La Cnil demande l'arrêt du stockage de nos données de santé par Microsoft

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE VENDREDI 9 OCTOBRE 2020

Dans le cadre d'un recours visant à obtenir la suspension du Health Data Hub, le projet de plateforme centralisant l'ensemble de nos données de santé, la commission a transmis au Conseil d'État un mémoire demandant à l'ensemble des acteurs de cesser de confier leur hébergement à Microsoft ou toute autre société soumise *« au droit étatsunien »*.

La Commission nationale de l'informatique et des libertés demande, dans un mémoire transmis au Conseil d'État jeudi 8 octobre que Mediapart a pu consulter, à l'ensemble des acteurs stockant des données de santé de cesser *« dans un délai aussi bref que possible »* de confier leur hébergement à Microsoft ou toute autre société soumise *« au droit étatsunien »*.

Ce n'est que quelques heures avant le début de l'audience que ce mémoire a été versé au dossier d'une procédure visant le Health Data Hub (HDH), la gigantesque plateforme devant à terme centraliser l'ensemble des données de santé des Français et dont l'hébergement a été confié à la société américaine Microsoft, *via* sa filiale irlandaise.

Dans ce recours, les requérants – le collectif SantéNathon regroupant des professionnels de la santé, des syndicats et des acteurs du secteur du logiciel libre – demandent au Conseil d'État d'annuler un décret publié le 21 avril dernier et accélérant, au nom de l'état d'urgence sanitaire, le déploiement du HDH en y intégrant les données issues de l'épidémie de Covid-19.

Créé par la loi santé du 24 juillet 2019, le HDH doit remplacer l'actuel Système national des données de santé (SNDS) qui centralise déjà les principaux fichiers de santé, dont celui de l'assurance-maladie, tout en élargissant considérablement sa portée. À terme, toute donnée collectée dans le cadre d'un acte remboursé par l'assurance-maladie sera centralisée dans le HDH, des données des hôpitaux à celles du dossier médical partagé ou celles des logiciels professionnels utilisés par les médecins et les pharmaciens.

© Reuters

La mise en place de ce projet particulièrement sensible, et vivement contesté en raison du choix de la solution d'hébergement en cloud Azure de Microsoft, a fait durant de nombreux mois l'objet de discussions entre le gouvernement et la Cnil. Mais la publication du décret du 21 avril avait pris de court la commission et celle-ci avait rendu, dans la foulée, un avis particulièrement sévère.

La mise en place du Health Data Hub faisait l'objet d'*« un plan d'action conséquent de mise en œuvre de mesures de sécurité s'étalant sur une période de plusieurs mois »*, y rappelait la commission qui s'interrogeait *« donc sur les conditions de démarrage anticipé de la solution technique dans un contexte où la plateforme de données de santé a dû accomplir en quelques semaines des opérations, dont certaines structurantes, pourgarantir la sécurité des données traitées, qui étaient prévues pour s'étaler sur plusieurs mois »*.

Plus gênant, l'avis révélait que des données confiées à Microsoft, qui sont actuellement stockées dans des serveurs situés aux Pays-Bas, pourront être transférées aux États-Unis dans certains cas. Selon la Cnil, qui a pu consulter le contrat liant le HDH à Microsoft, celui-ci prévoit bien une localisation par défaut des données au sein de l'UE.

En revanche, *« cette localisation ne s'applique qu'aux données "au repos", alors même que le contrat mentionne l'existence de transferts de données en dehors de l'Union européenne dans le cadre du*

fonctionnement courant de la plateforme, notamment pour les opérations de maintenance ou de résolution d'incident ».

La Cnil s'inquiétait par ailleurs également de la manière dont sont gérées les clefs de chiffrement, permettant de déchiffrer les données, et dont une copie sera conservée *« par l'hébergeur au sein d'un boîtier chiffrant, ce qui a pour conséquence de permettre techniquement à ce dernier d'accéder aux données »*, ainsi que d'un manque d'encadrement des procédures d'accès des administrateurs de la plateforme.

En se fondant sur cet avis, le collectif SantéNathon avait déposé, au début du mois de juin, un premier recours en référé devant le Conseil d'État afin de demander la suspension du déploiement du HDH. Les requérants, défendus par M^es^ Jean-Baptiste Soufron et Juliette Alibert, soulignaient notamment les risques d'accès aux données de santé des Français permis par plusieurs lois américaines, comme le Cloud Act qui, depuis 2018, autorise les autorités américaines à exiger la transmission de données personnelles à toute entreprise basée sur son sol, et ce même si ses serveurs sont situés à l'étranger, sans avoir besoin de recourir à une demande d'entraide judiciaire.

Dans une décision rendue le 19 juin, le Conseil d'État avait rejeté le recours au motif que le transfert de données vers les États-Unis a été validé et encadré par le Bouclier de protection des données, ou Privacy Shield, un mécanisme négocié par l'Union européenne et entré en vigueur le 1^er^ août 2016. Le juge administratif avait cependant accompagné son rejet de plusieurs injonctions à l'adresse du gouvernement, lui demandant de préciser certains points techniques et d'indiquer, sur son site, que les données pourront être transférées hors de l'UE.

Le raisonnement de la plus haute juridiction administrative française a cependant été remis en cause par **une décision historique** de la Cour de justice de l'Union européenne (CJUE) rendue le jeudi 16 juillet et invalidant le Privacy Shield. Saisie par le militant autrichien Max Schrems, la cour a estimé que la législation américaine, et son caractère extraterritorial lui permettant de s'appliquer en dehors des États-Unis, ne permettait pas de garantir un niveau de protection suffisant des données de citoyens européens.

Dans son arrêt, la CJUE soulignait les dangers de deux textes, le Foreign Intelligence Surveillance Act (Fisa) et l'Executive Order 12333, régissant des programmes de surveillances américains *« qui instituent des programmes permettant l'accès des autorités publiques étatsuniennes à des fins de sécurité nationale aux données personnelles transférées de l'UE vers les États-Unis, de façon particulièrement large et sans ciblage »*. Parmi ces programmes figurent Prism et UpStream, dont l'ampleur avait été révélée par Edward Snowden en 2013 **et depuis maintenus**. De plus, poursuivait la cour, *« cette législation n'accorde pas aux personnes concernées des droits de recours devant des juridictions contre les autorités étatsuniennes »*.

Sur la base de cette invalidation du Privacy Shield, le collectif SantéNathon avait déposé un nouveau recours en référé devant le Conseil d'État. C'est dans le cadre de cette procédure que l'avis de la Cnil a de nouveau été sollicité pour savoir quelles conséquences tirer de cette décision de la CJUE et à quel point celle-ci impactait le HDH.

« Évaluer en urgence l'existence de fournisseurs alternatifs »

Dans son mémoire, la commission réitère ses inquiétudes quant aux possibilités de transferts de données vers les États-Unis et d'accès aux clefs de chiffrement.

Ainsi, si elle reconnaît que ces clefs sont stockées dans un dispositif appelé *« Customer Lockbox »* qui *« constitue une garantie de limitation des transferts »*, elle pointe également une faille dans le contrat qui prévoit une exception *« dans le cadre de scénarios inattendus ou imprévisibles correspondant à des catastrophes ou en cas d'accès fortuit aux données par un ingénieur de Microsoft »*.

La Cnil a également eu accès à un avenant négocié au début de l'été entre le HDH et Microsoft afin, comme le révélait Mediapart **au mois de juin**, de répondre aux inquiétudes quant aux risques de transferts de données.

Le mémoire de la commission reconnaît que cet avenant *« limite fortement les transferts à l'initiative de Microsoft »*, mais pointe également que celui-ci stipule par ailleurs que Microsoft *« ne divulguera ni ne donnera accès à une quelconque donnée traitée aux autorités, sauf si la loi l'exige »* (souligné par la Cnil).

En conséquence, la commission estime, tout comme la CJUE, *« que, même dans le cas où l'absence de transferts de données personnelles en dehors de l'UE à des fins de fourniture du service serait confirmée, la société Microsoft peut être soumise, sur le fondement du FISA, voire peut-être de l'EO 123333, à des injonctions des services de renseignement l'obligeant à leur transférer des données stockées et traitées sur le territoire de l'Union européenne »*.

Cette invalidation du Privacy Shield, désormais acté par la Cnil, prive de base légale toute demande de transfert des données par les autorités américaines. Ces demandes, précise le mémoire, *« devraient être considérées comme des divulgations non autorisées par le droit de l'Union »* et contraires au règlement général sur la protection des données (RGPD). De plus, la commission souligne que les programmes de surveillance américains permettent d'accéder à des données en dehors des États-Unis et de les collecter par exemple lors de leur circulation dans les câbles transatlantiques assurant le trafic internet entre plusieurs grandes zones géographiques. De ce fait, *« il ne suffit pas que l'hébergeur ait son siège social hors des États-Unis pour ne pas être soumis en partie au droit étatsunien »*, pointe le document.

© AFP

Pour la Cnil, les conséquences de l'arrêt de la CJUE sont claires : les données des citoyens européens ne peuvent plus être confiées à une société américaine, même si celle-ci dispose d'un siège et de serveurs dans l'Union européenne. En conséquence, *« cette situation doit conduire selon elle à modifier les conditions d'hébergement de la PDS* [plateforme de données de santé – ndlr], *ainsi que celles des autres entrepôts de données de santé qui sont hébergés par des sociétés soumises au droit étatsunien. La solution la plus effective consiste à confier l'hébergement de ces données à des sociétés non soumises au droit étatsunien »*. Et ce changement d'hébergement *« devrait intervenir dans un délai aussi bref que possible »*.

La commission a conscience de l'impact potentiellement considérable de cette prise de position, Microsoft équipant un nombre très important d'administrations françaises, notamment en logiciels de bureautique, comme les ministères de l'Éducation nationale ou celui de la défense. *« La commission n'est pas sans ignorer que cette situation* […] *dépasse largement le cadre du seul HDH »*, précise le mémoire. Celui-ci précise que l'analyse de la Cnil se limite, pour l'instant, aux seules données de santé. *« Elle réserve son appréciation des conséquences qu'il convient d'en tirer dans d'autres secteurs et pour d'autres données présentant une moindre sensibilité »*, précise le mémoire.

Mais, même en se limitant au domaine de la santé, de nombreux établissements de santé ont déjà recours aux services de sociétés américaines et *« sont donc placées dans la même situation que le HDH »*. Ces acteurs vont donc devoir modifier les conditions d'hébergement de leurs données, au risque de se voir refuser, par la Cnil, leurs *« autorisations de traitement de ces données, notamment dans le cadre de recherches scientifiques »*.

Pour éviter un blocage total et une perte de données, la Cnil propose de mettre en place, de manière transitoire, *« un fondement juridique permettant, le cas échéant, de délivrer de telles autorisations, sous certaines garanties. Cependant*, prévient-elle, *cette période de transition doit rester limitée à ce qui est nécessaire et impérativement mise à profit pour garantir, par des démarches actives, la modification des conditions d'hébergement des données »*. Elle appelle donc

les autorités à *« évaluer en urgence l'existence de fournisseurs alternatifs et leurs capacités, tant en volume de stockage qu'en qualité de service, afin d'évaluer la durée nécessaire pour cette transition, la plus courte possible »*.

Cette demande de la Cnil semble en tout cas avoir déjà été entendue par le gouvernement. **Jeudi après-midi**, alors que se tenait l'audience devant le Conseil d'État, le secrétaire d'État au numérique Cédric O a annoncé lors d'une audition au Sénat que ses services et ceux du ministre de la santé Olivier Véran travaillaient déjà sur un tel scénario. *« Nous travaillons avec Olivier Véran, après le coup de tonnerre de l'annulation du Privacy Shield, au transfert du Health Data Hub sur des plateformes françaises ou européennes »*, a affirmé Cédric O. *« Nous aurons sur ce sujet des discussions avec nos partenaires allemands »*, a ajouté le secrétaire d'État.

Lors de l'audience devant le Conseil d'État, à laquelle Mediapart assistait, le représentant du ministère de la santé a alerté sur les *« conséquences sur d'autres acteurs privés et publics »* d'une prise en compte de l'analyse de la Cnil et de la *« source de désordre considérable »* qui en résulterait. Selon le gouvernement, il n'existerait aucune alternative à Microsoft, un argument vivement contesté par les requérants, et même si elle existait, *« il faudrait au moins des mois »* pour la mettre en place.

La présidente, de son côté, a annoncé qu'elle rendrait sa décision en début de semaine prochaine. Elle a cependant d'ores et déjà demandé au représentant du ministère de la santé si certains engagements concernant le non-transfert de données pouvaient être inscrits dans un *« acte réglementaire »*, ce que celui-ci a accepté. Le Health Data Hub, uniquement déployé au nom de l'état d'urgence sanitaire, doit en effet encore faire l'objet d'un décret précisant ses conditions de fonctionnement et devant être pris avant la fin du mois d'octobre. La présidente a cependant précisé qu'il n'était *« pas évident que cela suffise dans le cadre du conflit »* qu'elle avait à trancher.

Directeur de la publication : Edwy Plenel
Direction éditoriale : Carine Fouteau et Stéphane Alliès
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 24 864,88€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Laurent Mauduit, Edwy Plenel (Président), Sébastien Sassolas, Marie-Hélène Smiéjan, François Vitrani. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart, Société des salariés de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 24 864,88€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.