Cloud souverain, où en est la France ?

Le 15 septembre 2021, le directeur interministériel du numérique Nadi Bou Hanna a publié un communiqué à destination des ministères afin de les informer que l'offre Office 365 sur le Cloud Azure de Microsoft ne répondait pas aux exigences de la doctrine cloud de l'État (Cloud au Centre[1]) et en particulier à sa règle R9. Celle-ci prévoit en effet que le traitement de données sensibles ne doit être possible que par des hébergeurs qui sont qualifiés SecNumCloud[2] et également immunisés contre toute loi extraterritoriale (cloud Act, FISAA, …). Suite à ce communiqué, les administrations françaises ne devraient donc plus utiliser le service hébergé par Microsoft.

En réponse à ce communiqué, huit acteurs français se sont regroupés afin de proposer un panel de solutions alternatives à Office 365[5]. Atolia, Jalios, Jamespot, Netframe, Talkspirit, Twake, Whaller et WIMI regroupent 3 millions d'utilisateurs et une offre 100% souveraine hébergée chez des acteurs européens. Le collectif mentionne que l'ensemble de ces solutions sont éligibles pour une intégration dans des infrastructures certifiées SecNumCloud.

L'Agence Nationale des Systèmes d'Informations (ANSSI) propose depuis 2016 un visa de sécurité nommé SecNumCloud. Ce label s'adresse aux fournisseurs de services cloud (IaaS, PaaS, et SaaS) souhaitant apporter des garanties sur la qualité du service fournit et sur le niveau de confiance qui peut leur être accordé. Il constitue également un fort atout marketing car le label SecNumCloud est largement reconnu en France et atteste d'un niveau de sécurité à l'état de l'art attesté par l'ANSSI. Ce label est attribué aux fournisseurs respectant l'ensemble des exigences de sécurité définies par l'ANSSI et ayant fait l'objet d'une évaluation de conformité par un organisme agréé. Le label SecNumCloud permet ainsi aux clients d'être confiants quant à la sécurité mise en œuvre dans l'offre cloud qu'ils souscrivent. Lors des Assises de la Cybersécurité 2021, l'ANSSI a publié une nouvelle version de SecNumCloud. Cette nouvelle version apporte des critères d'immunité contre les lois extracommunautaires, notamment américaines. Elle traite également des aspects de Container-as-a-Service (CaaS), la sélection d'autorités de certification européennes pour l'usage certificats de clé publique.

Le cas du Health Data Hub

L'interdiction d'utiliser Office 365 hébergé par Microsoft dans les administrations françaises remet donc en question la légitimité de l'hébergement des données de santé du Health Data Hub[3] (HDH) dans les infrastructures de Microsoft qui n'est pas certifié SecNumCloud et qui est soumis aux lois américaines. Le HDH, créé en 2019, est un projet visant à regrouper les données de santé de plus de 67 millions de personnes et ayant pour but de favoriser le développement de l'intelligence artificielle dans le domaine de la santé en fournissant de la donnée aux différents pôles de la recherche médicale. Microsoft avait été sélectionné pour héberger ces données, notamment en vertu de sa certification « Hébergeurs de données de santé » (HDS[4]). Ce choix, avait été vivement critiqué dans la mesure où les États-Unis disposent d'outils législatifs (FISAA, cloud Act) pouvant porter atteinte à la confidentialité

[1] https://www.legifrance.gouv.fr/download/pdf/circ?id=45205
[2] https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/
[3] https://www.health-data-hub.fr/
[4] https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante
[5] https://www.jalios.com/upload/docs/application/pdf/2021-10/cloud_souverain_les_8_champions_francais_de_la_dw.pdf

des données hébergées chez des fournisseurs de cloud soumis aux lois américaines, quand bien même celles-ci seraient localisées dans des datacenters sur le territoire européen.

Afin d'encadrer les transferts de données personnelles vers les États-Unis, un accord, désigné sous le terme « *Privacy Shield* » avait été formalisé en 2016 avec l'Europe. Le « *Privacy Shield* » fournissait des garanties sur la protection des données personnelles des citoyens européens stockées et traitées par des sociétés basées aux États-Unis. Le « *Privacy Shield* » permettait donc, en théorie, de protéger les données personnelles stockées dans les infrastructures Office 365 de Microsoft par exemple.
Cependant, le 16 juillet 2020, la Cour de Justice de l'Union Européenne a invalidé le « *Privacy Shield* », l'estimant non conforme au Règlement Général sur la Protection des Données (RGPD), et rendant ainsi illégaux les transferts de données personnelles vers les États-Unis en l'absence de mesures supplémentaires. Suite à l'invalidation du « *Privacy Shield* » et par crainte de transfert des données de santé vers les Etats-Unis, des associations et syndicats ont saisi le Conseil d'État afin de demander une suspension en urgence de la plateforme HDH. Le 14 octobre 2021, le Conseil d'État a indiqué, qu'aucune donnée personnelle hébergée dans le datacenter de Microsoft ne pouvait être transférée en dehors de l'Union Européenne dans le cadre du contrat conclu avec Microsoft. Néanmoins, le juge a démontré qu'il n'était pas exclu que les autorités américaines, dans le cadre de programmes de surveillances et de renseignements, puissent demander à Microsoft et à sa filiale irlandaise l'accès à certaines données.

Afin de répondre à cette problématique à court terme et le temps de trouver une solution pérenne, le Conseil d'État a demandé à la CNIL de travailler avec Microsoft afin de renforcer les mesures de sécurité liées au HDH. Il a cependant estimé que le risque identifié ne justifiait pas une suspension à court terme du HDH. Concernant l'avenir du HDH, le ministre de la santé évoquait en novembre 2020 la volonté de trouver de « nouvelle solution technique » afin de protéger le HDH contre « d'éventuelles divulgations illégales aux autorités américaines (…) dans un délai qui soit autant que possible compris entre 12 et 18 mois et, en tout état de cause, ne dépassant pas deux ans ». L'objectif étant de laisser le temps aux acteurs français et européens d'être prêts à héberger le HDH.

Pourquoi les fournisseurs de cloud américains représentent un risque pour la souveraineté des données françaises ?

Les États-Unis disposent, notamment, de deux armes législatives permettant aux autorités fédérales d'accéder aux données des clients des fournisseurs de cloud.

La première, le Cloud Act, permet notamment aux instances de justice américaines de solliciter auprès des fournisseurs de services opérant aux États-Unis, les communications personnelles d'un individu sans que celui-ci n'en soit informé, ni les autorités de son pays de résidence, ni celles du pays où sont stockées ces données. Le Cloud Act s'applique également aux entreprises étrangères actives sur le sol américain (OVH US par exemple).

La deuxième, nommée FISAA (FISA Amendments Act) est un amendement de la loi FISA (Foreign Intelligence Surveillance Act) de 1978 décrivant les procédures des surveillances physiques et électroniques, et permettant la collecte d'information sur des puissances étrangères. FISAA permet une surveillance de masse et s'étend à toute donnée présente notamment dans le cloud. Le but visé, notamment par la NSA (*National Security Agency*), est d'avoir la possibilité d'intercepter, de déchiffrer, de copier, d'analyser et de stocker, l'ensemble des communications mondiales qu'elles passent par satellites, par câbles, …. C'est notamment cette loi qui a autorisé l'usage d'outils de surveillance utilisés par la NSA et le FBI dans le cadre du projet PRISM révélé par Edward Snowden en 2013.

Ces deux lois permettent donc aux autorités fédérales de forcer les acteurs de cloud américains à fournir des données à la demande, même sur des serveurs situés en Europe et sans informer les personnes ou organismes ciblés.

Stratégie numérique nationale : cloud, pas cloud ? GAFAM, pas GAFAM ?

Le 17 mai 2021, les ministres Bruno Le Maire, Amélie de Montchalin et le secrétaire d'État Cédric O ont annoncé la nouvelle doctrine « Cloud au Centre » de l'État. L'objectif de cette doctrine est de promouvoir l'utilisation du cloud dans les collectivités territoriales et à terme, faire du cloud la plateforme par défaut de l'hébergement des données publiques. La stratégie de cette doctrine s'articule autour de trois piliers que sont le label « cloud de confiance », la politique « Cloud au Centre » des administrations et enfin une politique industrielle mise en œuvre dans le prolongement de France Relance. Seul le premier pilier est traité dans la suite de cet article.

L'adoption du label « cloud de confiance » apporte de la cohérence en termes de souveraineté et de sécurité de la donnée notamment avec le projet Gaia-X. Gaia-X est une initiative germano-française lancée en juin 2020 qui a pour objectif de proposer une réponse européenne à la montée en puissance des GAM (Google, Amazon, Microsoft) et d'Alibaba cloud (fournisseur cloud chinois) à travers le partage de la donnée technologique et industrielle entre ses membres. L'idée n'est pas de créer une société unique et un cloud surpuissant mais plutôt de se fonder sur le principe de décentralisation pour créer une « infrastructure européenne des données ». Par exemple, pour les activités de recherche sur les voitures autonomes, Gaia-X pourrait permettre de fournir une quantité de données en très forte volumétrie grâce à l'ensemble de ses membres actifs sur ce segment (BMW par exemple).

Le projet Gaia-X a néanmoins été récemment critiqué lorsque de nouveaux membres Google, Microsoft, Amazon, Alibaba, Palantir, Huawei… ont fait leur apparition au sein de l'association. Pour les défenseurs de la souveraineté numérique, l'adhésion de ces membres est en contradiction avec l'objectif initial du projet et vient décrédibiliser les objectifs poursuivis.

De son côté Gaia-X répond qu'il n'a jamais été question de faire émerger un écosystème cloud et de données souverain et sécurisé porté par des acteurs 100% européens, mais bien d'inviter à la table des fournisseurs américains et chinois sous réserve que ces derniers montrent patte blanche.

Quelles solutions souveraines pour l'hébergement des données de l'État ?

C'est dans ce contexte tendu qu'a été annoncée « Bleu », le 27 mai 2021, soit 10 jours après les annonces des ministres concernant la doctrine « cloud au centre ». Bleu est une entreprise créée par Orange et Capgemini destinée à répondre au label « cloud de confiance » de l'État et ainsi proposer une solution de cloud souverain aux entreprises et administrations françaises. Ce cloud s'appuiera néanmoins sur la technologie Azure et la suite bureautique de Microsoft mais sera, selon le communiqué de presse, hébergé dans une « infrastructure isolée, basée sur des centres de données situés en France » et exploité par des compétences françaises. Orange et Capgemini assurent donc que le cloud qu'ils mettront à disposition de leurs clients sera immunisé à l'égard de législations extraterritoriales. Orange et Capgemini souhaitent faire qualifier « Bleu » au label SecNumcloud de l'ANSSI afin de répondre aux plus hautes exigences de sécurité et ainsi pouvoir cibler des marchés très exigeants en matière de cybersécurité (Opérateur d'Importance Vitale, Opérateur de Service Essentiel, Ministères, …). Bleu a ainsi vocation à rejoindre à terme l'initiative européenne Gaia-X, dont Orange et Capgemini sont membres, afin de contribuer à la création de solutions souveraines à l'échelle européenne et participer au développement de cet écosystème.

Thales s'est également positionné dans la course au cloud en contractant un partenariat stratégique avec Google Cloud Plateform. Ce partenariat, à l'instar de Bleu, ambitionne de répondre aux exigences de l'Etat français pour le « cloud de confiance ». Bleu et Thales/GCP souhaitent ainsi proposer une offre qualifiée SecNumCloud et rejoindre les trois acteurs déjà labellisés : OVHcloud avec son private cloud IaaS, OoDrive et ses trois services en SaaS (BoardNox, iExtranet et PostFile) et enfin Outscale avec son offre IaaS. Autant de fournisseurs potentiels, présentant un excellent niveau de sécurité, pouvant être utilisés pour héberger des données sensibles de l'État français. Rappelons également que ces trois fournisseurs de services sont désormais détenteurs de la certification HDS, faisant d'eux des candidats idéaux pour l'hébergement du HDH !

En conclusion

Comme nous l'avons vu dans cet article, la souveraineté numérique dans le cloud n'est pas encore mature, il reste encore du travail afin de mettre en œuvre des solutions d'hébergement répondant à l'ensemble des enjeux techniques, juridiques et politiques de notre pays. Nous pouvons néanmoins saluer les multiples initiatives des acteurs français qui proposent des solutions pertinentes afin de répondre aux besoins de souveraineté de la nation et de se défaire des géants marketings et financiers que sont les GAM (Google, Amazon, Microsoft) dans nos institutions.