dposystem

Décryptage - Dans quelle mesure peut-on garantir la confidentialité des données personnelles transférées hors de l'Union Européenne ?

Le cas du Health Data Hub

RGPD, adéquation et clauses contractuelles types : ce que disent les textes

Le RGPD pose le cadre légal de la protection des données à caractère personnel des individus en Europe. Mais quelle protection juridique offrent les pays où le RGPD ne s'applique pas pour les données à caractère personnel transférées depuis l'Union Européenne et comment évaluer cette protection juridique ?

L'appréciation de la protection juridique se fait sur le fondement de l'article 45 du RGPD qui précise que le pays destinataire des données à caractère personnel doit offrir un niveau de protection adéquat. Ce niveau d'adéquation est apprécié par la Commission européenne par voie de décision. On parle donc de transferts sur décision d'adéquation.

Plusieurs pays dans le monde sont considérés « adéquats ». Les États-Unis ont bénéficié de décisions d'adéquation à plusieurs reprises dont la dernière a été invalidée le 16 juillet 2020 par la Cour de Justice de l'Union Européenne.

Quand des pays ne bénéficient pas de décisions d'adéquation, les transferts de données entre les pays européens et ces pays, pour être conformes, se font au moyen des clauses contractuelles types (CCT). Il existe deux types de modèles de clauses, un type pour encadrer les transferts de données de responsable de traitement à responsable de traitement, un autre pour le transfert de responsable de traitement à sous-traitant.

Le 11 novembre 2020, le CEPD a publié des recommandations à destination des organismes souhaitant transférer des données hors Union européenne : six étapes qui permettent de déterminer si des mesures complémentaires doivent être mises en place pour effectuer le transfert de données vers un pays tiers.

- **L'identification** et la connaissance des données transférées,
- La **vérification** des outils de transfert,
- **L'évaluation** de la réglementation du pays destinataire,
- L'identification et **l'adoption de mesures complémentaires** visant à renforcer le niveau de protection,
- Le **respect de procédures** formelles liées aux mesures retenues,
- Le **réexamen périodique** du niveau de protection dans le temps.

Health Data Hub : Centralisation des données personnelles santé de 67 millions de Français

Créée fin novembre 2019, la Plateforme des données de santé, également appelé « Health Data Hub » est un organisme public français qui a pour but de faciliter le partage des données des différents organismes de santé : hôpitaux, sécurité sociale, médecine généraliste, organismes de recherche et universités, etc. afin de favoriser la recherche. Outre les problèmes de confidentialité des données que posent une telle plateforme car il deviendrait plus facile de recouper des informations et d'identifier des personnes, la Plateforme a aussi signé, le 15 avril 2020, un contrat avec une filiale irlandaise de la société américaine Microsoft pour l'hébergement des données et l'utilisation des logiciels nécessaires à leur traitement.

Des données qui pourraient être exploitées par les renseignements américains

C'est dans ce contexte que des associations, syndicats et requérants individuels ont demandé au juge du référé-liberté du Conseil d'Etat, statuant en urgence, de suspendre le traitement des données liées à l'épidémie de covid-19 sur la Plateforme des données de santé « *en raison des risques que cette situation comporte au regard du droit au respect de la vie privée, compte tenu de possibles transferts de données vers les États-Unis* ». En effet, la loi américaine a une compétence d'application extraterritoriale. Ceci signifie que la loi américaine s'applique en-dehors du territoire américain, aux structures ayant un lien de nationalité avec les Etats-Unis.

Au regard de la réglementation américaine et au titre de la sécurité des Etats-Unis, un opérateur privé américain ne peut refuser de mettre en œuvre une requête des renseignements américains fondée sur le FISA (Foreign Intelligence Surveillance Act). Dans le cas du Health Data Hub, on comprend donc que les données personnelles des Français pourraient être transférées et exploitées aux Etats-Unis de manière légale, en dépit de la confidentialité de ces informations et de la protection juridique dont elles disposent au sein de l'Union Européenne.

Quel recours juridique ?
A cet égard, le juge des référés du Conseil d'Etat relève que la Plateforme des données de santé et Microsoft se sont engagés, *par contrat*, à refuser tout transfert de données de santé en dehors de l'Union européenne. De plus, un arrêté ministériel pris le 9 octobre 2020 interdit tout transfert de données à caractère personnel dans le cadre de ce contrat. Néanmoins, le juge des référés indique qu'il *ne peut être totalement exclu que les autorités américaines, dans le cadre de programmes de surveillance et de renseignement*, demandent à Microsoft et à sa filiale irlandaise l'accès à certaines données.

Le juge des référés précise cependant que des précautions devront être prises dans l'attente d'une solution qui permettra d'éliminer tout risque d'accès aux données personnelles par les autorités américaines. Ainsi, le secrétaire d'État au numérique a déclaré le 8 octobre 2020 (réf), devant les sénateurs, son souhait d'un changement de prestataire : *« au lieu de s'en remettre à Microsoft, l'actuel hébergeur du Health Data Hub, une solution française ou européenne doit être privilégiée ».*

« *Ce cas questionne sur la capacité de l'Union Européenne à garantir la sécurité des données personnelles de ses membres et à proposer des alternatives aux solutions américaines pour répondre à des besoins numériques et de traitements de données de plus en plus importants. Dans un article de La Tribune d'août 2020 (réf), certains s'interrogeaient « sur le risque de l'Europe, assise sur une gigantesque mine de données "or du XXIe siècle", d'en perdre totalement la maîtrise à force d'utiliser les services des géants de l'informatique américains ». En effet, si le comité européen de la protection des données a publié encore tout récemment des recommandations à destination des organismes souhaitant transférer des données hors de l'Union Européenne (ref), est-ce suffisant face aux risques ? Cette problématique peut sembler uniquement d'ordre juridique mais elle embarque en réalité des enjeux politiques, économiques et sociétaux forts.* » Vincent Ferrara, président de dposystem