

RÉPUBLIQUE FRANÇAISE
AU NOM DU PEUPLE FRANÇAIS

CONSEIL D'ETAT
Statuant au contentieux
Ordonnance du 13 octobre 2020

N° 444937

LE JUGE DES RÉFÉRÉS

Vu la procédure suivante :

Par une requête, enregistrée le 28 septembre 2020 au secrétariat du contentieux du Conseil d'Etat, l'association le Conseil national du logiciel libre (CNLL), l'association Ploss Rhône-Alpes, l'association SoLibre, la société Nexedi, l'association Interhop, les hôpitaux français pour l'interopérabilité et le partage libre des algorithmes, Mme B... I..., M. C... A..., le syndicat national des journalistes (SNJ), le syndicat de la médecine générale (SMG), l'union française pour une médecine libre (UFML), M. H... J..., M. D... G..., l'union générale des ingénieurs, cadres et techniciens CGT (UGICT-CGT), l'union fédérale médecins, ingénieurs, cadres, techniciens CGT santé et action sociale (UFIMCT – CGT santé et action sociale), Mme L... K..., M. E... F..., l'association Constances, l'association les Actupiennes et l'association française des hémophiles (AFH) demandent au juge des référés du Conseil d'Etat, sur le fondement de l'article L. 521-2 du code de justice administrative :

1°) à titre principal, d'ordonner la suspension de la centralisation et du traitement des données en lien avec l'épidémie de covid-19 sur la Plateforme des données de santé, ainsi que toutes mesures nécessaires aux fins d'assurer l'absence d'atteinte grave et manifestement illégale au droit à la vie privée et à la protection des données personnelles en lien avec le traitement et la centralisation des données de santé sur le Health Data Hub ;

2°) à titre subsidiaire, de solliciter la Commission nationale de l'informatique et des libertés, notamment aux fins de statuer sur les implications de l'invalidation du « Privacy Shield » sur le traitement et la collecte des données au sein de la Plateforme des données de santé ;

3°) de mettre à la charge de l'Etat la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Ils soutiennent que : – ils justifient d'un intérêt leur donnant qualité pour agir ; – la condition d'urgence est remplie eu égard, tout d'abord, à la situation d'urgence sanitaire déclarée depuis le 23 mars 2020, dont les effets ont été reconduits par l'arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé, ensuite, à la portée de la mesure litigieuse permettant une collecte et une centralisation très larges de données particulièrement sensibles, ainsi qu'aux réserves émises par la Commission nationale de l'informatique et des libertés, et, enfin, aux risques mis en évidence par l'arrêt de la Cour de justice de l'Union européenne du 16 juillet 2020 ; – il est porté une atteinte grave et

manifestement illégale au droit au respect de la vie privée et au droit à la protection des données personnelles, eu égard à la soumission au droit américain de la société choisie pour assurer la solution technique de la Plateforme des données de santé, sans garanties suffisantes au regard des risques qu'emportent, d'une part, le transfert de données vers les Etats-Unis, mis en évidence par l'arrêt de la Cour de justice de l'Union européenne du 16 juillet 2020, et, d'autre part, l'application extraterritoriale du droit américain.

Par un mémoire en défense, enregistré le 7 octobre 2020, le ministre des solidarités et de la santé conclut au rejet de la requête. Il soutient que la condition d'urgence n'est pas remplie et qu'aucune atteinte grave et manifestement illégale n'est portée à une liberté fondamentale.

La Commission nationale de l'informatique et des libertés a produit des observations, enregistrées le 8 octobre 2020.

La requête a été communiquée au Premier ministre, à la Plateforme des données de santé et à la société Microsoft France, qui n'ont pas produit de mémoire.

Après avoir convoqué à une audience publique, d'une part, le Conseil national du logiciel libre et les autres requérants et, d'autre part, le Premier ministre, le ministre des solidarités et de la santé, la Plateforme des données de santé et la société Microsoft France, ainsi que la Commission nationale de l'informatique et des libertés ;

Ont été entendus lors de l'audience publique du 8 octobre 2020, à 14 heures 30 :

- les représentants du CNLL et des autres requérants ;
- les représentants du ministre des solidarités et de la santé ;
- les représentants de la Plateforme des données de santé ;
- les représentants de la société Microsoft France ;

à l'issue de cette audience, le juge des référés a reporté la clôture de l'instruction au 13 octobre à 12 heures ;

Vu les observations, enregistrées le 9 octobre 2020, présentées par la société Microsoft France ;

Vu les nouveaux mémoires, enregistrés les 12 et 13 octobre 2020, présentés par le CNLL et des autres requérants, qui tendent au mêmes fins que leur requête ;

Vu les nouvelles pièces et le nouveau mémoire, enregistrés les 10 et 13 octobre 2020, produits par le ministre des solidarités et de la santé, tendant au même fin que son précédent mémoire ;

Vu la note en délibéré, enregistrée le 13 octobre 2020, présentée par le CNLL et des autres requérants ;

Vu les autres pièces du dossier ;

Vu : – la charte des droits fondamentaux de l’Union européenne ; – le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ; – le code de la santé publique ; – la loi n° 78-17 du 6 janvier 1978 ; – la loi n° 2019-774 du 24 juillet 2019 ; – la loi n° 2020-856 du 9 juillet 2020 ; – l’arrêté du ministre des solidarités et de la santé du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l’épidémie de covid-19 dans les territoires sortis de l’état d’urgence sanitaire et dans ceux où il a été prorogé ; – le code de justice administrative ;

Considérant ce qui suit :

1. Aux termes de l’article L. 511-1 du code de justice administrative : « Le juge des référés statue par des mesures qui présentent un caractère provisoire. Il n’est pas saisi du principal et se prononce dans les meilleurs délais ». Aux termes de l’article L. 521-2 du même code : « Saisi d’une demande en ce sens justifiée par l’urgence, le juge des référés peut ordonner toutes mesures nécessaires à la sauvegarde d’une liberté fondamentale à laquelle une personne morale de droit public ou un organisme de droit privé chargé de la gestion d’un service public aurait porté, dans l’exercice d’un de ses pouvoirs, une atteinte grave et manifestement illégale. Le juge des référés se prononce dans un délai de quarante-huit heures ».

Sur l’office du juge des référés :

2. Il résulte de la combinaison des dispositions des articles L. 511-1 et L. 521-2 du code de justice administrative qu’il appartient au juge des référés, lorsqu’il est saisi sur le fondement de l’article L. 521-2 et qu’il constate une atteinte grave et manifestement illégale portée par une personne morale de droit public à une liberté fondamentale, résultant de l’action ou de la carence de cette personne publique, de prescrire les mesures qui sont de nature à faire disparaître les effets de cette atteinte, dès lors qu’existe une situation d’urgence caractérisée justifiant le prononcé de mesures de sauvegarde à très bref délai et qu’il est possible de prendre utilement de telles mesures. Celles-ci doivent, en principe, présenter un caractère provisoire, sauf lorsque aucune mesure de cette nature n’est susceptible de sauvegarder l’exercice effectif de la liberté fondamentale à laquelle il est porté atteinte.

3. Le droit au respect de la vie privée, qui comprend le droit à la protection des données personnelles, constitue une liberté fondamentale au sens des dispositions de l’article L. 521-2 du code de justice administrative.

Sur le cadre juridique :

En ce qui concerne le droit de l’Union européenne en matière de protection des données :

4. D’une part, aux termes de l’article 44 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ou règlement général sur la protection des données : « Un transfert, vers un pays tiers (...), de données à caractère personnel qui font ou sont destinées à

faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant (...). Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis ». L'article 45 de ce règlement prévoit que : « 1. Un transfert de données à caractère personnel vers un pays tiers (...) peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers (...) assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique. / 2. Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte, en particulier, des éléments suivants : / a) l'état de droit, le respect des droits de l'homme et des libertés fondamentales, (...) l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, (...) ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées; (...) / 3. La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers (...), assure un niveau de protection adéquat (...) ». Aux termes de l'article 46 de ce règlement : « 1. En l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives. / 2. Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par : / (...) / c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2 (...) ».

5. D'autre part, aux termes de l'article 48 du même règlement : « Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre ». L'article 28 de ce règlement prévoit que : « 1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée. / (...) / 3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui (...) prévoit, notamment, que le sous-traitant : / a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis ; dans ce cas, le sous-

traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public (...) ».

6. Par un arrêt de grande chambre du 16 juillet 2020, Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems, C-311/18, la Cour de justice de l'Union européenne a dit pour droit que l'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du règlement 2016/679 doivent être interprétés en ce sens que les garanties appropriées, les droits opposables et les voies de droit effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne par ce règlement, lu à la lumière de la charte des droits fondamentaux de l'Union européenne. A cet effet, l'évaluation du niveau de protection assuré doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union européenne et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci, notamment ceux énoncés à l'article 45, paragraphe 2, du règlement.

7. Par cet arrêt, la Cour de justice a également jugé que la 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 Union européenne – Etats-Unis, prise sur le fondement de la directive 95/46 et valant décision d'adéquation au sens de l'article 45, paragraphe 3, du règlement général sur la protection des données, était invalide au motif que, même dans ce cadre, les Etats-Unis n'assuraient pas un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies dans ce pays. Elle a, en effet, relevé des ingérences dans les droits fondamentaux des personnes dont les données à caractère personnel sont ainsi transférées, du fait des possibilités d'accès à ces données et d'utilisation de celles-ci par les autorités publiques américaines, dans le cadre de programmes de surveillance fondés sur l'article 702 du « Foreign Intelligence Surveillance Act » (FISA) ou loi sur la surveillance en matière de renseignement extérieur et, d'autre part, de l' « Executive Order (EO) 12333 » ou décret présidentiel n° 12333, qui ne sont pas limitées au strict nécessaire. L'article 702 du FISA ne limite pas l'habilitation qu'il comporte et le tribunal de surveillance du renseignement extérieur des Etats-Unis vérifie seulement si ces programmes correspondent à l'objectif d'obtention d'informations en matière de renseignement extérieur, mais non si les personnes sont correctement ciblées à cette fin. Quant à l'EO 12333, il doit être mis en œuvre dans le respect de la « Presidential Policy Directive 28 » (PPD-28), qui permet toutefois de procéder à une collecte « en vrac » d'un volume relativement important d'informations ou de données lorsque les services de renseignement ne peuvent pas utiliser d'identifiant associé à une cible spécifique pour orienter la collecte, rendant possible un accès à des données en transit vers les Etats-Unis sans surveillance judiciaire ni encadrement suffisant. Enfin, pour ces différents programmes de surveillance, il n'existe pas de texte conférant aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux, leur permettant de bénéficier d'un droit de recours effectif. Dans ces conditions, les limitations de la protection des données à caractère

personnel qui découlent de la réglementation interne des Etats-Unis ne sont pas encadrées de façon à répondre à des exigences substantiellement équivalentes à celles requises par la charte des droits fondamentaux de l'Union européenne, dont l'article 52 ne permet des limitations de l'exercice des droits et libertés qu'elle reconnaît que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

En ce qui concerne les dispositions nationales encadrant la collecte et le traitement des données en lien avec l'épidémie de covid-19 sur la Plateforme des données de santé :

8. D'une part, l'article L. 1462-1 du code de la santé publique, dans sa rédaction issue de la loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, prévoit qu'un groupement d'intérêt public, dénommé « Plateforme des données de santé » et constitué entre l'Etat, des organismes assurant une représentation des malades et des usagers du système de santé, des producteurs de données de santé et des utilisateurs publics et privés de données de santé, y compris des organismes de recherche en santé, est notamment chargé de réunir, organiser et mettre à disposition les données du système national des données de santé mentionné à l'article L. 1461-1 du même code et de promouvoir l'innovation dans l'utilisation des données de santé. L'avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé » ou « Health Data Hub » a été approuvé le 29 novembre 2019 par un arrêté de la ministre des armées, de la ministre des solidarités et de la santé, du ministre de l'économie et des finances, de la ministre du travail, du ministre de l'éducation nationale et de la jeunesse, du ministre de l'action et des comptes publics, de la ministre de l'enseignement supérieur, de la recherche et de l'innovation et du ministre de l'agriculture et de l'alimentation.

9. D'autre part, aux termes du premier alinéa de l'article L. 3131-1 du code de la santé publique : « En cas de menace sanitaire grave appelant des mesures d'urgence, notamment en cas de menace d'épidémie, le ministre chargé de la santé peut, par arrêté motivé, prescrire dans l'intérêt de la santé publique toute mesure proportionnée aux risques courus et appropriée aux circonstances de temps et de lieu afin de prévenir et de limiter les conséquences des menaces possibles sur la santé de la population. Le ministre peut également prendre de telles mesures après la fin de l'état d'urgence sanitaire prévu au chapitre I er bis du présent titre, afin d'assurer la disparition durable de la situation de crise sanitaire ». L'article 30 de l'arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé, pris sur le fondement de ces dispositions et de celles de l'article L. 3131-16 du code de la santé publique, prévoit, au sein d'un chapitre consacré au traitement des données à caractère personnel du système de santé, que : « I.- 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, le groupement d'intérêt public mentionné à l'article L. 1462-1 du code de la santé publique et la Caisse nationale de l'assurance maladie sont autorisés à recevoir les catégories de données à caractère personnel suivantes : / – les données issues du système national des données de santé mentionné à l'article L. 1461-1 du même code ainsi que, dans le respect de son référentiel de sécurité : / – des données de pharmacie ; / – des données de prise en charge en ville telles que des

diagnostics ou des données déclaratives de symptômes issues d'applications mobiles de santé et d'outils de télésuivi, télésurveillance ou télémedecine ; / – des résultats d'examen biologiques réalisés par les laboratoires hospitaliers et les laboratoires de biologie médicale de ville ; / – des données relatives aux urgences collectées par l'Agence nationale de santé publique dans le cadre du réseau de surveillance coordonnée des urgences ; / – des données relatives aux appels recueillis au niveau des services d'aide médicale urgente et des services concourant à l'aide médicale urgente ; / – des données relatives à l'activité et à la consommation de soins dans les établissements ou services médico-sociaux, notamment dans les établissements d'hébergement pour personnes âgées dépendantes ; / – des enquêtes réalisées auprès des personnes pour évaluer leur vécu ; / – des données non directement identifiantes issues du système d'identification unique des victimes mentionné à l'article L. 3131-9-1 du code de la santé publique ; / – des données cliniques telles que d'imagerie, de pharmacie, de biologie, de virologie, de comptes rendus médicaux de cohortes de patients pris en charge dans des centres de santé en vue de leur agrégation. / II.- Le groupement d'intérêt public et la Caisse nationale de l'assurance maladie ne peuvent collecter que les données nécessaires à la poursuite d'une finalité d'intérêt public en lien avec l'épidémie actuelle de covid-19. Ils sont responsables du stockage et de la mise à disposition des données. Ils sont autorisés à croiser les données mentionnées au I. / La Caisse nationale de l'assurance maladie est responsable des opérations de pseudonymisation dans le cadre du croisement des données et peut traiter le numéro d'inscription au répertoire national d'identification des personnes physiques à cette fin. / Seuls des responsables de traitement autorisés dans les conditions prévues aux articles 66 et 76 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, l'Etat mettant en œuvre des traitements mentionnés au 6° de l'article 65 de cette même loi, la Caisse nationale de l'assurance maladie mettant en œuvre des traitements mentionnés au 3° de l'article 65 de cette même loi, ou les organismes et les services chargés d'une mission de service public mentionnés à l'article 67 de cette même loi, peuvent traiter les données ainsi rassemblées par le groupement d'intérêt public. / III.- Les données ne peuvent être traitées que pour des projets poursuivant une finalité d'intérêt public en lien avec l'épidémie actuelle de covid-19 et jusqu'à l'entrée en vigueur des dispositions prises en application de l'article 41 de la loi du 24 juillet 2019 susvisée et au plus tard le 30 octobre 2020. / Les données ne peuvent être traitées que sur la plateforme technologique du groupement d'intérêt public et sur la plateforme de la Caisse nationale de l'assurance maladie, et ne peuvent pas en être extraites. Au sein de ces plateformes, les données ci-dessus mentionnées ne peuvent contenir ni les noms et prénoms des personnes, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques, ni leur adresse. / Le groupement d'intérêt public établit et met à disposition sur son site internet un répertoire public qui recense la liste et les caractéristiques de tous les projets portant sur ces données ». Ces dispositions prorogent jusqu'au 30 octobre 2020 les effets de celles de l'arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire.

Sur les conclusions principales de la requête :

10. Pour les besoins du stockage et de la mise à disposition des données de santé dont elle est chargée, la Plateforme des données de santé a signé le 15 avril 2020 avec la société de droit irlandais Microsoft Ireland Operations Limited, filiale de la société américaine Microsoft

Corporation, un contrat lui donnant accès à un ensemble de produits « Microsoft Azure », comprenant en particulier l'hébergement des données de santé mentionnées au point 9 et la concession de licences de logiciels nécessaires au traitement de ces données pour les finalités légalement autorisées. L'association le Conseil national du logiciel libre et les autres requérants font valoir les risques que cette situation comporte au regard du droit au respect de la vie privée, compte tenu de possibles transferts de données vers les Etats-Unis, soit en application du contrat conclu avec la société Microsoft Ireland Operations Limited, soit en raison de demandes qui seraient adressées à cette société en dehors même des transferts contractuellement consentis par la Plateforme des données de santé.

En ce qui concerne le risque de transferts de données personnelles en application du contrat conclu avec Microsoft :

11. Il résulte de l'arrêt de la Cour de justice de l'Union européenne du 16 juillet 2020 qu'aucun transfert de données à caractère personnel vers les Etats-Unis ne peut plus avoir lieu sur le fondement de l'article 45 du règlement général sur la protection des données. Si un transfert reste possible sur le fondement de l'article 46, c'est à la condition que soient prévues des garanties appropriées et que les personnes concernées disposent de droits opposables et de voies de droit effectives. Or il résulte du même arrêt que, dans le cas où les autorités publiques américaines auraient accès, sur le fondement de l'article 702 du FISA ou de l'EO 12333, à des données à caractère personnel transférées depuis l'Union européenne, les personnes concernées ne disposeraient pas de droits opposables aux autorités américaines devant les tribunaux, sans qu'il apparaisse, en l'état de l'instruction, que des garanties appropriées puissent être prévues pour y remédier. Dans ces conditions, tout transfert de données personnelles vers les Etats-Unis, par une entreprise pouvant faire l'objet de demandes des autorités américaines sur les fondements mentionnés ci-dessus, est susceptible de contrevenir par lui-même aux articles 44 et suivants du règlement général sur la protection des données, sauf à pouvoir être justifié au regard de son article 49, qui comporte des dérogations pour un certain nombre de situations particulières.

12. Il résulte de l'instruction, d'une part, que les données traitées par la Plateforme des données de santé sont hébergées dans des centres de données situés aux Pays-Bas, avant de l'être prochainement dans des centres de données situés en France. D'autre part, la Plateforme des données de santé et la société Microsoft Ireland Operations Limited ont conclu, le 3 septembre 2020, un avenant prévoyant, pour les services en ligne « Azure » qu'il énumère, que Microsoft ne traitera pas les données de la Plateforme en dehors de la zone géographique spécifiée par celle-ci sans son approbation et que dans l'hypothèse où un accès aux données serait nécessaire pour les besoins des opérations d'exploitation des services en ligne et de résolution d'incident menées par Microsoft depuis un lieu extérieur à cette zone, il serait soumis à l'autorisation préalable de la Plateforme. La Plateforme des données de santé s'est engagée à l'égard de la Commission nationale de l'informatique et des libertés à refuser tout transfert. Enfin, il résulte également de l'instruction que les seules données dont le transfert en dehors de l'Union européenne présente une utilité sont des données de télémétrie, pour contrôler le bon fonctionnement des services offerts par Microsoft, ainsi que des données de facturation. Ainsi, il n'apparaît pas, en l'état de l'instruction, que la Plateforme des données de santé puisse se trouver contrainte, pour des raisons techniques, de donner son accord à un transfert de données de santé.

13. En outre, par un arrêté du 9 octobre 2020 postérieur à l'introduction de la requête, le ministre des solidarités et de la santé a complété l'article 30 de l'arrêté du 10 juillet 2020, relatif aux mesures concernant le traitement des données à caractère personnel du système de santé, pour prévoir que : « Aucun transfert de données à caractère personnel ne peut être réalisé en dehors de l'Union européenne ». Ces dispositions font ainsi désormais obstacle à ce que la Plateforme des données de santé puisse faire usage de la faculté qui lui reste ouverte dans le contrat conclu avec Microsoft d'autoriser un transfert de données à caractère personnel du système de santé. Il appartiendra à la Plateforme, qui a indiqué à l'audience, en accord avec son cocontractant, que les services énumérés par l'avenant du 3 septembre 2020 correspondaient à l'intégralité des services couverts par le contrat conclu avec Microsoft susceptibles de comporter le traitement de données de santé, sans que ce point puisse être vérifié au regard des documents constitutifs du contrat versés par ailleurs au contradictoire, de justifier, dans un délai de quinze jours à compter de la notification de la présente ordonnance, de la conclusion d'un nouvel avenant destiné à apporter cette précision.

14. Dans ces conditions, en l'état de l'instruction, il n'apparaît 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. Par suite, les requérants ne sont pas fondés à soutenir que, en raison de tels transferts, une atteinte grave et manifestement illégale serait portée au droit au respect de la vie privée, comprenant le droit à la protection des données personnelles.

En ce qui concerne le risque d'autres transferts de données personnelles :

15. Les requérants font valoir que, du fait de sa soumission au droit américain, la société Microsoft Corporation et, du fait de sa qualité de filiale d'une société de droit américain, la société Microsoft Ireland Operations Limited peuvent être l'objet de demandes d'accès à certaines données de santé par les autorités américaines, dans le cadre de programmes de surveillance fondés sur l'article 702 du FISA ou sur l'EO 12333, alors même que ces données sont hébergées sur le territoire de l'Union européenne et que les termes du contrat conclu entre la Plateforme des données de santé et Microsoft s'y opposeraient. En faisant application aux relations entre responsable du traitement et sous-traitant des critères appliqués par la Cour de justice dans son arrêt du 16 juillet 2020, il convient de vérifier le niveau de protection assuré lors du traitement des données en prenant en considération non seulement les stipulations contractuelles convenues entre le responsable du traitement et son sous-traitant, mais aussi, en cas de soumission de ce sous-traitant au droit d'un Etat tiers, les éléments pertinents du système juridique de celui-ci.

16. S'agissant des stipulations contractuelles convenues entre la Plateforme des données de santé et Microsoft, elles incluent une annexe 3 à l'addendum sur la protection des données pour les services en ligne Microsoft, par laquelle la société s'engage à respecter les conditions du règlement général sur la protection des données, notamment son article 28, en traitant les données à caractère personnel « conformément aux instructions documentées du client, y compris en ce qui concerne le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins que Microsoft ne soit tenue d'y procéder en vertu du droit de l'Union ou du droit de l'Etat membre auquel Microsoft est soumise ». Si

l'addendum sur la protection des données, auquel renvoie l'avenant conclu le 3 septembre 2020, prévoit également que « Microsoft ne divulguera pas les données traitées aux pouvoirs publics, sauf si elle y est tenue par la loi », il ne peut ainsi faire référence qu'au droit de l'Union européenne ou de l'un de ses Etats membres, ainsi qu'il conviendra de le préciser à l'occasion de la conclusion de l'avenant mentionné au point 13. En outre, la même annexe prévoit que Microsoft devra immédiatement informer la Plateforme si la société estime qu'une instruction constitue une violation du règlement général ou d'autres dispositions du droit de l'Union européenne ou d'un Etat membre relatives à la protection des données.

17. Toutefois, la Commission nationale de l'informatique et des libertés, dans les observations qu'elle a produites à la suite de la communication de la requête, estime, en l'état des informations dont elle dispose, que le risque d'une demande telle que celles mentionnées au point 15 ne peut être totalement écarté. En outre, il résulte de l'instruction que les mesures techniques mises en œuvre par Microsoft ou susceptibles de l'être à brève échéance n'écartent pas toute possibilité pour cette entreprise d'accéder aux données traitées sous la responsabilité de la Plateforme des données de santé, en dépit des précautions, limitant ce risque, qui entourent le chiffrement dont elles font l'objet et le stockage des clés de chiffrement utilisées. Il ne peut ainsi être totalement exclu, sur le plan technique, que Microsoft soit amenée à faire droit à une demande des autorités américaines fondée sur l'article 702 du FISA, ce qui méconnaîtrait alors les articles 28 et 48 du règlement général sur la protection des données, cités au point 5, qui interdisent qu'un sous-traitant transfère des données à caractère personnel vers un pays tiers si ce n'est sur instruction du responsable du traitement ou en vertu d'une obligation prévue par le droit de l'Union européenne ou d'un Etat membre, et que puisse être reconnue ou rendue exécutoire une décision d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel, sauf sous certaines conditions qui ne seraient en l'espèce pas remplies.

18. Il convient cependant de relever, en premier lieu, que la Cour de justice s'est seulement prononcée, dans son arrêt du 16 juillet 2020, sur les conditions dans lesquelles peuvent avoir lieu des transferts de données à caractère personnel vers les Etats-Unis et non sur celles dans lesquelles de telles données peuvent être traitées, sur le territoire de l'Union européenne, par des sociétés de droit américain ou leurs filiales en qualité de sous-traitants, voire de responsables de traitement. A fortiori, elle ne s'est pas prononcée sur les conséquences que pourraient avoir les constats opérés par son arrêt sur de tels traitements, alors même que, s'agissant des transferts de données à caractère personnel vers des pays tiers, son arrêt en mentionne la possibilité sur le fondement de l'article 49 du règlement général sur la protection des données, qui permet notamment les transferts nécessaires pour des motifs importants d'intérêt public reconnus par le droit de l'Union ou le droit de l'Etat membre auquel le responsable du traitement est soumis.

19. En deuxième lieu, les requérants n'invoquent pas de violation directe du règlement général sur la protection des données mais seulement le risque d'une telle violation, dans l'hypothèse où Microsoft ne serait pas en mesure de s'opposer à une demande d'accéder à certaines données formulée par les autorités américaines, si celles-ci y voyaient un intérêt au regard de l'objectif d'obtention d'informations en matière de renseignement extérieur poursuivi par les programmes de surveillance déjà mentionnés, alors au surplus que ces

données sont pseudonymisées par la Caisse nationale de l'assurance maladie, conformément à l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé et à la convention conclue les 14 et 15 juin 2020 entre la Plateforme des données de santé et la Caisse nationale, avant d'être transmises à la Plateforme et chiffrées au moyen des outils mis à sa disposition par Microsoft.

20. En troisième lieu, il existe un intérêt public important à permettre la poursuite de l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le SARS-CoV-2 et, à cette fin, de permettre le recours aux moyens techniques, sans équivalent à ce jour, dont dispose la Plateforme des données de santé par le biais du contrat passé avec Microsoft, sous réserve, pour chaque projet, ainsi qu'il découle de l'arrêté du 10 juillet 2020, que ce recours, et le stockage des données qu'il implique, soit une mesure 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 sa conduite et de l'absence de solution technique alternative satisfaisante permettant d'y procéder dans les délais utiles.

21. Eu égard à la sensibilité particulière des données de santé, les autorités publiques ont fait part de leur volonté d'adopter, dans les délais les plus brefs possibles, des mesures propres à éliminer tout risque, telles que le choix d'un nouveau sous-traitant, évoqué publiquement par le secrétaire d'Etat chargé de la transition numérique et des communications électroniques, ou le recours à un accord de licence, suggéré par la Commission nationale de l'informatique et des libertés dans ses observations. Dans l'intervalle, il appartient à la Plateforme des données de santé de continuer de rechercher, en vertu de l'article 28 du règlement général sur la protection des données, la mise en œuvre par Microsoft des mesures techniques et organisationnelles appropriées pour garantir au mieux la protection des droits des personnes concernées. A cet égard, la société doit d'ailleurs, en vertu de l'annexe 3 à l'addendum sur la protection des données mentionnée ci-dessus, mettre à sa disposition toutes les informations nécessaires pour démontrer le respect des obligations prévues à cet article 28 et permettre la réalisation d'audits. Il appartient en outre à la Commission nationale de l'informatique et des libertés, lorsqu'elle autorise, conformément aux articles 66 et 76 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, des projets appelés à traiter les données rassemblées par la Plateforme des données de santé, de vérifier qu'ils poursuivent une finalité d'intérêt public en lien avec l'épidémie de covid-19 et que le recours à la Plateforme remplit les conditions mentionnées au point 20.

22. En revanche, il n'apparaît pas, en l'état de l'instruction, que les mesures propres à éliminer tout risque de la nature de celui mentionné au point 19 et proportionnées à l'intérêt public mentionné au point 20 relèveraient des mesures de sauvegarde que le juge des référés, statuant sur le fondement des dispositions de l'article L. 521-2 du code de justice administrative, peut ordonner en cas d'atteinte grave et manifestement illégale portée de façon avérée par une personne morale de droit public à une liberté fondamentale et dans le très bref délai que ces dispositions prévoient.

Sur les conclusions subsidiaires et accessoires :

23. Si les requérants demandent au juge des référés, à titre subsidiaire, de solliciter la Commission nationale de l'informatique et des libertés, pour qu'elle se prononce notamment sur les implications que peut avoir, sur le traitement et la collecte des données au sein de la Plateforme des données de santé, l'invalidation de la décision d'exécution de la Commission du 12 juillet 2016 relative à l'adéquation de la protection assurée par le bouclier de protection des données Union européenne – Etats-Unis, les observations produites par cette autorité dans le cadre de la présente instance satisfont à cette demande, qui est ainsi devenue sans objet.

24. Les dispositions de l'article L. 761-1 du code de justice administrative font obstacle à ce qu'il soit fait droit aux conclusions des requérants présentées à ce titre.

ORDONNE:

Article 1er : La Plateforme des données de santé justifiera avoir conclu, dans un délai de quinze jours à compter de la notification de la présente décision, un nouvel avenant aux documents contractuels l'unissant à la société Microsoft Ireland Operations Limited pour préciser que la loi applicable dont il est fait mention dans l'avenant du 3 septembre 2020 est celle du droit de l'Union ou du droit de l'Etat membre auquel la société est soumise et que les modifications que cet avenant apporte à l'addendum sur la protection des données pour les services en ligne Microsoft s'appliquent à l'ensemble des services fournis par Microsoft susceptibles d'être utilisés pour le traitement de données à caractère personnel du système de santé. La Plateforme des données de santé en communiquera copie au secrétariat du contentieux du Conseil d'Etat.

Article 2 : Il n'y a pas lieu de statuer sur les conclusions de la requête de l'association le Conseil national du logiciel libre et des autres requérants en ce qu'elles tendent à l'adoption d'une mesure telle que celle mentionnée au point 13 et à la saisine de la Commission nationale de l'informatique et des libertés.

Article 3 : Eu égard au rappel fait au point 20 de la portée de l'arrêté du ministre des solidarités et de la santé du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé, le surplus des conclusions de la requête de l'association le Conseil national du logiciel libre et des autres requérants est rejeté.

Article 4 : La présente ordonnance sera notifiée à l'association le Conseil national du logiciel libre, premier dénommé, pour l'ensemble des requérants, au ministre des solidarités et de la santé et à la Plateforme des données de santé. Copie en sera adressée au Premier ministre, à la Commission nationale de l'informatique et des libertés et à la société Microsoft France.