CONSEIL D'ETAT
statuant
au contentieux

N° 450163

RÉPUBLIQUE FRANÇAISE

_____

ASSOCIATION INTERHOP et autres

_____

AU NOM DU PEUPLE FRANÇAIS

Ordonnance du 12 mars 2021

LE JUGE DES RÉFÉRÉS

Vu la procédure suivante :

Par une requête, deux mémoires complémentaires, un mémoire en réplique et un nouveau mémoire, enregistrés les 26 et 27 février, et les 1er, 5 et 7 mars 2021 au secrétariat du contentieux du Conseil d'Etat, l'association InterHop, l'association Constances, l'association Actions Traitement, l'association les Actupiennes, l'association Actup santé sud ouest, le syndicat de la Médecine générale (SMG), l'Union française pour une médecine libre (UFML), le Sndicat national des jeunes médecins généralistes (SNJMG), la Fédération des médecins de France (FMF), Mme A... D..., en son mandat de représentante des usagers du Conseil de surveillance de l'AP-HP, M. B... C..., la Fédération SUD santé sociaux et la Ligue des droits de l'Homme demandent au juge des référés du Conseil d'Etat, statuant sur le fondement de l'article L. 521-2 du code de justice administrative :

1°) d'ordonner la suspension du partenariat avec la société Doctolib en ce qu'il repose sur un hébergement des données de santé auprès d'une société américaine, le rendant incompatible avec le règlement général sur la protection des données (RGPD) ;

2°) d'ordonner au ministre de la santé et des solidarités d'avoir recours à d'autres solutions de gestion de la prise de rendez-vous de la campagne de vaccination contre la Covid-19, respectueuses des exigences au droit à la protection des données ;

3°) à titre subsidiaire, de solliciter pour avis la Commission nationale de l'informatique et des libertés (CNIL) aux fins de statuer sur les implications du recours au partenariat avec la société Doctolib pour la gestion de la prise de rendez-vous de la campagne de vaccination contre la Covid-19, en ce qu'elle repose sur un hébergement des données de santé auprès d'une société américaine, la rendant incompatible avec le RGPD ;

4°) d'ordonner 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 les choix de partenariat pour la gestion des prises de rendez-vous dans le cadre de la campagne de vaccination contre la Covid-19 ;

5°) 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 à agir ;
- la condition d'urgence est satisfaite eu égard à la situation d'état d'urgence sanitaire prorogé récemment par la loi du 15 février 2021, au fait que les données de santé de millions de personnes risquent de ne pas bénéficier d'un régime de protection adéquate compte tenu du caractère dominant de la solution Doctolib dans l'offre de prise de rendez-vous en ligne, au caractère particulièrement sensible des données en cause, à l'impossibilité pour l'Etat de garantir la protection des données de santé dans le cadre du contrat conclu entre la société Doctolib et la société Amazon Web Services et des atteintes au droit à la protection des données rendues possibles par le droit américain et ses effets extraterritoriaux ;
- la mesure contestée porte une atteinte grave et manifestement illégale à plusieurs libertés fondamentales ;
- elle porte une atteinte grave au droit au respect de la vie privée et au droit à la protection des données personnelles dès lors, d'une part, que les données traitées par la plateforme Doctolib dans le cadre de la gestion de la politique de vaccination contre la Covid-19 sont susceptibles de donner une indication précise sur l'état de santé de la personne et constituent des informations directement identifiantes et, d'autre part, que les potentielles demandes d'accès aux données personnelles par les autorités américaines ne peuvent faire l'objet d'aucune opposition concrète par les sociétés américaines, que ces accès sont massifs, indiscriminés et non minimisés, et qu'elles ne peuvent faire l'objet de contrôles ou de droit d'opposition auprès d'autorités indépendantes ;
- elle porte une atteinte manifestement illégale au droit à la protection des données dès lors que l'hébergement des données personnelles recueillies par la plateforme Doctolib au sein des serveurs appartenant à une société américaine soumise au droit américain est incompatible avec le RGDP en ce que l'état de la législation américaine ne permet pas d'assurer un niveau de protection approprié des données personnelles au regard de ce règlement ;
- elle méconnaît les dispositions du RGPD eu égard, d'une part, à l'éventualité d'un transfert vers les Etats-Unis des données collectées par Doctolib par le biais du sous-traitant hébergeant ces données Amazon Web Services et, d'autre part, même en l'absence de transfert de données, au risque de demande d'accès par les autorités américaines auprès de la société Amazon Web Services ;
- elle n'est ni nécessaire, ni proportionnée, ni adaptée dès lors que d'autres solutions numériques alternatives, reposant sur un hébergement des données réalisé par des sociétés de droit français, existent.

Par un mémoire en défense, enregistré le 5 mars 2021, le ministre des solidarités et de la santé conclut au rejet de la requête. Il soutient qu'il n'est porté aucune atteinte grave et manifestement illégale aux libertés fondamentales invoquées et qu'il existe un intérêt public visant à permettre la poursuite de l'utilisation des services de gestion des rendez-vous de vaccination de Doctolib pour les besoins de la gestion de l'urgence sanitaire et de la lutte contre la pandémie de SARS-CoV-2.

Par un mémoire en défense et un nouveau mémoire, enregistrés les 5 et 7 mars 2021, la société Doctolib conclut au rejet de la requête. Elle soutient qu'il n'est porté aucune atteinte grave et manifestement illégale au droit à la protection des données personnelles.

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 ;
- le code de justice administrative ;

Après avoir convoqué à une audience publique, d'une part, l'association Interhop et les autres requérants et, d'autre part, le ministre des solidarités et de la santé et la société Doctolib ;

Ont été entendus lors de l'audience publique du 8 mars 2021, à 10 heures 30 :

- les représentants des requérants ;

- Me Piwnica, avocat au Conseil d'Etat et à la Cour de cassation, avocat de la société Doctolib ;

- les représentants de la société Doctolib ;

- les représentants du ministre des solidarités et de la santé ;

à l'issue de laquelle le juge des référés a clos l'instruction.

Vu la note en délibéré, enregistrée le 11 mars 2021, présentée par l'association InterHop et autres ;

Considérant ce qui suit :

1. Aux termes de l'article L. 521-2 du code de justice : « *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* ».

2. Dans le cadre de la campagne de vaccination contre la covid-19, le ministère des solidarités et de la Santé a confié la gestion des rendez-vous de vaccination sur internet à différents prestataires dont la société Doctolib. L'association InterHop et les autres requérants demandent au juge des référés, statuant sur le fondement de l'article L. 521-2 du code de justice administrative, de suspendre le partenariat avec la société Doctolib en ce qu'il repose sur un hébergement des données de santé auprès d'une société américaine le rendant incompatible avec le 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.

Sur le cadre juridique :

3. 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 (...)* ».

4. 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 (...) ».

5. Par un arrêt de grande chambre du 16 juillet 2020, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian 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.

6. 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.

Sur la demande en référé :

7. Pour les besoins de l'hébergement de ses données, la société Doctolib a recours aux prestations de la société de droit luxembourgeois AWS Sarl, filiale de la société américaine Amazon Web Services Inc. L'association InterHop 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. Si la société AWS est certifiée « hébergeur de données de santé » en application de l'article L. 1111-8 du code de la santé publique, que les données traitées par la société AWS sont hébergées dans des centres de données situés en France et en Allemagne et que le contrat conclu entre la société Doctolib et AWS ne prévoit pas le transfert de données pour des raisons techniques aux Etats-Unis, l'association InterHop et les autres requérants font valoir que, du fait de sa qualité de filiale d'une société de droit américain, la société AWS peut faire 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. 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.

8. Il résulte de l'instruction que, pour accélérer la campagne de vaccination contre la Covid-19, la gestion de prise de rendez-vous de vaccination est assurée par trois sociétés différentes, dont la société Doctolib. Les données litigieuses comprennent les données d'identification des personnes et les données relatives aux rendez-vous mais pas de données de santé sur les éventuels motifs médicaux d'éligibilité à la vaccination, les personnes intéressées se bornant, au moment de la prise de rendez-vous, à certifier sur l'honneur qu'elles entrent dans la priorité vaccinale, qui est susceptible de concerner des adultes de tous âges sans motif médical particulier. Ces données sont supprimées au plus tard à l'issue d'un délai de trois mois à compter de la date de rendez-vous, chaque personne concernée ayant créé un compte sur la plateforme pour les besoins de la vaccination pouvant le supprimer directement en ligne. La société Doctolib et la société AWS ont conclu un addendum complémentaire sur le traitement des données instaurant une procédure précise en cas de demandes d'accès par une autorité publique aux données traitées pour le compte de Doctolib prévoyant notamment la contestation de toute demande générale ou ne respectant pas la règlementation européenne. La société Doctolib a également mis en place un dispositif de sécurisation des données hébergées par la société AWS par le biais d'une procédure de chiffrement reposant sur un tiers de confiance situé en France afin d'empêcher la lecture des données par des tiers. Eu égard à ces garanties et aux données concernées, le niveau de protection des données de prise de rendez-vous dans le cadre de la campagne de vaccination contre la Covid-19 ne peut être regardé comme manifestement insuffisant au regard du risque de violation du règlement général de protection des données invoqué par les requérants. Si l'association requérante a également invoqué des risques liés au recours à d'autres prestataires qu'AWS, il ne résulte pas de l'instruction que ces prestataires interviendraient dans l'hébergement des données en litige. Ainsi, et sans qu'il soit besoin de

saisir la Commission nationale de l'informatique et des libertés d'une demande d'avis, il n'apparaît pas, en l'état de l'instruction, que la décision du ministre des solidarités et de la santé de confier à la société Doctolib, parmi d'autres voies possibles de réservation de rendez-vous, la gestion de rendez-vous de vaccination contre la Covid-19 porte une atteinte grave et manifestement illégale au droit au respect de la vie privée et au droit à la protection des données personnelles.

9. Il résulte de ce qui précède que la requête de l'association InterHop et autres doit être rejetée.

10. Les dispositions de l'article L. 761-1 du code de justice administrative font obstacle à ce qu'une somme soit mise à la charge de l'Etat, qui n'est pas, dans la présente instance, la partie perdante.

O R D O N N E :

Article 1er : La requête de l'association InterHop et autres est rejetée.

Article 2 : La présente ordonnance sera notifiée à l'association InterHop, première dénommée, pour l'ensemble des requérants ainsi qu'au ministre des solidarités et de la santé et à la société Doctolib.