L'émergence d'un cloud souverain européen

Avec l'annulation par la Cour de justice l'Union européenne, le 16 juillet dernier, de la décision d'adéquation qui permettait à toute société américaine « auto-certifiée » aux standards RGPD d'exporter sans autre formalité des données à caractère personnel outre-Atlantique, l'heure d'un cloud souverain européen a véritablement sonné pour Me Eric Le Quellenec.

Par Eric LE QUELLENEC

Avocat
Directeur du département informatique conseil
Alain Bensoussan Avocats Lexing
Membre du Conseil de l'Ordre

➔RLDI 5927

Alors que la crise sanitaire actuelle pousse l'Europe à réfléchir aux moyens techniques et économiques de sa souveraineté, elle vient déjà de franchir une étape cruciale avec l'adoption d'un référentiel commun en matière de cloud computing. Cette initiative, appuyée par les institutions européennes mais aussi la France et l'Allemagne, fait suite à de nombreuses alertes sur la nécessité stratégique de disposer de telles ressources informatiques, après notamment quelques échecs à l'échelon national, tout particulièrement en France.

Après un rapide recensement des risques juridiques pesant sur le cloud computing « mondialisé » (I), les solutions proposées par le projet Gaia-X sont présentées (II).

I. LES RISQUES JURIDIQUES DU CLOUD MONDIALISÉ

Le modèle unique d'un cloud mondial unique avec un service qui soit le même pour tous (concept technique, commercial et contractuel du « one to many ») ne résiste pas aux contraintes légales nationales qui se développent partout dans le monde.

C'est d'abord et surtout le Cloud Act[1] adopté le 23 mars 2018 qui a marqué un tournant très fort.

Le Cloud Act est l'acronyme de « clarifying lawful overseas use of data act » signifiant en français : loi de clarification du transfert légal de données Outre-mer. Cette loi vient réformer le Stored Communications Act de 1986 qui exigeait de fastidieuses demandes d'entraides judiciaires internationales, fondées sur des traités bilatéraux pour obtenir la communication de la moindre donnée hébergée en dehors du territoire américain. Sur simple réquisition judiciaire, toute société de droit américain doit désormais fournir de telles informations, indépendamment de la localisation physique de l'information. Le Cloud Act s'applique à toute « United States person », définie très largement comme étant pour les personnes morales, toute société de droit américain, filiale étrangère incluse.

Comme cela a été mis en exergue par le député Raphaël Gauvain dans un rapport qui a fait date[2], cette loi conjuguée aux législations à vocation extra-territoriale de lutte contre le terrorisme[3], la corruption ou encore la contrefaçon peut permettre à « l'Oncle Sam » d'accéder à un nombre d'informations considérable[4].

L'onde de choc a été très importante et l'émergence de législations équivalentes en Chine[5] ou en Russie[6] a renforcé les craintes de nombres entreprises cherchant alors par des clouds privés coûteux, à défaut de clouds souverains, à relocaliser et cloisonner autant que faire se peut leurs données stratégiques.

Dans le même temps, le délégué à la protection des données personnelles pour les institutions européennes, appelé « contrôleur européen à la protection des données personnelles » s'est alarmé des nombreuses insuffisances des contrats Microsoft pour son service phare appelé Azure, de type Infrastructure as a Service (IaaS).

Ces travaux ont été menés en coopération avec le ministre néerlandais de la justice qui, parallèlement, s'était engagé dans la réalisation d'une étude d'impact sur le service bureautique phare de Microsoft, Office 365, hébergé dans le cloud « maison », Azure.

Le Contrôleur européen a relevé en 2019 :

– l'absence de transparence sur la circulation des données personnelles, notamment hors de l'Union européenne ;

(1) US Cloud Act – Extrait du Consolidated Appropriations Act 2018 / H.R.4943 – CLOUD Act, 115th Congress (2017-2018).

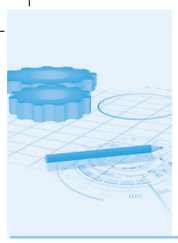
(2) Rapport Gauvain du 26 juin 2019 traitant de « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale ».

(3) Le Patriot Act adopté suite aux attentats du 11 septembre 2001 a toujours été perçu comme une menace pour la souveraineté européenne.

(4) A noter qu'il existe déjà une coopération active entre services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis dite « five eyes ».

(5) Loi chinoise sur le renseignement national, 28 juin 2017.

(6) Loi russe n°242-FZ, entrée en application dès le 1er septembre 2015.



– l'impossibilité de « prendre le contrôle total » de ses données, notamment du fait de l'activation automatique d'outils de traçabilité des actions utilisateurs et de statistiques ;

– la difficulté pour l'utilisateur à pouvoir faire valoir ses droits dans les interfaces actuellement disponibles.

Dès 2012, l'Agence européenne de cybersécurité, l'Enisa avait déjà formulé ses recommandations sur la contractualisation des services dans le cloud[1]. Pour proposer plus concrètement des clauses types pouvant s'appliquer à toute administration publique, un forum dit de la Haye[2] a été mis en place pour réunir les parties intéressées, utilisateurs et prestataires mais aussi toute partie concernée, à se joindre à ces travaux. Avec les travaux du forum, il s'agit désormais d'aller bien au-delà des préconisations de l'Enisa, alors que le cadre réglementaire est de plus en plus précis et contraignant. Il est d'ailleurs possible de considérer, au moins pour la gestion des données personnelles, que le contrat cloud est désormais un contrat nommé[3].

Microsoft avait pris publiquement l'engagement formel de revoir ses contrats[4]. La nouvelle version des Online Services Terms (OST) est intervenue début 2020. A la lumière des critiques formulées par le contrôleur, outre les travaux du ministre néerlandais de la justice, les dispositions suivantes devraient être revues.

Une clause doit garantir la possibilité pour le responsable du traitement d'assurer leurs droits effectifs aux utilisateurs. Ces personnes concernées doivent ainsi disposer de toute information utile sur l'usage de leurs données et pouvoir directement exercer leurs droits dans les outils utilisés.

La clause d'audit sur site devrait être désormais présente au contrat selon des conditions à préciser. Elle était jusqu'alors refusée par Microsoft au prétexte que les certifications à diverses normes, dont la norme ISO 27001 complétée de la norme ISO 27018 sur l'hébergement de données personnelles, devaient suffire en soi.

Enfin, dans la mesure où le Contrôleur européen et le CEPD[5] ont déjà exprimé leur inquiétude sur le Cloud Act[6], il devrait être prévu que le prestataire, dès lors que cela peut être envisageable par cette loi, devrait s'engager à en contester la mise en œuvre auprès du juge compétent.

(1) Guide achat cloud, Enisa, 2012, https://www.enisa.europa.eu/news/enisa-news/prs-in-french/acheter-de-facon-securisee/view.

(2) https://thehagueforumforcloudcontracting.eu/.

(3) Le Quellenec E, « Les contrats informatiques et la protection des données à caractère personnel : aspects pratiques », AJ contrat, D. 2019, p.420.

(4) https://news.microsoft.com/europe/2019/11/18/introducing-more-privacy-transparency-for-our-commercial-cloud-customers/.

(5) Comité européen à la protection des données personnelles regroupant les autorités de contrôles nationales.

(6) Lettre de couverture sur le Cloud Act du 10 juillet 2019 r : https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_coverletter_en.pdf

Le 2 juillet 2020, le Contrôleur ne devait finalement relever que de modestes progrès du côté des documents contractuels Microsoft[7].

Le 16 juillet 2020, l'arrêt dit Schrems II[8], a annulé la décision d'adéquation qui permettait à toute société américaine « auto-certifiée » aux standards RGPD d'exporter sans autre formalité des données à caractère personnel outre-Atlantique.

L'heure d'un cloud souverain européen a véritablement sonné.

II. GAIA-X : UN CADRE SOUPLE ET PARTICIPATIF

Avant d'envisager un cloud un cloud souverain, il a été tiré les conclusions de l'échec des initiatives nationales, notamment en France. Proposer un service standard déconnecté du réel besoin du marché, tout en contraignant des concurrents à travailler ensemble, ne peut que mener à l'échec.

C'est donc sur la base d'un cadre résolument plus souple et mieux connecté aux attentes des clients que l'initiative européenne devait se construire.

Les lignes directrices du cloud européen Gaia-X sont désormais connues. Le 4 juin 2020, le Ministre de l'Economie, Bruno Le Maire et son homologue allemand, Peter Altmaier ont officialisé le lancement du cloud européen, Gaia-X[9]. Ainsi, face à la domination des géants américains et chinois, ce projet commun à la France et à l'Allemagne vise à affirmer la souveraineté numérique européenne[10].

Annoncée en 2019 lors du Sommet numérique, le projet européen répond à trois principaux objectifs :

– concrétiser la conception technique et économique des infrastructures ;

– créer un écosystème commun d'utilisateurs et de prestataires issus d'organisations de l'administration publique, de la santé publique, des entreprises et des institutions scientifiques ;

– créer un cadre favorable et des structures de soutien.

Empruntant son nom à la déesse grecque de la Terre, Gaia-X a vocation à devenir une plateforme d'offre multi-services, multi-prestataires de stockage des données.

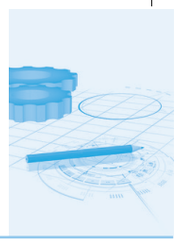
Conçu comme un moteur de recherche amélioré, Gaia-X se présente comme un « méta cloud » en ce qu'il fixe un référentiel technique commun à tous les adhérents à la fondation, structure juridique qui le porte et qu'il permet à tout utilisateur en fonction de sa « cloud strategy » de sélectionner la configuration la mieux adaptée. Cette plate-

(7) Rapport public disponible sur : https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html

(8) CJUE Facebook Ireland Ltd vs. Maximillian Schrems, C-311/18 : NDLR : voir comm. Lassalle M. *supra* n°5913 ; égal. *supra* n°5918. .

(9) Communiqué conjoint, « Sous l'impulsion de l'Allemagne et la France, l'Europe fait un premier pas vers une infrastructure de données », 4 juin 2020.

(10) Manifeste franco-allemand pour une politique industrielle européenne, 19 février 2019.



forme offrira à terme un catalogue de services numériques porté par des hébergeurs et des éditeurs de logiciels, préalablement engagés autour de standards visant à renforcer la confiance des utilisateurs.

Ainsi, le projet européen n'a pas vocation à directement concurrencer les géants américains, chinois ou indiens. Il s'agit davantage de rassembler les acteurs européens existants autour de standards et d'attributs communs.

Gaia-X fonctionnera autour de trois principes :

- Interopérabilité : les plateformes doivent communiquer entre elles, sans placer le client dans une situation trop fort de dépendance technique. Il s'agit aussi de la réversibilité des données. Les utilisateurs pourront récupérer leurs données hébergées chez un fournisseur pour les transférer chez un autre fournisseur ; et ce, grâce à des API aisément configurables ;
- Transparence : les entreprises devront indiquer le lieu de stockage des données et d'implantation des data centers ;
- Confiance : chaque membre de la fondation doit faire certifier[11] tout ou partie des services proposés.

Seules les offres répondant aux normes de sécurité, d'intégrité et de protection des données du projet y seront alors proposées.

A ce jour, 22 entreprises allemandes et françaises ont accepté de prendre part au projet Gaia-X. Parmi elles, on peut citer Dassault Systèmes, Orange, Siemens, SAP, Atos, Scaleway et Robert Bosch.

En réunissant les acteurs majeurs du Cloud français et allemand, Gaia-X va donc permettre une meilleure visibilité des offres européennes. L'écosystème de cloud européen offrira alors aux entreprises européennes une alternative de confiance aux opérateurs dominants du marché.

Toutefois, Gaia-X ne ferme pas la porte aux acteurs non européens qui respecteraient les normes de confidentialité les plus strictes. On pense notamment à Microsoft et son offre cloud, Azure Stack.

Très attendus, les premiers services de Gaia-X devraient être proposés d'ici à 2021.

Plus que l'adoption d'un Cloud Act européen[12] qui viendrait frontalement s'opposer au Cloud act américain, Gaia-X est la réponse à la fois technique, commerciale et juridique au cloud act américain. La méthode Monnet-Schuman dite des « petits-pas » reposant sur la réalisation de projets concrets devrait, une fois encore, faire ses preuves dans la construction d'une souveraineté numérique européenne. ■

(11) Des initiatives franco-allemandes entre l'ANSSI et le BSI existent déjà avec succès à ce sujet avec le label ESCloud : https://www.ssi.gouv.fr/actualite/escloud-un-label-franco-allemand-pour-les-services-informatique-en-nuage-de-confiance/.

(12) « Vers l'adoption prochaine d'un Cloud act européen ? », Post Le Quellenec E. ., 17 janv. 2019, https://www.alain-bensoussan.com/avocats/bientot-un-cloud-act-europeen/2018/08/23/.