Cloud : réglementations et souveraineté, Gaia-X

Par Anne-Sophie TAILLANDIER
Directrice de TeraLab-IMT

Et Alban SCHMUTZ
Co-fondateur de CISPE (Cloud Infrastructure Services Providers in Europe)

Avec les deux dernières années de pandémie de Covid-19, 82 % des décideurs IT ont accru leur usage du *cloud*. Entre 2021 et 2027, le marché européen du *cloud* devrait plus que quadrupler en passant de 63 à 260 milliards d'euros d'après un dernier rapport KPMG[1]. Pas moins de 550 000 emplois créés et 200 milliards d'euros d'investissements sont aussi attendus.

Or 70 % du marché de l'infrastructure *cloud* sont occupés par trois acteurs principaux. Aucun d'entre eux n'est européen. Ces *hyperscalers* dépendent de juridictions nord-américaines, mettant en lumière le conflit entre régulations extra-territoriales et la protection des données des entreprises et des citoyens.

Introduction

Aujourd'hui, huit des dix principales capitalisations boursières ont une partie de leurs activités liées aux technologies *cloud*, contre deux il y a quinze ans. Ce seul chiffre démontre s'il en était besoin la place essentielle de la technologie dans les écosystèmes.

En septembre 2020, dans son discours sur l'État de l'Union, la présidente de la Commission Européenne (CE), Ursula von der Leyen, annonçait que l'Europe devait assurer la souveraineté numérique avec une vision commune de l'UE en 2030, fondée sur des objectifs et des principes clairs. Selon le commissaire Thierry Breton, la souveraineté numérique repose sur trois piliers indissociables : la puissance de calcul, le contrôle de nos données et la connectivité sécurisée[2].

Le "Digital compass 2030"[3] a souligné l'ambition de la Commission de soutenir la transformation numérique pour la résilience de l'UE, avec l'objectif clair d'avoir 75 % des entreprises européennes dans le *cloud* d'ici 2030[4] .

Le chemin est encore long. Alors que le *cloud* est reconnu comme central pour la réussite de la transition environnementale et numérique, la part des acteurs européens du *cloud* sur le marché européen est passée de 28 à 16 % entre 2017 et 2021[5].

[1] https://home.kpmg/fr/fr/home/insights/2021/04/cloud-europeen-croissance-enjeux.html

[2] https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en

[3] https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[4] https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

[5] https://www.srgresearch.com/articles/european-cloud-providers-double-in-size-but-lose-market-share

Pour être capable de disposer d'une autonomie stratégique dans le *cloud*, il est essentiel de bien comprendre les dynamiques en cours, et la manière dont certaines initiatives actuelles peuvent y contribuer.

La crise du Covid-19 et la massification du télétravail ont mis à jour notre dépendance aux solutions technologiques disponibles sur le marché, qui ont permis à de nombreuses organisations de continuer d'opérer et d'assurer notre résilience.

Néanmoins, depuis l'invasion russe en Ukraine, des fournisseurs de services majeurs annoncent l'arrêt de produits et services en Russie : cela souligne que les instabilités politiques peuvent influencer notre indépendance technologique et que nos relations avec les acteurs du marché doivent être repensées.

Cloud & indépendance technologique

Afin de tirer parti des avantages offerts par le *cloud* (réactivité, résilience, élasticité, variabilité des coûts, efficacité énergétique, etc.), les entreprises ont besoin de garanties quant à la protection et la sécurité de leurs données, qui sont aujourd'hui des actifs stratégiques. Au-delà des conditions contractuelles qui lient les utilisateurs de *cloud* à leur(s) fournisseur(s) de service, trois paramètres essentiels doivent être pris en compte : les maîtrises technologique, économique et du contexte juridique applicable.

La maîtrise technologique doit pouvoir s'appliquer sur la chaîne complète : si une entreprise confie ses données à un tiers, a-t-elle le niveau de service adéquat (sécurité, réseau, élasticité...), mais aussi la capacité de récupérer ses données ou ses licences et de les porter dans un autre environnement *cloud* ? Il est important pour l'entreprise de connaître et de mesurer son niveau d'adhérence à une solution proposée par un fournisseur.

Si l'analyse des donneurs d'ordres ne doit pas s'arrêter à la capacité technique des fournisseurs, la maîtrise du contexte juridique est une composante essentielle trop souvent « oubliée » par facilité ou manque de compréhension des enjeux. Un service dépendant d'une autre juridiction que celle de l'utilisateur peut poser question, comme l'a rappelé l'arrêt Schrems II de la CJUE (Cour de justice de l'Union européenne).

Pour une meilleure compétitivité et indépendance technologique, il est nécessaire de disposer d'une gamme de choix parmi plusieurs fournisseurs de *cloud*. L'Europe dispose déjà d'acteurs de référence. Mais le plus grand d'entre eux ne dépasse pas 2 % de parts de marché au niveau mondial. Les stratégies multi-*cloud* des entreprises ne prennent généralement pas en compte la composante juridique décrite ci-dessus et s'appuient souvent sur des fournisseurs de la même origine géographique comme des *hyperscalers* américains par exemple. Ce qui ne les affranchit pas de possibles pressions politiques. Par exemple : fermetures par les sociétés américaines de services en Russie après l'invasion russe en Ukraine.

Il serait essentiel de diversifier les fournisseurs dans les approches multi-*cloud* en incluant des fournisseurs européens à hauteur de 30 ou 50 % du volume. Cela permet également de répondre à certains besoins réglementaires comme la capacité d'opérer des banques systémiques ou d'autres infrastructures critiques.

Quelles problématiques à résoudre ?

Quatre éléments fondamentaux pour la souveraineté numérique doivent être pris en compte :

- liberté de choix technologique ;
- contrôle de la protection des données ;
- maîtrise de la sécurité et de la résilience ;
- contrôle de la protection juridique et des juridictions applicables.

L'ambition de la CE est de soutenir la transformation économique pour une meilleure compétitivité. Mais la CE a également identifié des problèmes à résoudre, tant du côté de l'offre que de la demande :

- les données produites en Europe sont souvent stockées et traitées en dehors de l'Europe, et leur valeur peut être extraite en dehors de l'Europe ;
- l'évolution des règles et des normes de l'UE, en particulier en matière de protection des données, a créé une incertitude pour les clients de l'UE en ce qui concerne l'utilisation des fournisseurs de services *cloud* (CSP ou *cloud service provider*) ;
- les CSP opérant dans l'UE peuvent également être soumis à la législation de pays tiers en conflit avec les lois et les valeurs de l'UE ;
- les micro-entreprises, les jeunes pousses et les PME subissent un préjudice économique en raison de problèmes liés aux contrats (par exemple les clauses contractuelles abusives) ;
- les entreprises de l'UE ne sont pas toujours en mesure d'offrir des services *cloud* ;
- les entreprises européennes peuvent subir un préjudice économique en raison du manque d'interopérabilité et de portabilité des solutions de certains fournisseurs.

Initiatives au service des utilisateurs du *cloud*

Initiatives réglementaires

Plus d'une vingtaine de textes législatifs sont actuellement en cours de discussion au niveau européen pour réglementer de nombreux aspects des fournisseurs de services *cloud*, et viennent compléter certains textes déjà en vigueur comme le Règlement général sur la protection des données (RGPD) ou le Règlement sur la libre circulation des données non personnelles.

Ainsi, le "Digital Markets Act"[6] vise à créer des obligations pour les sociétés en position dominante en leur imposant des obligations *ex ante*, là où le droit de la concurrence actuel impose des procédures longues pour faire reconnaître un abus de position dominante alors que les évolutions technologiques sont rapides. Le "Data Act"[7], quant à lui, vise à proposer une meilleure équité et accessibilité des données sur le marché européen. Le "Digital Services Act"[8] vise à imposer de nouvelles responsabilités au regard de la publication des contenus. La révision de la directive « Efficacité énergétique » devrait permettre une plus grande transparence du secteur dans le domaine environnemental.

Toutes ces initiatives visent à rendre plus claires par la loi les conditions d'exploitation de services *cloud* ou d'utilisation de données des entreprises et citoyens européens, afin de répondre aux ambitions politiques européennes sur le plan environnemental, de la concurrence équitable, de la responsabilité, de la sécurité ou encore de la portabilité des données.

[6] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_fr

[7] https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_1113

[8] https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment_fr#la-nouvelle-rglementation-en-bref

Initiatives d'autorégulation du secteur : exemples

Dans le domaine du *cloud*, la législation n'est pas en mesure de couvrir correctement tous les domaines, ni avec la bonne réactivité (plusieurs années *vs* quelques mois), ni avec la finesse nécessaire.

C'est pourquoi l'autorégulation a une place essentielle pour le secteur, afin de préciser les modalités d'application de régulation existante (ex. RGPD), ou de pallier leur absence dans d'autres cas (ex. neutralité climatique, conditions équitables de licences dans le *cloud*).

Neutralité climatique

En janvier 2021, le secteur du *cloud* a lancé le "Climate Neutral Data Centre Pact"[9], avec le soutien de Frans Timmermans, vice-président exécutif de la CE en charge du "Green Deal", qui engage l'ensemble du secteur des infrastructures de *cloud* et des *data centres* à la neutralité climatique d'ici 2030.

Si l'ambition d'un continent neutre sur le plan climatique en 2050 avait été annoncée par la CE, aucune mesure sectorielle définissant des métriques claires n'avait été publiée. C'est pourquoi la communauté des fournisseurs d'infrastructure *cloud* a contacté en 2019 la CE, afin de définir des métriques et de démontrer une atteinte de neutralité climatique en 2030. Ainsi, la CE avait pu intégrer cet objectif de neutralité climatique des *data centres* pour 2030 dans le cadre de sa stratégie digitale publiée en février 2020.

Cette démarche conjointe de l'industrie et de la Commission a ainsi permis au secteur de définir des objectifs mesurables sur cinq piliers :

- efficacité énergétique ;
- 100 % d'énergie renouvelable ;
- conservation de l'eau ;
- recyclage ;
- réutilisation de la chaleur.

Plus de 90 signataires, dont les plus grands acteurs du marché (Google, AWS, Microsoft, IBM, Equinix, Interxion, OVHcloud, 3DS Outscale, ATOS, et tant d'autres). Conçu pour l'Europe, ce pacte ouvre également la voie en dehors de l'Europe.

Les métriques pourront servir de référence aux législations nationales ou européennes qui pourraient viser à traiter ces questions, sur la base d'un produit solide d'auto-régulation.

Juste concurrence dans le cloud

Le *lock-in* (ou enfermement propriétaire) des clients par certains acteurs informatiques historiques est ancien. Néanmoins avec le développement du *cloud*, certaines pratiques abusives viennent renforcer la capacité de certains à créer de nouvelles situations de domination, notamment dans le cadre des conditions de licences.

Ainsi, en avril 2021, pour la première fois, les utilisateurs et les fournisseurs d'infrastructure *cloud* ont uni leurs forces pour lutter contre ces pratiques de concurrence déloyale de certains fournisseurs historiques au détriment des clients et des autres fournisseurs d'infrastructure *cloud*. Initialement élaborée par CISPE[10] et le CIGREF[11], une charte de

[9] https://www.climateneutraldatacentre.net/

[10] Cloud Infrastructure Services Providers in Europe, https://cispe.cloud

[11] Club informatique des grandes entreprises françaises, https://www.cigref.fr

10 principes de licence logicielle équitable[12] a été publiée et lancée dans de nombreux pays européens, avec le soutien d'associations professionnelles locales d'utilisateurs ou de fournisseurs (France, Italie, Allemagne, Espagne, Royaume-Uni...).

Cette démarche s'appuie sur plusieurs études, dont celle du Professeur Jenny[13], universitaire et président du comité de la concurrence de l'OCDE, qui met notamment en cause les pratiques d'acteurs comme Microsoft, Oracle ou SAP. Des questions similaires ont été soulevées dans le cadre d'affaires de concurrence opposant par exemple les sociétés Nextcloud[14] ou encore OVHcloud[15] à Microsoft auprès des autorités européennes et allemandes de la concurrence.

Ces comportements devraient être naturellement captés dans le cadre du "Digital Markets Act". Mais il apparaît dans les récentes discussions que cela serait tout au mieux partiel. C'est pourquoi l'auto-régulation du secteur serait donc encore nécessaire pour compléter les dispositifs sur lesquels le législateur aura statué.

Protection des données : code de conduite sectoriel

Le RGPD[16] est entré en vigueur en mai 2018. Celui-ci prévoit notamment dans son article 40 que « les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement [...] ». Le législateur encourage ici les acteurs d'un secteur en particulier à proposer aux autorités de protection des données (qui doivent l'approuver) des codes de conduite précis dont la bonne application par les acteurs de l'industrie pourra être certifiée par des auditeurs indépendants.

Ainsi, en mai 2021, le Comité européen de la protection des données (CEPD) a approuvé deux codes de conduite, dont le CISPE Data Protection Code of Conduct[17], premier code de conduite paneuropéen pour les infrastructures de *cloud*. Lancé en septembre 2016 en anticipation du RGPD, son autorité de tutelle est la CNIL[18], et compte aujourd'hui trois auditeurs indépendants accrédités par la CNIL au nom des autorités européennes : Bureau Veritas, LNE et EY CertifyPoint. L'approbation du code a été saluée par de nombreux acteurs majeurs du marché[19].

Le code CISPE permet aux utilisateurs du *cloud* de choisir des offres d'infrastructures fiables répondant aux exigences de protection des données personnelles. Il garantit en outre le choix pour les clients de pouvoir stocker et traiter leurs données exclusivement en Europe.

CISPE, en tant que membre fondateur de Gaia-X, a amené son expertise dans la description des « valeurs européennes » de ses codes de conduite à l'initiative Gaia-X.

[12] https://www.fairsoftware.cloud

[13] https://www.fairsoftwarestudy.com

[14] https://www.theregister.com/AMP/2021/11/29/onedrive_antitrust/

[15] https://www.wsj.com/articles/microsoft-faces-antitrust-complaint-in-europe-about-its-cloud-services-11647463334?mod=flipboard

[16] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fr

[17] https://www.codeofconduct.cloud/

[18] https://www.cnil.fr/fr/la-cnil-approuve-le-premier-code-de-conduite-europeen-dedie-aux-fournisseurs-de-services

[19] https://cispe.cloud/key-market-players-welcome-cispes-code-for-focus-on-data-sovereignty-independence-and-cloud-infrastructure-services/

Initiatives technologiques : l'exemple Gaia-X

L'initiative Gaia-X a été créée par des industriels, dans le sens d'un bien commun et dans la logique de permettre au tissu de PME, ETI et grands utilisateurs de faire des choix éclairés, évitant le *lock-in* (ou enfermement propriétaire).

Son objectif est de favoriser une meilleure circulation des données privées en fournissant un cadre à la fois technique et juridique permettant aux fournisseurs de données d'avoir les garanties sur leur protection et leur utilisation. De ces espaces de données pourront apparaître de nouveaux modèles économiques pour les entreprises en travaillant en écosystèmes.

Genèse de Gaia-X

En février 2020, un *position paper*[20] franco-allemand pose les bases de ce que sera Gaia-X, qui sera confirmée en juin 2020 par son lancement officiel par 22 membres fondateurs[21]. Le projet doit permettre de porter les valeurs européennes de transparence, protection des données, sécurité et portabilité, afin d'aider les utilisateurs européens de *cloud* à reprendre leur destin en main. Gaia-X s'appuie sur deux axes majeurs :

- la définition et la mise en œuvre de « services fédérés » utilisés par les fournisseurs de *cloud* pour faciliter le passage d'un fournisseur à un autre, et aider à mettre fin au verrouillage de certains fournisseurs ;
- le développement d'espaces de données (*data spaces*) pour les marchés verticaux (santé, fabrication, santé...) afin de créer de la valeur dans le partage des données.

Si l'origine du projet est franco-allemande, Gaia-X est une association sans but lucratif, qui a lancé plus de 20 *hubs* nationaux dans de nombreux pays d'Europe (Belgique, Finlande, Italie, France, Allemagne, Espagne, etc.) ou d'ailleurs (Corée du Sud...). Début 2022, plus de 300 organisations sont membres de Gaia-X.

Les fondamentaux de Gaia-X

Le conseil d'administration (CA) de Gaia-X est composé exclusivement d'organisations qui ont leur siège social mondial en Europe. Néanmoins, l'association est ouverte à toute nationalité de membres du moment qu'ils respectent les règles de l'organisation. Le CA valide les principaux documents proposés par les groupes de travail.

Policy rules & labels

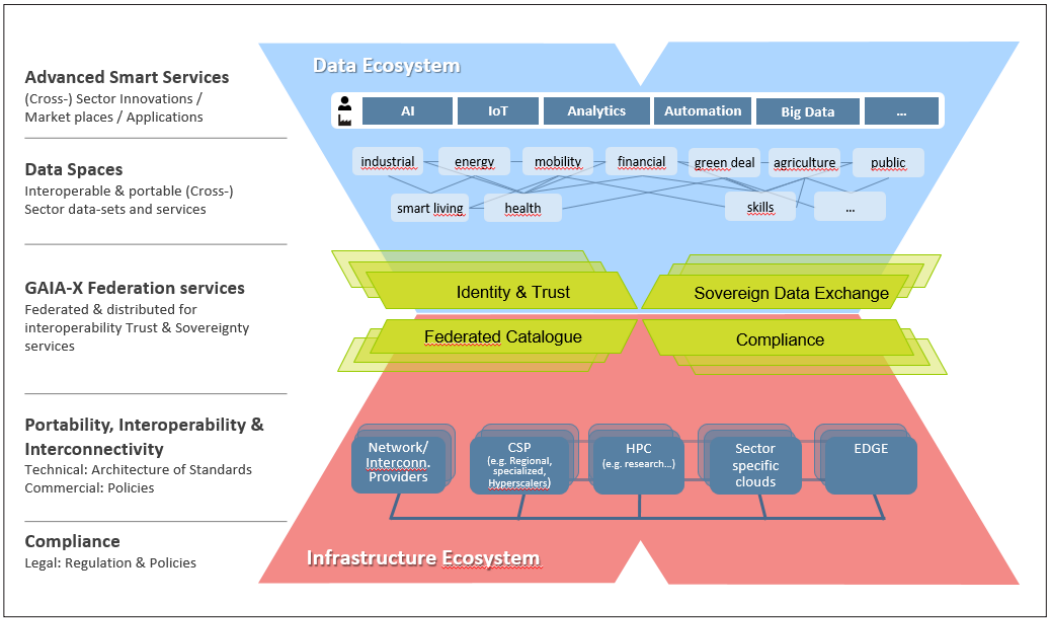
Afin de transcrire en contrôles vérifiables les « valeurs européennes » prônées par Gaia-X, l'association a publié dès son lancement en juin 2020 des *policy rules* qui permettent de vérifier la compatibilité de services *cloud* avec les attentes de l'organisation en termes de protection des données, de sécurité, de portabilité ou encore de transparence. Les fournisseurs devant s'appuyer sur des référentiels externes (codes de conduite ou certifications) référencés par l'organisation sur chaque critère, lorsque cela est possible. Le document a été mis à jour plusieurs fois depuis[22].

Pour compléter ces *policy rules*, Gaia-X a annoncé en novembre 2021 la création de trois niveaux de labels, afin notamment, pour le label le plus élevé, de garantir une immunité

[20] https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf

[21] 22 membres fondateurs (11 allemands et 11 français) : 3DS Outscale, Amadeus, Atos, Beckhoff Automation, BMW, Bosch, CISPE, DE-CIX, Deutsche Telekom, Docaposte, EDF, Fraunhofer, German Edge Cloud, Institut Mines-Télécom (IMT), IDSA, Orange, OVHcloud, PlusServer, Safran, SAP, Scaleway, Siemens.

[22] Dernière version de novembre 2011, https://gaia-x.eu/sites/default/files/2022-01/Policy_Rules_Document_21.11.pdf



The Gaia-X ecosystem of services and data (Source D. R.)

vis-à-vis des accès non européens aux données les plus critiques pour les entreprises. Les labels, outre les *policy rules*, intègrent le respect de l'architecture et des spécifications techniques de Gaia-X[23]. L'une des innovations majeures de Gaia-X est l'automatisation à venir de la chaîne de confiance, en s'appuyant sur des mécanismes de "v*erifiable credentials*" émis par des tiers de confiance pour chacun des critères (lorsque cela est possible).

Architecture & Spécifications

Des documents d'architecture[24], régulièrement ouverts à consultation, sont publiés par Gaia-X *via* son comité technique sur le site de l'association.

L'objectif est de créer un écosystème où des données sont mises à disposition, rassemblées et échangées dans un environnement fiable, les propriétaires des données conservant la pleine souveraineté sur leurs données.

Pour que cette fédération puisse émerger, elle doit se baser sur des principes fondamentaux, des architectures communes, des standards et des ontologies. De la même façon, les espaces de données doivent être construits sur des briques fonctionnelles interopérables. Les services couverts par les spécifications de Gaia-X sont : *identity access management, self description, trust framework* (implémentation des critères des labels et *policy rules*), par exemple.

Les standards, les documents tels que les *policy rules*, les architectures et spécifications, les codes *open source* permettant de créer cette fédération de services, ont un objectif commun : aider l'utilisateur à faire des choix éclairés, correspondant à la gouvernance qu'il ou elle souhaite pour ses données et ses services, en fonction du niveau d'indépendance technologique qu'il ou elle souhaite.

[23] Document soumis à validation par la communauté Gaia-X en février 2022, https://gaia-x.eu/sites/default/files/2022-02/Labelling_Criteria_Whitepaper_v07.pdf

[24] https://gaia-x.eu/sites/default/files/2022-01/Gaia-X_Architecture_Document_2112.pdf

Gaia-X : quelques perspectives

Les différents services fédérés, *trust framework* et politiques d'usages de Gaia-X vont permettre de construire des indicateurs de transparence. Les utilisateurs de *cloud* pourront choisir les services de *cloud* en connaissance de cause, et comparer leurs offres (tel un nutriscore dans l'agroalimentaire).

Conclusion

L'ensemble de ces initiatives visent à renforcer à la fois l'autonomie des utilisateurs européens du *cloud* et l'écosystème européen. Ces deux axes doivent marcher main dans la main. Pour appuyer financièrement cette volonté, les États Membres ont décidé de lancer un PIIEC[25] qui viendra soutenir les principes développés dans Gaia-X, tout comme la proposition de *roadmap* technologique pour la prochaine génération d'offre *cloud-edge*[26], remise par les industriels européens au commissaire Thierry Breton, et qui propose un co-investissement de 19 milliards d'euros dans les cinq prochaines années.

[25] PIIEC = Projet important d'intérêt européen commun : https://www.entreprises.gouv.fr/files/files/secteurs-d-activite/numerique/ressources/consultations/appel-manifestation-interet-ipcei.pdf

[26] https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf