CONSEIL D'ÉTAT - ORDONNANCE DE REFERE, 19 JUIN 2020, ASSOCIATION LE CONSEIL NATIONAL DU LOGICIEL LIBRE ET AUTRES, N°440916

MOTS CLEFS : crise sanitaire – données de santé – base de données – transfert de données – information – Cloud Act – Privacy Shield – sécurisation des données – pseudonymisation des données – atteinte à la vie privée – référé

Créée par un arrêté du 29 novembre 2019, la Plateforme des Données de Santé (PDS), aussi appelée « Health Data Hub », permet de faciliter la recherche médicale en croisant et regroupant les données de santé des français au sein d'une même entité. Ce projet, très critiqué quant à l'extrême sensibilité des données qu'il traite, est pourtant conforté dans sa mise en œuvre par le Conseil d'État, qui valide notamment l'hébergement polémique de ses données chez le géant américain Microsoft.

FAITS : Le 23 avril 2020, un arrêté prévoit le déploiement accéléré de la Plateforme dans le cadre de l'état d'urgence sanitaire. Il autorise en particulier le Health Data Hub et la Caisse nationale de l'assurance maladie à collecter un grand nombre de données *« aux seules fins de faciliter l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le virus Covid-19 ».*

PROCEDURE : Une quinzaine de requérants, dont des associations, syndicats et personnalités, telles que le Conseil National du logiciel libre ou encore le Syndicat de la médecine générale, ont saisi le Conseil d'État d'une action en référé afin que l'arrêté du 23 avril 2020 soit suspendu en raison d'atteintes graves et manifestement illégales au droit au respect de la vie privée et au droit à la protection des données personnelles. Sont notamment critiquées par les requérants les modalités d'hébergement et de sécurisation de celles-ci, ainsi que le transfert potentiel de ces données de santé dans des états tiers, en raison du choix de l'entreprise américaine Microsoft en tant qu'hébergeur de celles-ci.

PROBLEME DE DROIT : Le décret du 23 avril 2020, en ce qu'il autorise la collecte et le traitement des données de santé par le Health Data Hub, porte-t-il atteinte au droit au respect de la vie privée et au droit à la protection des données personnelles ?

SOLUTION : Dans une ordonnance de référé rendue le 19 juin 2020, le Conseil d'État va répondre à cette question par la négative. Il ordonne toutefois à la plateforme de fournir à la CNIL dans un délai de 5 jours, tous éléments relatifs aux procédés de pseudonymisation utilisés, afin que celle-ci en vérifie la conformité et s'assure que l'exigence de sécurité afférente aux données de santé soit effectivement satisfaite.

SOURCES :

Conseil d'État, « Plateforme Health Data Hub – Décision en référé du 19 juin » conseil-etat.fr
COSTES (L.), « Validation par le Conseil d'État du Health Data Hub », RLDI n°172, juillet 2020

NOTE :

La notion de donnée de santé s'entend d'après l'article 4 du Règlement Général sur la Protection des Données (RGPD) comme *« toute donnée relative à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèle des informations sur l'état de santé de cette personne. »* Puisqu'elle est particulièrement sensible, elle doit être soumise à un régime juridique particulier garantissant sa sécurité lors de sa collecte et de son traitement.

Le risque de transfert des données, élément non susceptible de porter atteinte de manière grave et illégale aux libertés fondamentales protégées par le RGPD

Point central contesté par les requérants : le fait que la société américaine Microsoft soit désignée comme hébergeur des données de la plateforme, car les instances étatiques américaines pourraient potentiellement y avoir accès. En effet, en vertu du Cloud Act de 2018, un juge américain peut ordonner la fourniture des données traitées par une société étasunienne pour les besoins d'une enquête criminelle, quel que soit le lieu de leur hébergement. Toutefois, le juge administratif va balayer cet argument car il estime les requérants ne démontrent pas que la présence des données du Health Data Hub au sein des serveurs de Microsoft induirait nécessairement *« que les données de santé (…) seraient susceptibles de faire l'objet de demandes d'accès sur ce fondement. »*

La juridiction administrative indique que Microsoft adhère au Privacy Shield, accord entre les États-Unis et l'Union Européenne, selon lequel *« les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis »*, et serait ainsi à même de garantir un certain niveau de sécurité vis à vis de ces données françaises. Elle reste néanmoins prudente sur ce dernier argument en raison de la requête exercée devant le Tribunal de l'Union Européenne pour certifier la conformité de cet accord au RGPD, dont nous savons aujourd'hui qu'il a été invalidé, mais qui à l'époque des faits était toujours en vigueur.

Des mesures de sécurité nécessaires et proportionnées au regard de l'objectif poursuivi

Sur la problématique de la sécurité des données personnelles, le Conseil d'État va tout d'abord opposer le fait que des contrôles externes aient été effectués et soient également prévus dans le futur : *« un nouvel audit par la société Orange Cyberdéfense, (…) prévu en septembre 2020, après un premier audit par la société Amossys en novembre 2019. »*

Ensuite, il validera le choix de la société Microsoft comme hébergeur en raison de sa certification « hébergeur de données de santé » obtenue en 2018, certification obligatoire pour toute opération d'hébergement de ce type de données selon l'article L1111-8 du code de la santé publique. Il rappelle également que les données collectées le sont dans le respect du principe de la minimisation de la collecte édicté à l'article 5 du RGPD : Sont collectées uniquement les données relatives à la finalité poursuivie, pendant la durée de l'épidémie de Covid-19, données qui seront détruites si elles ne disposent plus de base légale.

Enfin, contrairement à ce que les requérants soutenaient, le juge des référés rappelle que le droit au respect de la vie privée n'implique pas obligatoirement que les données soient anonymisées, mais qu'elles peuvent seulement être pseudonymisées en vertu du RGPD[1] si l'anonymisation *« ne permettrait pas de poursuivre les travaux de recherche nécessaires »*, ce qui est le cas ici. Le mode de fonctionnement de la plateforme, prévoyant trois pseudonymisations successives, « *n'apparaît pas manifestement inapproprié au regard des exigences du règlement général sur la protection des données. »*
Toutefois, le juge ne s'estimant pas compétent pour vérifier la suffisance de ces

[1] Article 89 du RGPD

mesures, il ordonne au Health Data Hub de fournir à la CNIL dans un délai de 5 jours à compter de la notification cette décision les éléments relatifs aux procédés de pseudonymisation utilisés, afin qu'elle vérifie la fiabilité de ceux-ci par rapport à la criticité des données visées.

Justine Bondu
Master 2 Droit des médias électroniques
AIX-MARSEILLE UNIVERSITE, LID2MS-IREDIC 2020

ARRET :

CE, Ordonnance de référé, 19 juin 2020, *Association le conseil du logiciel libre et autres, n°440916*

(…) Sur le respect du principe de minimisation de données :

15. En outre, seuls pourront être légalement menés les projets poursuivant une finalité d'intérêt public en lien avec l'épidémie pour lesquels le recours à la Plateforme des données de santé pour traiter des données rassemblées en vertu de l'arrêté du 21 avril 2020, avant même l'entrée en vigueur des dispositions issues de la loi du 24 juillet 2019, pourra être regardé comme une mesure nécessaire et proportionnée aux risques sanitaires encourus et appropriée aux circonstances de temps et de lieu, compte tenu, tout à la fois, de l'urgence s'attachant à la conduite du projet et de l'absence de solution technique alternative satisfaisante permettant d'y procéder dans les délais utiles. (…) Seules pourront être hébergées par la plateforme les données nécessaires à la conduite de ces projets, lesquelles ne pourront être traitées que pour la durée de l'état d'urgence sanitaire et devront être détruites si, au terme de celui-ci, la poursuite des traitements n'a plus de base légale.

(…) Sur le risque de transferts de données dans un état tiers :

24. En premier lieu, par une décision d'exécution (UE) 2016/1250 du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, la Commission a considéré, aux fins de l'article 25 de la directive 95/46/CE, dont les dispositions ont été reprises à l'article 45 du règlement général sur la protection des données, que « les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis dans le cadre du bouclier de protection des données UE-États-Unis. (…) Il résulte de l'instruction que la société Microsoft figure sur la liste des organisations adhérant au « bouclier de protection des données ». Si la décision d'exécution (UE) 2016/1250 fait l'objet de requêtes pendantes devant le Tribunal de l'Union européenne et si sa conformité au règlement général sur la protection des données pourrait être appréciée à l'occasion d'un recours pendant devant la Cour de justice de l'Union européenne, elle est toujours en vigueur à la date de la présente ordonnance.

(…) Sur la pseudonymisation des données :

33. (…) Le droit au respect de la vie privée n'implique pas que des données, même aussi sensibles que les données de santé, fassent dans tous les cas l'objet d'une anonymisation avant d'être traitées à des fins d'évaluation ou de recherche mais seulement, ainsi que le prévoient les dispositions du règlement général sur la protection des données citées au point 31, que des garanties appropriées soient prévues, qui peuvent comprendre la pseudonymisation, lorsque l'anonymisation ne permettrait pas de poursuivre les travaux de recherche nécessaires. Or il résulte de l'instruction que l'anonymisation des données considérées conduirait soit à un appauvrissement, soit à une agrégation des données disponibles, affectant ainsi la pertinence des travaux d'évaluation ou de recherche conduits.

(…) ORDONNE :

Article 1er : La Plateforme des données de santé (…) fournira à la Commission nationale de l'informatique et des libertés (…) tous éléments relatifs aux procédés de pseudonymisation utilisés, propres à permettre à celle-ci de vérifier que les mesures prises assurent une protection suffisante des données de santé (…).