Cloud Souverain, Cloud de Confiance et Cloud Européen : chimère ou réalité en devenir ?

Face à l'hégémonie des MAGMA (Meta, AWS : Amazon Web Service, Google Cloud, Microsoft Azure, Apple) sur le marché des fournisseurs de service Cloud, les acteurs de l'industrie financière français et européens sont devant un dilemme difficile à résoudre : entre embrasser les avantages technologiques fournis par ces acteurs américains pour accélérer leur transformation IT ou protéger leurs services stratégiques ainsi que les données de leurs clients. Est-ce que l'émergence de nouvelles offres de Cloud Souverain, Cloud de Confiance et Cloud Européen est la réponse à leur besoin ou une nouvelle contrainte de plus à intégrer dans leur migration vers le Cloud ?

Qu'il soit « souverain », « de confiance », ou « Européen », le cloud est en pleine mutation pour répondre à la pression réglementaire croissante et assurer la sécurité des données. Pour s'y retrouver, commençons par quelques définitions :

- Le Cloud Souverain, est un terme à l'origine utilisé par les régulateurs et les entreprises pour parler de cloud qui comme son nom l'indique, a pour objectif de protéger la souveraineté des états et des entreprises. Il garantit l'immunité au regard des autorités extraterritoriales et favorise ainsi des fournisseurs de cloud locaux.

- Le Cloud de Confiance, est un terme plus récent et créé par le secteur privé. Il désigne un service de cloud fondé sur des principes tels que la transparence, la souveraineté ou la sécurité.

- Le Cloud Européen, désigne un service cloud qui répond aux standards et volontés de l'Union Européenne. Il assure notamment l'ouverture, l'interopérabilité et la sécurité des données pour tous ses utilisateurs états, entreprise et particuliers.

Les problèmes de souveraineté des données sont anciens et ont été mis en avant par plusieurs événements comme les affaires Snowden ou Cambridge Analytica. Ainsi les régulateurs se sont penchés sur le problème et il s'avère intéressant de faire un petit tour du monde des différentes lois concernant le cloud.

Dans l'Union Européenne, le RGPD (Règlement Général sur la Protection des Données), entré en vigueur en 2016, est la principale réglementation européenne sur l'utilisation des données et est l'une des plus contraignante au monde en matière de protection des données personnelles et de droits des citoyens.

Résumés par la CNIL[1], les 5 grands principes du RGPD sont les suivants :

- Finalité légitime
- Proportionnalité et de pertinence
- Durée de conservation limitée
- Sécurité et de confidentialité
- Droits des personnes

Toute infraction au sens du RGPD peut conduire à une amende pouvant atteindre 20m€ ou 4% du CA annuel consolidé.

Le DORA[2] (Digital Operational Resilience Act) impose depuis 2021 des règles de résilience et de sécurité pour l'industrie financière et leurs fournisseurs tiers. Même si les fournisseurs de cloud sont contraints de se plier à ces règles, ils sont ainsi favorisés car ils proposent souvent des infrastructures plus résilientes que les infrastructures internes des institutions financières, souvent moins redondantes et moins sécurisées.

Partons maintenant aux Etats-Unis qui a instauré le CLOUD Act (Clarifying Lawful Overseas Use of Data Act), en 2018. Il impose la règle suivante : les données stockées à l'intérieur et en dehors des USA par un prestataire de service soumis à la loi américaine, peuvent être transmisses au gouvernement américain sur assignation d'un tribunal.
Il est complété par le FISA (Foreign Intelligence Surveillance Act), instauré en 1978 et amendé en 2015 il permet aux autorités américaines d'accéder aux données transitant sur le sol américain.

Grâce au CLOUD Act, des données hébergées dans un cloud Microsoft, même au sein de l'Élysée, sont saisissables par la justice américaine

Enfin, la Loi Chinoise, le PIPL[3] (Personal Information Protection Law) de 2021, est plus restrictive que le CLOUD Act et astreint les fournisseurs de cloud à des contrôles de sécurité conduits par le gouvernement. Cette loi favorise les fournisseurs Chinois et le stockage de données sur le territoire national. Elle autorise également les autorités à mener des actions extraterritoriales pour défendre la sécurité nationale et « l'intérêt général du peuple Chinois ». Concrètement la Chine s'autorise à accéder à des données de pays étranger sans restriction et par quelque moyen que ce soit. C'est notamment pourquoi les produits Huawei (antennes 4G/5G, mobiles etc.) sont soupçonnés d'aider les renseignements chinois.

Concernant les transferts de données entre les états, le Privacy Shield (2016-2020) était la seule base légale autorisant le transfert de données personnelle entre l'Union Européenne et les Etats Unis d'Amérique. Il a été invalidé par la Cour de Justice de l'Union Européenne, à la suite de la plainte d'un militant pour la protection des données (M. Schrems). La cour a considéré que les programmes de surveillance américains n'étaient pas compatibles avec les principes du RGPD.

En conséquence, les réglementations Européennes et Américaines ont été jugées incompatibles et irréconciliables car la législation américaine autorise les autorités à accéder aux données hébergées par des fournisseurs américains n'importe où dans le monde alors qu'en Union Européenne, l'accès aux données par les pouvoirs publics est très réglementé et contrôlé. Pour rappel, l'un des principes du RGPD est d'assurer la sécurité et la confidentialité des données.

En résumé, depuis la promulgation du CLOUD Act, les prestataires américains ne peuvent plus garantir la confidentialité des données personnelles des Européens à l'égard des autorités Américaines. Depuis l'invalidation du Privacy Shield, les

[1] https://www.cnil.fr/fr/cnil-direct/question/quels-sont-les-grands-principes-des-regles-de-protection-des-donnees
[2] RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52020PC0595&from=FR
[3] Personal Information Protection Law of the People's Republic of China – Stanford University/Digichina https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

entreprises transférant des données personnelles de citoyens européens sur des serveurs en dehors de l'Union Européenne n'ont plus de base légale et sont ainsi passibles de poursuites judiciaires.

A la mi-mars 2022, les Etats-Unis et l'Union Européenne ont signé en pleine guerre en Ukraine un accord de principe sur les transferts de données transatlantiques. Cet accord devrait imposer de nouvelles obligations pour les entreprises traitant des données européennes et limiter l'accès des autorités américaines aux données européennes. Si les deux parties se réjouissent de cet accord, le projet est encore loin d'avoir été adopté par la commission et les entreprises ne peuvent pas se reposer sur un accord tant qu'il n'est pas adopté. Max Schrems, le célèbre militant à l'origine de l'invalidation du Privacy Shield, a déjà dénoncé une annonce purement politique et un manque de réforme substantielle côté américain[4].

En résumé, les lois Américaines et Chinoises favorisent les fournisseurs de cloud nationaux et ont pour objectif de défendre leurs intérêts et leurs économies, à l'opposé des lois Européennes qui visent à protéger les données des citoyens et des entreprises.

A l'instar de certains gouvernements, les fournisseurs de cloud ont eux aussi tendance à privilégier leurs intérêts économiques en dépit de l'intérêt de leurs clients. Premièrement, il faut noter que les fournisseurs proposent souvent des contrats standards non négociables. En effet, même si ces contrats d'adhésion et politiques commerciales sont légaux, ils ne prévoient pas de marge de négociation.
De plus, ces contrats peuvent contenir des clauses abusives telles que des clauses obligeant le client à accorder un droit et une licence libres de redevance, mondiaux et non exclusifs (inclus technologies, marques, contenus, informations produites, données, matériaux et autres produits ou informations du client).

Enfin, les fournisseurs ont souvent des conditions de vente permissives, leur permettant d'accéder et d'exploiter (modifier, copier et distribuer) tout ou partie des données industrielles confidentielles précieuses de ses clients (e.g. propriété intellectuelle, tarifs, conditions commerciales…).

Pour faire face à tous ces défis, tout en développant une industrie stratégique, L'Union Européenne sponsorise l'association Gaia-X qui a pour objectif de proposer un label de conformité Européen et de dessiner le futur en matière d'utilisation des données.

Les services cloud de l'état Français doivent respecter la plupart des principes de Gaia-X:

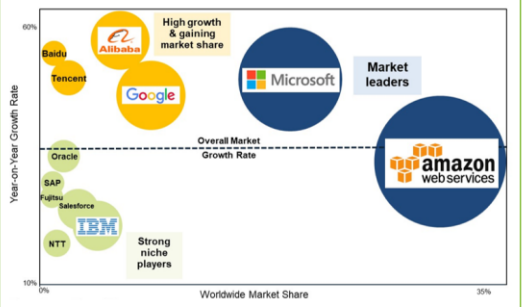
- ✓ Être conformes et soumis exclusivement à la loi européenne
- ✓ Être situées en Union Européenne (holding, infrastructures, support client, sous-traitants…)
- ✓ Garantir la portabilité et la réversibilité
- ✓ Assurer un niveau élevé de sécurité
- ✓ Garantir la transparence sur l'utilisation des données client

Dans le sillage de l'Union Européenne, la France avec son Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a développé un visa de sécurité obligatoire pour les services numériques vitaux : le visa SECNUM Cloud. Basé sur la norme ISO 27001, il possède des exigences complémentaires à Gaia-X :

- ✓ Audits et tests de l'ANSSI
- ✓ Visa valide 3 ans
- ✓ Documentation renforcée
- ✓ Normes de souveraineté et de sécurité drastiques

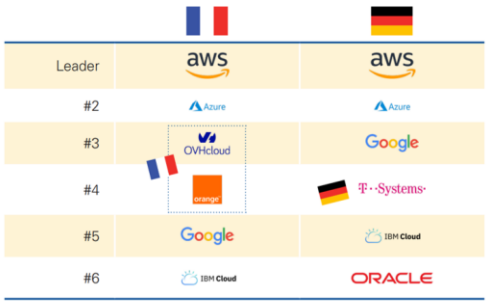
[4] Le privacy Shield 2.0 ? – Première réaction par Max Schrems, noyb, 25 Mars 2022

Positionnement compétitif mondial des fournisseurs de cloud (T1 2021)



Source : Synergy Research Group

Classement des acteurs du cloud en France et en Allemagne (2020)



Source : KMPG

Les grands pays Européens possèdent leur propre visa de sécurité AgID en Italie, ENS en Espagne, et C5 en Allemagne.

Au-delà des défis réglementaires, le cloud est une industrie stratégique qui pèsera autant que le marché des télécommunications en 2027 (soit plus de 250mds€)[5].

Sans surprise, les leaders mondiaux sont des Américains, filiales des MAGMA (Meta, AWS : Amazon Web Service, Google Cloud,

Microsoft Azure). AWS, premier fournisseur de cloud, détient environ 40% de la valeur du marché dans le monde et même plus de 50% en Europe. Il est suivi par Microsoft Azure (20% part de marché dans le monde et 9% en Europe) puis par Google avec moins de 10% de parts de marché. Cependant, leur rivale chinois, les BATX (Baidu, Alibaba, Tencent, Xiaomi) ne sont pas en reste. Ainsi, avec 5% du marché mondial, Alibaba est venu se hisser à la 4ème place mondiale en 2020, devant IBM et ses 4% de parts de marché.

Les fournisseurs français tentent de se démarquer en proposant leur cloud de confiance. Certains d'entre eux ont choisi de s'associer avec des géants du cloud Américain. C'est le cas de Capgemini et Orange qui se sont associés à Microsoft Azure ou encore de Thales qui s'est associé avec Google Cloud. Leurs projets sont similaires avec des objectifs tels que : obtenir le visa de sécurité SECNUM Cloud (compliqué dès lors qu'un fournisseur américain est impliqué), créer un écosystème dédié (infrastructures, service client etc.), avoir un actionnariat majoritairement français et être capable de supporter tous les services de leurs clients y compris les services vitaux.

La liste des services qualifiés mise à jour par l'ANSSI en février 2022 [6], ne contient seulement que trois fournisseurs de cloud, et ils sont tous Français. Il s'agit de Worldline, Dassault Outscale et OVH. Ces fournisseurs qui peuvent ainsi servir les services vitaux mais seulement pour l'hébergement de leurs infrastructures (IaaS). Aucun fournisseur n'a à ce jour obtenu une certification PaaS (plateforme) ou SaaS (service). Ces services de cloud souverain impliquent un surcoût d'au moins 15%[7] par rapport à un cloud de confiance.

Qu'elles soient territoriales ou extraterritoriales, les réglementations sur la gestion des données ont tendance à s'appliquer partout dans le monde, mettant en danger la souveraineté des états et des entreprises.

[5] Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030 – KPMG – Avril 2021
[6] Services qualifiés par l'ANSSI / Informatique en nuage https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

[7] Grille tarifaire OVH https://www.ovhcloud.com/fr/enterprise/products/secnumcloud/prices/

La réponse de l'Union Européenne via les recommandations sur sa vision du cloud Européen a pour but de protéger ses entreprises et ses citoyens en mettant en place une politique de protection des données personnelles la plus ambitieuse mais aussi de faire évoluer les fournisseurs de service Cloud par un cadre réglementaire le plus contraignant.

Ces derniers, qui avaient tendance à imposer des contrats très permissifs, proposent désormais un Cloud de Confiance en partenariat avec des acteurs locaux Européens qui tentent de répondre aux problématiques de souveraineté des entreprises et des états tout en leur offrant l'opportunité de bénéficier des avantages du cloud (économies, flexibilité, temps réduits de développement et de déploiement…) mais en France leur certification SecNum Cloud se fait attendre.

Les programmes de transformation IT eux n'attendant pas, les acteurs des services financiers doivent naviguer entre nouveaux partenariats et contraintes réglementaires pour tirer les bénéfices du Cloud dans leur transformation. Nous verrons dans notre prochain épisode comment les principaux acteurs financiers adaptent leur migration vers le Cloud.

Retrouvez la version électronique de notre étude en flashant ce QR code.

Retrouvez la version électronique de notre étude en flashant ce QR code.

Retrouvez la version électronique de notre étude en flashant ce QR code.

Retrouvez toutes nos publications sur
https://www.ailancy.com

Ont contribué à la réalisation de cette note de conviction :

Fabien SCANVIC – Consultant
Mob. +33 6 77 47 95 80
fabien.scanvic@ailancy.com

Jean-Charles MEURISSE - Directeur Associé
Mob. +33 6 72 47 60 19
jean-charles.meurisse@ailancy.com

Armand LEMAL – Manager
Mob. +33 6 70 19 31 48
armand.lemal@ailancy.com