DOCTRINE

DONNÉES PERSONNELLES

Health Data Hub hébergé par Microsoft : et le Cloud Act ?

Si le choix de Microsoft comme hébergeur des données de la plateforme des données de santé Health Data Hub est justifié par ses garanties de sécurité technique et sa structure d'hébergement, il pose des questions par rapport au Cloud Act américain en termes de risque d'ingérences extérieures.

Depuis début janvier 2020, une nouvelle plateforme de données de santé intitulée « *Health Data Hub* », a été lancée[1], à l'initiative du gouvernement. Elle a pour finalité de centraliser plusieurs sources de données de santé des citoyens français sur une même plateforme, afin de permettre son accès à différents acteurs du monde de la santé (chercheurs, institutions, start-ups...).

On peut s'étonner qu'un tel projet mené par les services publics ait été doté d'une appellation anglaise : « *Health Data Hub* ». Ceci ne laissait cependant pas présager que la gestion technique de cette plateforme serait laissée aux mains d'une entité américaine, membre des « *Gafam* » (Google, Apple, Facebook, Amazon et Microsoft), à savoir Microsoft.

Le traitement de données sensibles des citoyens français par un prestataire non français, et qui plus est américain, est susceptible de soulever des difficultés. Comme toute entité américaine, Microsoft est en effet soumise au Cloud Act, réglementation américaine, qui autorise des ingérences du gouvernement américain dans les bases de données de l'entreprise.

L'hébergement des données de santé, une prestation strictement encadrée par la loi

Les données de santé sont des données considérées comme « *sensibles* », dont le traitement est, par principe, interdit par le Règlement UE n°2016/679 dit « *RGPD* ». Si ces données de santé peuvent être, dans certains cas limitativement énumérés, traitées, ce traitement se fait dans un cadre juridique strict, et requiert des garanties de protection supplémentaire, comme par exemple le consentement explicite de la personne concernée.

Outre la mise en place de garanties supplémentaires lors de leur collecte, la conservation de ces données dites sensibles et surtout leur hébergement, est soumis à un régime strict et spécifique. En effet, dans le cas où ces données de santé ne sont pas sauvegardées directement chez un professionnel de santé autorisé à les conserver, tout hébergement de ces dernières, par un prestataire technique extérieur, devra faire l'objet d'une procédure spécifique.

L'article L1111-8 du code de la santé publique impose ainsi que le prestataire technique, hébergeur de données de santé, soit certifié « *Hébergeur de données de santé* » (« *HDS* ») dans des conditions fixées par décret du Conseil d'Etat[2]. La procédure de certification passe par une phase d'audit, au cours de laquelle un organisme certificateur s'assurera que la structure de la société candidate est conforme aux référentiels de certification[3]. Une fois le certificat HDS délivré par l'organisme certificateur, celui-ci est valable pour une durée de trois ans, avec un audit de surveillance réalisé chaque année.

La loi française n'interdit pas aux prestataires étrangers d'obtenir cette certification HDS. C'est ainsi qu'en novembre 2018, la société américaine Microsoft Corporation, c'est-à-dire la société de droit américain, obtient la certification HDS[4], ce qui lui permet de proposer ses services Cloud au secteur français de la santé et donc d'héberger les données de santé des citoyens français.

La certification HDS ne protège pas d'un accès et d'une captation des données de santé des citoyens français, sous couvert du Cloud Act

Le Cloud Act, dont l'acronyme signifie « *Clarifying Lawful Overseas Use of Data* », est une loi américaine

(H.R.4943) bipartisane, votée par le 115ème Congrès américain et promulguée le 23 mars 2018 par le Président Donald Trump.

Cette réglementation permet aux autorités d'enquêtes et de poursuites américaines de demander l'accès à toute donnée numérique stockée par un fournisseur de service Cloud présentant un « *lien suffisant* » avec les Etats-Unis, et susceptible d'intéresser les autorités dans le cadre d'une enquête. Le plus souvent, cette demande d'accès et de captation de données, est endossée par un juge. Cependant, il est des cas où cette ingérence est opérée hors de tout cadre judiciaire. Enfin, et tel que rapporté par Edward Snowden[5], il n'est jamais exclu que les données et bases de données constituées à partir de ces accès contrôlés, donnent ensuite lieu à une utilisation détournée.

Pour mémoire, cette demande d'accès et de captation, dans la mesure où elle répond notamment à une lutte légitime contre le terrorisme international, se fait indépendamment de la nationalité des personnes concernées et de la localisation des données. Il est également établi que les prestataires concernés par ce « *partenariat public – privé* » légalisé par la loi américaine[6], sont toutes des « *US Persons* », c'est-à-dire non seulement toutes sociétés établies sur le sol nord-américain, y compris les filiales européennes des maisons mères, mais également les filiales des sociétés européennes.

En résumé, il est donc possible pour les autorités américaines de demander l'accès et la captation de données concernant des citoyens français, pour des informations hébergées en France, à un prestataire américain, tel que Microsoft Corporation.

Le Cloud Act outrepasse la réglementation européenne et notamment le RGPD en permettant le transfert de données personnelles de citoyens français vers les Etats-Unis, en dehors de toute convention internationale, sans le consentement de la personne concernée, et sans aucune garantie.

L'obtention d'une certification HDS par un prestataire américain ne protège pas les citoyens français d'un tel transfert, qui pourrait s'opérer sans leur consentement et même sans qu'ils en soient informés, dès lors que le prestataire a accès à leurs données et donc se trouve en position d'avoir à répondre à une demande des autorités américaines.

Si cette certification apporte des garanties de sécurités techniques, sur la structure d'hébergement, elle ne peut donc prémunir des ingérences extérieures.

Face à ce risque réel, on peut se demander s'il est possible, par contrat, de protéger voire d'interdire le transfert des données des citoyens français dans ce cadre. La réponse est à notre sens négative. Pour rappel, l'article 6 du code civil énonce qu'« *on ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs* ». Ce principe de droit est universel. L'ordre public prévaut toujours sur le contrat, expression de la volonté de deux personnes. Le Cloud Act, considéré comme loi étatique et d'ordre public, ne devrait donc pas pouvoir être détourné ou mis en échec par un contrat.

En conclusion

Il est nécessaire que les autorités publiques françaises, à l'origine du Health Data Hub, apportent plus de précisions quant au rôle exact que jouera Microsoft dans le fonctionnement de la plateforme. Il est toujours possible d'organiser la prestation de telle sorte que le prestataire ne puisse ni avoir accès ni extraire des données de la plateforme qu'il opère. En Allemagne par exemple, l'opérateur Deutsch Telecom a passé un accord avec Microsoft, aux termes duquel l'opérateur allemand intervient comme « *data trustee* », tiers de confiance des données pour le Cloud de Microsoft en Allemagne, en prenant la responsabilité de protéger les données des clients de Microsoft[7].

Le choix de Microsoft par le gouvernement est probablement justifié par le fait que le prestataire est de bonne qualité, c'est certain, et surtout, comme l'a reconnu le gouvernement lui-même, qu'il est le seul « *capable de répondre à leur demande* ».

Cette situation met une fois de plus en lumière les difficultés rencontrées par l'Union européenne depuis 15 ans, à mettre en place une politique publique facilitant l'émergence d'acteurs de grandes tailles, capables de fournir des services alternatifs aux Gafam. En réalité, les Gafam ne sont pas à blâmer, c'est nous, européens, avec nos contradictions et nos incohérences, qui le sommes.

Il reste désormais à espérer que ce type d'initiatives n'ouvrent pas la porte à des atteintes, même de bonne foi, aux droits des personnes concernées résidant dans l'Union européenne.

Alexandra ITEANU
Avocat
Cabinet ITEANU

Notes

(1) La loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé a permis de créer et définir le GIP Plateforme de données de santé (le Health data hub). L'arrêté du 29 novembre 2019 définit quant à lui les modalités d'organisation de cette nouvelle structure.

(2) Décret 2018-137 du 26 février 2018

(3) Le référentiel de certification fait référence aux normes ISO 27001 « système de gestion de la sécurité des systèmes d'information » et ISO 20000 « système de gestion de la qualité des services »

(4) Numéro de certification HDS 701569

(5) « Mémoires vices » d'Edward Snowden (Ed ; du Seuil)

(6) Il l'était déjà précédemment, notamment avec l'USA PATRIOT ACT de novembre 2001, mais prend une nouvelle ampleur avec cette nouvelle Loi

(7) https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-to-act-as-data-trustee-for-microsoft-cloud-in-germany-362074