



DONNÉES PERSONNELLES

Cnil et plateformes collaboratives : les prestataires américains de nouveau dans le viseur

Le 27 mai 2021, la Cnil a publié une recommandation mettant en garde les établissements d'enseignement supérieur et de recherche au sujet du recours à des plateformes collaboratives américaines¹. Cette nouvelle recommandation de la Cnil s'inscrit dans la lignée de celle relative à la plateforme nationale d'hébergement des données de santé des citoyens français, le Health Data Hub², en février 2021, dans laquelle la Cnil recommandait déjà aux autorités françaises de faire appel à des prestataires établis au sein de l'Union européenne.

En se fondant une nouvelle fois sur le désormais célèbre arrêt Schrems II rendu par la Cour de justice de l'Union européenne le 16 juillet 2020, (affaire C311/18)³, invalidant le Privacy Shield, la Cnil reconnaît et confirme qu'il existe bel et bien un risque juridique consécutif au transfert des données personnelles des résidents européens vers des infrastructures des prestataires établies sur le sol des Etats-Unis, quand bien même ces données sont hébergées sur des serveurs localisés en Union européenne. En creux, le Cloud Act, cette loi américaine votée en mars 2018 par le Congrès américain, et autorisant le transfert de données notamment d'Européens, détenues par des prestataires sous juridictions américaines même si ces données sont localisées à l'extérieur des Etats-Unis, au bénéfice des autorités d'enquête et de poursuites américaines, est sans doute l'autre motif d'inspiration de la Cnil.

Invalidation du Privacy Shield et ses conséquences : le service public directement visé

L'année 2020 a été un réel tournant entraînant une prise de conscience des risques que pouvaient représenter le recours sans précautions à des prestataires Cloud américains, surtout par les services publics.

Le 16 juillet 2020, l'arrêt Schrems II a tout d'abord permis de reconnaître que les transferts depuis l'Union européenne vers les Etats-Unis ne présentaient plus de garanties suffisantes au regard du règlement UE n°2016/679 dit RGPD. Jusqu'à la décision Schrems II, les Etats-Unis bénéficiaient en effet de la décision d'adéquation « *Privacy Shield* », adoptée en 2016 par la Commission européenne, qui rendait conforme au RGPD tout transfert de données entre l'Union européenne et les opérateurs américains adhérant à ses principes de

protection des données, sans autre formalité. En invalidant le Privacy Shield, la Cour de justice de l'Union européenne a reconnu officiellement que les transferts de données personnelles de l'Europe vers les Etats-Unis ne présentaient pas de garanties suffisantes et n'assuraient pas la protection des données à caractère personnel des citoyens européens. Cette décision a sonné le premier son de cloche, et ses conséquences se sont fait sentir très rapidement.

Le 13 octobre 2020, suite aux avertissements de la Cnil, le Conseil d'Etat rend une ordonnance et reconnaît que le recours à un hébergeur américain, la société Microsoft, pour l'hébergement de la plateforme de données de santé nationale « *Health Data Hub* » est un risque, et exige de l'Etat d'adopter des mesures et garanties supplémentaires.

Cette décision a même été plus loin, en reconnaissant que même sans transfert vers les Etats-Unis,

il existait un risque d'ingérence des services de surveillance américains pour les données stockées sur des serveurs américains mais localisées dans l'Union européenne.

Sur le fondement de ces décisions, et des avertissements de la Cnil, le ministère de la Santé s'est engagé à confier l'hébergement du Health Data Hub à un prestataire européen, offrant « *une solution technique permettant de ne pas exposer les données hébergées à d'éventuelles demandes d'accès illégales au regard du RGPD* » dans un délai compris entre 12 et 18 mois et, en tout état de cause, ne dépassant pas deux ans⁴.

En mai 2021, suite également à ce fameux arrêt Schrems II, c'est au tour du secteur de l'enseignement et de la recherche de saisir la Cnil : la Conférence des présidents d'université et la Conférence des grandes écoles s'inquiètent de l'utilisation de « *suites collaboratives pour l'éducation* » proposées par des sociétés américaines.

Le 27 mai 2021, la Cnil publie une recommandation qui s'inscrit dans la lignée de celle du Health Data Hub.

Mise en garde de la Cnil aux établissements d'enseignement secondaire et de la recherche utilisant des plateformes américaines : un risque d'accès par les autorités américaines même pour des données stockées en Europe

La Cnil s'est fondée sur les éléments transmis par la Conférence des grandes écoles (CGE) et la Conférence des présidents d'université (CPU) pour constater que le secteur de l'enseignement et de la recherche a recours à des « *suites collaboratives pour l'éducation* » américaines.

La Cnil relève tout d'abord que cette utilisation d'outils proposés par des prestataires américains pourrait impliquer le transfert de données à caractère personnel vers les Etats-Unis, ne garantissant plus aujourd'hui un niveau de protection suffisant.

Pour évaluer concrètement le risque que peut présenter l'utilisation de ces outils américains, la Cnil a identifié les données à caractère personnel et les personnes impliquées par ce transfert. L'autorité de contrôle a ainsi relevé que ce transfert concernait un grand nombre d'utilisateurs (étudiants, chercheurs, enseignants, personnel administratif) et surtout des données pouvant être qualifiées de « *sensibles* », comme par exemple des données de santé.

Plus inquiétant, la Cnil réaffirme, tout comme pour le cas Health Data Hub, qu'il existe un risque d'ingérence des autorités américaines, même pour des données stockées au sein de l'Union européenne, par ces prestataires américains :

« *indépendamment de l'existence de transferts, les législations américaines s'appliquent aux données stockées par les sociétés étatsuniennes en dehors de ce territoire. Il existe donc un risque d'accès par les autorités américaines aux données stockées. Cet accès, s'il n'est pas fondé sur un accord international, constituerait une divulgation non autorisée par le droit de l'Union, en violation de l'article 48 du RGPD.* »

La Cnil reconnaît et confirme que l'utilisation de services SaaS américains, même sans transfert révélé vers les Etats-Unis, comporte un risque d'accès par les autorités américaines aux données stockées.

Face à ce constat qui touche à la réglementation interne américaine

et sur laquelle l'Europe n'a aucun pouvoir, la seule alternative proposée aux utilisateurs européens est de se tourner vers des acteurs européens.

En conclusion, les bénéficiaires du RGPD ne sont plus à prouver et apportent de réelles garanties de protection pour les données à caractère personnel des citoyens européens. Cependant, l'invalidation du Privacy Shield et la promulgation du Cloud Act laissent aujourd'hui un vide juridique pouvant affaiblir la portée du règlement.

Les prestataires américains ne sont pas le problème, mais les lois américaines auxquelles ils sont soumis ne permettent pas à ce jour de garantir la protection des données à caractère personnel des citoyens européens. Si la solution proposée par la Cnil est le recours à des prestataires européens, encore faut-il que cette offre suive.

Il serait temps d'investir et de donner notre confiance aux acteurs du numérique français et européens, afin de leur permettre de proposer des services qui ne seraient pas des choix par défaut, mais qui deviendraient de véritables incontournables sur le marché.

Alexandra ITEANU

Avocat à la Cour

Iteanu société d'avocats

Notes

(1) <https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche>

(2) <https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub>

(3) Arrêt dans l'affaire C-311/18 Data Protection Commissioner/Maximilian Schrems et Facebook Ireland

(4) Source Cnil : <https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub>



Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info