégrante d'une stratégie numérique d'ensemble qui associe la DINUM, l'ANSSI, le ministère de la Défense et de l'Intérieur et tous les autres acteurs pertinents.

La seconde est qu'il reste essentiel d'accélérer le déploiement du Cloud. Pour permettre à l'État de capturer le plus rapidement les bénéfices d'un déploiement Cloud, et matérialiser la volonté politique exprimée, il est important d'atténuer les obstacles qui freinent aujourd'hui sa mise en place. La sensibilisation et la formation en amont des personnels et des départements informatiques des administrations, couplées à une transparence accrue des solutions disponibles, semblent ici clés. Néanmoins, cette pression pour passer rapidement sur le Cloud ne doit pas empêcher une prise en compte approfondie des dimensions de sécurité et de souveraineté.

Troisièmement, sur le sujet de la **souveraineté des données,** l'État doit trouver un équilibre entre garanties nationales de contrôle, face aux lois extra-territoriales, et le risque de se priver par principe de techniques et de savoir-faire étrangers - et notamment américains. Cette problématique comprend les choix des fournisseurs mais également un enjeu pour l'État de réussir à **concilier recours à des acteurs privés pour une partie de son infrastructure digitale, tout en maintenant les compétences essentielles de cybersécurité.**

Enfin, derrière le Cloud se dresse un débat plus général autour de la nécessité d'une **politique industrielle du numérique en Europe.** Alors que la politique de concurrence européenne se focalise historiquement sur les droits du consommateur, cette logique est de plus en plus contestée. L'annonce, au mois de juillet 2021 d'une politique européenne visant à faire du continent un *hub* mondial pour la fabrication de semi-conducteurs[87], peut représenter un premier pas vers une politique industrielle des nouvelles technologies, dont un futur volet logiciel apparaît comme la suite logique. Au niveau national la France doit veiller à **maintenir un écosystème performant**, afin d'être pleinement acteur de ce mouvement.

[87] Financial Times (2021), "Semiconductors: Europe's expensive plant to reach the top tier of chipmakers", Sam Fleming, Peggy Hollinger et Ben Hall, 21 juillet 2021

10 Recommandations pour une mise en place, efficace et responsable, d'un Cloud d'État :

Face à chacun de ces problèmes, et en nous basant sur les témoignages recueillis, nous proposons ici plusieurs recommandations pour (I) accélérer la mise en place d'une infrastructure de Cloud d'État, (II) concilier souveraineté des données et savoir-faire étrangers, et (III) assurer un maintien des compétences clés de l'État. Par rapport à la nouvelle doctrine du Cloud publiée le 17 mai 2021, nous estimons qu'il est essentiel d'aller au-delà des seules questions d'infrastructure, et d'ajuster et de replacer cette doctrine dans le cadre plus large d'une stratégie numérique de l'État.

Faciliter le déploiement du Cloud d'État

1. Développer un **plan de migration sur le Cloud** pour les administrations. Ce plan d'adoption pourrait allier des initiatives de formation pour les DSI et les administrations concernées, tout en proposant des objectifs chiffrés d'applications à faire migrer sur le Cloud, afin d'assurer un suivi quantifié. La formation pourrait inclure par exemple des sessions dédiées à la prévention des risques principaux d'utilisation. L'intérêt d'un plan de migration est aussi de donner de la visibilité, facilitant l'agencement des grandes étapes de cette migration vers le Cloud en fonction du développement d'offres pertinentes par des acteurs français et européens.

2. **S'appuyer sur les réussites passées** du Cloud de l'État pour construire les réussites de demain. Dans un contexte où les freins au déploiement restent nombreux au sein des administrations, il est important d'inclure les DSI et les parties prenantes dans un processus concerté. En ciblant des usages clés et en offrant visibilité et transparence sur ces réussites - de l'application Géoportail de l'IGN au système de traitement des demandes d'asile du ministère de l'Intérieur - il sera possible de renforcer une adhésion au projet Cloud de la part des utilisateurs finaux, c'est-à-dire les DSI et les personnels du secteur public.

La souveraineté des données de l'État : concilier contrôle total et savoir-faire étranger

3. **Définir publiquement les critères d'étanchéité que les autorités de règlementation peuvent exiger entre filiales françaises et maisons-mères internationales des fournisseurs Cloud**. Les autorités de règlementation (CNIL, Service des Achats de l'État) ainsi que l'ANSSI[88] et les fournisseurs Cloud peuvent bénéficier d'un travail commun sur la définition de ces critères et sur l'élaboration de solutions conjointes. Un rapport du Sénat en 2019[89] propose notamment d'assurer l'étanchéité juridique des filiales géographiques des fournisseurs Cloud. Dans le cas des fournisseurs extra-européens, l'étanchéité juridique pourrait se matérialiser par l'ouverture du capital à des acteurs locaux, ouvrant la voie au développement de *joint-ventures* de l'État ou des entreprises françaises avec les *hyperscalers*.

4. **Responsabiliser les administrations vis-à-vis des enjeux de souveraineté**. Les choix de prestataires et de solutions ayant lieu au niveau des administrations, il est important de s'assurer que ces décideurs soient sensibilisés à ces enjeux. Cela passe par une transparence des données, pour que

[88] Nous tenons à préciser ici que l'ANSSI n'est pas une agence de régulation et donc ne définit pas elle-même ces critères même si elle peut émettre son avis

[89] Sénat français, « Le devoir de souveraineté numérique », http://www.senat.fr/rap/r19-007-1/r19-007-13.html [dernier accès le 27 février 2021]

les décisions décentralisées de souveraineté au cas par cas soient éclairées. Il faut aussi aller plus loin en responsabilisant les administrations vis-à-vis du risque juridique – de plus en plus présent dans les questions numériques – lié à la contractualisation avec des acteurs soumis à des lois étrangères.

5. **Mettre en place une obligation de transparence sur les choix des fournisseurs de solutions Cloud pour l'État** (sous réserve de contre-indication de sécurité nationale).

6. **Agir au niveau communautaire pour limiter l'applicabilité des lois étrangères. L'Union européenne**, qui se pose de plus en plus en régulateur face aux géants de la Tech, **peut se doter de leviers politiques** pour empêcher une utilisation abusive des législations étrangères. Dans le cas des lois américaines, des négociations ont été engagées dès septembre 2019 – sans succès jusqu'à présent - afin d'obtenir un encadrement de l'application du Cloud Act et la mise en place d'une réciprocité[90]. La France peut servir de force de proposition pour relancer ce sujet, particulièrement avec la présidence française du Conseil de l'Union Européenne de 2022.

Maintien des compétences de l'État : assurer une mise en place efficace, ne se faisant pas au détriment du savoir-faire étatique

7. Développer un **plan de maîtrise des compétences essentielles** jugées critiques à garder en interne pour l'État. De manière précise, l'État devrait agir pour assurer la maîtrise de toutes les compétences nécessaires à la gestion de data centers. Ceci pourrait être fait au niveau interministériel avec, par exemple, un Groupement d'Intérêt Public comme il en existe pour maintenir les compétences liées au réseau interne de l'État (RIE). Un des enjeux majeurs liées à ce plan de maîtrise est également de rendre la fonction publique plus attractive pour les profils ingénieurs.

8. **Profiter du sujet du Cloud étatique pour développer des institutions essentielles à la stratégie numérique de l'État.** Pour définir cette même stratégie, il serait utile, comme l'a proposé Tariq Krim, de désigner un **Chief Technology Officer** (CTO)[91] de l'État, sur le modèle de ce qui existe aux États-Unis depuis l'administration Obama. Le CTO serait apolitique et aurait comme vocation de s'informer sur les évolutions de la technologie et des cas d'usage et d'en dégager une doctrine pour l'État. Pour faciliter l'exécution de cette stratégie, et précisément dans le cas du déploiement du Cloud, on peut imaginer la mise en place d'un plan de ***roll-out* de l'agile et de la conduite du changement au sein de l'État**, coordonné par la DINUM. L'objectif principal du Cloud, qui est de permettre aux développeurs de l'État de se focaliser sur le service et ainsi d'améliorer la réactivité et le temps de lancement de nouvelles applications, n'aura de sens que si les manières de travailler suivent l'évolution des solutions techniques.

Développement de l'écosystème numérique français et européen : faire de l'Europe un acteur du logiciel

9. Intégrer, au sein du plan de déploiement du Cloud de l'État, des **créneaux de commande réservés aux acteurs nationaux et européens**. La déclaration du secrétaire d'État au numérique en juillet 2020 selon laquelle il n'existe aucun acteur français capable de concurrencer le niveau de ser-

[90] Mignon, Emmanuelle (2020), "The CLOUD Act: unveiling European Powerlessness", publié dans la revue européenne du droit, 5 septembre 2020, https://legrandcontinent.eu/fr/2020/09/05/the-cloud-act-unveiling-european-powerlessness/

[91] Krim (2021), « Lettre à ceux qui veulent faire tourner la France sur l'ordinateur de quelqu'un d'autre », Tariq Krim, 14 juillet 2021

vice des *hyperscalers* américains a suscité de vives réactions. Surtout que des acteurs nationaux tels qu'*OVHcloud* ou *Scaleway* sont parmi les leaders européens du Cloud[92]. Ces entreprises rappellent que les avantages des *hyperscalers* sont en partie le résultat de subventions indirectes réalisées via les commandes publiques de l'État fédéral. **La France pourrait imiter cette approche qui a si bien fonctionné**. L'État devrait veiller à ne pas créer de rente, mais au contraire permettre à ces acteurs de devenir des leaders internationaux compétitifs. Au-delà de ça, cette commande publique peut être un moyen pertinent pour faire émerger des nouvelles conceptions du Cloud adaptées aux besoins des administrations françaises, différentes du *« more is better »* des *hyperscalers*.

10. **Clarifier, au niveau européen, les ambitions en matière de développement d'acteurs du numérique et du Cloud**. S'il existe un consensus pour faire émerger des géants européens du numérique, deux questions demeurent 1) quant aux domaines d'expertise de ces acteurs et 2) quant à la nécessité ou non de fermer le marché européen aux acteurs extra-communautaires. La Chine, par exemple, a fait émerger ses propres équivalents aux GAFAM (*Alibaba*, *Baidu* et *Tencent*) au prix d'une fermeture du marché intérieur. Notre conviction est que l'Europe doit suivre le modèle d'*Airbus*, qui a su se développer face à ses concurrents américains sans leur interdire l'accès au marché communautaire. Pourquoi ne pas chercher à faire émerger un « Cloud européen » dont les fonctionnalités et les objectifs seraient adaptés aux enjeux de notre Vieux Continent ?

La crise de la COVID-19 a été vécue par la plupart des citoyens comme une période à oublier. Pourtant, derrière les difficultés du quotidien, **cette crise a été l'occasion pour de nombreuses entreprises et administrations de gagner en maturité digitale**. La nécessité de faire travailler à distance les fonctionnaires, la dématérialisation accrue des services publics et le besoin de résoudre des problèmes techniques au quotidien, ont mis en lumière les besoins nouveaux d'un service moderne de l'État.

La politique de Cloud de l'État, dont le Cercle III est devenu opérationnel en janvier 2021, arrive ainsi comme une opportunité à ne pas manquer. Au milieu des multiples chantiers de l'État - management du changement, mise en place du travail en mode agile, coopération interministérielle - le déploiement de cette offre IaaS doit permettre d'accélérer cette transition numérique si fondamentale pour une efficacité étatique. Dispensés de se poser des questions d'infrastructure, les programmeurs de l'État pourraient ainsi se concentrer pleinement sur le développement de services à forte valeur ajoutée, avec une rapidité auparavant inespérée.

Néanmoins, cette valeur apportée par le Cloud d'État ne sera possible qu'avec un soutien des politiques et des administrations. Ce rapport appelle donc de ses vœux la mise en place d'un processus structurant, guidé par la DINUM, permettant à l'État d'améliorer durablement ses fondamentaux. Mais si ce changement doit avoir lieu, et être porté par les politiques, il doit se faire sans exclure d'autres parties prenantes au niveau de l'État. Ce n'est qu'avec une adhésion et un engagement global des administrations que les gains apportés par le Cloud pourront se matérialiser.

[92] Idem

FONDATION CONCORDE

Le Think Tank
dédié à la **croissance**,
la **compétitivité** et **l'emploi**

fondationconcorde.com

17, rue de l'Amiral Hamelin
75116 Paris

01 72 60 54 39
info@fondationconcorde.com