DONNÉES PERSONNELLES

Cloud non-souverain et données de santé : *le Conseil d'Etat au secours de la Cnil*

Le Conseil d'Etat a récemment rendu plusieurs décisions[1], par lesquelles il confirme la possibilité pour le Groupement d'intérêt public Plateforme des données de santé (le « Health Data Hub ») de recourir à Microsoft pour l'hébergement d'un entrepôt de données de santé. Est-ce que cela signifie qu'il est donc possible d'héberger des données de santé sur des cloudnon-souverains ?

Le Health Data Hub, « *chargé par la loi de recueillir les bases de données de santé les plus importantes du pays* », a conclu un contrat de services avec l'Agence européenne du médicament (EMA). Ce contrat porte notamment sur « *la constitution d'un entrepôt de données de santé visant à permettre des recherches, études et évaluations en pharmaco-épidémiologie* ». « *Un appariement entre une fraction des données de la base principale du système national des données de santé (SNDS) et les dossiers médicaux fournis par quatre établissements partenaires en France* » y est prévu. Ce projet est dénommé « *EMC2* ».

Le cas de l'entrepôt de données de santé « EMC2 » du Health Data Hub

Pour mémoire, la Cnil a publié un référentiel relatif « *aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données de santé dans le domaine de la santé* ». Ce référentiel concerne uniquement les traitements « *nécessaire[s] à l'exercice d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement* ». Ainsi, un organisme, responsable de traitement, souhaitant mettre en œuvre un entrepôt de données de santé doit, par principe, s'assurer de sa conformité à ce référentiel. Dans le cas où l'organisme considère être en stricte conformité avec le référentiel, il peut alors se contenter d'une déclaration de conformité auprès de la Cnil. Dans l'hypothèse, en revanche, où il existe des écarts avec les exigences prévues au référentiel, il appartient à l'organisme de saisir la Cnil d'une demande d'autorisation spécifique préalable. Dans la mesure où le projet « *EMC2* » ne répondait pas à toutes les exigences prévues dans ledit référentiel, en particulier celles relatives au sous-traitant, le Health Data Hub avait saisi la Cnil d'une demande d'autorisation.

À noter, en particulier, que le projet « *EMC2* » prévoyait de recourir à l'hébergeur Microsoft Ireland Ltd (avec la solution Microsoft Azure), société irlandaise, dont la maison mère est située aux Etats-Unis. Le risque d'accès par des tiers à des données personnelles sensibles a été un des points d'attention de la Cnil.

Une analyse de la Cnil sujette à débats

Dans sa décision[2], la Cnil a relevé plusieurs éléments semblant pencher pour un refus d'autorisation. Tout d'abord, la Cnil a estimé qu'il existe – en dépit du « *Data Privacy Framework* » (à savoir la décision d'adéquation du 10 juillet 2023 reconnaissant que le cadre de transfert des données à caractère personnel « *Etats-Unis/UE* » assure un niveau de protection adéquat) - bien un risque d'accès aux données par les autorités américaines puisque la maison mère de la société Microsoft Ireland Ltd est située aux Etats-Unis (et donc soumise au droit de cet Etat).

La Cnil a ensuite rappelé sa recommandation « *pour les bases de données les plus sensibles* », selon laquelle il appartient à l'organisme de ne faire appel qu'à un hébergeur exclusivement soumis au droit européen et certifié « *SecNumCloud* ». À cet égard, la Cnil a indiqué que les entrepôts de données de santé appariés avec le SNDS doivent faire l'objet d'une vigilance particulière (« *malgré le fait que ces données soient pseudonymisées* »), dans la mesure où « *la CNIL a toujours demandé aux porteurs de projet, publics et privés, de s'assurer que l'hébergeur des données n'est pas soumis à une législation extra-européenne* ». La circulaire de la Première Ministre du 31 mars 2023 demandait d'ailleurs, comme l'a souligné la Cnil, que les autorités publiques s'assurent que « *les données 'd'une sensibilité particulière' hébergées dans le cloud ne soient pas soumises à des lois extra-européennes* ». La Cnil en a conclu que le choix du Health Data Hub « *apparaît en très nette contradiction avec [ces] éléments* ».

Mais d'autres éléments ont conduit la Cnil à refaire pencher la balance... La Cnil a, d'une part, déploré qu'aucun prestataire, susceptible de répondre actuellement aux besoins exprimés par le Health Data Hub, « *ne protège les données contre l'application de lois extraterritoriales de pays tiers* » (alors que, selon la Cnil, « *le projet EMC2 aurait pu être retenu par le [Health Data Hub] pour préfigurer la solution souveraine vers laquelle il doit migrer* »), et, d'autre part, souligné « *qu'il est nécessaire que les engagements pris vis-à-vis de [l'Agence européenne du médicament] puissent être honorés* ».

La Cnil a alors décidé d'autoriser la mise en œuvre de l'entrepôt de données de santé « *EMC2* » avec un hébergement chez Microsoft pour une durée de 3 ans (durée de la migration de la plateforme).

Cette décision a fait l'objet de plusieurs critiques dans la mesure où elle reconnaît notamment le non-respect du projet « *EMC2* » à des exigences nationales de souveraineté tout en validant ce projet, tandis que d'autres projets similaires hébergés par Microsoft avaient été refusés par la Cnil. Plusieurs organismes ont saisi le Conseil d'Etat en annulation pour excès de pouvoir de la décision de la Cnil, notamment l'association Internet Society France[3]. À cette occasion, plusieurs requérants ont remis en cause la légalité du « *Data Privacy Framework* ».

La position de la Cnil, validée par le Conseil d'Etat

Dans un premier temps, le Conseil d'Etat a souligné que l'objet de l'autorisation de la Cnil portait sur « *la création d'un entrepôt de données de santé, hébergées dans des centres de données situés en France* » et non pas sur « *un transfert de données personnelles vers les Etats-Unis* », sachant que seules les « *données techniques d'usage de la plateforme* » sont susceptibles de faire l'objet d'un tel transfert. Ce faisant, le Conseil d'Etat a considéré que les critiques portant sur l'illégalité du « *Data Privacy Framework* » et la méconnaissance par la Cnil de textes encadrant le transfert de données à caractère personnel vers des pays tiers[4], en l'occurrence les Etats-Unis, n'avaient pas lieu d'être.

Dans un deuxième temps, le Conseil d'Etat a analysé la critique selon laquelle la décision de la Cnil méconnaîtrait l'article 28.1 du RGPD, en application duquel le sous-traitant – ici Microsoft Ireland Ltd – doit présenter des « *garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée* ». Sur ce point, la Haute Juridiction a jugé que, certes, le risque « *ne peut être totalement exclu* » que les autorités américaines, « *sur le fondement des lois de ce pays, par l'intermédiaire de la société-mère de l'hébergeur* », puissent faire des demandes d'accès aux données du traitement autorisé, données qualifiées « *d'une sensibilité particulière eu égard à leur nature de données de santé mais aussi au potentiel scientifique et économique de leur exploitation* ». Pour autant, le Conseil d'Etat a relevé plusieurs éléments permettant de justifier le respect des dispositions de l'article 28.1 du RGPD, à savoir : (i) la pseudonymisation multiple des données par la Caisse nationale d'assurance maladie et par le Health Data Hub « *avant toute mise à disposition au sein de l'entrepôt « EMC2* », (ii) la certification « *HDS* » de Microsoft Ireland Ltd « *qui implique un audit régulier par un organisme accrédité* » (en ayant, par ailleurs, relevé que Microsoft Ireland Ltd « *ne peut bénéficier de la certification « SecNumCloud* » délivrée par (...) [l'ANSSI] dès lors qu'elle est la filiale d'une société soumise au droit des Etats-Unis ») et (iii) la durée de l'autorisation de la Cnil, limitée à 3 ans.

En troisième lieu, le Conseil d'Etat a estimé que, au regard des éléments et des finalités d'intérêt public poursuivies par le traitement, il n'y avait pas « *d'atteinte disproportionnée au droit à la vie privée* ».

Enfin, la Haute Juridiction a relevé notamment que la « *méconnaissance des prescriptions de la doctrine d'utilisation de l'informatique en nuage par l'Etat* » - à savoir la circulaire de la Première Ministre susvisée – par la Cnil étant sans incidence. La Cnil n'est effectivement pas contrainte de respecter une telle doctrine.
En conséquence, le Conseil d'Etat a rejeté les recours.

Que peut-on en retenir ?

La Haute Juridiction a validé la décision de la Cnil admettant donc la possibilité d'un hébergement temporaire de données de santé sur un cloud non-souverain, faute de mieux.

Des garanties telles que la pseudonymisation, la certification HDS (bien que moins exigeante que la certification « *Secnumcloud* ») et ce, pour des finalités spécifiques d'intérêt public et une durée limitée du traitement concerné peuvent permettre de « *légaliser* », dans une certaine mesure, un hébergement de données de santé sur un cloud non-souverain.

La prudence reste toutefois de mise compte tenu du contexte particulier du traitement objet du projet « *EMC2* » et des travaux gouvernementaux à venir sur la mise en place / l'exigence d'un cloud souverain.

À suivre...

Alexandre FIEVEE
Avocat associé

Alice ROBERT
Avocate of Counsel

Derriennic Associés

Notes

(1) Conseil d'Etat, 13 novembre 2024, décision n°475297 ; Conseil d'Etat, 13 novembre 2024, décision n°492895 ; Conseil d'Etat, 19 novembre 2024, décision n°491644.

(2) Délibération Cnil 21 décembre 2023, publiée le 31 janvier 2024.

(3) À noter que d'autres recours ont été formés devant le Conseil d'Etat sur la même problématique, en l'occurrence concernant la décision de refus du ministère des solidarités et de la santé de prendre « les mesures propres à éliminer la violation du (...) (RGPD) résultant de l'hébergement des données de la Plateforme des données de santé par la société Microsoft ».

(4) À savoir les articles 44 à 48 du RGPD sur les transferts de données à caractère personnel vers des pays tiers et l'article R.1461-1 du code de la santé publique qui dispose en son dernier alinéa « Les données du système national des données de santé sont hébergées au sein de l'Union européenne. Aucun transfert de données à caractère personnel ne peut être réalisé en dehors de l'Union européenne, sauf dans le cas d'accès ponctuels aux données par des personnes situées en dehors de l'Union européenne, pour une finalité relevant du 1° du I de l'article L.1461-3 ».