CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Vos réf. : 444937 – CONSEIL NATIONAL DU LOGICIEL LIBRE c/ MINISTERE DES SOLIDARITES ET DE LA SANTE

CONSEIL D'ÉTAT

SECTION DU CONTENTIEUX

REFERE L. 521-2 CJA

MEMOIRE EN OBSERVATIONS

Pour :

La Commission nationale de l'informatique et des libertés (CNIL) dont le siège est 3 place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07, représentée par sa Présidente.

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif. Les personnes concernées peuvent exercer leurs droits informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

FAITS ET PROCÉDURE

La Plateforme des données de santé (PDS), également appelée « *Health Data Hub* », a été créée par la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (OTSS) et par arrêté du 29 novembre 2019 pour faciliter le partage des données de santé afin de favoriser la recherche. Dans ce cadre, la PDS a vocation à centraliser l'ensemble des données du système national des données de santé[1], regroupant les données de santé de l'ensemble de la population soignée en France. Elle est « responsable du traitement » au sens du RGPD.

La PDS a fait le choix de recourir aux services de Microsoft, société dont le siège est situé aux Etats-Unis, en tant que « sous-traitant » au sens du RGPD, afin d'héberger informatiquement les données de santé actuellement en sa possession (services AZURE dits de *Cloud computing*).

La société Microsoft avait adhéré au *Privacy Shield*, instrument encadrant les transferts de données à caractère personnel vers les Etats-Unis ayant fait l'objet de la décision d'adéquation 2016/1250, par la Commission européenne. Les transferts de données à caractère personnel opérés dans ce cadre sont en outre encadrés par l'intermédiaire de clauses contractuelles types annexées au contrat.

Le 5 octobre 2020, la Commission nationale de l'informatique et des libertés a été rendue destinataire, pour production d'observations, de la requête en référé déposée par le Conseil National du Logiciel Libre (« CNLL ») et autres sur le fondement de l'article L. 521-2 du Code de justice administrative, enregistrée au greffe de la Section du Contentieux du Conseil d'Etat sous le n° 444937.

La requête en référé met principalement en cause la contrariété au RGPD des transferts potentiels des données en cause vers les Etats-Unis, à l'initiative de Microsoft ou d'autorités publiques des Etats-Unis, notamment des services de renseignement.

Le CNLL et autres sollicitent ainsi que le traitement et la centralisation des données en lien avec l'épidémie de Covid-19 sur la Plateforme des données de santé (« *Health Data Hub* ») soient suspendus aux fins de mettre un terme à une atteinte grave et manifestement illégale au droit à la vie privée et à la protection des données personnelles, à ce qu'il soit enjoint toutes les 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*, à titre subsidiaire, que la CNIL soit sollicitée aux fins notamment 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.

---

[1] Article L. 1461-1 du CSP : Notamment, l'ensemble des données liées à l'hospitalisation issues du programme de médicalisation des systèmes d'Information ou PMSI, les données de l'assurance maladie obligatoire ou SNIIRAM, les données relatives au statut vital et aux causes médicales de décès ou CépiDC, les données des maisons départementales des personnes handicapées ou MDPH, des données provenant des organismes d'assurance maladie complémentaires, toute donnée recueillie ou produite à l'occasion des activités de prévention, de diagnostic ou de soins, c'est-à-dire notamment tous les dossiers médicaux constitués par un établissement, un professionnel de santé libéral, etc., des données relatives à la perte d'autonomie, des données des enquêtes dans le domaine de la santé, les données recueillies lors des visites médicales et de dépistage obligatoires dans les écoles, les données issues des centres de protection maternelle et infantile ou PMI, des données collectées dans le cadre de la médecine du travail.

L'affaire telle qu'elle se présente appelle, de la part de la CNIL et sans qu'elle n'entende se positionner sur chacun des arguments soulevés par la requête, les observations suivantes.

OBSERVATIONS

1. La position de la CNIL avant l'intervention de l'arrêt de la CJUE du 16 juillet 2020 dit *Schrems II* (CJUE 16 juill. 2020, DPC c. Facebook Ireland Ltd et M. Schrems, aff. C-311/18)

La CNIL a été saisie en avril dernier de la question de l'utilisation de la PDS dans le cadre de la crise sanitaire de la Covid-19[2]. A cette occasion, si elle avait reconnu la qualité des mesures de sécurité protégeant les données à caractère personnel, elle s'était inquiétée du fait que le choix de Microsoft pour l'hébergement des données impliquait, malgré les précautions prises par la PDS, que des transferts de données vers les Etats-Unis soient réalisés. A l'époque, les transferts en question restaient couverts par la décision d'adéquation 2016/1250 du *Privacy Shield*.

En vertu de la jurisprudence de la CJUE (CJUE, 6 octobre 2015, C-362/14, dit *Schrems I*), il appartenait à la CNIL et aux autorités françaises de respecter cette décision tant qu'elle n'avait pas été invalidée par la CJUE, une procédure étant alors en cours. En outre, les transferts étaient encadrés par des clauses contractuelles types. Malgré cela, la CNIL a rappelé dans son avis du 20 avril 2020 que le Comité européen de la protection des données (CEPD) avait exprimé à plusieurs reprises ses inquiétudes concernant l'accès particulièrement large par les autorités des Etats-Unis aux données à caractère personnel transférées aux Etats-Unis ou traitées sur des plateformes techniques opérées par des sociétés étatsuniennes.

La CNIL, sans estimer que la situation serait illégale et aurait justifié un avis défavorable, a donc appelé le gouvernement à une extrême vigilance s'agissant des conditions de conservation et des modalités d'accès aux données, et a recommandé que, à plus long terme, l'hébergement et les services de gestion de la PDS puissent être « *réservés à des entités relevant exclusivement des juridictions de l'Union européenne* ». La CNIL avait d'ailleurs reçu des assurances sur le fait que les services de l'Etat et de la PDS travaillaient à la réversibilité des travaux de constitution du HDH, destinée à rendre possible un changement d'hébergeur après la montée en puissance du système en cours de déploiement.

[2] Délibération n° 2020-044 du 20 avril 2020 portant avis sur un projet d'arrêté 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

2. Les conséquences de l'arrêt de la CJUE du 16 juillet 2020 dit *Schrems II* (CJUE 16 juill. 2020, DPC c. Facebook Ireland Ltd et M. Schrems, aff. C-311/18)

L'arrêt du 16 juillet 2020 a radicalement changé la situation du recours à des solutions d'hébergement fournies par des acteurs étatsuniens, de façon générale et en particulier pour les entrepôts de données de santé.

La CJUE, dans son arrêt C-311/18 du 16 juillet 2020[3] dit ***Schrems II***, a estimé :

- D'une part, que les exigences de la section 702 du *Foreign Intelligence Surveillance Act* (FISA) et *l'Executive Order 12333* du droit étatsunien, qui instituent des programmes permettant l'accès des autorités publiques étatsuniennes à des fins de sécurité nationale aux données personnelles transférées de l'UE vers les États-Unis, de façon particulièrement large et sans ciblage, entraînent des limitations de la protection des données personnelles qui ne sont pas circonscrites de manière à satisfaire à des exigences essentiellement équivalentes à celles requises par le droit de l'UE ;
- D'autre part, que cette législation n'accorde pas aux personnes concernées des droits de recours devant les juridictions contre les autorités étatsuniennes (la CJUE souligne que ces programmes ne prévoient aucune limitation du pouvoir conféré aux autorités étatsuniennes, ni l'existence de garanties pour les personnes potentiellement ciblées non étatsuniennes).

En ce sens, la Cour a estimé que le droit étatsunien, du fait de la section 702 du FISA et l'*Executive Order 12333*, n'assure pas un niveau de protection essentiellement équivalent au droit européen relatif à la protection des données à caractère personnel.

Ainsi, du fait de l'ampleur de l'atteinte portée aux droits fondamentaux des personnes dont les données sont transférées vers ce pays tiers, **la CJUE a, en premier lieu, déclaré invalide la décision d'adéquation 2016/1250 du *Privacy Shield*.** La Cour a par ailleurs relevé que la législation précitée s'applique à tout transfert vers les États-Unis par voie électronique qui relève du champ d'application de cette législation, et ce quel que soit l'outil de transfert utilisé[4].

Si la Cour n'a pas, en second lieu, invalidé les clauses contractuelles types élaborées par la Commission européenne, elle a néanmoins indiqué que, pour les utiliser valablement, il appartient au responsable de traitement d'évaluer si le pays tiers dans lequel les données à caractère personnel seront transférées assure un niveau de protection essentiellement équivalent à celui de l'Union européenne. Si ce n'est pas le cas, il devra mettre en place des mesures additionnelles pour assurer le niveau de protection des données requis, ou notifier à l'autorité de protection des données compétente son intention de continuer à transférer des données sans ces garanties.

---

[3] CJUE, C-311/18, 16 juillet 2020.

[4] L'article 702 du FISA s'applique à tous les « *fournisseurs de services de communication électronique* » *(voir la définition figurant à l'article 50 USC § 1881(b)(4)), tandis que l'Executive Order 12333 organise la surveillance électronique, qui est définie comme « l'acquisition d'une communication non publique par des moyens électroniques sans le consentement d'une personne qui est partie à une communication électronique ou, dans le cas d'une communication non électronique, sans le consentement d'une personne qui est visiblement présente sur le lieu de la communication, à l'exclusion de l'utilisation d'un équipement radiogoniométrique uniquement pour déterminer l'emplacement d'un émetteur* » (3.4 ; b).

Dans ces conditions, si des transferts sont effectivement envisagés à destination des Etats-Unis, notamment sur la base de clauses contractuelles types, **des mesures additionnelles doivent être prévues par le responsable de traitement.** Elles apparaissent particulièrement difficiles à apporter. Deux situations sont à distinguer dans la mesure où les programmes de surveillance régis par le FISA et l'EO12333 ne couvrent pas l'ensemble des organismes états-uniens mais seulement certains d'entre eux, notamment les fournisseurs de service de communication électronique.

- Lorsque le destinataire des données (non chiffrées ou déchiffrables par lui) est directement soumis à la surveillance et aux demandes des autorités de renseignements régies par le FISA et l'EO12333, la mise en œuvre de garanties additionnelles protégeant cette surveillance apparaît particulièrement délicate à mettre en œuvre. C'est la situation dans laquelle se trouve Microsoft aux Etats-Unis.

- Lorsque le destinataire n'est pas directement dans le champ de la surveillance instituée par les deux normes jugées incompatibles avec le standard minimum de protection exigé par le RGPD et l'article 8 de la Charte des droits fondamentaux de l'Union européenne (par exemple une société industrielle aux Etats-Unis), les données sont, malgré cela, généralement soumises aux programmes de surveillance en question lors de leur transit vers le destinataire. En effet, ce transit utilise des canaux de communication qui sont soumis aux programmes de surveillance examinés par la CJUE. Des mesures additionnelles de chiffrement sont, en revanche, probablement de nature à permettre, sous certaines conditions, le maintien d'un niveau de protection suffisant des données. Le CEPD (Comité européen de protection des données) travaille à préciser ces conditions. Il faut en outre, en tout état de cause, que le destinataire apporte également des garanties suffisantes sur le traitement qu'il fera des données, notamment lors de leur transfert entre ses différents sites potentiels par le biais de canaux soumis à ces législations et prenne en considération les autres dispositions de la législation étatsunienne.

Enfin, en troisième lieu, 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 renseignement étatsuniens, ainsi que le mentionne la requête (voir ci-après).

3. Sur l'existence de transferts de données de la PDS vers les Etats-Unis à l'initiative de la PDS, de ses utilisateurs ou de Microsoft.

Lorsqu'elle a examiné la situation en avril, la Commission a conclu à l'existence de transferts résiduels de données de santé vers les Etats-Unis, ce qui, s'agissant d'une plateforme appelée à centraliser une quantité considérable de données, a justifié un appel de la Commission à une extrême vigilance et à des efforts supplémentaires pour supprimer ces transferts.

En effet, s'il était établi que les données au repos étaient stockées en Europe et si l'utilisation des données par les chercheurs, pour leur calcul, ne doit pas, selon les indications dont dispose la Commission, donner lieu à des transferts, ceux-ci restaient possibles dans le cadre des

diverses opérations d'administration des systèmes d'information que Microsoft sera amené à réaliser. Il faut relever que les clés de chiffrement sont détenues par Microsoft.

La PDS a choisi de recourir à un dispositif mis en place par Microsoft qui institue un système de contrôle des accès des administrateurs de Microsoft aux données, à la main de la PDS, dénommé « *Customer Lockbox* ». Ce système constitue une garantie de limitation des transferts, dans la mesure où la PDS assure qu'elle refusera tout transfert. Cependant, ce dispositif, encadré par certains éléments du contrat, comporte des exceptions au principe de contrôle a priori de la PDS, « *dans le cadre de scénarios inattendus ou imprévisibles correspondant à des catastrophes ou en cas d'accès fortuit aux données par un ingénieur Microsoft* ».

La pseudonymisation des données personnelles est par ailleurs souvent avancée comme une autre garantie permettant de limiter les détournements de données. Si cette mesure permet effectivement de limiter les risques, la CNIL estime qu'elle ne permet pas de lever tout risque d'identification des personnes. En effet, les données détenues par la PDS sont des données de santé très détaillées et donc très fortement identifiantes. Elles le seront de plus en plus à mesure que cette nouvelle infrastructure montera en puissance. Même si les noms et prénoms n'y figurent pas, il sera possible de ré-identifier une part, probablement substantielle, des personnes en croisant les données de santé avec d'autres sources de données.

Cette analyse a justifié la position qu'a prise la Commission dans son avis du 20 avril dernier.

A la suite de cet avis, la PDS a conclu avec Microsoft un nouvel avenant, communiqué à la Commission et qui limite encore davantage les transferts. En effet, l'avenant prévoit que les données de la PDS seront entreposées (au repos) dans la zone géographique déterminée par la PDS, et confirme la possibilité pour la PDS de déterminer également la zone dans laquelle les données seront traitées, y compris pour la résolution d'incidents. Ce paragraphe de l'avenant mentionne une liste limitative de services spécifiques. Si cette liste devait couvrir l'ensemble des services auxquels recourt la PDS pour la mise en place du *health data hub*, la signature de cet avenant amènerait à conclure qu'il n'y a plus aucune possibilité de transferts de données vers les Etats-Unis qui soit possible à l'initiative de Microsoft, sous réserve également que la PDS s'engage à ne jamais les autoriser. Cependant, la CNIL a interrogé la PDS sur le fait qu'il n'est pas sûr, à la lecture des documents, que l'avenant couvre l'ensemble des services en ligne Azure souscrits par le contrat principal. Elle souhaite également s'assurer que cet avenant l'emporte sur les documents contractuels relatifs à la « *Custormer lockbox* » qui, eux, prévoient des exceptions, comme cela a été indiqué. Ces points sont en cours d'instruction. Il n'est donc pas possible de conclure de manière certaine, à ce stade de l'instruction, à l'absence de transfert de données personnelles, notamment relatives à la santé. Il est renvoyé sur ces points aux précisions qui seront apportées par la PDS.

Si des transferts devaient subsister, ils seraient donc illégaux à la suite de l'intervention de l'arrêt *Schrems II*.

4. Indépendamment de l'existence de transferts à l'initiative de la plateforme ou de Microsoft, sur la possibilité de transferts à la demande des services de renseignement des Etats-Unis.

Indépendamment de cette question des transferts opérés par Microsoft dans le cadre de l'administration de la solution technologique offerte à la PDS, se pose la question, soulevée par

la requête, des transferts opérés par Microsoft à la demande des services de renseignement des Etats-Unis.

De ce point de vue, la CNIL s'est réinterrogée depuis l'intervention de l'arrêt *Schrems II* sur le point de savoir si la législation américaine contraint légalement Microsoft à communiquer aux services de renseignement des données entreposées et traitées uniquement hors du territoire étatsunien, pour lesquelles il détient les clés de chiffrement. La CNIL relève de ce point de vue que l'avenant signé récemment par la PDS, qui limite fortement les transferts à l'initiative de Microsoft, stipule également que Microsoft « *ne divulguera ni ne donnera accès à une quelconque Donnée Traitée aux autorités, sauf si la loi l'exige* » (soulignement ajouté).

Si on laisse de côté le *Clarifying Lawful Overseas Use of Data Act* ou « *CLOUD Act* », qui n'a pas été examiné dans l'arrêt *Schrems II* (mais dont le caractère extraterritorial ne fait aucun doute), la CNIL estime, en l'état des informations dont elle dispose, que les législations FISA et EO 123333 s'appliquent aux données stockées en dehors du territoire des Etats-Unis.

S'agissant de la loi « *Foreign Intelligence Surveillance Act* » FISA, Section 702

La section FISA 702 concerne le « *ciblage de personnes dont on peut raisonnablement penser qu'elles se trouvent en dehors des États-Unis pour obtenir des informations de renseignements étrangers* » et s'applique aux « *fournisseurs de services de communication électronique*».[5]

La section FISA 702, paragraphe (h), dispose que les autorités étatsuniennes peuvent ordonner à un fournisseur de services de communication électronique de « *fournir immédiatement au gouvernement toutes les informations, installations ou assistance nécessaires pour réaliser l'acquisition d'une manière qui protégera le secret de l'acquisition et produira un minimum d'interférence avec les services que ce fournisseur de services de communication électronique fournit à la cible de l'acquisition* ». Cette disposition confirme l'absence de notification aux personnes ou entreprises concernées par les éventuelles demandes d'accès.

En 2016, le G29 avait considéré que la section 702 FISA « *vise les fournisseurs de services de communications électroniques établis aux États-Unis pour la collecte d'informations de renseignement étranger sur des personnes situées en dehors des États-Unis. Elle inclut notamment* « les informations relatives à une puissance étrangère ou à un territoire étranger qui se rapportent à la conduite des affaires étrangères des États-Unis », *ce qui soulève une certaine incertitude quant au type d'informations qui peuvent être recueillies en pratique* ».

Contrairement au *Cloud Act*, la section 702 FISA n'apporte pas de précision explicite sur la portée extraterritoriale des ordres à produire mais ne restreint pas non plus ces demandes aux seules données stockées sur le territoire étatsunien. Le champ d'application matériel de ce texte, portant sur les informations de renseignements étrangers (« *foreign intelligence information* ») et concernant des personnes dont on peut raisonnablement penser qu'elles se trouvent en dehors

[5] *y compris « (A) une entreprise de télécommunications, au sens de la section 3 du Communications Act de 1934 (47 U.S.C. 153) ; (B) un fournisseur de services de communication électronique, tel que ce terme est défini à la section 2510 du titre 18 du US Code ; "(C) un fournisseur de services informatiques à distance, tel que ce terme est défini à la section 2711 du titre 18 du US Code ; (D) tout autre fournisseur de services de communication qui a accès à des communications électroniques ou filaires, soit au moment où ces communications sont transmises, soit au moment où ces communications sont stockées ; ou (E) un dirigeant, un employé ou un agent d'une entité décrite aux sous-paragraphes (A), (B), (C) ou (D) ».*

des États-Unis, implique la possibilité d'un accès à ces informations en dehors du territoire étatsunien. **Les autorités étatsuniennes confirment elles-mêmes l'existence de demandes concernant des données stockées sur le territoire de l'Union**, en particulier dans le récent Livre Blanc sur les suites de l'arrêt *Schrems II* publié en septembre 2020 conjointement par le Département du Commerce, le Département de la Justice, et le Bureau du Directeur du Renseignement (ODNI) qui fait référence aux « *entreprises qui transfèrent des données depuis l'UE et qui ont reçu des ordres autorisés par la FISA 702 exigeant la divulgation de données aux agences de renseignement américaines à des fins de renseignements étrangers* » (soulignement ajouté).

S'agissant de *l'Executive Order 12 333 :*

Ce décret présidentiel fonde principalement les techniques d'interceptions à des fins de renseignement sur les signaux («signal intelligence») et donc en particulier les techniques de collecte et filtrage sur les données en transit, vers ou en dehors des Etats-Unis (câbles sous-marins, communications satellitaires, etc…). En 2016, le G29 avait considéré que « *le champ d'application de l'EO12333 est large ; en principe, toute collecte de données de renseignements étrangers peut avoir lieu à la discrétion du président des États-Unis sur la base du décret, mais on a fait valoir que depuis l'introduction de la FISA,* ***l'EO12333 ne peut être utilisé que pour la collecte de données en dehors du territoire américain.***[6] *Le G29 note que l'EO12333 ne fournit pas beaucoup de détails sur sa portée géographique, sur la mesure dans laquelle les données peuvent être collectées, conservées ou diffusées, ni sur la nature des infractions susceptibles de donner lieu à une surveillance ou sur le type d'informations qui peuvent être collectées ou utilisées* ».

A titre principal, ce décret ne concerne donc pas les demandes adressées directement à des opérateurs soumis au droit américain, les services de renseignement procédant eux-mêmes aux interceptions. Le décret pourrait toutefois fonder **d'autres techniques de renseignement et d'interceptions de données, principalement en dehors du territoire étatsunien, sans exclure la possibilité de demandes d'assistance à des entités soumises au droit américain.**

La partie 2 de l'*Executive Order* 12333, relative à la conduite des activités de renseignement, précise en effet que le décret vise à « *améliorer les techniques de collecte humaine et technique, en particulier celles entreprises à l'étranger, et l'acquisition de renseignements étrangers importants* » (EO 12333, 2.2).7 L'EO 12333 couvre un champ très large d' « informations » pouvant être obtenus par les services de renseignement, qui incluent les « *informations constituant des renseignements étrangers ou du contre-espionnage, y compris de telles*

---

[6] Gras ajouté.

[7] Le décret dispose également : « *2.2 Purpose. This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency* ».

informations concernant des sociétés ou d'autres organisations commerciales. » (EO 12333, 2.3).

Contrairement à la section 702 FISA, le décret reste certes vague sur la forme que peuvent prendre les acquisitions et interceptions. Au regard des informations dont dispose la CNIL, il n'est pas exclu que cette acquisition puisse également se faire par des demandes d'assistance ou d'accès adressées aux fournisseurs de services.

****

En conclusion sur ce point, en l'état de ses instructions, la CNIL estime donc que, même dans le cas où l'absence de transferts de données personnelles en dehors de l'UE à des fins de fourniture du service serait confirmée, la société Microsoft peut être soumise, sur le fondement du FISA, voire peut-être de l'E0 123333, à des injonctions des services de renseignement l'obligeant à leur transférer des données stockées et traitées sur le territoire de l'Union européenne.

5. Sur l'illégalité qui en résulte pour le HDH et les entrepôts de données de santé hébergés par des acteurs soumis au droit états-unien.

La CNIL estime que les demandes des autorités états-uniennes, émises en vertu de la section 702 FISA ou du décret EO 12333, et adressées à Microsoft pour des traitements soumis au RGPD, devraient être considérées comme des **divulgations non autorisées par le droit de l'Union, en application de l'article 48 du RGPD**[8]. En effet, d'une part, ces demandes interviennent en dehors de tout accord international ou traité d'entraide judiciaire.[9] D'autre part, ces demandes ne peuvent se fonder sur aucun autre cas prévu par le chapitre V du RGPD, sous réserve de ce qui sera dit plus bas sur les dérogations de l'article 49, dans la mesure où la cour a jugé que les programmes de surveillance établis par ces normes, ainsi que l'absence de recours juridictionnel, rendaient ces transferts structurellement incompatibles avec le standard de protection minimale.

La Commission n'est pas sans ignorer que cette situation, induite par l'arrêt *Schrems II*, dépasse largement le cadre du seul HDH en cause dans la requête. **Elle réserve son appréciation des conséquences qu'il convient d'en tirer dans d'autres secteurs et pour d'autres données présentant une moindre sensibilité**. S'agissant des données de santé, elle souligne cependant qu'il existe, à sa connaissance, de nombreux entrepôts de données de santé, dépendant d'établissements hospitaliers ou d'autres responsables de traitement, qui sont hébergés par sociétés étatsuniennes et qui sont donc placés dans la même situation que le HDH, voire autorisent plus largement les transferts vers les Etats-Unis à la main du sous-traitant, notamment

---

[8] *Article 48 :* Transferts ou divulgations non autorisés par le droit de l'Union : « *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* ».

[9] Un tel accord devrait en outre être conforme à l'article 8 de la Charte des droits de l'Union européenne, ce qui apparaît délicat à la lecture des motifs de l'arrêt *Schrems II*, en l'absence de garanties supplémentaires consenties par les Etats-Unis.

pour les opérations d'administration. Par conséquent, la poursuite des autorisations de traitement de ces données, notamment dans le cadre de recherches scientifiques, apparait problématique du fait de l'intervention de l'arrêt *Schrems II*.

6. Sur l'obligation qui en résulte de modifier les conditions d'hébergement des données de santé, notamment au sein de la PDS, et la possibilité de ménager une période transitoire.

La Commission en tire pour conséquence que le souhait qu'elle avait émis dans son avis du 20 avril 2020 repose désormais sur une obligation légale, l'arrêt *Schrems II* devant conduire selon elle, pour le cas des données de santé et en particulier dans la perspective de leur centralisation au sein de la PDS, à soustraire ces données à la possibilité d'une communication aux services de renseignement sur le fondement du FISA , voire de l'EO123333.

Dans la mesure où cette conclusion ne résulte pas directement de l'arrêt *Schrems II*, qui concernait les transferts, mais de l'application de ses motifs à des demandes de communication de données non encore transférées aux services de renseignements états-uniens, **la Commission souligne qu'elle fonde sa position sur les particularités des données de santé et n'émet d'opinion que sur ce seul cas.**

Cette situation doit conduire selon elle à modifier les conditions d'hébergement de la PDS, ainsi que celles des autres entrepôts de données de santé qui sont hébergés par des sociétés soumises au droit étatsunien. La solution la plus effective consiste à confier l'hébergement de ces données à des sociétés non soumises au droit étatsunien, sans préjudice du respect de la législation sur les contrats et sur les marchés publics. La CNIL souligne qu'il ne suffit pas que l'hébergeur ait son siège social hors des Etats-Unis pour ne pas être soumis en partie au droit étatsunien, s'il exerce une activité dans ce pays. Il revient dans ce cas à l'hébergeur de montrer que des mesures organisationnelles appropriées lui permettent d'assurer le niveau de protection requis. La filialisation des activités déployées aux Etats-Unis constitue l'une des pistes avancées par les acteurs. La CNIL étudie cette question en lien avec ses homologues.

Il est également peut-être possible de mettre en place un dispositif contractuel par lequel la société américaine met en place un accord de licence avec une société européenne qui a seule la possibilité d'agir sur les données déchiffrées, et qui bénéficie des services et de l'expertise de la société américaine, sans que celle-ci n'ait jamais un accès aux données. Un tel montage, qui peut dépendre également de la nature des services requis, devrait être assorti de garanties particulièrement fortes. Sa faisabilité est actuellement étudiée en lien avec ses homologues par la CNIL, dans le cadre des travaux sur les « mesures additionnelles » envisagées par l'arrêt *Schrems II* pour les clauses contractuelles types.

La CNIL estime que le changement de la solution d'hébergement du HDH et des autres entrepôts de santé hébergés par les sociétés soumises au droit étasunien devrait intervenir dans un délai aussi bref que possible. Une période de transition est nécessaire, afin d'assurer ces changements sans perte de données ou de technologie et sans compromettre les usages qui sont aujourd'hui faits de ces données dans le cadre, par exemple, des urgences liées à la gestion de la crise sanitaire ou de la recherche médicale. L'objectif consacré par le législateur de permettre à terme la centralisation des données de santé dans une infrastructure d'une taille inédite et facilitant de nouveaux usages de recherche peut également justifier que les premiers

développements mis en place bénéficient du temps nécessaire pour migrer vers d'autres solutions. Enfin, une grande partie des traitements des données de santé, notamment pour les entrepôts et les recherches, demeurent soumis à un régime d'autorisation préalable de la CNIL. Si la situation actuelle des hébergeurs de données de santé soumis aux programmes de renseignement américain est bien illégale, il devrait en résulter une impossibilité d'autoriser ces traitements. Il est donc nécessaire, tant que la situation n'est pas régularisée, de disposer d'un fondement juridique permettant, le cas échéant, de délivrer de telles autorisations, sous certaines garanties. Cependant, cette période de transition doit rester limitée à ce qui est nécessaire et impérativement être mise à profit pour garantir, par des démarches actives, la modification des conditions d'hébergement des données.

Juridiquement, la Commission estime, en première analyse, que cette période transitoire pourrait être fondée sur le d) du 1 de l'article 49, qui autorise des dérogations aux exigences minimales de protection des transferts pour des motifs importants d'intérêt public, à condition qu'ils soient reconnus par le droit de l'Etat membre. D'ordinaire, la CNIL a une approche particulièrement restrictive de cette disposition, mais elle relève que l'invalidation du *Privacy Shield* et les motifs de l'arrêt *Schrems II* de la CJUE entrainent juridiquement l'obligation de cesser un très grand nombre de transferts, ce qui peut, dans certains cas, porter une atteinte disproportionnée à l'intérêt général. Elle relève également que la cour a, au point 202 de son arrêt, refusé de moduler dans le temps les effets de sa décision, au motif que l'invalidation ne créait pas un vide juridique interdisant tout transfert vers les Etats-Unis dès lors que les dérogations prévues à l'article 49 permettent, à certaines conditions, de continuer certains transferts en l'absence de décision d'adéquation ou d'autres garanties appropriées. Les conditions de l'article 49 doivent être lues à la lumière de la situation inédite ouverte par l'arrêt *Schrems II,* pour régler ces situations transitoires.

L'article 49 autorise à titre dérogatoire certains transferts ; or toute demande de divulgation de données présentes sur le sol européen adressée par les services de renseignements états-uniens à un opérateur soumis aux lois américaines donnera lieu à un transfert. Ces transferts ne sont évidemment pas par eux-mêmes d'intérêt public. Cependant, il y a un intérêt public manifeste à ménager cette période de transition, pour garantir la continuité de l'hébergement des données de santé et des usages qui y sont liés. Il en résulte que maintenir temporairement le risque de ces transferts aux services de renseignement états-uniens, risque qui existait déjà et sur lequel la CNIL avait attiré l'attention du gouvernement dans son avis d'avril dernier, s'avère provisoirement nécessaire pour garantir une transition satisfaisante vers un dispositif d'hébergement souverain des données de santé, que la CNIL appelle de ses vœux.

Une telle dérogation devrait résulter d'une disposition normative spécifique et temporaire.

S'agissant de la durée de cette période, elle doit être limitée au strict nécessaire. La CNIL recommande aux autorités publiques d'évaluer en urgence l'existence de fournisseurs alternatifs et leurs capacités, tant en volume de stockage qu'en qualité de service, afin d'évaluer la durée nécessaire pour assurer cette transition, la plus courte possible. La Commission ne dispose pas d'informations suffisantes pour se prononcer elle-même à ce stade sur la durée admissible de cette période de transition.

Telles sont les observations que la CNIL, éclairée par un débat au sein du collège de la Commission lors de sa séance plénière du 8 octobre 2020, entend faire connaître à votre Haute juridiction.

À Paris, le 08 OCT. 2020

La Présidente

M.-L. Denis

Marie-Laure DENIS