L'hébergement de la plateforme des données de santé par Microsoft : une validation sous surveillance

Lucie Cluzel-Métayer

CE ord. 13 octobre 2020, n°444937, *Assoc. Le Conseil national du logiciel libre*, dite *Health Data Hub*

L'hébergement de la plateforme des données de santé par Microsoft : une validation sous surveillance

Lucie Cluzel-Métayer, Professeure à l'Université de Paris Nanterre, CRDP

Résumé *: Si l'urgence sanitaire conduit le juge des référés à valider l'hébergement de la plateforme des données de santé par Microsoft, sa décision est assortie de multiples injonctions et recommandations. Le risque d'un transfert de ces données aux Etats-Unis, mis en évidence par l'arrêt Schrems II, est ainsi placé sous haute surveillance.*

Mots-clés : Données personnelles - données de santé – plateforme – Health Data Hub – Shrems II – Privacy shield – CNIL – Covid 19 – injonctions – recommandations – compliance – RGPD – droit américain

L'ordonnance du Conseil d'Etat du 13 octobre 2020 dite *Health Data Hub*, est la première décision européenne à appliquer la jurisprudence de la Cour de Justice de l'Union Européenne *Schrems II* (CJUE, 16 juillet 2020, C-311/18 *Data Protection Comissioner/Maximillian Schrems et Facebook Ireland*). Le contentieux de l'hébergement des données de santé du *Health Data Hub* confié à Microsoft donne en effet l'occasion au Conseil d'Etat de s'aligner sur la nouvelle jurisprudence de la Cour de justice qui, invalidant le *Privacy Shield*, oblige à repenser les transferts de données personnelles vers les Etats-Unis.

Saisi d'un référé-liberté, le Conseil d'Etat rejette, certes, le recours des requérants qui contestaient l'hébergement des données de santé par cette entreprise états-unienne, mais il ne valide le dispositif que pour un temps, celui de l'urgence de la crise sanitaire. En dépit des apparences, la solution pragmatique qu'il adopte s'inscrit ainsi dans le mouvement de résistance orchestré par la CJUE et relayé par la CNIL contre les potentielles atteintes à la vie privée et à la protection des données personnelles qui pourraient être portées par des Etats tiers.

Créée en juillet 2019 (art. 41 de la loi 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé) à la suite du rapport Villani de mars 2018 sur l'Intelligence artificielle, la Plateforme des données de santé (PDS) ou *Health Data Hub* (HDH) vise à centraliser et faciliter le partage des données de santé issues de sources très variées. L'objectif est à la fois de soutenir la recherche mais aussi d'améliorer la compétitivité de la France sur le plan international grâce à la libération de ces données, particulièrement nombreuses et ordonnées en France.

Prenant la suite de l'Institut national des données de santé, le HDH, créé sous forme de groupement d'intérêt public (arrêté du 29 novembre 2019), est ainsi chargé de « réunir, organiser et mettre à disposition les données du Système National des Données de Santé (SNDS) » (Art. L. 1462-1 CSP). Il rassemble 56 partenaires dont l'Etat, bien sûr, des organismes assurant une représentation des malades et des usagers du système de santé, des producteurs des données de santé, comme certains hôpitaux – dont l'APHP - et des utilisateurs publics et privés de ces données, y compris des organismes de recherche, comme le CNRS ou encore l'INSERM. Le décret d'application de la loi de 2019 permettant la mise en œuvre d'un « SNDS élargi et centralisé» est en cours d'élaboration, mais la loi nous renseigne déjà sur l'ampleur de son périmètre : en plus des données du Programme médicalisé des systèmes d'informations (PMSI), du Système national d'information interrégimes de l'assurance maladie (SNIIRAM), de la base de données sur les causes de décès (CépiDC de l'INSERM), sont ajoutées les données médico-sociales, les données issues des visites médicales scolaires, des visites de santé au travail… C'est ainsi une des plus grandes bases de données de santé au

monde qui est en train de se mettre en place. Son caractère centralisé interroge d'autant plus que les données concernées sont particulièrement sensibles.

Entendues de manière large par le RGPD comme des « données relatives 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 révèlent des informations sur l'état de santé de cette personne » (art. 4. 15), ces données sont sensibles en ce qu'elles révèlent une part d'intimité. Sensibles, elles le sont également au regard de leur valeur : sur le *dark web*, elles sont vendues en moyenne trois fois plus cher que des données classiques ce qui explique la multiplication récente des cyberattaques sur ce type de données. C'est ainsi qu'un régime particulier a été adopté pour les protéger : en principe, leur utilisation et leur exploitation sont interdites, sauf exceptions justifiées par des finalités d'intérêt public. Les finalités de traitement à des fins médicales pour la recherche de la plateforme des données de santé en font naturellement partie (art L. 1460-1 CSP). Mais l'accès aux données est très encadré puisque chaque dossier fait l'objet d'une double instruction : l'une par le comité d'éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES) pour vérifier la pertinence du projet par rapport à l'intérêt général, l'autre par la CNIL, pour s'assurer de la protection des données. L'hébergeur des données est en outre soumis à toute une série d'exigences et doit être titulaire d'un certificat de conformité (L. 1111-8 CSP).

Compte tenu de ces éléments, la CNIL a souligné l'importance d'une mise en route encadrée et sans précipitation du HDH (Délib. 2020-044 du 20 avril 2020). Mais la pandémie a au contraire accéléré sa mise en place. Un arrêté du 21 avril 2020 lui a ainsi permis de recevoir plusieurs catégories 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 ». A ce titre, le HDH a été autorisé à centraliser les « données issues des applications mobiles de santé et d'outils de télésuivi, télésurveillance ou télémédecine », mais aussi les données du SNDS, des laboratoires, des officines pharmaceutiques… La plateforme a même été autorisée à croiser ces données (article 10-7 de l'arrêté).

L'accroissement du périmètre de cette plateforme qui vise à centraliser toutes les données de santé a été d'autant plus critiqué qu'il a été décidé de recourir à Microsoft pour héberger les données en question. Pour permettre au HDH d'être opérationnel le plus vite possible, un contrat a en effet été conclu avec Microsolf Ireland Operations Limited, filiale de la société américaine Microsoft Corporation, pour accéder à ses services de Cloud, Azure.

Plusieurs associations « pro-logiciel libre » saisirent alors le juge administratif d'un référé-liberté. Relayant les craintes de la CNIL, les requérants invoquèrent les risques pour la protection des données du recours à un prestataire américain. Mais le Conseil d'Etat considéra que le choix de Microsoft, certifiée « hébergeur de données de santé », adhérant au *Privacy Shield (*Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016, relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis), ne transférant que des données de maintenance et non des données de santé aux Etats-Unis et ce, de manière très marginale, ne portait pas « atteinte grave et manifestement illégale au droit au respect à la vie privée et au droit à la protection des données personnelles » (CE ord. 19 juin 2020, *Plateforme Health Data Hub*). L'invalidation du *Privacy Shield* par l'arrêt *Schrems II* de la CJUE du 16 juillet 2020 allait naturellement rebattre les cartes. Dès lors qu'était acté le fait que le droit des Etats-Unis n'assurait pas une protection équivalente à celle du RGPD, les risques d'un transfert ne pouvaient plus être négligés. Anticipant les répercussions de cet arrêt, la plateforme des données de santé signa d'ailleurs un avenant contractuel le 3 septembre 2020 avec Microsoft précisant que cette dernière ne traiterait pas les données du HDH en dehors de l'Union européenne sans son approbation et que l'accès aux données nécessaire aux opérations

d'exploitation des services en ligne et de résolutions d'incidents menées par Microsoft depuis un lieu extérieur serait soumis à l'autorisation de la plateforme.

Mais ces précautions n'empêchèrent pas deux nouvelles saisines du juge des référés. La première, sur le fondement de l'article L. 521-4 du CJA, ne put prospérer (CE ord. 21 septembre 2020). La seconde, qui nous intéresse ici, se fonde cette fois sur l'article L. 521- 2 du CJA qui permet au juge, si l'urgence le justifie, d'ordonner toutes mesures nécessaires à la sauvegarde d'une liberté fondamentale à laquelle il serait porté une atteinte grave et manifestement illégale. Ce référé-liberté - voie de recours originale en matière contractuelle - conduit une fois encore à une solution de rejet. Mais, bien que rendue dans les limites d'une procédure d'urgence, sa portée ne saurait être négligée. Appliquant la jurisprudence *Schrems II*, le Conseil d'Etat ne néglige pas les risques de transfert des données aux Etats-Unis pour la vie privée mais il les juge pour l'heure hypothétiques et, face à l'urgence sanitaire qui commande de maintenir le HDH en service, il considère que ces risques ne sont pas constitutifs d'une illégalité grave et manifeste justifiant sa suspension. L'argumentation est cependant embarrassée : comme si le juge ne pouvait se satisfaire lui-même de cette solution, il encadre la validation du HDH de toute une série d'injonctions et de recommandations, qui n'en améliore pas la clarté, mais qui témoigne d'une convergence de vues avec la CJUE et la CNIL.

I. L'appréciation des risques

Forts de la jurisprudence *Schrems II*, les requérants demandent au juge des référés la suspension de la centralisation et du traitement des données en lien avec l'épidémie de covid 19 sur le HDH et l'adoption de toutes mesures permettant d'éviter qu'une atteinte grave et manifestement illégale au droit à la vie privée ne se réalise, eu égard aux risques qu'emportent le choix d'une société américaine pour l'hébergement de ces données sensibles. L'appréciation de ces risques suppose que le juge vérifie que le contrat interdit effectivement tout transfert de données aux Etats-Unis, mais aussi que l'hébergeur, en tant qu'entreprise américaine, ne puisse être contraint d'y donner accès sur injonction des autorités américaines. Pour des raisons différentes, le juge des référés considère que l'atteinte grave et manifestement illégale au droit à la vie privée n'est caractérisée dans aucune des deux hypothèses.

A. L'éviction du risque de transfert de données dans le cadre contractuel

Dans un premier temps, il s'agit d'apprécier le risque d'un transfert de données aux Etats-Unis en application du contrat conclu entre le HDH et Microsoft. C'est exactement l'hypothèse de la jurisprudence *Schrems II*.

Dans son ordonnance rendue en juin 2020, le juge des référés avait écarté ce risque en jugeant que si tout transfert n'était pas absolument exclu, il ne présentait pas de risque pour la vie privée puisque Microsoft adhérait au *Privacy Shield*, décision par laquelle la Commission avait assuré l'adéquation de la législation états-unienne à la législation européenne de protection des données personnelles. Mais la Cour de justice a invalidé cette décision. Elle a considéré que les exigences de la section 702 du *Foreign Intelligence Surveillance Act* (FISA) et l'*Executive order* (EO) 12333 américain, permettant l'accès des autorités publiques états-uniennes à des fins de sécurité nationale aux données personnelles transférées de l'Union européenne vers les Etats-Unis, de façon particulièrement large et sans ciblage[1], entrainaient des limitations de la

[1] Parmi ces programmes figurent *Prism* et *UpStream*, dont l'ampleur avait été révélée par Edward Snowden en 2013 et depuis maintenus.

protection des données personnelles qui n'étaient pas circonscrites de manière à satisfaire à des exigences équivalentes à celles requises par le droit de l'Union. Elle a ainsi considéré que cette législation n'accordait pas aux personnes concernées des droits de recours devant les juridictions contre les autorités étatsuniennes. Jugeant que le droit des Etats-Unis n'assurait pas un niveau de protection équivalent au droit européen, elle invalida le *Privacy Shield* (B. Bertrand, J. Sirinelli, « Schrems II : on prend les mêmes et on recommence », *Dalloz IP/IT*, nov. 2020). Elle n'invalida pas les clauses contractuelles types élaborées par la Commission, mais pour les utiliser valablement, elle exigea que le responsable de traitement évalue si le pays tiers assure un niveau de protection équivalent. En cas contraire, des mesures additionnelles pour assurer le niveau de protection requis devaient être prises. Par conséquent, aucun transfert ne pouvait plus avoir lieu sur le fondement des articles 45 et 46 du RGPD.

Le Conseil d'Etat ne pouvait ignorer ce bouleversement. Dans l'ordonnance du 13 octobre, il prend effectivement acte de la jurisprudence *Schrems II*, mais son application ne le conduit pas à inverser la solution adoptée le 19 juin 2020 pour deux raisons. Il considère, d'une part, que les données de santé ne sont pas hébergées aux Etats-Unis mais sur le territoire de l'Union européenne (aux Pays-Bas, et « prochainement » en France). Seules les données de télémétrie et de facturation pourraient potentiellement être transférées aux Etats-Unis, non les données de santé. Il ajoute, d'autre part, que l'avenant conclu le 3 septembre 2020 interdit à Microsoft de traiter les données en dehors de l'Union sans l'approbation du HDH et impose, si d'aventure l'entreprise devait malgré tout accéder aux données, de requérir l'autorisation de la plateforme. Or, celle-ci s'est engagée à l'égard de la CNIL « à refuser tout transfert ». Depuis, le transfert a même été interdit, comme le demandait la CNIL (Mémoire en observations, 8 oct. 2020), par un arrêté du 9 octobre 2020. Le juge estime par conséquent qu'« en l'état de l'instruction, il n'apparait pas que des données à caractère personnel du système de santé puissent à ce jour faire l'objet de transferts en dehors de l'Union européenne en application du contrat conclu entre la Plateforme des données de santé et Microsoft ». Mais restait une autre question à trancher : celle du risque de transfert de données en dehors du cadre contractuel, sur injonction des autorités américaines.

B. La prise en compte du risque extérieur aux parties

La deuxième question soulevée par les requérants – la plus délicate - était celle de la possibilité de transferts de données personnelles en dehors de toute initiative des contractants. Du fait de l'extraterritorialité de la loi FISA et de l'EO, Microsoft pouvait en effet être soumise, en tant qu'entreprise américaine, au respect de potentielles injonctions des services de renseignements des Etats-Unis. Les requérants avaient également invoqué, lors de leur premier recours, les risques de l'application du *Clarifying Lawful Overseas Use of Data* (*Cloud Act*). Adopté en 2018 pour mettre fin au conflit entre la justice américaine et Microsoft qui persistait depuis 2013, cet acte concerne la possibilité pour la justice américaine d'avoir accès aux données des entreprises américaines, même si leur activité se situe sur le territoire de l'Union, en cas de procédure judiciaire de nature criminelle. Les requérants n'ont cependant pas réexploité l'argument, sans doute parce que cette législation américaine n'a pas été examinée dans l'arrêt *Schrems II*.

La question posée alors se situe d'ailleurs dans « l'angle mort » de l'arrêt *Schrems II* (B. Bertrand, « Polyphonie dans l'appréciation du recours à une solution technique américaine pour la Plateforme Health Data Hub : le Conseil d'Etat et l'art de la fugue », *Sem. Jur. Ed G*. n°49, nov. 2020, 1358), puisque la Cour s'était alors prononcée seulement sur l'hypothèse d'un transfert prévu par le contrat, non sur un transfert subi par les parties. Mais

comme l'a souligné la CNIL, « si la Cour ne s'est penchée que sur le cas où un opérateur transfère de sa propre initiative des données personnelles vers les Etats-Unis, qui était celui de l'espèce, les motifs de sa décision impliquent d'examiner la licéité d'une situation où un opérateur traitant des données sur le sol européen s'expose à devoir les transférer sur injonction judiciaire ou administrative aux services de renseignements étatsuniens » (Mémoire en observations p. 5), ce que le Conseil d'Etat accepte effectivement de vérifier. Il va alors évaluer le niveau de protection assuré en considération des stipulations contractuelles et des éléments pertinents du système juridique de l'Etat tiers. Ce contrôle réalisé dans le cadre d'une instruction en référé nécessairement limitée, conduit le Conseil à une solution pragmatique. Sans nier l'existence des risques, il en minore la portée et ce faisant, valide le dispositif du HDH.

Selon les stipulations contractuelles, (annexe 3 à l'addendum sur la protection des données pour les services en ligne de Microsoft) la société s'engage à appliquer le RGPD et en particulier l'interdiction des transferts hors Union (art. 28 et 44). Le juge concède néanmoins que les demandes de renseignements par les autorités américaines ne peuvent être complètement écartées. Selon la plateforme, puisque Microsoft ne peut pas avoir accès aux données qu'elle héberge, elle ne peut pas, techniquement, déférer aux demandes d'autorités de renseignement. Mais la CNIL a mis en évidence une faille dans le contrat qui permet à Microsoft d'y accéder « dans le cadre de scénarios inattendus ou imprévisibles ». Dans cette hypothèse, elle pourrait être tenue de faire droit à une demande de renseignement des autorités américaines fondées sur la loi FISA ou l'EO. En admettant l'existence d'un tel risque existe, le Conseil se fait ainsi l'écho des inquiétudes de la CNIL.

Il juge cependant ce risque d'atteinte à la vie privée acceptable et rejette la demande de suspension du traitement des données pour plusieurs raisons. D'abord, il considère que ce risque est hypothétique ; il ne s'agit pas d'une violation directe du RGPD. Ensuite, le risque est minime, ne serait-ce que par ce que les données sont pseudonymisées par la CNAM. Les mises en gardes de la CNIL concernant les possibilités de réidentification n'ont pas été relevées par le juge. Enfin et surtout, le Conseil d'Etat juge le risque acceptable au regard de l'enjeu : il s'agit de ne pas bloquer la mise en route du HDH, qui doit permettre d'améliorer la gestion de l'urgence sanitaire et les connaissances sur le virus. L'intérêt public impose ainsi que la mise en route du HDH ne soit pas interrompue. Or, selon le Conseil – reprenant les analyses du gouvernement et du HDH sur ce point – en l'absence de solution technique alternative satisfaisante, « sans équivalent à ce jour », et compte tenu de l'urgence, il y a « un intérêt public important à permettre la poursuite de l'utilisation des données de santé » et partant, à permettre l'hébergement des données par Microsoft. Aussi, alors que la condition de l'urgence du référé n'est pas appréciée par le juge – ce qui est commun dans une ordonnance de rejet dès lors que l'atteinte grave et manifeste à une liberté fondamentale n'est pas caractérisée, comme c'est le cas ici - elle est paradoxalement mobilisée pour justifier le maintien de la mesure. « En référé, le juge est confronté à deux urgences et l'urgence sanitaire semble faire obstacle à l'urgence du référé » (B. Bertrand, précité). Le juge fait primer l'enjeu sanitaire sur la protection des données personnelles et conclut à l'absence d'atteinte immédiate à un intérêt public.

En l'absence d'atteinte grave et manifestement illégale à la protection de la vie privée, le recours est rejeté et Microsoft peut continuer à héberger les données du HDH. Le dispositif est, pour ainsi dire, « sauvé ». Mais, non sans ambiguïté, si le juge des référés considère qu'il ne peut ordonner la suspension du dispositif en tant que mesure de sauvegarde fondée sur l'article L. 521-2 du CJA, il utilise son pouvoir d'injonction et formule de multiples recommandations aux parties de manière à ce qu'elles en assurent la mise en conformité.

II. Les injonctions et recommandations de mise en conformité

Le HDH n'est pas suspendu, mais compte tenu des risques pour la protection des données, clairement mis en évidence par la CNIL, le Conseil d'Etat demande aux parties d'assurer la mise en conformité du dispositif. Dans une démarche proactive, il utilise son pouvoir d'injonction pour demander aux parties de garantir la conformité du contrat et formule, en complément, diverses recommandations. S'ouvre alors une période transitoire que les parties devront mettre à profit pour assurer le respect du RGPD en se pliant aux injonctions du juge de préciser certains points par avenants, et en s'efforçant de respecter ses recommandations, dans une logique de *compliance.*

A. Les injonctions d'intervenir par voie d'avenant au contrat

Le juge des référés compense le rejet du recours par l'adoption de mesures d'injonction imposant aux parties de mettre le dispositif d'hébergement des données en conformité avec les exigences du RGPD par voie d'avenants au contrat. Cette injonction aux cocontractants, surprenante en dehors d'un contentieux contractuel, s'inscrit en réalité dans le prolongement de l'évolution du contrat que les parties avaient déjà initiée. Elle porte sur deux points.

D'abord, le juge enjoint aux parties de conclure un nouvel avenant sous quinze jours précisant que tous les services couverts par le contrat sont concernés par l'interdiction de transfert (point 13). Il relaie ce faisant les inquiétudes de la CNIL qui, dans son mémoire en observation soulignait que le premier avenant ne semblait pas couvrir l'ensemble des services.

Ensuite, pour faire face au risque de transferts sur demande des autorités américaines, le juge impose aux cocontractants de préciser par le même avenant que l'autorisation d'accès ne peut résulter que d'une disposition du droit de l'Union européenne ou du droit d'un Etat membre (point 16). Il s'agit là de lever un doute résultant de l'addendum auquel renvoie l'avenant conclu le 3 septembre 2020 en vertu duquel *« Microsoft ne divulguera pas les données traitées aux pouvoirs publics, sauf si elle y est tenue par la loi »*. L'avenant, dit le Conseil d'Etat, doit impérativement préciser que la loi en question ne saurait être la loi américaine, mais bien le droit de l'Union, donc le RGPD, ou encore le droit interne d'un Etat membre.

Palliatifs d'une décision en référé qui ne préjuge pas, rappelons-le, d'une éventuelle décision sur le fond, ces injonctions sont en outre assorties de diverses recommandations.

B. Les recommandations du juge des référés

Dans une logique de *compliance* visant une régulation partagée avec les opérateurs dans le but de prévenir l'apparition d'un risque, le juge adopte, là encore, une posture originale, l'éloignant de son office traditionnel. Conformément au nouveau paradigme posé par le droit européen de la protection des données personnelles (A. Bensamoun, B. Bertrand, (dir.), *Le Règlement général sur la protection des données*, Mare et Martin, 2020 ; L. Cluzel, E. Debaets, « La loi du 20 juin 2018 relative à la protection des données personnelles », *RFDA* nov-déc. 2018), le juge s'inscrit dans une « *direction juridique non autoritaire des conduites* » (P. Amselek, « L'évolution générale de la technique juridique dans les sociétés occidentales », *RDP*, 1982, n°2, pp. 275 et s.), en formulant des recommandations.

Dans l'attente d'une solution définitive, le juge des référés demande au HDH et à Microsoft de « rechercher les meilleures solutions techniques et organisationnelles possibles pour garantir le respect de la protection des données personnelles ». Microsoft

doit, notamment, mettre à la disposition du HDH toutes les informations nécessaires pour démontrer le respect des obligations et permettre la réalisation d'audits. Dans la logique du RGPD, il s'agit de responsabiliser les parties en leur demandant de mettre tous les moyens en œuvre pour démontrer le respect de leurs obligations (T. Douville, *Droit des données à caractère personnel*, Gualino, 2021, p. 201 et s.).

Aussi, comme pour mieux faire accepter la décision de rejet, le juge explique que le risque et les palliatifs dont il demande la mise en œuvre, ne sauraient être que provisoires. Il fait en effet état de la volonté des autorités publiques d'adopter « des mesures propres à éliminer tout risque », notamment par le choix d'un nouveau sous-traitant ou le recours à un accord de licence. L'hypothèse d'une résiliation du contrat avec Microsoft est ainsi évoquée. Le ministre de la santé s'est d'ailleurs engagé auprès de la Cnil à mettre un terme, d'ici deux ans, à l'hébergement par Microsoft du HDH (*Le Monde*, 9 oct. 2020). Une « étude de réversibilité » a déjà été lancée. On s'orienterait vers le projet *Gaïa X*, un projet de « cloud souverain » européen mené par la France et l'Allemagne. En cas de résiliation, il faudrait alors procéder à l'indemnisation des pertes subies et des bénéfices perdus par Microsoft, indemnisation qui se négocierait sans doute âprement. Aussi, bien que le recours soit rejeté, les conséquences de l'application de la jurisprudence *Schrems II* ne sont pas négligeables. Au-delà de l'affaire du HDH, les solutions d'hébergement de nombreux acteurs, entreprises comme administrations, qui ont recours à des sociétés américaines, vont devoir être révisées. Pour remédier à cette insécurité juridique, la Commission européenne adoptera sans doute de nouvelles clauses contractuelles types ainsi qu'une nouvelle décision remplaçant le *Privacy Shield*, à la condition que les Etats-Unis apportent des garanties de protection des données personnelles réellement équivalentes au droit européen. L'idéal serait sans nul doute l'adoption d'un traité international pour fixer des principes communs en matière de protection des données personnelles (A. Aguila, J. Apostle, J. Crouzet, G. Léonard, Tribune, *Le Monde*, 29 oct. 2020).

En attendant, la vigilance est de mise. La CNIL s'inquiète déjà des dispositions du décret « SNDS élargi », actuellement en préparation, qui fait entrer le dispositif jusqu'alors limité aux « données Covid », dans le droit commun. Ce seront alors toutes les données de santé des français qui pourraient être hébergées par Microsoft. La CNIL estime à cet égard « indispensable que la garantie prévue par l'arrêté du 9 octobre 2020 au bénéfice des données de l'entrepôt « Covid » soit étendue à l'ensemble des données composant le SNDS et, qu'ainsi, il soit fait interdiction à l'ensemble des données composant le SNDS de faire l'objet d'un transfert de données en dehors de l'Union européenne ». (Délibération CNIL du 29 octobre 2020 portant avis sur un projet de décret relatif au SNDS, point 5). Si d'aventure le Conseil d'Etat était saisi d'un recours contre ce décret, il se pourrait qu'il soit moins clément que pour le dispositif des « données Covid », qu'il n'a finalement étudié que dans le cadre d'un référé. Les injonctions et recommandations de l'ordonnance du 13 octobre pourraient en effet laisser place à une annulation si l'interdiction de transfert des données hors Union européenne n'était pas clairement établie et plus largement, si le droit de la protection des données personnelles n'était pas respecté. Cette première décision d'application de l'arrêt *Schrems II* laisse en tout cas penser que la partition du Conseil d'Etat commence à s'accorder avec celle de la Cour de justice et avec celle de la CNIL dans l'application du RGPD. L'affaire du HDH révèle également toutes les limites d'une régulation partagée avec les opérateurs : pour des données aussi sensibles que les données de santé, le système d'autorisation par la CNIL est encore, nous semble-t-il, le plus approprié.