PANTHÉON-ASSAS
UNIVERSITÉ
PARIS

Banque des mémoires

Master de Droit du numérique
Dirigé par Monsieur le Professeur Jérôme Passa
2024

Transfert des données de santé et souveraineté numérique : Enjeux juridiques et défis de l'hébergement en nuage

Lou Daudier

Sous la direction de Lorraine Maisnier-Boché

UNIVERSITÉ PARIS-PANTHÉON-ASSAS

Master de Droit du numérique

Dirigé par Monsieur le Professeur Jérôme Passa

2023-2024

« Transfert des données de santé et souveraineté numérique : Enjeux juridiques et défis de l'hébergement en nuage »

Lou DAUDIER

Sous la direction de Maître Lorraine Maisnier-Boché

Remerciements

Tout d'abord, je remercie Maître Lorraine Maisnier-Boché pour son accompagnement dans la direction de mon mémoire. Ses conseils avisés et le temps qu'elle a pu consacrer à ma formation ont rendu ma démarche extrêmement enrichissante.

Un grand merci à ma tutrice de stage Joséphine Flament qui m'a épaulée tout au long de mes recherches. Je la remercie tout particulièrement pour son soutien et sa bienveillance pendant ce stage.

Egalement, j'adresse mes remerciements à Monsieur le Professeur Jérôme Passa, directeur du Master de Droit du numérique pour m'avoir permis de suivre cette formation enrichissante permettant d'allier la théorie à la pratique, ainsi que les nombreux intervenants impliqués au sein du Master qui nous ont fourni les outils nécessaires à la réussite de cette année universitaire.

Enfin, je tiens à remercier mes parents, mes sœurs et mes proches pour leurs encouragements et particulièrement Jeanne et Alonzo pour les moments partagés.

Tables des abréviations

Abréviation	Correspondance
Aff.	Affaire
ANS	Agence du Numérique en Santé
ANSSI	Agence nationale de la sécurité des systèmes d'information
Art.	Article
CCT	Clauses Contractuelles Types
CDFUE	Charte des Droits Fondamentaux de l'Union Européenne
CE	Conseil d'Etat
CEDH	Cour Européenne des Droits de l'Homme
CEPD/EDPB	Comité Européen de la Protection des Données
CESREES	Comité d'Éthique et de Soutien à la Recherche en Santé
CJUE	Cour de Justice de l'Union Européenne
comm.	Commentaire
Cons. Const.	Conseil Constitutionnel
Conv EDH	Convention Européenne des Droit de l'Homme
CNIL	Commission Nationale de l'Informatique et des Libertés
CSP	Code de la santé publique
DPF	Data Privacy Framework
DNS	Délégation au Numérique en Santé
Ed.	Edition
EEE	Espace Economique Européen
EO 12 333	Executive Order 12 333
EUCS	European Union Cybersecurity Certification Scheme for Cloud Services
FISA	Foreign Intelligence Surveillance Act of 1978
HDH / PDS	Health Data Hub / Plateforme de Données de Santé
HDS	Hébergeur de Données de Santé
LIL	Loi Informatique et Libertés

n°	Numéro
Obs.	Observations
p.	Page
PE	Parlement Européen
RGPD	Règlement général sur la protection des données
SI	Système d'information
UE	Union Européenne

Sommaire

Introduction

« Les données de santé considérées à la fois comme un « trésor national » à protéger et un « bien commun » à partager, à une échelle européenne voire mondiale[1] » sont au cœur de la souveraineté numérique. La pandémie de COVID-19 a entraîné un accroissement du partage des données de santé, multipliant les flux internationaux et suscitant de vives inquiétudes chez les personnes concernées. L'essor de nouveaux acteurs dans le domaine a mis en exergue la nécessité de concilier la souveraineté numérique, des implications économiques et le besoin accru de partage des données de santé pour la recherche et la gestion de la crise sanitaire[2]. Plus généralement en 2013 déjà, le Rapport sur la gouvernance et l'utilisation des données de santé dressait le constat suivant : « avant même l'essor d'internet le législateur a voulu encadrer l'utilisation des données personnelles, d'abord contre la puissance publique considérée comme le principal danger car elle stockerait les données et en ferait une utilisation de manière floue, injustifiée ou disproportionnée. C'est dans ce contexte qu'a été adoptée la loi du 6 janvier 1978 qui a créé la CNIL[3] ».

La protection des données personnelles, et plus particulièrement des données de santé, représente un enjeu fondamental aujourd'hui. Ces données, en raison de leur nature sensible, requièrent des mesures de sécurité et de confidentialité fortes pour garantir le respect des droits et des libertés fondamentaux des individus. Ces dernières sont définies à l'article 4, paragraphe 15 du Règlement général sur la protection des données (RGPD) comme « toutes données relatives à la santé physique ou mentale d'une personne, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ». Selon l'article 9 du RGPD, « le traitement de ces données est interdit[4] », sauf dans certaines conditions strictes, telles que le consentement explicite de la personne concernée ou pour des

---

[1] BERNELIN Margo, « Plateformes de données de santé : enjeux d'éthique, un avis du CCNE et du CNPEN à ne pas manquer », Dalloz Actualités, 5 juin 2023.

[2] *Ibid.*

[3] CONSEIL D'ETAT, « Santé et protection des données », *Un colloque organisé par le Conseil d'Etat le 1er décembre 2017,* Conseil d'Etat Droits et Débats n°29, Conseil d'Etat, La Documentation française.

[4] LEFEBVRE DALLOZ, « Traitement des données de santé », Fiche thématique Droit des affaires - Protection des données personnelles (RGPD), 8 décembre 2023.

motifs d'intérêt public dans le domaine de la santé publique. Le traitement des données de santé est également encadré par la Loi « Informatique et Libertés » (LIL)[5] en France, qui impose des obligations supplémentaires pour garantir la sécurité et la confidentialité de ces informations. Si le traitement des données de santé n'est pas prohibé c'est qu'il présente des avantages indéniables. Les données de santé sont essentielles pour élaborer et évaluer les politiques de santé publique, aidant à adapter les mesures aux besoins réels de la population[6]. En outre, elles optimisent le parcours de soin des patients et fournissent des informations précieuses sur l'évolution des dépenses en santé. Ainsi, le traitement des données de santé est nécessaire à la gestion du système de santé.

Les bénéfices du traitement de données de santé sont encore accentués par l'augmentation des flux internationaux de données. Toutefois cela se heurte à la souveraineté numérique. La notion de souveraineté numérique renvoie à la capacité d'un État ou d'une organisation à exercer un contrôle et une gouvernance complète sur ses infrastructures numériques et les données hébergées. En l'absence de définition légale, Lorraine Maisnier-Boché en propose une approche selon un classement des obligations de souveraineté en fonction de leur niveau d'exigence. Dans l'ordre croissant, il s'agira d'abord de l'obligation de traiter les données sur des serveurs situés physiquement en Europe. Ensuite, il s'agira de l'interdiction d'accéder aux données ou de les exploiter, à partir d'un pays hors de ce territoire. Le niveau le plus exigeant requiert d'être soumis exclusivement au droit de l'Union ou de l'EEE[7]. Dans un environnement numérique mondialisé, cette souveraineté est souvent mise à l'épreuve par les défis posés par l'hébergement des données sur des services de cloud situés hors de l'Union européenne, notamment aux États-Unis[8].

---

[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[6] BRAS Pierre-Louis et LOTH André, « Rapport sur la gouvernance et l'utilisation des données de santé », septembre 2023, p. 43.

[7] MAISNIER-BOCHÉ Lorraine, « Du consensus sur la localisation aux divergences sur l'immunité », Les Doctrines du mois, Expertises n°501, Expertises Droit, Technologies & Prospectives, mai 2024, p. 22 s.

[8] NAVARRO Patrice, « Union européenne – Souveraineté numérique – Souveraineté numérique européenne : entre faux-semblants et opportunités », La Semaine Juridique Edition Générale, n°04, 29 janvier 2024, doctr. 142. Lexis Nexis.

Selon l'Agence du Numérique en Santé (ANS) et les articles L. 1111-8 et R. 1111-8-8 du Code de la santé publique (CSP), il existe trois catégories de services d'hébergement de données de santé : l'hébergement de données de santé sur support papier, l'hébergement de données de santé en format numérique dans le cadre d'un service d'archivage électronique, et l'hébergement de données de santé en format numérique dans les autres cas. Les développements se concentreront sur le dernier type d'hébergement. Plus précisément, l'hébergement de données de santé sous forme numérique consiste à réaliser, pour le compte d'un tiers, tout ou partie des activités suivantes définies à l'article R. 1111-9 du Code de la santé publique. Ces activités permettent d'identifier les fournisseurs d'infrastructure physique et les hébergeurs infogérants. L'hébergement cloud, « en nuage » en français, désigne l'utilisation de serveurs distants via Internet pour stocker, gérer et traiter des données, plutôt que d'utiliser un serveur local ou un ordinateur personnel. Cette technologie facilite l'accès aux ressources informatiques de manière plus efficiente et économique. Sur le plan juridique, l'hébergement cloud est encadré par plusieurs dispositions légales et réglementaires au niveau européen et national[9]. Le RGPD pose les bases pour un traitement sécurisé, incluant les données hébergées sur des plateformes cloud. En France, la LIL complète ces exigences[10]. La Commission Nationale de l'Informatique et des Libertés (CNIL) a également émis des recommandations pour l'utilisation du cloud. Elles insistent sur l'importance de sélectionner des prestataires de services cloud qui respectent les normes de sécurité élevées et les réglementations en vigueur pour assurer la protection des données personnelles. La CNIL souligne la nécessité d'évaluer les risques liés aux transferts de données vers des pays tiers et de garantir que de telles opérations respectent les exigences du RGPD et de la LIL. De plus, « la Commission européenne se place en faveur de la création d'un cloud européen pour contrer les géants américains[11]. » En effet, l'extraterritorialité des lois américaines permet aux autorités américaines d'accéder aux données hébergées par des entreprises américaines, même si ces données se trouvent physiquement en Europe via des filiales européennes. Cela permet

---

[9] CNIL, BOUCHER DE CREVECOEUR Erik, Webinaire « Etablissements de santé : les référentiels en santé et la « gouvernance » de la protection des donnée », 11 octobre 2022.

[10] Loi informatique et libertés, article 35.

[11] FONTAINE Quentin et STROWEL Alain, « La stratégie européenne pour les données », *La politique européenne du numérique*, sous la direction de BERTRAND Brunessen. Collection Droit de l'Union européenne dirigée par Fabrice Picod, Collection Monographie. Ed. Bruylant, 2023, p. 727.

de distinguer les cloud souverains des cloud non-souverains. Un cloud souverain garantit que les données sont hébergées exclusivement dans le cadre légal et géographique d'un pays, assurant une protection maximale contre les ingérences étrangères. En revanche, un cloud non souverain utilise des infrastructures et des services situés en dehors des frontières légales locales, ce qui peut exposer les données à des lois et réglementations extraterritoriales. En l'espèce, recourir à un cloud souverain signifierait recourir à un cloud français ou européen exclusivement soumis au droit national ou européen.

Dès lors, « les régimes applicables aux données de santé sont bouleversés par les usages numériques que l'on en fait et la mondialisation des échanges[12] ». L'hébergement des données de santé dans le cloud pose la question d'un équilibre délicat entre plusieurs droits fondamentaux, dont le droit à la vie privée et le droit à la santé. Ces droits doivent être conciliés pour garantir une protection adéquate des individus tout en permettant l'innovation et l'efficacité des systèmes de santé. Le droit à la vie privée est un droit fondamental protégé par plusieurs instruments juridiques internationaux et européens. L'article 8 de la Convention européenne des Droits de l'Homme prévoit que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». De même, l'article 7 de la Charte des Droits fondamentaux de l'Union européenne (CDFUE) reconnaît le droit au respect de la vie privée et familiale. En matière de données personnelles, l'article 8 de la CDFUE pose les principes fondamentaux de leur traitement. Le RGPD, entré en vigueur en mai 2018, renforce ces protections. L'article 9 du RGPD interdit en principe le traitement des données de santé, sauf dans des conditions spécifiques, afin de garantir une protection renforcée de ces informations sensibles.

Parallèlement, le droit à la santé est également un droit fondamental reconnu à l'échelle internationale par l'article 35 de la CDFUE. Le droit implique non seulement l'accès aux soins de santé mais aussi l'utilisation des technologies de l'information pour améliorer la qualité et l'efficacité des services de santé. L'innovation dans le domaine des technologies de la santé, notamment à travers l'utilisation des données de santé pour la recherche et le développement, est nécessaire pour améliorer les soins de santé et répondre aux besoins des populations.

---

[12] FAVREAU Amélie, « Données de santé : vers l'émergence d'un droit spécial ? », *L'émergence d'un droit des données*, sous la direction de Jean-Michel Bruguière. Thèmes & Commentaires La propriété intellectuelle autrement. Lefebvre Dalloz, Dalloz. 2024, p. 171.

La conciliation du droit à la vie privée et du droit à la santé pose un défi particulier lorsqu'il s'agit de l'hébergement des données de santé dans le cloud. L'hébergement cloud « cristallise les tensions classiques entre les exigences de sécurité et les libertés individuelles »[13]. D'une part, les données de santé doivent être protégées contre tout accès non autorisé pour préserver la confidentialité et la vie privée des individus. D'autre part, l'utilisation de ces données est essentielle pour permettre des avancées médicales, favoriser la recherche et garantir un accès équitable aux soins de santé. Les réglementations européennes, notamment le RGPD, cherchent à établir un équilibre entre ces droits en imposant des conditions strictes pour le traitement des données de santé tout en permettant leur utilisation sous certaines conditions spécifiques. Le Comité international de bioéthique (CIB) de l'Unesco résume le paradoxe ainsi : « les citoyens veulent bien protéger leur vie privée mais ils veulent aussi profiter des avancées de la science. En somme, comment faire se conjuguer le bien commun et l'intérêt particulier[14] ? ».

Egalement, la jurisprudence de la Cour de justice de l'Union européenne (CJUE) a joué un rôle important dans la protection des données personnelles européennes contre les ingérences américaines[15]. En France, des décisions du Conseil d'État ont souligné la nécessité de renforcer la protection des données de santé contre les accès non autorisés par des autorités étrangères.

Dans un contexte où les données de santé nécessitent une protection accrue de par leur caractère sensible et où la question de la souveraineté numérique de l'Europe fait débat, les enjeux liés à l'hébergement des données du Health Data Hub (HDH) sur un service de cloud

---

[13] DELMAS-LINEL Béatrice, « Enjeux sociétaux : Cloud computing, nouveau prisme des libertés publiques et des souverainetés nationales »*, Le cloud computing – L'informatique en nuage*, Actes du Colloque du 11 octobre 2023, sous la direction de Bénédicte Fauvarque-Cosson et Célia Zolynski. Collection colloques volume 22, Société de la législation comparée, p. 97.

[14] STANTON-JEAN Michèle et FEINHOLZ Dafna, « Que penser sur les mégadonnées en santé selon le Comité international de bioéthique (CIB) de l'Unesco », *Innovations en santé publique, des données personnelles aux données massives (big data) - Aspects cliniques, juridiques et éthiques*, Contribution sous la direction de Christian Hervé et Michèle Stanton-Jean. Thèmes & Commentaires - Ethique biomédicale et normes juridiques, Editions Dalloz, 2019, p. 60.

[15] CJUE, arrêt de la Cour (grande chambre) du 6 octobre 2015, Maximillian Schrems contre Data Protection Commissioner. Demande de décision préjudicielle, introduite par la High Court (Irlande). Affaire C-362/14; EUROPEAN PARLIAMENT, resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 — Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)).

américain Microsoft Azure, malgré les réserves de la CNIL[16], illustrent ce paradoxe[17]. Le Health Data Hub est une plateforme française centralisant des données de santé pour faciliter leur accès et leur utilisation par les chercheurs, les professionnels de santé et les institutions publiques. Son objectif principal est de favoriser l'innovation dans le domaine de la santé, en soutenant la recherche médicale et l'amélioration des soins grâce à l'analyse de grandes quantités de données. Il assure également la protection des données personnelles en conformité avec le RGPD et les réglementations nationales. Le HDH occupe une place particulière dans le paysage de la gestion des données de santé en raison de son statut de Groupement d'intérêt public (GIP). Ce statut lui confère une mission de service public, ce qui implique une responsabilité renforcée. En tant que GIP, le HDH est étroitement lié à l'État, ce qui renforce l'idée d'exemplarité dans la gestion des données de santé. Le fait que le HDH soit directement impliqué dans la collecte, le traitement et l'hébergement de données sensibles sous la tutelle de l'État le place à un niveau d'attente de conformité aux normes très élevé. Ainsi, le choix d'hébergeur cloud concernant le HDH illustre les défis et les solutions possibles pour concilier les impératifs de compétitivité et de souveraineté[18]. Il faut noter que l'Espace européen des données de santé[19], pourra apporter des solutions à cette problématique à l'avenir[20]. La problématique réside dans le fait que le partage de données de santé représente

---

[16] CNIL, 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.

[17] NEVEJANS Nathalie, « Les aspects juridiques et éthiques de l'utilisation de l'IA comme outil de lutte contre la COVID-19 », *L'utilisation du numérique dans la lutte contre la Covid - Enjeux techniques, éthiques et juridiques*, sous la direction de Yves Poullet et David Doat, Collection « Droit, Société et Risque », Ed. L'Harmattan, 2022 p.165.

[18] MAXWELL W. J. « Protection des données aux Etats-Unis », *Le cloud computing – L'informatique en nuage*, Actes du Colloque du 11 octobre 2023 sous la direction de Bénédicte Fauvarque-Cosson et Célia Zolynski. Collection colloques volume 22, Société de la législation comparée, p. 76.

[19] PARLEMENT EUROPÉEN ET CONSEIL, Proposition de règlement relatif à l'espace européen des données de santé, COM/2022/197 final.

[20] DE GROVE-VALDEYRON Nathalie et BLANQUET Marc, « Politique de santé et politique du numérique », *La politique européenne du numérique*, sous la direction de BERTRAND Brunessen. Collection Droit de l'Union européenne dirigée par Fabrice Picod, Collection Monographie, Ed. Bruylant, p. 515.

« un avantage considérable pour la communauté des patients[21] » mais aussi un « danger pour la protection individuelle des patients dont les données sont divulguées[22] ».

Dès lors, comment concilier les impératifs de souveraineté des données de santé dans un contexte numérique mondialisé avec les défis juridiques et techniques engendrés par l'hébergement des données du Health Data Hub sur des services de cloud américains lorsque les exigences des deux côtés semblent intrinsèquement contradictoires ? Cette problématique soulève une question fondamentale : peut-on véritablement parvenir à une conciliation alors que d'un côté, la nécessité de protéger les données sensibles se heurte à l'impératif de partage international essentiel pour la veille sanitaire, l'innovation et la recherche, et de l'autre, la politique française en faveur de la souveraineté numérique se trouve en marge des décisions européennes en faveur des flux internationaux de données ?

L'essor des flux internationaux de données a transformé le traitement des données de santé, soulevant des enjeux juridiques et techniques complexes. Dans ce contexte, la souveraineté numérique se heurte aux réalités d'un environnement numérique globalisé. Le Health Data Hub illustre cette tension, centralisant des données de santé tout en s'appuyant sur un service de cloud américain. Chronologiquement, il s'agit d'une problématique en débat jusqu'à l'adoption de l'actuelle décision d'adéquation (Chapitre 1), décision qui ne permet pas d'assurer la souveraineté numérique, entrainant alors le renforcement des mesures et des certifications encadrant l'hébergement des données de santé (Chapitre 2).

Chapitre 1 : La problématique persistante de l'hébergement des données de santé aux Etats-Unis

L'année 2024 marque un tournant pour la souveraineté numérique. Cependant, la question de l'hébergement des données de santé françaises sur des cloud américains n'est pas nouvelle.

---

[21] EL BIAD Nahela, « Le paradoxe de la e-santé : entre promotion d'un mode de soins innovant et protection des droits des patients », *Santé, numérique et droit-s*, IFR Actes de colloques n°34 sous la direction de Isabelle Poirot-Mazères, Presses de l'Université Toulouse 1 Capitole, 2018, p.191.

[22] *Ibid.*

Les données de santé étant sensibles, elles sont soumises à un régime particulier pour renforcer leur protection et assurer leur confidentialité. En effet, leur nature sensible justifie un régime de traitement particulier. Si ces données bénéficient d'un traitement spécifique, ce n'est pas le cas de l'hypothèse du transfert hors de l'EEE. Dès lors, la conciliation des exigences de souveraineté avec la nécessité d'assurer des transferts de données de santé à l'international semble plus difficile à envisager.

Déjà sous l'empire de la directive de 1995, puis du RGPD, la reconnaissance et l'encadrement du transfert des données de santé vers les Etats-Unis faisait débat. Après plusieurs recours, le Data Privacy Framework, décision d'adéquation actuelle, permet de connaitre le régime de transfert des données de santé vers les Etats-Unis, dont les garanties tendent à remettre en cause la souveraineté de la France et de l'Union à l'égard des données de santé.

Ainsi, si le traitement et le transfert des données de santé sont encadrés dans les textes européens et nationaux (Section 1), cette reconnaissance en marge des exigences de souveraineté numérique, est remise en question par les différents recours à l'encontre des décisions d'adéquation de la Commission européenne (Section 2).

Section 1 : La reconnaissance encadrée du transfert des données de santé dans les textes

Les textes européens et nationaux reconnaissent le caractère sensible des données de santé. Il s'agit d'une notion interprétée largement qui permet de conférer un statut particulier ainsi qu'un régime particulier à ce type de données. En effet, le traitement des données de santé fait l'objet de dispositions plus protectrices que celles encadrant les données personnelles « classiques », ce qui permet d'assurer un haut niveau de confidentialité et de sécurité. Toutefois, l'encadrement du transfert des données vers des pays tiers à l'EEE ne diffère pas selon le caractère sensible ou non des données. Ainsi, l'hébergement des données de santé sur des cloud américains caractérise un transfert de données personnelles vers les Etats-Unis mais ne bénéficie pas de garanties particulières contre l'extraterritorialité de certaines lois américaines.

Dès lors, le caractère sensible des données de santé justifie un encadrement spécifique protecteur pour leur traitement (I) mais cette exigence ne se retrouve pas dans l'encadrement

des transferts de données vers les Etats-Unis, exposant les données de santé françaises à l'extraterritorialité des lois américaines (II).

I - Le traitement particulier de données d'une sensibilité particulière, les données de santé

Le traitement des données de santé peut avoir un impact significatif sur la vie privée et les droits fondamentaux des individus. Reconnaitre leur caractère sensible permet de leur conférer un régime particulier permettant de protéger davantage ces données sensibles et donc garantir le respect de la vie privée et la protection des droits fondamentaux des personnes conformément aux principes de confidentialité et de protection des données énoncés dans le RGPD.

Ainsi, le caractère sensible des données de santé apprécié largement (A) justifie que leur traitement fasse l'objet de mesures spécifiques et protectrices[23] (B).

A - Le caractère sensible des données de santé, une notion large

En France, la notion de données sensibles vient de la Loi Informatique et Libertés qui la définit comme « les données nominatives qui, directement et indirectement, font apparaitre les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales des personnes[24] ». Cette notion a fait l'objet de plusieurs modifications jusqu'à la version actuelle du RGPD qui la définit comme des données qui « méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour [les] libertés et droits [fondamentaux][25] ». Parmi ces données se trouvent les données de santé[26] à l'article 4 paragraphe 15 du RGPD. S'ajoutent les données de l'orientation sexuelle et données biométriques et génétiques. Le considérant 35

[23] GAMBARDELLA Sophie, « Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé », 3 février 2020.

[24] Loi Informatiques et Libertés, article 31 ancien.

[25] RGPD, article 9.

[26] Loi Informatiques et Libertés, article 6 ; RGPD, article 9.

précise qu'il s'agit de « l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée ou encore d'un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé[27] ». Les données de santé sont donc appréciées largement pour permettre d'englober un maximum de données relatives à la vie privée de la personne physique. Cela s'est fait sous l'impulsion de la jurisprudence européenne[28], la jurisprudence française ayant plutôt une approche restrictive[29]. Ces données peuvent inclure notamment des informations sur l'état de santé passé, les traitements et les diagnostics d'un patient.

La sensibilité de ces données découle de leur nature intime, elles révèlent ce qu'il y a de plus personnel pour la personne physique, leur divulgation peut donc avoir des répercussions graves pour la vie privée. De plus, une divulgation des données de santé peut donner lieu à des faits de discrimination et de stigmatisation de la personne concernée dans des domaines tels que ceux de l'emploi ou de l'assurance.

La reconnaissance du caractère sensible des données de santé permet de leur conférer un régime de traitement particulier pour permettre une protection accrue[30]. En effet, de leur sensibilité découle un principe d'interdiction de traitement. Ce principe est atténué par l'existence de nombreuses dérogations. L'idée serait ainsi de concilier la souveraineté numérique et le besoin d'utiliser les données de santé à des fins primaires ou secondaires.

B - La nécessité d'un encadrement propre au traitement des données de santé

Le traitement des données de santé en France, bien que soumis à une interdiction de principe en vertu du RGPD et de la « Loi Informatique et Libertés » (LIL), peut être réalisé en

[27] RGPD, considérant 35.

[28] CJUE, 6 nov. 2003, aff. C-101/1 Bodil Lindqvist et G29, 15 février 2007, WP131.

[29] CE, 19 juil. 2010, n° 317182 Base Elèves et CE, 28 mars 2014, n°361042.

[30] DOUVILLE Thibault, « Droit des données à caractère personnel », Manuel, Précis Domat, Droit privé / public, LGDJ, Lextenso, 2023, p. 105.

conformité avec certaines conditions strictes. Ces conditions permettent de concilier la protection des données sensibles avec la nécessité de leur traitement à des fins légitimes[31].

Les données de santé bénéficient d'un régime juridique particulier en raison de leur sensibilité. Des contraintes règlementaires découlent de leur encadrement juridique tant sur le plan du traitement que de l'hébergement[32]. L'article 6 du RGPD prévoit les bases légales pour que le traitement soit licite. Il peut s'agir par exemple du consentement de la personne concernée[33] ou de l'exécution d'une mission d'intérêt public[34].

Selon l'article 9(1) du RGPD, le traitement des données de santé est en principe interdit. En France, ce principe d'interdiction est consacré par l'article 6-1 de la loi Informatique et Libertés. Cependant, l'article 9(2) du RGPD énonce plusieurs exceptions qui permettent ce traitement sous certaines conditions. Il s'agit notamment du « consentement explicite[35] » de la personne concernée. Selon l'article 9(2)(a), le traitement est possible si la personne concernée donne son consentement explicite pour une ou plusieurs finalités spécifiques. Une autre exception concerne l'intérêt public dans le domaine de la santé publique. Conformément à l'article 9(2)(i), le traitement des données de santé est autorisé pour des raisons d'intérêt public, tel que la « protection contre les menaces transfrontalières graves pour la santé »[36] ou pour garantir des normes élevées de qualité et de sécurité des soins de santé. Le traitement des données de santé est également permis lorsqu'il est nécessaire à des fins de médecine préventive, de diagnostic médical, de prestation de soins ou de traitements de santé, ou de gestion des systèmes et services de santé, conformément à l'article 9(2)(h). Une fois la conformité à l'article 9 du RGPD vérifiée, il faut se demander si le traitement entre ou non dans le champ d'application de la LIL. En effet, le RGPD laisse aux Etats une marge de manœuvre dans certains domaines dont celui de la santé. La LIL a ainsi dédié un chapitre aux données de santé dans lequel elle prévoit des exceptions à l'interdiction de principe du

---

[31] CANTERO Isabelle et CAPRIOLI Eric, « Informatique et libertés - Traitement et hébergement de données de santé : entre protection et risques », Etudes, Revue pratique de la prospective et de l'innovation n° 2, dossier 21, novembre 2021.

[32] *Ibid.*

[33] RGPD, article 6 1) a).

[34] RGPD, article 6 1) e).

[35] *Supra note n°9.*

[36] *Supra note n°9.*

traitement des données de santé. Elle distingue un régime pour le traitement de l'ensemble des données de santé et un régime spécial applicable aux traitements dans le cadre de la recherche. La loi définit les traitements qui entrent dans son champ d'application, ces traitements doivent avoir une finalité d'intérêt public. Il faut ensuite vérifier si les traitements ont une finalité de recherche ou non. Selon l'article 44, les personnes réalisant le traitement de données sensibles telles que les données de santé, ainsi que celles qui ont accès aux données sur lesquelles il porte, sont soumises à une obligation de secret professionnel. Une distinction doit être faite entre les données de santé traitées hors recherche médicale et celles traitées à des fins de recherche scientifique. Concernant les traitements automatisés dont la finalité est ou devient la recherche, les études dans le domaine de la santé, ou l'analyse des pratiques ou des activités de soins ou de prévention, un régime d'autorisation est prévu[37]. Ce régime impose la réalisation de formalités auprès de la CNIL, notamment en démontrant la présence d'un intérêt public pour obtenir une autorisation[38]. Cela nécessite une autorisation de la CNIL conformément à l'article 66 de la LIL.

Pour les recherches, il est possible d'obtenir cette autorisation soit de manière ad hoc, soit en se conformant à une des méthodologies de référence publiées par la CNIL. Cette dernière procédure permet de se dispenser de demander une autorisation à la CNIL. Si tel n'est pas le cas, une autorisation doit être demandée, laquelle intervient après enregistrement auprès du Health Data Hub (HDH) et avis du Comité d'Éthique et de Soutien à la Recherche en Santé (CESREES).

En conclusion, bien que le traitement des données de santé soit soumis à une interdiction de principe, le RGPD et la LIL offrent des exceptions et des conditions strictes permettant leur traitement. Ces conditions visent à protéger les droits des individus tout en permettant une utilisation contrôlée et sécurisée des données de santé, dans un contexte où « la souveraineté numérique et la protection de la vie privée sont des priorités essentielles »[39].

---

[37] ULYS, « Article 9 : Traitement portant sur des catégories particulières de données à caractère personnel », Article, GDPR.expert.com.

[38] CNIL, « Demande d'autorisation d'une recherche en santé : les informations à fournir et les critères d'octroi », Avis, 11 janvier 2023.

[39] BOSSY MALAFOSSE Jeanne, « La Commission européenne valide le nouvel accord de protection des données entre l'Europe et les Etats-Unis », DELSOL Avocats, Blog Données personnelles, 11 juillet 2023.

Si des dispositions spécifiques aux données de santé sont prévues dans la LIL et dans le RGPD, ce n'est pas le cas concernant le transfert des données de santé vers des pays tiers à l'EEE.

Le traitement des données de santé soulève des enjeux majeurs en termes de souveraineté numérique et de protection de la vie privée. La souveraineté numérique implique que les données de santé des citoyens soient protégées et contrôlées au niveau national, réduisant ainsi les risques associés au transfert de données vers des juridictions aux réglementations moins strictes. La protection de la vie privée des individus est essentielle pour prévenir les risques de discrimination, de stigmatisation et de violations de la confidentialité. En conciliant ces exigences, le cadre juridique en vigueur cherche à garantir que les données de santé soient traitées de manière sécurisée et conforme, tout en soutenant l'innovation et la recherche dans le domaine de la santé.

II - Le transfert de données d'une sensibilité particulière, les données de santé

Le caractère sensible des données de santé justifie un traitement particulier. Toutefois, ce n'est pas ce qui est prévu dans le cadre de leur transfert hors de l'Union. Si un tel transfert est un principe interdit, des exceptions le permettent dans la pratique. Le transfert de données de la France vers les Etats-Unis ainsi encadré, cela ne suffirait pas à assurer la souveraineté des données. En effet, l'extraterritorialité de certaines lois américaines laisse à penser que les autorités pourraient avoir un accès aux données de santé françaises.

Ainsi, le principe du transfert de données hors de l'UE (A) remet en cause la souveraineté numérique du fait de l'extraterritorialité des lois américaines (B).

A - Le principe du transfert de données de santé vers des pays tiers

Les transferts de données vers des Etats tiers à l'EEE ne sont pas définis par le RGPD, la CNIL et le CEPD sont venus apporter des précisions. La CNIL définit le transfert de données personnelles hors de l'UE comme « toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union

européenne[40]». Dès lors, tout le chapitre 5 du RGPD s'applique. Le CEPD donne trois critères cumulatifs permettant de caractériser un tel transfert[41]. Premièrement, le responsable de traitement ou le sous-traitant doit être soumis au RGPD pour le traitement donné, il est appelé « l'exportateur ». Deuxièmement, l'exportateur doit transmettre ou mettre à disposition d'un autre responsable de traitement ou d'un autre sous-traitant « l'importateur » les données personnelles qui font l'objet du traitement donné. Troisièmement, l'importateur doit être situé dans un pays tiers ou une organisation internationale, qu'il soit ou non soumis au RGPD. Ainsi, lorsqu'un exportateur de données tel que le HDH, soumis au RGPD, stocke des données de santé en les mettant à disposition d'un fournisseur de services en nuage américain, il s'agit d'un transfert de données personnelles hors de l'UE[42].

Le RGPD pose le principe de l'interdiction des transferts de données hors UE. Par exception, les transferts sont permis dans certaines hypothèses[43]. Ils peuvent faire l'objet d'une décision d'adéquation rendue par la Commission européenne en vertu de l'article 45 du RGPD. Quinze pays en font aujourd'hui l'objet. Pour eux, les transferts de données s'effectuent librement, il n'y a pas d'obligation d'encadrement, les flux s'opèrent comme dans les pays de l'UE. Les Etats-Unis font l'objet d'une décision d'adéquation, le Data Privacy Framework, par lequel les entreprises américaines s'auto-certifient. Cette décision sera étudiée en suivant.

En dehors des décisions d'adéquation, les transferts doivent être fondés sur des garanties appropriées[44]. Il peut s'agir des clauses contractuelles types qui sont rédigées par la Commission européenne et qui s'appliquent même aux transferts hors du groupe d'entreprises. Il existe également les règles d'entreprises contraignantes[45] qui autorisent les transferts au sein du groupe d'entreprises uniquement, après avoir été approuvées par les

---

[40] CNIL, définition en ligne.

[41] CEPD, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, adoptées le 10 novembre 2020.

[42] GALICHET Charlotte, « Nouvelles Clauses Contractuelles Types relatives au transfert de données vers un pays tiers : Quels changements ? », Données personnelles, Blog de Charlotte Galichet, 22 juin 2021.

[43] CNIL, « Webinaire Transferts de données hors de l'UE : quelles sont les règles de base ?», 7 juin 2024 à 11h.

[44] RGPD, article 46.

[45] RGPD, article 47.

autorités de la protection européenne des données et soumises au CEPD. Enfin, l'article 49 du RGPD prévoit une liste de dérogation à l'interdiction de principe.

Ainsi, aucune disposition n'encadre de manière spécifique les transferts de données de santé hors de l'UE.

D'une part, du point de vue de la souveraineté numérique, cela est regrettable car les transferts de données de santé vers des pays tiers s'effectuent alors comme les transferts de simples données commerciales dépourvues de caractère sensible. D'autre part, cela peut se comprendre en se plaçant du point de vue du développement de la recherche et de l'innovation. En effet, pour progresser la santé a besoin de flux internationaux. Dès lors, ne pas conférer aux données de santé un régime plus exigeant pour leur transfert permet de ne pas brider le partage de telles données.

Toutefois, l'absence de garanties spécifiques aux données de santé est problématique car les lois américaines ont une portée extraterritoriale. Il s'agit notamment de lois permettant aux autorités américaines d'avoir accès aux données personnelles hébergées par des filiales européennes de société mère américaine.

B - Les données de santé européennes face à l'extraterritorialité des lois américaines

Le transfert à l'international des données de santé est problématique car il les expose à un risque d'accès par les autorités américaines. En effet, plusieurs lois américaines ont une portée extraterritoriale.

Tout d'abord, la section 102 de la loi FISA[46] permet aux autorités d'ordonner à un fournisseur de services de communication électronique de leur fournir toutes les informations nécessaires, sans en préciser la liste, ce qui inclut sans doute les données personnelles hébergées chez les fournisseurs de cloud. La CNIL, dans son mémoire sur la décision relative au HDH, indiquait que « 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 états-unien. Le champ d'application matériel de ce texte, portant sur

[46] LOI FISA, section 702 (b).

les informations de renseignements étrangers et concernant des personnes dont on peut raisonnablement penser qu'elles se trouvent en dehors des Etats-Unis, implique la possibilité d'un accès à ces informations en dehors du territoire états-unien[47]. ». De plus, alors que le FISA arrivait à son terme en avril 2024, les Etats-Unis ont renouvelé sa durée pour deux ans[48]. Cela pose question quant au sort de l'actuelle décision d'adéquation.

Ensuite, l'Executive Order 12 333 (EO 12333) est un décret américain qui organise la surveillance électronique[49] et permet la collecte de données en transit vers et en dehors des Etats-Unis à des fins de renseignements[50]. Le G29[51] a relevé le champ très large de la définition des informations susceptibles d'être collectées, laissant penser que tout type de données personnelles peuvent être concernées, y compris les données sensibles.

Dès lors, l'extraterritorialité de certaines lois américaines laisse à penser que les autorités américaines peuvent facilement avoir accès aux données de santé du HDH hébergées sur des services de cloud américains. Bien que des hébergeurs aient des filiales en Europe, ces lois s'appliquent également aux sociétés filles établies en UE dont la société mère est américaine[52]. Cela remet en cause la souveraineté numérique de l'Europe et de la France à l'égard de leurs données de santé et illustre la difficulté à concilier cette notion avec le fait que les transferts vers les Etats-Unis semblent aujourd'hui incontournables.

Ainsi, les transferts de données sont encadrés par les textes européens et nationaux. Toutefois, aucune disposition spécifique n'est prise pour le cas particulier des transferts des données de santé hors de l'Union. Cela pose question eu égard de l'extraterritorialité des certaines lois américaines qui permet aux autorités d'accéder aux données sensibles des citoyens français. C'est cette extraterritorialité qui a conduit à la remise en cause en pratique

---

[47] CNIL, Mémoire en observations, Conseil d'Etat, Section du contentieux, référé L. 521-2 CJA.

[48] VITARD Alice, « Les Etats-Unis renouvellent et étendent leur pouvoir de collecte de données sur les communications », L'Usine Digitale, 22 avril 2024.

[49] EXECUTIVE ORDER, article 3.4 b).

[50] CNIL « Invalidation du Privacy shield : les premières questions-réponses du CEPD », 31 juillet 2020.

[51] COMMISSION EUROPÉENNE, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (version adoptée le 13 avril 2016).

[52] DOUVILLE Thibault, « Droit des données à caractère personnel », Précis DOMAT, Droit privé / public, LGDJ Lextenso, 2023, p. 356.

de l'encadrement des transferts de données vers les Etats-Unis avec la contestation des décisions d'adéquation successives.

Section 2 : La remise en cause du transfert des données de santé dans la pratique

En théorie, le traitement et le transfert des données personnelles sont strictement encadrés, l'idée étant d'assurer une protection maximale à l'égard des données de santé françaises. Toutefois en pratique, l'extraterritorialité de certaines lois américaines a conduit à remettre en cause les décisions d'adéquation successives jusqu'à l'actuelle décision DPF. Des mesures ont été prises pour renforcer la souveraineté numérique à l'égard des données de santé mais des contestations s'élèvent.

Ainsi, la remise en cause des anciennes décisions d'adéquation encadrant le transfert de données vers les Etats-Unis (I) a permis d'aboutir à une décision plus protectrice des données de santé françaises hébergées aux Etats-Unis qui reste toutefois très contestée (II).

I - La remise en cause historique des décisions d'adéquation encadrant les transferts

Le transfert des données personnelles vers les Etats-Unis n'est pas une question nouvelle. En effet, sous l'empire de la directive de 1995 puis du RGPD deux décisions d'adéquation ont été invalidées par la CJUE, mettant en lumière la difficile conciliation entre la nécessité d'assurer les flux internationaux et la protection des données sensibles des Européens.

En effet, le Safe Harbor a d'abord fait l'objet d'une invalidation par la CJUE au regard de la directive de 1995 (A), avant que le Privacy Shield ne connaisse le même sort sous l'empire du RGPD (B).

A - L'invalidation du Safe Harbor, le manque de protection des données de santé au regard de la directive de 1995

Sous l'empire de la directive de 1995[53], les transferts de données entre les Etats-Unis et l'Europe étaient encadrés par la décision d'adéquation n°2000/520[54] dite « Safe Harbor » de la Commission européenne. Dans l'affaire dite « Schrems I[55] » était en cause le transfert de données d'utilisateurs résidant en Europe d'un réseau social vers des serveurs américains. La CJCE a été amenée à se prononcer sur le point de savoir si la décision d'adéquation permettait d'assurer un niveau de protection des données personnelles équivalent à celui requis en Europe. Elle invalide la décision le 6 octobre 2015. La CJCE soulève le fait que les principes de protection contenus par la décision d'adéquation de s'appliquent pas aux autorités américaines. Dès lors, si une société américaine adhère à la sphère de sécurité, alors cela entraine « présomption de niveau de protection adéquat des données »[56] mais cela ne garantit pas que les autorités américaines n'y aient pas accès. Cela porte atteinte au droit au respect de la vie privée garanti par la Charte fondamentale des Droits de l'Union. La CJCE note également que les sociétés adhérentes à la sphère de sécurité doivent écarter ses principes protecteurs dès lors qu'elles font face à des exigences de sécurité nationale américaine, d'intérêt public et de respect des lois américaines. Enfin, la Cour relève qu'il n'y a aucun système de recours effectif en vigueur aux Etats-Unis qui permette aux Européens d'obtenir réparation du dommage qui résulterait de l'accès à ses données personnelles. Dès lors, pour transférer des données aux Etats-Unis il n'était plus possible de se fonder sur la décision d'adéquation, il fallait se fonder sur les garanties appropriées.

---

[53] PARLEMENT EUROPÉEN ET CONSEIL, Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[54] COMMISSION EUROPÉENNE, Décision du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique.

[55] CJUE, Arrêt de la Cour (grande chambre) du 6 octobre 2015, Maximillian Schrems contre Data Protection Commissioner. Demande de décision préjudicielle, introduite par la High Court (Irlande), C-362/14.

[56] *Ibid*.

Cette affaire Schrems illustre pour la première fois la volonté de la CJCE de protéger largement les données personnelles des européens face aux ingérences des autorités américaines[57]. Il s'agit d'un pas en faveur de la souveraineté numérique. Ainsi, avant même que le RGPD n'entre en vigueur et le développement des services de cloud, l'Europe et la CJCE se sont saisis de la problématique de l'hébergement des données européennes sur des serveurs situés aux Etats-Unis. Cette décision marque le début d'un mouvement jurisprudentiel concernant l'hébergement des données sur des cloud non souverains. Prémisse de la question de l'hébergement des données de santé, la CJCE rend une décision en faveur de la protection des données personnelles des Européens. Un an plus tard, une nouvelle décision d'adéquation dite « Privacy Shield » est rendue par la Commission européenne. Cette dernière sera invalidée une nouvelle fois par la CJUE, cette fois-ci sous l'empire des principes de RGPD. Cela va donner lieu à d'autres décisions en droit national qui vont permettre d'aborder plus particulièrement la question de l'hébergement des données sur des services de cloud soumis au droit américain. De plus, cela permet d'illustrer la difficulté à conjuguer deux objectifs qui semblent presque être trop contradictoires pour être conciliés[58].

B - L'invalidation du Privacy Shield, le manque de protection des données de santé au regard du RGPD

Le 1er aout 2016, une nouvelle décision d'adéquation de la Commission européenne[59] en faveur des transferts de données entre l'Europe et les Etats-Unis entre en vigueur[60]. Il s'agit du « Bouclier de protection des données » ou « Privacy Shield ». C'est un mécanisme d'auto-certification des entreprises américaines qui se voient transférer des données depuis l'Europe. La Commission européenne reconnait ainsi que le niveau de protection à l'égard des

[57] LASSALLE Maxine, « La responsabilisation des acteurs du numérique dans le transfert de données personnelles vers des Etats tiers », Revue Lamy Droit de l'Immatériel, n°173, 1er août 2020.

[58] DARNAULT Cécilia, « Les outils de transfert des données hors UE », *Les outils de transfert des données hors UE,* Observatoire de la Compliance, 19 août 2021.

[59] CJUE, Décision d'exécution (UE) 2023/1795 de la Commission du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis. C/2023/4745.

[60] COMMISSION EUROPÉENNE, « Le bouclier de protection des données UE-Etats-Unis : Foire aux questions », Fiche d'information, 12 juillet 2016.

données est équivalent à celui conféré par le chapitre 5 du RGPD[61] et permet donc le transfert des données vers les entreprises certifiées.

Le 16 juillet 2020, la CJUE rend un arrêt dit « Schrems II »[62] et invalide la décision d'adéquation de la Commission européenne. A partir de cette date, le niveau de protection n'est plus équivalent à celui du RGPD, les transferts de données vers les Etats-Unis ne peuvent plus avoir lieu en vertu de la décision Privacy Shield. Cette décision est notamment fondée sur l'extraterritorialité de certaines lois américaines[63] qui permet aux autorités d'accéder aux données européennes dans des conditions qui ne sont pas celles d'une protection suffisante pour la CJUE. Afin de ne pas bloquer tout transfert, la CJUE a admis la validité de principe du recours à l'article 46 du RGPD[64] qui prévoit le recours aux CCT pour encadrer les transferts.

La validité de ces clauses doit faire l'objet d'une analyse au cas par cas[65]. Le CJUE précise que pour le cas spécifique du transfert de l'UE vers les Etats-Unis il existe un risque que les données soient accessibles aux autorités publiques ce qui illustre l'insuffisance de protection des droits des personnes concernées. Dès lors, des mesures des protections supplémentaires aux CCT devaient être prises pour le cas spécifique du transfert vers les Etats-Unis[66].

Les décisions de la jurisprudence française sont venues apporter des précisions quant à la mise en œuvre des transferts UE-Etats-Unis dans le cadre, notamment, de la question de l'hébergement des données de santé sur des cloud américains.

---

[61] RGPD, Chapitre 5.

[62] CJUE, Arrêt de la Cour (grande chambre) du 16 juillet 2020. Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems. Demande de décision préjudicielle, introduite par la High Court (Irlande), C-311/18.

[63] MERMET Mahaut, « Lois de surveillance et protection des données personnelles – Ou une analyse de l'arrêt Schrems II », Mémoire sous la direction de Maître Lorraine Maisnier-Boché, Université Panthéon-Assas, 2020-2021.

[64] RGPD, article 46. 2. c) et d).

[65] PADOVA Yann, « Les transferts internationaux de données, entre approche par les risques et positions de principe », Commentaire critique des recommandations de l'E DPB 01/2020 (PARTIE I), Revue Lamy Droit de l'Immatériel, nº 184, 1er août 2021.

[66] *Supra note n°57.*

Le 13 octobre 2020, le Conseil d'Etat rend une décision en référé concernant le Health Data Hub[67]. Le 15 avril 2020, le HDH signe un contrat avec une filiale irlandaise de Microsoft pour héberger les données de santé de la PDS[68]. Cela constitue de possibles transferts de données vers les Etats-Unis et c'est sur ce fondement qu'il a été demandé au juge du référé-liberté de suspendre le traitement des données. Dans une ordonnance du 13 octobre 2020[69], le Conseil d'Etat reconnait qu'il « n'est pas exclu que les autorités américaines aient accès aux données » de santé via sa filiale irlandaise, même si ces données sont sur des serveurs physiquement situés dans l'Union. Toutefois, cela ne constitue pas une illégalité grave et manifeste qui nécessiterait de suspendre immédiatement le traitement de données par le HDH. Le juge justifie cela par le fait que la CJUE n'a pas interdit de confier le traitement à une société américaine et par le fait que la violation au RGPD serait caractérisée si la filiale ne pouvait pas d'opposer à une telle demande des autorités américaines. Le Conseil d'Etat relève également que les données de santé sont pseudonymisées et qu'il est d'intérêt public de permettre l'utilisation des données de santé dans le cadre de l'épidémie de Covid-19.
Le Conseil d'Etat demande tout de même au HDH de travailler avec Microsoft sous le contrôle de la CNIL pour renforcer la protection des droits des personnes à l'égard de leurs données de santé.

Le Conseil d'Etat a rendu une autre décision concernant les données de santé, il s'agit d'une décision Doctolib du 12 mars 2021[70]. Toujours dans le contexte de la pandémie de Covid-19, la gestion de la prise de rendez-vous sur internet pour la vaccination a été confiée à Doctolib qui a eu recours à la société AWS, filiale de la société américaine Amazon Web Services Inc.
Des associations et syndicats professionnels de la santé ont demandé au juge des référés du Conseil d'État de suspendre le partenariat entre le ministère de la Santé et Doctolib, invoquant

---

[67] CONSEIL D'ETAT, Juges des référés, 13 octobre 2020, 444937, Recueil Lebon.

[68] CONSEIL D'ETAT, « Health Data Hub et protection de données personnelles : des précautions doivent être prises dans l'attente d'une solution pérenne », Actualités, 14 octobre 2020.

[69] CNIL, « Le Conseil d'Etat demande au Health Data Hub des garanties supplémentaires pour limiter le risque de transfert vers les Etats-Unis », Avis du 14 octobre 2020.

[70] CONSEIL D'ETAT, Communiqué de presse, Le juge des référés ne suspend pas le partenariat entre le ministère de la santé et Doctolib pour la gestion des rendez-vous de vaccination contre la covid-19, 12 mars 2021.

des risques liés à l'hébergement des données par une filiale d'une société américaine, notamment le risque d'accès par les autorités américaines[71]. Par une ordonnance du 12 mars 2021, le Conseil d'État a rejeté cette demande. Il a d'abord souligné que les données recueillies lors des rendez-vous de vaccination ne comportaient pas de données de santé sensibles. En outre, le Conseil d'État a noté que des garanties robustes avaient été mises en place pour protéger contre d'éventuelles demandes d'accès par les autorités américaines. Ces garanties comprenaient un contrat entre Doctolib et AWS, précisant une procédure pour contester toute demande d'accès ne respectant pas la réglementation européenne, ainsi qu'un dispositif de sécurisation des données par chiffrement, supervisé par un tiers de confiance situé en France, empêchant ainsi la lecture des données par des tiers non autorisés. En conclusion, le Conseil d'État a estimé que les mesures de protection mises en place étaient suffisantes pour répondre aux préoccupations des requérants, justifiant ainsi le maintien du partenariat entre le ministère de la Santé et Doctolib.

Ainsi, la problématique de l'hébergement des données de santé européennes sur des services de cloud américains n'est pas nouvelle. Les craintes d'un accès illégitime des autorités américaines se font ressentir, poussant les autorités nationales et européennes à réagir. Toutefois, aucune mesure concrète ne semble clairement pouvoir faire face à ce possible accès américain, si ce n'est un arrêt du traitement. Cependant, les cloud américains semblaient alors les seuls capables de répondre aux exigences techniques de l'hébergement des données de santé notamment, éloignant l'idée d'une souveraineté numérique à l'égard de ces données.

L'invalidation de ces deux décisions d'adéquation illustre la difficulté à concilier les exigences de souveraineté à l'égard des données de santé et la nécessité de maintenir les flux internationaux de données. Les contestations à ce sujet ont été prises en compte et une nouvelle décision d'adéquation a été adoptée par la Commission européenne suite aux engagements pris par les Etats-Unis. Toutefois, il n'est pas certain que cette décision permette d'assurer pleinement la souveraineté numérique.

[71] VITARD Alice, « Le cloud souverain n'est-il qu'un fantasme ? », L'Usine digitale, 20 octobre 2021.

II - Le Data Privacy Framework, la consécration contestée d'une nouvelle décision d'adéquation encadrant les transferts

Une nouvelle décision d'adéquation Data Privacy Framework encadre les transferts de données vers les Etats-Unis. Si celle-ci prend en compte les critiques passées en introduisant certains principes du RGPD, l'accès des autorités américaines est toujours possible puisqu'aucun rempart n'est dressé contre le caractère extraterritorial de certaines de lois.

Ainsi, la décision encadrant actuellement les transferts de données vers les Etats-Unis a pris en considération les critiques qui avaient conduit à l'invalidation des décisions Schrems I et Schrems II (A). Cette décision reste toutefois contestée au point d'être l'objet de recours car elle ne permettrait pas de garantir l'immunité des données personnelles des Européens face à un accès potentiel des autorités étrangères (B).

A - Le DPF, une décision d'adéquation prise en considération des critiques passées

Le 10 juillet 2023, la Commission européenne adopte une nouvelle décision d'adéquation en faveur des transferts de données entre les Etats-Unis et l'Europe[72].
Cette décision d'adéquation encadre les transferts de manière sectorielle[73]. En effet, seules les entreprises qui relèvent du département du commerce ou du transport peuvent adhérer à l'accord. Elles s'engagent ainsi annuellement à respecter les principes du cadre prévu. Cela repose sur un mécanisme d'auto-certification, comme pour le Privacy Shield, à renouveler chaque année. Les entreprises auto-certifiées peuvent ainsi recevoir les données transférées de la part d'organismes européens soumis au droit européen et particulièrement au RGPD[74].

---

[72] COMMISSION EUROPÉENNE, Adequacy decision for the EU-US Data Privacy Framework, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework 10 juillet 2023.

[73] ROSIER Karen et DE TERWANGNE Cécile, « Le règlement général sur la protection des données », Chapitre 3 - L'acceptation des modes alternatifs de régulation et les flux transfrontaliers, Section 2 - Les mécanismes alternatifs dans le cadre du « Privacy Shield », 2018, p. 357.

[74] G'SELL Florence, « L'avenir incertain des flux de données transatlantiques - Les constats multiples d'une souveraineté numérique déficiente », Enjeux numériques n°23, Annales des Mines, septembre 2023.

C’est aux organismes soumis au droit européen de vérifier qu’ils transfèrent les données vers d’autres organismes américains certifiés. Le 18 juillet, le CEPD a publié une note permettant de préciser certains principes du DPF[75]. Si l’organisme en question ne relève pas de la liste des organismes certifiés assurant un niveau de protection des données équivalent, aucun transfert ne peut être fondé sur la décision d’adéquation. Il faudra passer par le mécanisme classique des garanties appropriées.

Sur le fond, la décision d’adéquation reprend certains principes de la décision Privacy Shield en y ajoutant certains principes du RGPD et des voies de recours effectives. Cela permet de répondre aux critiques qui avaient fondé l’annulation de cette décision. Le principe de détermination des finalités est ainsi consacré[76]. Il en est de même pour le principe de limitation dans la collecte des données[77]. Cela confère à la décision des principes similaires à la conception européenne de la protection des données de santé en tant que droit fondamental. Également, un droit au recours est consacré dans la législation américaine. En effet, il est toujours permis aux autorités américaines d’accéder aux données personnelles transférées, mais cela doit être fait sur accord et sous le contrôle d’un juge. Ce recours s’exercera devant une nouvelle Cour dédiée, la Data Protection Review Court.

Ces nouvelles exigences s’appliquent à l’hébergement des données de santé du HDH chez Microsoft Azure. En effet, Microsoft Azure est une société sous la tutelle du département du commerce américain. Dès lors, la décision d’adéquation peut lui être appliquée. Microsoft s’est auto-certifiée conforme au DPF[78]. Ainsi, le HDH en tant qu’exportateur de données européen soumis au RGPD peut transférer les données afin qu’elles soient hébergées chez Microsoft Azure, société américaine offrant une protection équivalente à celle du RGPD en vertu de la décision d’adéquation[79] .

---

[75] LENOIR Noëlle, « La Commission européenne valide les conditions de l'adéquation des États-Unis à la libre circulation des données personnelles de part et d'autre de l’Atlantique », Petites affiches, n°07-08, Labase-Lextenso, 31 août 2023, p.5.

[76] RGPD, article 5. 1. b).

[77] RGPD, article 5. 1. c).

[78] BOSSY MALAFOSSE Jeanne, « La Commission européenne valide le nouvel accord de protection des données entre l’Europe et les Etats-Unis », DELSOL Avocats, Blog Données personnelles, 11 juillet 2023.

[79] *Ibid*.

Une telle certification rassure quant au niveau de sécurité dont bénéficient les données de santé du HDH. Des garanties supplémentaires sont apportées pour répondre aux craintes d'accès par les autorités américaines aux données. Il s'agit d'un pas en avant pour concilier la protection des données sensibles et leur transfert à l'étranger. Cependant, si Microsoft Azure est certifiée comme assurant une telle protection à l'égard des données, cela ne semble pas être satisfaisant pour certains acteurs de l'écosystème des données de santé. En effet, rien dans le DPF ne confère aux données de santé des garanties supplémentaires au titre de leur sensibilité. De plus, un accès aux données par les autorités américaines reste possible. La souveraineté à l'égard des données de santé n'est pas abordée, ce qui donne lieu à de nombreuses contestations.

B - Le DPF, une décision d'adéquation demeurant contestée

La décision DPF a fait l'objet de nombreuses critiques. Tout d'abord, le CEPD s'était montré réservé[80] à l'idée de l'adoption de cette décision et le Parlement européen s'y été opposé[81]. La CNIL s'est prononcée favorablement à cette nouvelle décision en affirmant que « les transferts de données personnelles depuis l'Union européenne vers les organismes peuvent donc s'effectuer librement, sans encadrement spécifique par des « clauses contractuelles types » ou un autre instrument de transfert[82] ». Ainsi, avant même son adoption, la décision d'adéquation était sujette à débat.

Cette décision n'a pas encore été jugée par la CJUE sur le fond. Cela pourrait vraisemblablement arriver. Deux recours ont déjà été introduits[83]. Un par l'association NOYB

[80] COMMISSION EUROPÉENNE, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. 28 février 2023.

[81] *Ibid* et HAAS AVOCATS, « Accord UE-US sur le transfert des données : un pastiche shield ? », Blog du cabinet HAAS Avocats, 4 septembre 2023.

[82] CNIL, « Transferts de données vers les États-Unis : la Commission européenne adopte une nouvelle décision d'adéquation », Transferts de données vers les États-Unis : la Commission européenne adopte une nouvelle décision d'adéquation, 10 juillet 2023.

[83] CHAGNY Murielle, « Les transferts intra et extra-communautaires », Le Lamy Droit économique, Partie 5, Livre 1, Titre 2, Chapitre 1, Section 5 La règlementation des transferts internationaux des données, point 4879, mis à jour 02/2024.

de Maximilien Schrems[84] et l'autre par le député et membre de la CNIL Philippe Latombe[85]. Le recours de ce dernier a été écarté au motif qu'il ne subissait pas de préjudice grave[86]. Il reprochait à la décision de n'être conforme ni au RGPD ni à la Charte des Droits fondamentaux de l'UE.

Maximilien Schrems lui, relève que même si les principes de nécessité et de proportionnalité ont été consacrés dans le texte du DPF, le système judiciaire américain n'en a pas la même définition, ce qui fait craindre qu'en pratique rien ne change réellement. Concernant le recours des Européens permettant de voir le préjudice subi par l'accès aux données par les autorités américaines réparé devant une cour spéciale, Maximilien Schrems émet une réserve quant à l'indépendance de cette Cour. En effet, elle est créée par décret présidentiel et est rattachée à l'exécutif américain.

Plus particulièrement concernant les données de santé, le texte du DPF ne prévoit aucune disposition propre aux données de santé. Ainsi, le transfert de telles données ne fait pas l'objet de mesures de protection plus strictes qui auraient pu être justifiées par leur caractère sensible. Cela aurait pu permettre au HDH de transférer ses données de santé de manière plus sécurisée. Cela aurait également permis de renforcer la souveraineté de l'UE à l'égard de ses données et de rassurer les personnes concernées quant au sort de leurs données les plus intimes.

Enfin, rien n'est prévu concernant le cas où la décision DPF serait invalidée par la CJUE, ce qui ne semble pas inenvisageable au regard des différents recours déjà déposés. Dans un tel cas, il faudra revenir au mécanisme de garanties appropriées, telles que les clauses contractuelles types. Que se passerait-il alors pour les données de santé du HDH déjà transférées sur les cloud américains ? Il faut imaginer qu'un tel traitement serait interrompu et que toutes les personnes dont les données ont déjà été transférées puissent alors introduire un recours, le manque de sécurité à l'égard de leurs données étant alors confirmé.

---

[84] NOYB Association, « La Commission européenne soumet les transferts de données entre l'UE et les Etats-Unis à un troisième examen par la CJUE », News Noyb Data Transfers, 10 juillet 2023.

[85] SCHMIEDT Morgan, « DATA PRIVACY FRAMEWORK – Le député et membre de la CNIL Phillipe Latombe dépose un recours à la CJUE pour obtenir l'annulation de la décision d'adéquation avec les États-Unis », Blog eWatchers.org, Information du 8 septembre 2023.

[86] ORDONNANCE DU PRÉSIDENT DU TRIBUNAL « Référé – Protection des données à caractère personnel – Cadre de protection des données UE-États-Unis – Décision constatant l'adéquation du niveau de protection – Demande de sursis à exécution – Défaut d'urgence », 12 octobre 2023.

Ainsi, jusqu'à l'actuel DPF encadrant les transferts vers les Etats-Unis, l'hébergement de données santé sur des cloud américains est contesté car il ne semble pas permettre la réalisation de la souveraineté numérique à l'égard des données de santé. Le caractère sensible de ces données voudrait que leur soit appliqué un régime spécifiquement protecteur pour assurer un transfert vers les Etats-Unis à l'abri de l'extraterritorialité des lois américaines. Toutefois, de tels transferts internationaux doivent rester possibles pour favoriser la recherche et ne pas brider l'innovation. Cela transparait au travers de la volonté de la Commission européenne de permettre de tels transferts en adoptant de nouvelles décisions d'adéquation malgré le caractère sensible de certaines données.

Aujourd'hui, le DPF répond à certaines inquiétudes émises lors de l'invalidation du Safe Harbor et du Privacy Shield mais ne permet pas d'affirmer que la souveraineté numérique est pleinement assurée en France et dans l'UE.

Puisque la conciliation entre la souveraineté numérique et le besoin d'assurer les flux UE-Etats-Unis semble difficilement envisageable, il faut se pencher sur d'autres mécanismes permettant de garder un certain contrôle sur ses données de santé sans pour autant brider les initiatives nécessaires au développement du soin et de la recherche. Cela se concrétise avec l'apparition de différents agréments et certifications, nationaux et bientôt européen, qui s'imposent aux hébergeurs de données de santé. Toutefois, de tels mécanismes illustrent les désaccords et les divergences quant aux critères à mettre en place dans ces référentiels. Ces désaccords montrent encore une fois la difficulté de parvenir à une conciliation entre les enjeux de vie privée et de sécurité des données et ceux des flux internationaux de données de santé. Par ailleurs, tous les acteurs de l'écosystème de l'hébergement des données de santé sont concernés et les hébergeurs, souverains comme non souverains, prennent des initiatives pour faire entendre leur voix dans ces débats.

Chapitre 2 : Le nécessaire renforcement des mesures d'encadrement de l'hébergement des données de santé vers les Etats-Unis

À l'heure actuelle, l'hébergement des données de santé sur des cloud américains est encadré par une décision d'adéquation de la Commission européenne. Face à une conciliation

qui semble impossible entre les exigences de souveraineté numérique et celles en faveur des flux de données internationaux, d'autres mécanismes de protection sont envisagés. Différents référentiels voient le jour et s'imposent aux hébergeurs de données de santé. Toutefois, leurs critères parfois discordants illustrent les désaccords entre la politique européenne qui autorise les transferts vers les Etats-Unis et la politique française très axée sur la souveraineté numérique. Les différents référentiels français ne s'alignent pas sur les mêmes exigences créant des incertitudes juridiques à l'égard des hébergeurs souverains qui souhaitent être en mesure d'héberger les données du Health Data Hub rapidement. De plus, l'Union européenne a fait connaitre sa volonté de parvenir à une certification européenne qui remplacerait les certifications nationales avec un référentiel encore différent, complexifiant encore la situation des hébergeurs de données de santé. Dès lors, dans une volonté de maintenir le partage de données de santé, les hébergeurs souverains et non souverains tentent de démontrer leur conformité aux politiques européenne et française.

Ainsi, les critères discordants de certification des hébergeurs de santé (Section 1) conduisent les acteurs de l'écosystème de cloud à prendre part aux discussions en apportant leurs initiatives (Section 2).

Section 1 : Les critères discordants de certification des hébergeurs de données de santé

La France a mis en place des référentiels permettant de certifier les hébergeurs de données de santé comme assurant le niveau de protection nécessaire pour ces données. Le référentiel HDS est propre aux données de santé tandis que le référentiel SecNumCloud s'applique à tout hébergeur. Leurs exigences sont différentes, en particulier sur le point de l'immunité des données face à un accès des autorités américaines en vertu de l'extraterritorialité de certaines lois. En effet, la doctrine « cloud au centre » avait pour ambition d'imposer une telle exigence aux hébergeurs. Cette doctrine ambitieuse est reconsidérée au regard de la décision de la CNIL autorisant l'hébergement de l'entrepôt de données de santé EMC2 sur un cloud américain, illustrant la difficulté à concilier la souveraineté numérique avec les exigences techniques d'un tel hébergement.

Ainsi, si l'évolution du référentiel HDS va dans le sens de la souveraineté numérique (I), cette volonté d'y parvenir est à nuancer au vu de l'ambiguïté de la doctrine « cloud au centre » (II).

I - L'évolution du référentiel HDS vers un renfort de la souveraineté à l'égard des données de santé

La certification HDS est obligatoire pour tout hébergeur qui souhaite héberger des données de santé. Il s'agit d'une certification propre à ce type de donnée dont les critères ont été renouvelés en mai 2024. Ce renouvellement des critères porte en particulier sur les transferts de données hors de l'EEE et permet d'illustrer la politique française en faveur de la souveraineté numérique. Cependant, l'absence d'alignement sur les critères d'autres certifications plus protectrices met à mal cette politique.

Si les critères du référentiel HDS ont été renouvelés vers un encadrement renforcé des transferts de données favorisant la souveraineté numérique (A), cela est remis en cause par l'absence d'alignement des critères sur la certification SecNumCloud (B).

A - Le renouvellement des critères pour un meilleur encadrement de l'hébergement aux Etats-Unis

Le décret n° 2018-137 du 26 février 2018[87] sur l'hébergement de données de santé à caractère personnel a introduit la certification HDS pour assurer la sécurité de ces données en France. C'est une certification propre à l'hébergement des données de santé. L'article L. 1111-8 du CSP[88] dispose que « tous les organismes publics ou privés qui hébergent, exploitent le système d'information de santé, ou réalisent des sauvegardes pour le compte d'un établissement de santé ou d'un tiers de santé doivent être certifiés HDS, à l'exception des services d'archivages informatiques qui ne sont pas concernés par ces obligations[89]. » Il s'agit

[87] MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ, Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel, JOFR n°0049 du 28 février 2018, Texte n° 16.

[88] Code de la santé publique, article L.1111-8, modifié par la loi n° 2016-41 du 26 janvier 2016.

[89] ANS, « HDS Certification Hébergeur de Données de Santé » Publication en ligne, Consultée le 13 mai 2024.

donc d'une obligation pour les sociétés proposant des services de cloud qui souhaitent héberger les données de santé. Microsoft Azure est certifiée HDS[90]. L'hébergeur du HDH est donc conforme au référentiel de certification.

L'attribution de cette certification découle d'une évaluation au référentiel de certification[91] par un organisme certificateur[92] au terme d'une procédure d'audits documentaire et sur site. Si l'hébergeur est conforme au référentiel, un certificat lui est délivré pour trois ans et un audit de surveillance se déroulera chaque année. C'est l'hébergeur des données de santé qui doit être certifié HDS. Ainsi, si une société sous-traite ce service d'hébergement cloud, le sous-traitant devra être titulaire de la certification. Le référentiel prévoit notamment un alignement sur les exigences de la norme ISO 27 001.

En 2022, l'Agence du Numérique en Santé (ANS) et la Délégation du numérique en Santé (DNS) ont annoncé un projet de révision du référentiel de certification HDS[93]. Une consultation publique a eu lieu la même année pour statuer sur ce texte. Le 13 juillet 2023, la CNIL s'est prononcée favorablement au projet de révision[94] tel qu'il a été modifié après la consultation publique[95]. Fin 2023, le projet d'arrêté qui approuve les projets de référentiel révisé a été soumis à la Commission européenne[96]. Ayant jusqu'au 6 mars 2024 pour faire connaitre ses objections et son silence valant accord, le projet de révision va être publié au Journal Officiel dans quelque temps et entrera en vigueur en novembre 2024[97]. Dans un

---

[90] DHURATA Jahiu, MAZZOLI Robert, « Hébergement de données de santé (HDS) », MICROSOFT AZURE, Article, France, 31 janvier 2024.

[91] ANS, Certification HDS – Référentiel d'accréditation, Version 1. 1 finale, Mai 2018.

[92] ANS, « Certification des hébergeurs de données de santé », publication en ligne, consultée le 8 mai 2024.

[93] ANS, « Hébergement des données de santé (HDS) : évolution des référentiels de certification et d'accréditation », ANS Actualités, 27 décembre 2023.

[94] CNIL, Ordre du jour de la séance plénière du 13 juillet 2023, 17 juillet 2023.

[95] DERRIENNIC ASSOCIÉS, « Certification HDS : un nouveau « nouveau projet de référentiel », Blog Derriennic Associés, 18 janvier 2024.

[96] COMMISSION EUROPÉENNE, Arrêté modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel, 6 mars 2024.

[97] BONFILLON Romain, « Nouveau référentiel HDS : ce qu'il va changer pour l'écosystème de la santé », MIND HEALTH, 6 mars 2024, mis à jour le 7 mars 2024.

communiqué du 26 avril 2024[98], l'ANS publie la cinquième version de la doctrine du numérique en santé dans laquelle elle intègre la version révisée du référentiel HDS[99].

Le projet de révision du référentiel de certification HDS comprend des modifications en faveur de la souveraineté numérique et de l'hébergement sur le territoire de l'EEE. Il s'agit dans un premier temps de préciser la définition de l'activité d'administration et d'exploitation des systèmes de santé (activité n°5) pour expliciter les activités pour lesquelles la certification a été obtenue. Il s'agit également d'intégrer les évolutions de la norme ISO 27 001 au référentiel HDS. Enfin, cela permettra de clarifier les obligations contractuelles de l'hébergeur et d'améliorer la lisibilité des garanties qu'il apporte[100].

Plus précisément sur la question des transferts des données de santé hors EEE et en faveur d'une souveraineté renforcée à l'égard des données de santé[101], quatre nouvelles exigences apparaissent au Point 7 du nouveau référentiel[102].

Premièrement, concernant la localisation des données de santé, l'exigence 28 dispose que ces données doivent physiquement être hébergées dans un pays membre de l'EEE. Cela est clairement en faveur d'une meilleure protection des données et en faveur des hébergeurs localisés sur le territoire européen. En effet, cette exigence impose que les données de santé ne soient pas stockées sur un cloud extraeuropéen tel que Microsoft Azure. Dès lors, seuls les cloud européens pourront héberger les données de santé européennes telles que celles du Health Data Hub. Deuxièmement, les exigences 29 et 30 précisent la situation dans laquelle un accès aux données aurait lieu depuis un Etat hors de l'UE. Cela englobe l'hypothèse dans laquelle l'hébergeur ou le sous-traitant accèdent aux données depuis un pays hors de l'EEE ou s'ils sont soumis à une législation extraeuropéenne dont le niveau de sécurité prévu n'est pas équivalent à celui de l'article 45 du RGPD. Dans ces hypothèses, le client doit en être informé dans le contrat. Le contrat doit en sus préciser les risques associés à un tel accès et les

---

[98] ANS, « Publication de la doctrine du numérique en santé » Communiqué de presse, Version 2023, 26 avril 2024.

[99] CARAVAGNA Léo, « Publication de la nouvelle version de la doctrine du numérique en santé », TICSANTÉ.com, 3 mai 2024.

[100] *Supra note n°95.*

[101] DE MOTA Thomas, « Le référentiel HDS : l'évolution », Le Club Cyber.com, 15 décembre 2023.

[102] *Supra note n°95.*

mesures techniques et juridiques prises pour les atténuer. Si la possibilité d'un accès extra-européen aux données de santé européennes n'est pas interdite, elle est encadrée. Cela permet d'assurer que cet accès, qui semble pour l'heure impossible à éviter, soit encadré juridiquement et techniquement. Cela permet aussi que la personne concernée soit informée d'un tel accès et puisse consentir au traitement en connaissance de cause. Troisièmement, l'exigence n°31 oblige les hébergeurs cloud à publier sur leur site internet tous les transferts de données hors de l'EEE auxquels ils s'adonnent. Cela s'inscrit dans une logique de transparence.

Ainsi, pour pouvoir héberger le HDH, les hébergeurs, qu'ils soient souverains ou non, devront se conformer aux nouvelles exigences de transparence et de souveraineté à l'égard des données de santé. Avoir une certification propre aux hébergeurs de santé permet d'instaurer un niveau de protection qui leur est propre compte tenu de leur caractère sensible. Cette évolution illustre la position française en faveur de la souveraineté numérique. Toutefois, cela est nuancé par le fait que la certification propre aux données de santé n'est pas la plus exigeante et ne permet pas une immunité des données de santé face à l'accès des autorités américaines.

La version finale du référentiel a pu être critiquée car elle n'impose pas la certification SecNumCloud mais propose plutôt une « matrice de correspondance SecNumCloud et ISO 27 001[103] » qui abaisse le niveau d'exigence en faveur de la souveraineté numérique. L'obligation d'héberger physiquement les données sur le territoire de l'Union est vue par certains comme un abaissement du niveau d'exigence au respect d'une « recommandation du CEPD en matière de transfert hors UE et des obligations d'information[104] ». Il faut toutefois souligner que d'un point de vue pratique, cela permet aux hébergeurs de se conformer plus facilement, certains craignant de ne pas être capables de se conformer au nouveau référentiel dans les délais impartis[105].

Cela rend l'articulation des règles complexe et illustre la difficulté de concilier des exigences de sécurité techniques avec l'impératif de partage de données de santé à une échelle européenne, voire internationale.

---

[103] *Ibid*.

[104] *Ibid*.

[105] DESMARAIS Pierre, « HDSv2 : Les référentiels 2024 prennent de front la CJUE et le CE », Blog Desmarais-Avocats, 22 mai 2024.

B - La certification HDS, une certification indépendante des critères de la certification SecNumCloud

Aujourd'hui, ce sont près des trois cents sociétés qui sont certifiées HDS[106]. La certification HDS est propre aux données de santé qui sont des données sensibles qui entrent donc dans la catégorie des données qui requièrent la plus grande protection contre les accès d'autorités tiers. La nouvelle version du référentiel a été publiée le 16 mai 2024[107]. Il faut noter que le référentiel HDS ne fait pas état d'exigences permettant une immunité des données de santé européennes face aux potentiels accès de puissances étrangères. Cela peut paraitre étonnant, d'autant que la certification SecNumCloud, qui sera abordée ensuite, le requiert alors qu'elle n'est pas spécifiquement créée pour encadrer le traitement des données de santé.

L'obligation d'être certifié SecNumCloud en plus de HDS pour héberger les données de santé avait été proposée dans le cadre des discussions autour du projet de loi[108] visant à sécuriser et réguler l'espace numérique[109] (loi SREN). Cette loi a été promulguée au Journal Officiel le 22 mai 2024[110]. En effet, le député Philippe Latombe avait proposé un amendement[111] visant à modifier l'article L. 1111-8 pour y introduire l'obligation de certification SecNumCloud « à compter du 1er juillet 2024, en cas d'archivage numérique au

---

[106] ANS, Liste des hébergeurs certifiés, 11 avril 2024.

[107] *Supra note n°95.*

[108] ASSEMBLÉE NATIONALE, « Compte rendu Commission spéciale chargée d'examiner le projet de loi visant à sécuriser et réguler l'espace numérique », Compte-rendu n°7, 21 septembre 2023.

[109] ASSEMBLÉE NATIONALE, Projet de loi visant à sécuriser et réguler l'espace numérique (ECOI2309270L). Dernière modification : 20 octobre 2023.

[110] LOI n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique – Journal officiel n°0117 du 22 mai 2024.

[111] SÉNAT, Amendement n°CS765, Projet de loi n°1514, adopté par le Sénat visant à sécuriser et réguler l'espace numérique, déposé le 15 septembre 2023.

moyen d'un service d'informatique en nuage[112] ». Cet amendement a été écarté dans la version finale du texte qui a été adoptée le 10 avril 2024[113].

Sans aller jusqu'à une telle exigence, la souveraineté reste en partie assurée par l'exigence de certification HDS pour l'archivage électronique des données de santé par les hébergeurs de cloud à compter du 1er juin 2025[114]. Ainsi, l'article L. 1111-8 étend le référentiel HDS aux fournisseurs de service d'archivage numérique de ces données à l'issue de leur durée de conservation au sens du RGPD[115].

Cette absence d'alignement des exigences de la certification HDS sur celles de SecNumCloud surprend mais permet de conserver deux certifications complémentaires différentes. Ces deux niveaux d'exigences pourraient permettre aux cloud de se conformer de manière graduée à un référentiel de moindre exigence dans un premier temps puis de converger vers une certification plus exigeante. Toutefois, le fait que ce soit la certification propre à l'encadrement des données les plus sensibles qui soit la moins exigeante peut interroger quant à la pertinence de l'articulation de ces différents niveaux d'exigence. Un début de réponse est donné dans l'avis de la Commission européenne sur le projet de révision du référentiel. Elle n'écarte pas la possibilité d'un alignement sur les exigences de la certification SecNumCloud mais rappelle qu'une future certification européenne pourrait voir le jour. Dès lors, et cela sera abordé ensuite, elle expose que concernant les exigences relatives à la protection face aux normes extraterritoriales de pays tiers, le choix fait est celui de ne pas s'aligner sur les exigences de SecNumCloud en attendant que les critères de la certification EUCS soient tranchés. Ainsi, cette question d'articulation des critères de certification HDS sera réévaluée à l'issue des discussions sur le référentiel EUCS, au plus tard en 2027[116].

---

[112] BRAC DE LA PERRIÈRE Marguerite, « Hébergement de données de santé, décryptage des évolutions à venir », DSIH – L'actualité des systèmes d'information hospitaliers et de la e-santé, 8 janvier 2024.

[113] ASSEMBLÉE NATIONALE, Projet de loi visant à sécuriser et à réguler l'espace numérique, Texte adopté n°286, 10 avril 2024.

[114] DPO Partagé, « Évolution du cadre réglementaire de l'hébergement des données de santé et du marché de l'information en nuage en France », Blog DPO Partagé, 10 avril 2024.

[115] *Ibid*.

[116] CLOUD TEMPLE, « Fiche réglementaire : Le nouvel HDS », 22 avril 2024.

Ainsi, la certification HDS voit ses critères renouvelés vers une meilleure prise en compte des transferts de données de santé vers des pays tiers. Toutefois, cela ne permet pas de retenir des exigences claires en matière d'hébergement des données de santé car les critères de certification HDS ne sont pas les mêmes que ceux requis pour être certifié SecNumCloud. En effet, la doctrine « cloud au centre » a mis en avant cette dernière certification pour garantir un niveau de confidentialité supérieur à ces données, permettant d'instaurer pleinement la souveraineté numérique. Cet engagement est mis à mal par les limites des capacités techniques de certains hébergeurs, menant la CNIL à limiter temporairement les effets de la doctrine.

II - L'ambiguïté de la doctrine « cloud au centre »

La doctrine française « cloud au centre » illustre la position française en faveur de la souveraineté numérique. Elle subordonne l'hébergement des données de santé à l'obtention de la certification SecNumCloud, certification qui pose la condition d'immunité des données de santé face à l'accès des autorités américaines. Toutefois, ce principe n'est pas aligné avec ceux de la certification HDS, créant des incertitudes chez les hébergeurs souverains. De plus, la récente délibération de la CNIL autorisant l'hébergement d'un entrepôt de données de santé chez Microsoft Azure qui n'est pas certifiée SecNumCloud rend la doctrine « cloud au centre » ambigüe dans sa mise en œuvre pratique.

Ainsi, la doctrine « cloud au centre » rend impérative la certification SecNumCloud pour les hébergeurs de santé (A) mais la délibération « EMC2 » de la CNIL illustre les difficultés pratiques d'une telle obligation (B).

A - L'hébergement des données de santé subordonné à l'obtention de la certification SecNumCloud

Pendant longtemps, l'hébergement des données de santé, données les plus intimes, n'a été encadré que par la certification HDS qui n'est pourtant pas la certification la plus

exigeante[117]. La « doctrine cloud au centre » est venue remédier à cela en rendant impérative la certification SecNumCloud[118] pour les hébergeurs cloud qui souhaiteraient héberger les données de santé du Health Data Hub.

SecNumCloud, élaboré par l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information) en 2016 est un référentiel visant à certifier la sécurité des fournisseurs de services cloud pour les entités publiques et privées. Il assure que ces fournisseurs respectent des normes strictes de sécurité, de confidentialité et de résilience, conformes aux standards français, notamment en s'appuyant sur la norme ISO 27001. La version 3.2, sortie en 2022, intègre des mesures supplémentaires de protection contre les lois extraterritoriales, garantissant ainsi que les données personnelles ne seront pas transférées à des autorités étrangères sans justification légale. La version en vigueur aujourd'hui est la version 3.2. Elle joue un rôle particulier dans l'encadrement de l'hébergement cloud des données de santé. En effet, la circulaire de l'Etat du 5 juillet 2021[119] prévoyait pour le cas du « recours à une offre commerciale d'informatique en nuage[120] », de passer par « l'hébergement des données d'une sensibilité particulière par des solutions disposant de la qualification SecNumCloud délivrée par l'Agence nationale de sécurité des systèmes d'information (ou une qualification européenne d'un niveau au moins équivalent) et immunisée contre toute réglementation extracommunautaire[121][122] ». Cela concerne l'usage du cloud par les services de l'État et les organismes sous sa tutelle. Cela a été repris dans la circulaire[123] de la Première ministre Elisabeth Borne, le 1er juin 2023 dans le cadre de la doctrine « cloud au centre ». La doctrine dispose que l'hébergement cloud de données nécessaire à l'accomplissement des missions essentielles de l'Etat, dont fait partie la protection de la santé, doit « impérativement respecter

---

[117] ISSARNI Alain, « Pourquoi il faut renforcer la sécurité des données de santé avec le SecNumCloud », L'Usine Digitale, 11 avril 2024.

[118] PREMIER MINISTRE ET ANSSI, « Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigence », Version 3.2 du 8 mars 2024.

[119] FRANCE RELANCE, « Stratégie nationale pour le cloud », Dossier de presse de France Relance, 17 mai 2021.

[120] *Ibid*.

[121] CARAVAGNA Léo, « Vers une qualification SecNumCloud obligatoire pour l'hébergement de données de santé (circulaire) », TICSANTE.com, *28 juin* 2023.

[122] *Ibid*.

[123] PREMIÈRE MINISTRE, « Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'Etat (« cloud au centre ») », Actualisation de la Circulaire n°6404/SG, 31 mai 2023.

la qualification SecNumCloud ». Dès lors, la protection de la santé implique la protection des données de santé donc cela entre dans le champ de l'obligation d'être certifié SecNumCloud.

Cette obligation est reprise par la CNIL dans un avis[124] du 31 janvier 2024. En effet, elle recommande « pour les bases de données les plus sensibles » dont font partie les bases de données de santé d'assurer une protection importante qui passe nécessairement par l'absence de transfert de données vers des États tiers ainsi que par le « recours à un hébergeur soumis exclusivement au droit européen ou bénéficiant de certifications spécifiques, notamment la certification SecNumCloud de l'ANSSI ». La CNIL justifie ces exigences par la quantité importante de données, et par leur caractère sensible, susceptibles d'être hébergée par le HDH[125].

Ainsi, les autorités françaises ont conscience et se saisissent de la problématique de l'hébergement cloud des données de santé du HDH. Leurs déclarations sont en faveur de l'élaboration d'un cloud souverain au haut niveau de sécurité et en dehors de tout transfert vers un Etat extraeuropéen.

La certification SecNumCloud atteste de mesures techniques, opérationnelles et juridiques qui « garantissent la protection du service cloud vis-à-vis du droit extraeuropéen[126] ». Les mesures juridiques garantissent l'application exclusive du droit européen. Elle doit être renouvelée tous les trois ans. La circulaire de 2023 apporte des précisions sur la question de l'extraterritorialité de lois étrangères et des données sensibles hébergées sur des cloud commerciaux[127].

Tout d'abord, la circulaire fait un rappel du principe quant aux transferts de données de santé vers des pays tiers. Elle appuie sur la nécessité de protéger les données personnelles contre les demandes d'autorités étrangères qui interviendraient en dehors d'un accord en vigueur sur le traitement entre les deux Etats en cause. Il s'agit là du rappel des règles du RGPD selon

---

[124] CNIL, « Les principaux avis et recommandations de la CNIL sur la Plateforme des données de santé », 31 janvier 2024.

[125] *Ibid*.

[126] ANSSI, « SecNumCloud pour les fournisseurs de services Cloud – Pourquoi et comment être qualifié SecNumClou ? », Publié le 29 septembre 2023 mis à jour le 25 avril 2024.

[127] LOUYER Adriane « L'hébergement des données de santé : Un sujet enfin réglé ? ». Blog Houdars & Associés Avocats. 4 juillet 2023.

lesquelles le transfert de données personnelles hors UE est possible à condition de fournir un niveau de protection équivalent à celui de l'Union.

Ensuite, la nouveauté introduite par la circulaire est que la certification SecNumCloud est rendue obligatoire pour toutes les offres de cloud commercial par lesquelles l'Etat ou les organismes sous sa tutelle feraient héberger les données sensibles. Plus précisément, la recommandation n°9 de la circulaire définit ce qui doit être entendu comme une donnée d'une « sensibilité particulière ». Il s'agit des données relevant du secret protégé par la loi telle que le secret médical et de celles nécessaires à l'accomplissement de ses missions essentielles par l'Etat dont la protection de la santé des personnes. Cela englobe donc l'ensemble des données de santé.

Ainsi, lorsque le HDH, GIP sous la tutelle de l'Etat[128], choisit une offre de cloud pour héberger les données de santé, il devrait s'assurer que l'hébergeur choisi est certifié SecNumCloud. Ce n'est pas le cas de Microsoft Azure. Toutefois, la circulaire accorde une période transitoire de douze mois pour se mettre en conformité. Dès lors, il faudrait qu'en juin 2024 le HDH soit hébergé sur un cloud souverain certifié SecNumCloud dans sa dernière version. Il s'agit d'une avancée nécessaire à la création d'un cloud souverain pour héberger les données de santé du HDH en dehors de la portée des lois extraterritoriales étrangères.

Toutefois, s'il était attendu qu'en juin 2024 les données du HDH soient hébergées sur un cloud souverain certifié SecNumCloud, la CNIL a rendu une décision en faveur de l'hébergement d'un entrepôt de données de santé EMC2 chez Microsoft Azure qui laisse penser que cette exigence ne sera pas remplie dans les temps prochains.

B - La remise en cause de la certification SecNumCloud par la décision EMC2

La circulaire « cloud au centre » a renforcé les exigences à l'égard des hébergeurs de données de santé qui doivent impérativement être certifiés SecNumCloud. Cependant, la

[128] LOI n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé. Mis à jour le 28 avril 2021.

CNIL a rendu une délibération[129] dans laquelle elle valide la création d'un entrepôt de données EMC2 par le Health Data Hub hébergé chez Microsoft Azure.

La constitution de cet entrepôt de données de santé vise à favoriser la réalisation de recherches, d'études et d'évaluations. Après avoir relevé la licéité du traitement, la CNIL détaille son raisonnement quant au recours à l'entreprise Microsoft Azure en tant qu'hébergeur de l'entrepôt de données de santé EMC2. En effet, le HDH a choisi Microsoft Azure en tant qu'hébergeur, ce qui pose la question du transfert des données vers les Etats-Unis où les risques d'ingérences des autorités américaines sont importants. Bien que la CNIL valide cet hébergement, son raisonnement témoigne de réticences importantes. Tout d'abord, la CNIL ne nie pas le problème posé par l'hébergement sur un cloud extra-européen non souverain. Si elle rappelle l'existence de la décision d'adéquation Data Privacy Framework, elle rappelle également sa volonté d'assurer la protection des données de santé contre les ingérences étrangères. Cette protection est assurée par le recours à un hébergeur soumis au droit européen exclusivement et titulaire de la certification SecNumCloud, telle que l'exige la recommandation n°9 de la circulaire « cloud au centre »[130].

« Ce choix apparaît en très nette contradiction avec les éléments rappelés ci-dessus[131] ». La CNIL ne cache pas sa position difficile quant à ce choix d'hébergement. Elle semble vouloir montrer que ce n'est pas parce qu'elle valide ce choix qu'il est satisfaisant et qu'il doit être réitéré. Pour justifier cette délibération, elle se fonde sur une mission d'expertise du 13 décembre 2023 qui lui a été remis et qui atteste qu'aucune solution plus satisfaisante n'était proposée par les cloud européens. Cette expertise statue que la mise en place d'un hébergeur souverain spécialement pour l'entrepôt EMC2 retarderait la migration globale du HDH, il est donc recommandé, en attendant la migration du HDH, de recourir à la même solution d'hébergement de Microsoft Azure.

---

[129] CNIL, Délibération n° 2023-146 du 21 décembre 2023 autorisant le groupement d'intérêt public " Plateforme des données de santé " à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données dans le domaine de la santé, dénommé « EMC2 ». (Demande d'autorisation n° 2229962v1). Publié le 31 janvier 2024.

[130] *Ibid*.

[131] *Ibid.*

Une fois encore, la CNIL admet qu'elle « regrette que la stratégie mise en place pour favoriser l'accès des chercheurs aux données de santé n'ait pas fourni l'occasion de stimuler une offre européenne à même de répondre à ce besoin[132] ». Ainsi, l'autorisation de création de EMC2 hébergé sur Microsoft Azure est délivrée pour trois ans afin qu'un cloud souverain exclusivement soumis au droit européen ait le temps de se développer afin de pouvoir accueillir le HDH à l'issue de cette période[133][134].

Cette décision a provoqué de vives réactions de la part des fournisseurs de cloud européens certifiés ou en cours de certification SecNumCloud[135]. En effet, ceux qui ont investi dans cette certification[136] se retrouvent dans une situation délicate se demandant le sens d'une telle exigence si elle n'entraine pas l'attribution de l'hébergement des données de santé. Alors que l'exigence de certification SecNumCloud aurait permis d'accélérer la mise à disposition des données de santé dans un environnement sécurisé[137], les acteurs du cloud européens ressentent un désaveu pour la certification SecNumCloud.

Un recours en annulation contre la délibération de la CNIL a été déposé[138], le Conseil d'Etat valide la délibération de la CNIL[139] au motif qu'il existe des garanties suffisantes permettant de réduire les risques résultant de l'utilisation des données de santé.

La délibération de la CNIL qui semble avoir été rendue du « bout des lèvres[140] » illustre la difficulté de réaliser la souveraineté numérique tout en restant compétitif et efficace.

---

[132] *Ibid*.

[133] FILIPPONE Dominique, « La Cnil adoube Microsoft pour l'hébergement des données de l'Assurance Maladie », Actualités Données personnelles, Le Monde informatique*,* 31 janvier 2024.

[134] ZIRAR Wassinia, « Health Data Hub : la CNIL lâche temporairement du lest sur l'hébergement chez Microsoft », Ticpharma.com, 2 février 2024.

[135] VITARD Alice, « Les données de santé d'EMC2 hébergées chez Azure, le label SecNumCloud désavoué ? », *L'Usine Digitale.* 5 février 2024.

[136] CARAVAGNA Léo, « Health Data Hub : la mission Marchand-Arvier propose de quitter Microsoft pour un hébergeur SecNumCloud d'ici deux ans », Ticpharma.com, 26 janvier 2024.

[137] MINISTERE DE LA SANTÉ, « Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé », Rapport*,* 5 décembre 2023.

[138] INTERNET SOCIETY – France CHAPTER, « L'Internet Society France demande l'annulation de la délibération de la CNIL autorisant l'hébergement par Microsoft des données de santé des Français *»,* Communiqué de presse, *13 avril 2024.*

[139] CONSEIL D'ÉTAT, Juge des référés, Inédit au recueil Lebon, 22 mars 2024

[140] MARTIAL-BRAZ Nathalie, « Souveraineté numérique – Souveraineté numérique en danger ! », Communication Commerce électronique n°5, mai 2024, repère 5, Lexis-Nexis.

La protection des droits fondamentaux des personnes se trouve mise en balance avec des intérêts techniques et économiques. Cette décision du Conseil d'Etat a été vivement critiquée, notamment car elle reviendrait à reconnaitre la primauté des intérêts économiques sur des intérêts supérieurs tels que la protection de la vie privée et des données de santé des citoyens français[141]. En effet, privilégier une société de cloud américain alors que la stratégie européenne pourrait favoriser l'émergence de cloud souverains interroge quant à la réalisation d'un tel projet.

Cependant, il est possible d'analyser la position de la CNIL et du Conseil d'Etat comme ne niant pas la possibilité d'un hébergement souverain pour les entrepôts de données de santé, dès lors qu'un délai de trois ans est laissé avant de basculer sur un cloud européen. Dès lors, la CNIL montre sa compréhension du problème de l'hébergement et ne cherche pas à le nier. Consciente des difficultés techniques actuelles des hébergeurs européens, elle leur donne un délai à l'issue duquel ils devront être capables d'assurer la migration du HDH et de ses projets sur leurs serveurs. Toutefois, l'obligation d'être certifié SecNumCloud pour héberger les données de santé parait paradoxale dès lors que les hébergeurs actuels n'ont pas cette certification. Cela illustre la difficulté de respecter les exigences de certification en faveur de la souveraineté numérique avec les barrières techniques et économiques de la pratique[142]. Si ces certifications sont nécessaires pour encadrer l'hébergement des données de santé sur des systèmes de cloud, elles se heurtent encore à des difficultés qui rendent la réalisation de la souveraineté numérique difficile.

Au-delà des réponses institutionnelles françaises et des décisions d'adéquation, les initiatives des acteurs de l'écosystème du cloud sont non négligeables. L'Europe envisage ainsi une certification de sécurité pour les données de santé, mais celle-ci présente actuellement des exigences inférieures à la certification SecNumCloud. Ces derniers mettent en avant cet enjeu pour démontrer leur volonté d'héberger le Health Data Hub à l'avenir. Parallèlement, les hébergeurs non souverains renforcent leur fiabilité en matière de sécurité des données pour conserver ce service sur leur cloud.

---

[141] *Ibid.*

[142] ROBERT Alice et FIEVEE Alexandre, « Un entrepôt de données de santé peut-il être hébergé par Microsoft ? », DSIH – L'actualité des systèmes d'information hospitaliers et de la e-santé, *26* février 2024.

Section 2 : Les réponses nuancées des acteurs de l'écosystème de l'hébergement des données de santé

Les différents acteurs de l'écosystème des services d'hébergement en nuage prennent des mesures en faveur de la souveraineté à l'égard des données de santé. L'Union européenne envisage la création d'une certification de sécurité pour les données de santé, visant ainsi à harmoniser les exigences à l'échelle européenne pour les hébergeurs de cloud qui souhaitent accueillir des données personnelles. Néanmoins, des divergences avec les normes existantes créent une incertitude juridique pour les hébergeurs souverains qui aspirent à se conformer au niveau de sécurité le plus élevé. Cette situation constitue un point de préoccupation majeur qu'ils mettent en avant pour illustrer leur engagement à être en mesure d'accueillir le Health Data Hub à l'avenir. Parallèlement, les hébergeurs non souverains prennent également des mesures pour maintenir ce service sur leurs plateformes cloud, démontrant ainsi leur fiabilité dans la préservation de la confidentialité des données.

Ainsi, l'Union européenne projette de renforcer l'harmonisation européenne autour de la création d'une norme qui s'imposerait à tout le territoire (I). Se joignent à elle dans une volonté de prendre part à l'encadrement de cet écosystème les hébergeurs, souverains ou non, qui proposent des services de cloud souhaitant accueillir à terme les données de santé du HDH (II).

I - La norme européenne EUCS, une nécessité dans un paysage européen fragmenté

Un projet de norme européenne de sécurité à l'égard des données à caractère personnel a vu le jour dans le but d'harmoniser les exigences de certification entre chaque Etat-membre. Cela a vocation à renforcer la position des cloud souverains et à leur permettre de prendre position sur la scène européenne. Toutefois à ce jour, les critères de cette certification sont moins exigeants que ceux de la certification SecNumCloud et ne garantissent pas l'immunité contre l'extraterritorialité des lois américaines.

L'European Union Cybersecurity Certification Scheme for Cloud Services[143] (EUCS) est une opportunité d'homogénéiser les exigences en matière de cybersécurité sur le territoire de l'Union européenne et permettrait de favoriser les fournisseurs de services cloud souverains (A). Toutefois, les différents niveaux de maturité des Etats-membres en matière de sécurité et le rejet d'une immunité contre l'accès des autorités américaines font craindre une remise en cause de l'objectif de souveraineté à l'égard des données de santé (B).

A - Une norme de sécurité à l'échelle européenne nécessaire à la souveraineté numérique européenne

Le 22 mars 2024, l'agence de l'Union européenne pour la cybersécurité (ENISA) a publié un nouveau schéma de certification pour le cloud[144] en Europe intitulé « EUCS ». Le texte a fait l'objet de plusieurs versions avant d'en arriver à celle-ci.

L'idée d'une certification de cybersécurité pour les cloud à dimension européenne est venue d'un constat : le paysage européen est fragmenté autour de la question de la certification des hébergeurs cloud. Les Etats-membres ont des positions différentes, voire divergentes, certains disposent de certifications déjà strictes tandis que d'autres n'en ont aucune.

La France est très avancée avec la certification SecNumCloud dont le niveau d'exigence est haut. Le niveau d'exigence de SecNumCloud n'est pas nécessairement celui requis pour obtenir les certifications d'autres Etats. Ainsi, si un hébergeur cloud a obtenu une certification dans un ou plusieurs Etats, cela n'implique pas nécessairement qu'il satisfera aux exigences requises pour obtenir la certification française. Il parait donc nécessaire de créer une certification qui s'applique à tous les Etats-membres afin de garantir un niveau de sécurité uniforme sur tout le territoire de l'UE[145]. La certification vise donc à remplacer les certifications nationales existantes pour harmoniser les exigences en matière de sécurité du

[143] EUROPEAN UNION AGENCY FOR CYBERSECURITY, « EUCS – CLOUD SERVICES SCHEME, EUCS, a candidate cybersecurity certification scheme for cloud services », décembre 2020.

[144] DEROUET Thierry, « La directive « cloud au centre » de l'Etat en péril », Itforbusiness.fr, 9 avril 2024.

[145] BRANDELA Hélène, « Projet européen de certification cloud (EUCS) : L'utopie d'un cloud souverain », Village de la Justice, *6 novembre* 2023.

cloud sur le territoire européen. Dès lors, ce nouveau référentiel permettra d'encadrer les transferts de données sensibles telles que les données de santé hors de l'UE.

Il faut noter que la mise en place d'une telle certification à l'échelle européenne implique des enjeux politiques et commerciaux importants qui influent sur les débats et sur les positions des Etats dans la discussion. Il n'y a pas véritablement de consensus à l'échelle européenne. La France, avec sa doctrine « cloud au centre[146] » et son référentiel SecNumCloud a œuvré en tant que chef de file pour concevoir cette certification européenne avec des critères stricts. De même, l'Espagne et l'Italie sont contre l'application des législations extraeuropéennes sur les données sensibles et souhaitent donc que soit mise en place une protection stricte de ces données[147].

La certification EUCS définit trois niveaux de certifications possibles : le niveau basique, le niveau substantiel et le niveau élevé. Ce sont des niveaux d'assurance qui sont classés en fonction du risque encouru[148].

Le premier niveau assure la minimisation des risques fondamentaux d'incidents de cyberattaques. Le deuxième niveau assure également cette minimisation mais également celle du risque de cyberattaque perpétrée par des acteurs aux ressources limitées. Le troisième niveau permet de minimiser les cyberattaques de pointes menées par des acteurs aux ressources importantes.

Le sort des données sensibles et donc des données de santé est particulièrement pris en compte. Ainsi, les entreprises non européennes doivent respecter certaines obligations à l'égard du stockage de ces données sur leur service de cloud. Pour mener à bien cette activité, les entreprises étrangères doivent coopérer avec une société européenne ou bien proposer le service de cloud en passant par une co-entreprise.

---

[146] *Supra note n°76.*

[147] SÉNAT, « Recherche et innovation - Constellation de connectivité sécurisée européenne - Proposition de résolution européenne », Comptes rendus de la Commission des affaires européennes, 21 juillet 2022.

[148] *Supra note n°95.*

Les versions précédentes faisaient état d'obligations plus strictes en ajoutant l'obligation « d'étroite collaboration avec une entreprise européenne » pour stocker les données de santé sur un service de cloud d'une entreprise non européenne. De plus, « les exigences de souveraineté ne font plus partie du niveau de certification le plus élevé[149] ». Les réactions ont été vives face à cette exclusion des exigences de souveraineté. En effet, alors qu'elles apparaissaient comme un des points les plus importants de la stratégie de certification européenne de cloud, celles-ci ne sont plus mentionnées comme devant faire l'objet du niveau de sécurité le plus haut. Il est donc à craindre que le projet d'EUCS « s'éloigne de son objectif essentiel de garantir un niveau élevé de sécurité et d'immunité contre les législations extraterritoriales non européennes[150] ». La protection des données de santé des Européens ne serait alors pas optimale pour lutter contre les ingérences d'Etats non européens qui abritent sur leurs services de cloud les données de santé européennes.

La suppression des exigences de souveraineté du plus haut niveau de protection de la certification EUCS pose question quant aux conséquences pour l'hébergement de la plateforme Health Data Hub chez Microsoft Azure. En effet, de telles exigences auraient pu répondre, au moins partiellement, aux attentes quant à la confidentialité requise pour les données de santé. Il aurait été possible d'imaginer que même Microsoft Azure coopère avec une entreprise européenne souveraine. Cela aurait permis aux hébergeurs souverains européens de prendre part à l'hébergement des données de santé tout en limitant l'accès des entreprises étrangères. Il aurait alors été possible d'anticiper la stratégie et de préparer les cloud souverains au futur hébergement du HDH sur leurs serveurs cloud d'ici quelques années. De même, conserver la souveraineté des données dans le niveau d'assurance le plus élevé de la certification aurait permis de garantir des normes de sécurité élevées et uniformes sur tout le territoire de l'Union et aurait illustrer une véritable volonté de s'emparer de la question de l'hébergement des données de santé face aux ingérences des entreprises de nationalité étrangères.

---

[149] *Supra note n°94.*

[150] CIGREF, « EUCS, le déclin d'une ambition – Lettre ouverte à la Commission européenne », Communiqué de presse, 11 avril 2024.

Ainsi, si la volonté de créer une certification de sécurité aux critères uniformes sur le territoire de l'Union semble nécessaire pour que les données de santé européennes soient hébergées dans le respect des règles de sécurité européennes, des questions se posent sur le niveau d'exigence des dispositions de cette certification. La question de la souveraineté des données pour l'Union face aux ingérences des autorités étrangères ne semble pas prise en compte de la manière la plus complète qu'il soit. Également, lutter contre la fragmentation des conditions de certification d'hébergeur cloud au sein de l'UE permettra aux hébergeurs européens souverains de répondre plus facilement aux exigences pour devenir un hébergeur capable d'héberger le HDH en toute sécurité. Toutefois, la certification EUCS ne se conforme pas aux critères de la certification très protectrice qu'est la certification SecNumCloud, ce qui remet en cause l'effectivité de la certification sur le territoire européen.

Dès lors, passer par des mécanismes de certification pourrait permettre d'assurer la confidentialité des données des citoyens européens malgré l'absence de conciliation parfaite entre la protection de la vie privée et la nécessité de maintenir des flux internationaux de données. Toutefois, ces mécanismes se heurtent aux différences de politiques entre l'Union qui prend des décisions en faveur du transfert des données de santé et la France qui se place pleinement en faveur de la souveraineté numérique.

B - La norme européenne EUCS, le rejet de l'immunité des données de santé face à l'extraterritorialité des lois américaines

La France, pionnière de l'Union en matière de certification de sécurité des hébergeurs cloud avec la certification SecNumCloud, est active dans l'élaboration d'une certification européenne.

En ce sens, elle a insisté pour que soient inclus dans les critères de la certification européenne les critères de SecNumCloud relatifs à la souveraineté.

Cela avait été entendu dans les versions antérieures du projet[151]. L'idée française était d'inclure ces critères de souveraineté dans un quatrième niveau de sécurité. La condition d'immunité face aux lois extraterritoriales aurait ainsi été reprise à l'échelle européenne. Cette exigence n'aurait été applicable que pour les données sensibles dont les données de santé.

[151] *Supra n° 122.*

L'incorporation des critères de SecNumCloud relatifs à la souveraineté des données sensibles aurait ainsi permis que les données de santé européennes soient protégées pour l'application extraterritoriale des lois américaines telles que le FISA. Ainsi, les données hébergées sur le HDH par le cloud de Microsoft Azure auraient pu être protégées contre les ingérences des autorités américaines. Ce point de vue est partagé par les acteurs de l'écosystème européen des cloud souverains. Jean-Noël De Galzain, président de l'association Hexatrust, qui regroupe des entreprises du « cloud de confiance » et auteur d'une tribune publiée en février dernier, écrivait qu'en cessant de combattre l'extraterritorialité américaine et en renonçant à l'exigence de localisation européenne des données[152], « l'Europe risque de se couper de la possibilité de rester autonome, et d'empêcher l'émergence d'une industrie européenne alternative du cloud et de la confiance (…) en s'enfermant un peu plus dans une dépendance technologique et économique aux GAFAM américains[153] ».

L'abaissement du niveau de protection des données pose question. Si l'ENISA n'a pas donné d'explications, il est possible d'imaginer que cela est justifié par la prise en compte des disparités techniques entre les Etats-membres. En effet, puisque tous n'ont pas les mêmes critères de certification, tous n'ont pas la même maturité technologique et politique. Prévoir des critères de certification moins hauts que ceux de SecNumCloud permet d'éviter les disparités entre Etats et d'imposer à certains des contraintes très éloignées de leur situation actuelle. Cela est donc problématique pour les Etats qui ont mis en œuvre des certifications de haute protection puisqu'elles vont devoir les mettre de côté au profit d'une certification moins exigeante.

Au-delà de l'abaissement du niveau de sécurité accordé, l'absence d'alignement sur les plus hautes exigences de sécurité déjà existantes risque de complexifier la situation des cloud souverains qui ont ou sont en train d'acquérir la certification SecNumCloud[154].

---

[152] BASCOU Stéphane, « EUCS : L'Europe en passe d'abandonner ses critères de souveraineté ? », Actualités 01net.com, 5 avril 2024.

[153] DE GALZAIN JEAN-NOËL, « Certification cloud européenne (EUCS) : l'Europe est-elle en train de passer à côté de sa souveraineté numérique ? », La Tribune, 12 février 2024.

[154] *Supra note n°148.*

C’est ce qu’illustre la réaction de plusieurs sociétés de cloud européennes : « plus d’un tiers des entreprises ont déjà investi dans des solutions de cloud souverain, et près de la moitié prévoit de le faire dans un avenir proche, ce qui montre la volonté des organisations d’aborder les questions de souveraineté[155] ».

En effet, la vocation de la certification EUCS est de remplacer les certifications nationales existantes, dont la certification SecNumCloud[156]. De fait, puisque la certification EUCS ne reprend pas les critères de SecNumCloud en matière de données de santé, le risque est d’aboutir *in fine* à une certification certes européenne mais met qui offre une protection moindre des données sensibles. Dès lors, l’hébergement des données de santé du HDH ne sera pas exclusivement réservé aux entreprises européennes.

La France a fait connaitre sa volonté de conserver sa certification SecNumCloud à l’échelle du pays[157]. Le vote a été reporté au mois de juin. Maintenir la certification SecNumCloud aux côtés de la certification européenne pourrait avoir l’avantage, si leurs critères sont complémentaires, d’imposer un niveau minimum de protection à l’échelle du territoire européen, tout en maintenant un haut niveau de protection dans les Etats qui y sont prêts telle que la France. Il serait ensuite possible d’imaginer, pour les autres Etats, un glissement vers des obligations de plus en plus protectrices à l’égard des données de santé pour parvenir de manière graduée à l’application de la norme SecNumCloud sur tout le territoire européen.

Face à cette incertitude qui plane au-dessus de l’articulation des certifications nationales et européenne, les hébergeurs, souverains ou non, mettent en avant des techniques et des initiatives pour montrer leur capacité à héberger les données de santé du HDH tout en préservant la souveraineté numérique.

---

[155] VITARD Alice, « EUCS : Des fournisseurs européens, dont OVHCloud et Orange, appellent à protéger les données sensibles », L’Usine Digitale, 12 avril 2024.

[156] *Supra note n°148.*

[157] BASCOU Stéphanie, « EUCS : Les critères de souveraineté sont-ils mis au placard ? Le vote est reporté au mois de juin », 01net.com, 18 avril 2024.

II - Les réponses des hébergeurs de données de santé, des engagements en faveur de la souveraineté et de la sécurité à l'égard des données de santé

Les fournisseurs de cloud quels qu'ils soient prennent des engagements dans le contexte de la gestion des données de santé du Health Data Hub. Des stratégies sont mises en place par les hébergeurs de cloud souverains pour légitimer leur rôle dans la protection des données sensibles, offrant ainsi une perspective sur la réponse européenne à cette problématique. Toutefois, des initiatives des hébergeurs cloud non souverains voient le jour, mettant en lumière leurs efforts pour assurer la sécurité et la confidentialité des données de santé.

Ainsi, les hébergeurs de cloud souverains prennent des engagements pour prouver leur légitimité à héberger les données de santé du HDH en toute sécurité (A) et ainsi faire face aux arguments des hébergeurs de cloud non souverains qui sont actuellement chargés de cet hébergement (B).

A - Les engagements des hébergeurs de cloud souverains pour renforcer leur légitimité à l'égard des données de santé

Dans le contexte actuel du Health Data Hub, les fournisseurs de cloud européens expriment leur désaccord concernant le choix d'héberger l'entrepôt de données de santé EMC2 en dehors de l'Europe. Leurs préoccupations sont légitimes et soulignent la nécessité de trouver des solutions conformes aux exigences réglementaires européennes. Parmi ces fournisseurs, OVH Cloud se distingue en ayant obtenu la certification SecNumCloud en janvier 2024[158], renforçant ainsi sa position en tant que meneur du cloud européen.

L'obtention de la certification SecNumCloud par OVH Cloud constitue un jalon significatif dans ses efforts pour répondre aux besoins d'hébergement du HDH. Cette certification, combinée à sa certification HDS et à sa position affirmée en tant que « champion du cloud européen »[159], témoigne de sa volonté de développer une offre adaptée aux exigences du

[158] OVH CLOUD BLOG, « ANSSI SecNumCloud : le plus haut niveau de sécurité pour les données sensibles et stratégiques ».

[159] LE FIGARO avec AFP, « Données de santé : OVH Cloud se positionne sur le Health Data Hub », Le Figaro Flash Eco, 9 janvier 2024.

HDH. En s'appuyant sur sa conformité aux exigences de sécurité françaises et européennes[160], OVH Cloud affirme pouvoir fournir un service de cloud véritablement souverain, garantissant ainsi que les données de santé sont hébergées en France, sous la certification SecNumCloud.
De plus, OVH Cloud insiste sur sa parfaite conformité au RGPD, assurant ainsi que les données ne sont pas soumises aux lois américaines de portée extraterritoriale. Cette argumentation souligne l'importance de la souveraineté numérique et met en avant la capacité des fournisseurs de cloud européens à répondre aux besoins spécifiques du HDH en matière de sécurité et de conformité réglementaire.

En parallèle, les fournisseurs de cloud européens soulignent que si eux sont tenus d'obtenir la certification SecNumCloud pour héberger des données de santé, ce n'est pas le cas de l'hébergeur actuel du HDH[161], qui n'est certifié que comme hébergeur HDS. Cependant, les fournisseurs souverains intensifient leurs efforts pour démontrer leur capacité à héberger les données de santé de manière sécurisée, mettant en avant leurs initiatives pour obtenir des certifications et se conformer aux normes de sécurité européennes.
Parmi ces initiatives, le label Gaia-X[162], soutenu par plusieurs sociétés, dont OVH Cloud, revêt une importance particulière. Fondé sur les principes de réversibilité, de transparence et d'indépendance vis-à-vis des lois étrangères extraterritoriales, ce label vise à promouvoir des services de cloud exclusivement soumis au droit européen[163]. En combinant ces différentes initiatives européennes, il est envisageable qu'à terme, le HDH migre vers un cloud souverain, offrant ainsi une solution conforme aux exigences de sécurité et de souveraineté des données[164].

---

[160] KLABA Octave, Publication du directeur générale d'OVH Cloud sur le réseau LinkedIn, 8 février 2024.

[161] *Ibid.*

[162] MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE, « Un nouvel élan pour Gaia-X : Accélération des espaces de données de confiance », Portail de la direction générale des Entreprises, 12 mars 2024.

[163] BAUER Delphine, « Vers une souveraineté numérique européenne ? » Petites Affiches, Gazette du Palais n°065, 1 avril 2021, p. 3.

[164] FONTAINE Quentin et STROWEL Alain, « La stratégie européenne pour les données », *La politique européenne du numérique*, sous la direction de BERTRAND Brunessen. Collection Droit de l'Union européenne dirigée par Fabrice Picod, Collection Monographie. Ed. Bruylant, 2023, p. 727.

Si les efforts des fournisseurs de cloud souverains pour répondre aux exigences du Health Data Hub en matière d'hébergement des données de santé sont incontestables, il faut également relever les arguments et les capacités des fournisseurs de cloud non souverains dans ce domaine. Alors que les fournisseurs souverains insistent sur leur conformité aux normes européennes, les fournisseurs non souverains avancent leurs propres garanties en matière de sécurité et de fiabilité.

B - Les engagements des hébergeurs cloud non souverains en faveur de la sécurité des données de santé

Dans le cadre de la discussion sur l'hébergement des données de santé du Health Data Hub sur des cloud non souverains comme Microsoft Azure, il faut se pencher sur les arguments avancés par ces hébergeurs non souverains pour justifier leur capacité à assurer la confidentialités de ces données sensibles malgré les contraintes réglementaires[165].

Les grands fournisseurs de cloud investissent massivement dans la sécurité de leurs infrastructures. Ils mettent en avant leurs certifications de conformité aux normes de sécurité internationales telles qu'ISO 27001, SOC 2, ou encore les exigences du Health Insurance Portability and Accountability Act (HIPAA), la loi américaine relative au traitement des données de santé aux États-Unis[166].

En outre, ces fournisseurs offrent des solutions de chiffrement avancées, comme le chiffrement homomorphique et le chiffrement de bout en bout, assurant ainsi la confidentialité des données de santé, même lorsqu'elles sont stockées ou transmises sur le cloud[167].

Leur infrastructure mondiale et robuste est également un argument majeur. Avec des centres de données répartis à travers le monde, ces fournisseurs garantissent une disponibilité élevée des données et une continuité de service même en cas d'incidents majeurs. Cet argument couplé à celui du coût de l'offre des cloud non souverains généralement avantageux explique

---

[165] MICROSOFT.COM, « Health Insurance Portability and Accountability Act (HIPAA) & Health Information Technology for Economic and Clinical Health (HITECH) Act », Document de conformité Microsoft Accessible en ligne, 31 janvier 2024.

[166] *Ibid.*

[167] MICROSOFT.COM, « Plan d'action RGPD Microsoft 365 - Principales priorités pour vos premiers 30 jours, 90 jours et au-delà », Document de conformité Microsoft Accessible en ligne, 17 mars 2023.

le recours à leurs services jusqu'à aujourd'hui. Par ailleurs, ils disposent d'équipes dédiées à la conformité réglementaire, chargées de garantir le respect des réglementations locales, notamment en ce qui concerne la protection des données de santé.

Enfin, ces fournisseurs mettent en place des mécanismes de transparence et d'audit permettant aux utilisateurs de vérifier comment leurs données sont traitées et stockées, renforçant ainsi la confiance dans leurs pratiques de gestion des données.

Dans le contexte spécifique du Health data hub, ces arguments revêtent une importance particulière. Bien que le choix de l'hébergement des données de santé sur des cloud non souverains puisse soulever des préoccupations concernant la souveraineté des données et la conformité réglementaire, les assurances fournies par ces fournisseurs quant à leur capacité à assurer la sécurité et la confidentialité des données sont essentielles.

Ainsi, les fournisseurs de cloud non souverains présentent des garanties solides quant à leur capacité à héberger et à gérer des données de santé, même dans des environnements réglementés de manière stricte. Cependant, il est impératif pour les parties prenantes, notamment le Health Data Hub, d'évaluer attentivement ces garanties et de prendre des mesures appropriées pour protéger la souveraineté et la confidentialité des données de santé.

Les élections européennes à venir et la future entrée en vigueur du règlement sur l'EHDS pourraient mener à un changement dans la stratégie européenne pour la souveraineté numérique des données de santé[168].

[168] COMMISSION EUROPÉENNE, Proposition de Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, 3 mai 2022.

Bibliographie

I - Ouvrages

- CHAGNY Murielle, « Les transferts intra et extra-communautaires », Le Lamy Droit économique, Partie 5, Livre 1, Titre 2, Chapitre 1, Section 5 La règlementation des transferts internationaux des données, point 4879, Lamy Expert, février 2024.

- DOUVILLE Thibault, « Droit des données à caractère personnel », Manuel, Précis Domat, Droit privé / public, LGDJ, Lextenso, 2023, p. 105.

- ROSIER Karen et DE TERWANGNE Cécile, « Le règlement général sur la protection des données », Chapitre 3 - L'acceptation des modes alternatifs de régulation et les flux transfrontaliers, Section 2 - Les mécanismes alternatifs dans le cadre du « Privacy Shield », 2018, p. 357.

II - Monographies et colloques

- DE GROVE-VALDEYRON Nathalie et BLANQUET Marc, « Politique de santé et politique du numérique », *La politique européenne du numérique*, sous la direction de BERTRAND Brunessen. Collection Droit de l'Union européenne dirigée par Fabrice Picod, Collection Monographie. Editions Bruylant, p. 515.

- DELMAS-LINEL Béatrice, « Enjeux sociétaux : Cloud computing, nouveau prisme des libertés publiques et des souverainetés nationales », *Le cloud computing – L'informatique en nuage*, Actes du Colloque du 11 octobre 2023 sous la direction de Bénédicte Fauvarque-Cosson et Célia Zolynski. Collection colloques volume 22, Société de la législation comparée, p. 97.

- EL BIAD Nahela, « Le paradoxe de la e-santé : entre promotion d'un mode de soins innovant et protection des droits des patients », *Santé, numérique et droit-s*, IFR Actes de colloques n°34 sous la direction de Isabelle Poirot-Mazères, Presses de l'Université Toulouse 1 Capitole, 2018, p.191.

- FONTAINE Quentin et STROWEL Alain, « La stratégie européenne pour les données », *La politique européenne du numérique*, sous la direction de BERTRAND Brunessen. Collection Droit de l'Union européenne dirigée par Fabrice Picod, Collection Monographie. Ed. Bruylant, 2023, p. 727.

- MAXWELL W. J. « Protection des données aux Etats-Unis », *Le cloud computing – L'informatique en nuage*, Actes du Colloque du 11 octobre 2023 sous la direction de Bénédicte Fauvarque-Cosson et Célia Zolynski. Collection colloques volume 22, Société de la législation comparée, p. 76.

III - Articles, commentaires et contributions

- BAUER Delphine, « Vers une souveraineté numérique européenne ? » Petites Affiches, Gazette du Palais n°065, 1 avril 2021, p. 3.

- CANTERO Isabelle et CAPRIOLI Eric, « Informatique et libertés - Traitement et hébergement de données de santé : entre protection et risques », Etudes, Revue pratique de la prospective et de l'innovation n° 2, dossier n°21, novembre 2021.

- FAVREAU Amélie, « Données de santé : vers l'émergence d'un droit spécial ? », *L'émergence d'un droit des données*, sous la direction de Jean-Michel Bruguière. Thèmes & Commentaires La propriété intellectuelle autrement, Ed. Lefebvre Dalloz, Dalloz. 2024, p. 171.

- GAMBARDELLA Sophie, « Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé », 3 février 2020.

- G'SELL Florence, « L'avenir incertain des flux de données transatlantiques - Les constats multiples d'une souveraineté numérique déficiente », Enjeux numériques n°23, Annales des Mines, septembre 2023.

- LASSALLE Maxine, « La responsabilisation des acteurs du numérique dans le transfert de données personnelles vers des Etats tiers », Revue Lamy Droit de l'Immatériel, n°173, 1er août 2020, p.5.

- LENOIR Noëlle, « La Commission européenne valide les conditions de l'adéquation des États-Unis à la libre circulation des données personnelles de part et d'autre de l'Atlantique », Petites affiches, n°07-08, Labase-Lextenso, 31 août 2023, p.5.

- MAISNIER-BOCHÉ Lorraine, « Du consensus sur la localisation aux divergences sur l'immunité », Les Doctrines du mois, Expertises n°501, Expertises Droit, Technologies & Prospectives, mai 2024, p. 22 s.

- NAVARRO Patrice, « Union européenne – Souveraineté numérique – Souveraineté numérique européenne : entre faux-semblants et opportunités », La Semaine Juridique Edition Générale n°04, 29 janvier 2024, doctr. 142. Lexis Nexis.

- NEVEJANS Nathalie, « Les aspects juridiques et éthiques de l'utilisation de l'IA comme outil de lutte contre la COVID-19 », *L'utilisation du numérique dans la lutte contre la Covid - Enjeux techniques, éthiques et juridiques*, sous la direction de Yves Poullet et David Doat, Collection « Droit, Société et Risque », Ed. L'Harmattan, 2022 p.165.

- PADOVA Yann, « Les transferts internationaux de données, entre approche par les risques et positions de principe », *Commentaire critique des recommandations de l'E DPB 01/2020 (PARTIE I)*, Revue Lamy Droit de l'Immatériel, nº 184, 1er août 2021.

- STANTON-JEAN Michèle et FEINHOLZ Dafna, « Que penser sur les mégadonnées en santé selon le Comité international de bioéthique (CIB) de l'Unesco », *Innovations en santé publique, des données personnelles aux données massives (big data) - Aspects cliniques, juridiques et éthiques*, Contribution sous la direction de Christian Hervé et Michèle Stanton-Jean. Thèmes & Commentaires - Ethique biomédicale et normes juridiques, Ed. Dalloz, 2019, p. 60.

IV - Thèses et mémoires - Ordre alphabétique par le nom de famille

- MERMET Mahaut, « Lois de surveillance et protection des données personnelles – Ou une analyse de l'arrêt Schrems II », Mémoire sous la direction de Maître Lorraine Maisnier-Boché, Université Panthéon-Assas, 2020-2021. https://docassas.u-paris2.fr/nuxeo/site/esupversions/5befab1b-68bd-4909-bd8c-94eb6f274d0d?inline

V - Textes, lois, directives règlements, circulaires

- **Textes européens**

- 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 (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)

- PARLEMENT EUROPÉEN ET CONSEIL, Proposition de règlement relatif à l’espace européen des données de santé, COM/2022/197 final.

- COMMISSION EUROPÉENNE, Proposition de Règlement du Parlement européen et du Conseil relatif à l’espace européen des données de santé, 3 mai 2022.

- Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du 4 novembre 1950.

- Charte des Droits fondamentaux de l’Union européenne du 7 décembre 2000.

- PARLEMENT EUROPÉEN ET CONSEIL, Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

- COMMISSION EUROPÉENNE, Adequacy decision for the EU-US Data Privacy Framework, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework 10 juillet 2023.

- COMMISSION EUROPÉENNE, Décision du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d’Amérique.

- COMMISSION EUROPÉENNE, Arrêté modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel, 6 mars 2024.

- COMMISSION EUROPÉENNE, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. 28 février 2023.

- COMMISSION EUROPÉENNE, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (version adoptée le 13 avril 2016).

- COMMISSION EUROPÉENNE, « Le bouclier de protection des données UE-Etats-Unis : Foire aux questions », Fiche d'information, 12 juillet 2016.

- CEPD, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, adoptées le 10 novembre 2020.

- EUROPEAN UNION AGENCY FOR CYBERSECURITY, « EUCS – CLOUD SERVICES SCHEME, EUCS, a candidate cybersecurity certification scheme for cloud services », décembre 2020.

• **Textes français**

- Code de la santé publique modifié par la loi n° 2016-41 du 26 janvier 2016.

- LOI n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique – Journal officiel n°0117 du 22 mai 2024.

- LOI n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé. Mis à jour le 28 avril 2021.

- LOI n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- ASSEMBLÉE NATIONALE, Projet de loi visant à sécuriser et réguler l'espace numérique (ECOI2309270L). Dernière modification : 20 octobre 2023.

- ASSEMBLÉE NATIONALE, Projet de loi visant à sécuriser et à réguler l'espace numérique, Texte adopté n°286, 10 avril 2024.

- MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ, Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel, JOFR n°0049 du 28 février 2018, Texte n° 16.

- PREMIÈRE MINISTRE, « Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'Etat (« cloud au centre ») » n°6404/SG, Actualisation de la Circulaire, 31 mai 2023.

- Conseil d'état :

CONSEIL D'ÉTAT, Juge des référés, Inédit au recueil Lebon, 22 mars 2024

ORDONNANCE DU PRÉSIDENT DU TRIBUNAL « Référé – Protection des données à caractère personnel – Cadre de protection des données UE-États-Unis – Décision constatant l'adéquation du niveau de protection – Demande de sursis à exécution – Défaut d'urgence », 12 octobre 2023.

CONSEIL D'ETAT, COMMUNIQUÉ DE PRESSE, Le juge des référés ne suspend pas le partenariat entre le ministère de la santé et Doctolib pour la gestion des rendez-vous de vaccination contre la covid-19, 12 mars 2021.

CONSEIL D'ETAT, « Health Data Hub et protection de données personnelles : des précautions doivent être prises dans l'attente d'une solution pérenne », Actualités, 14 octobre 2020.

CONSEIL D'ETAT, « Santé et protection des données », Conseil d'Etat Droits et Débats n°29 - Un colloque organisé par le Conseil d'Etat le 1er décembre 2017. Conseil d'Etat. La Documentation française.

- Sénat

SÉNAT, Amendement n°CS765, Projet de loi n°1514, adopté par le Sénat visant à sécuriser et réguler l'espace numérique, déposé le 15 septembre 2023.

SÉNAT, « Recherche et innovation - Constellation de connectivité sécurisée européenne - Proposition de résolution européenne », Comptes rendus de la Commission des affaires européennes, 21 juillet 2022. https://www.senat.fr/compte-rendu-commissions/20220718/europ.html

- Assemblée nationale

ASSEMBLÉE NATIONALE, « Compte rendu Commission spéciale chargée d'examiner le projet de loi visant à sécuriser et réguler l'espace numérique », Compte-rendu n°7, 21 septembre 2023. https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/espnum/l16espnum2223007_compte-rendu.pdf

- Rapports

MINISTERE DE LA SANTÉ, « Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé », Rapport, 5 décembre 2023.

INISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE, « Un nouvel élan pour Gaia-X : Accélération des espaces de données de confiance », Portail de la direction générale des Entreprises, 12 mars 2024.

- CNIL :

CNIL, « Les principaux avis et recommandations de la CNIL sur la Plateforme des données de santé », 31 janvier 2024. https://www.cnil.fr/fr/les-principaux-avis-et-recommandations-de-la-cnil-sur-la-plateforme-des-donnees-de-sante

CNIL, Délibération n° 2023-146 du 21 décembre 2023 autorisant le groupement d'intérêt public « Plateforme des données de santé » à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données dans le domaine de la santé, dénommé « EMC2 ». (Demande d'autorisation n° 2229962v1), 31 janvier 2024. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000049057224

CNIL, Ordre du jour de la séance plénière du 13 juillet 2023, 17 juillet 2023. https://www.cnil.fr/fr/ordre-du-jour-de-la-seance-pleniere-du-13-juillet-2023

CNIL, « Transferts de données vers les États-Unis : la Commission européenne adopte une nouvelle décision d'adéquation », Transferts de données vers les États-Unis : la Commission européenne adopte une nouvelle décision d'adéquation, 10 juillet 2023. https://www.cnil.fr/fr/transferts-de-donnees-vers-les-etats-unis-la-commission-europeenne-adopte-une-nouvelle-decision

CNIL, « Demande d'autorisation d'une recherche en santé : les informations à fournir et les critères d'octroi », Avis du 11 janvier 2023. https://www.cnil.fr/fr/demande-dautorisation-dune-recherche-en-sante-les-informations-fournir-et-les-criteres-doctroi

CNIL, « Le Conseil d'Etat demande au Health Data Hub des garanties supplémentaires pour limiter le risque de transfert vers les Etats-Unis », Avis du 14 octobre 2020. https://www.cnil.fr/fr/le-conseil-detat-demande-au-health-data-hub-des-garanties-supplementaires#:~:text=Le%20juge%20a%20confirmé%20qu,interruption%20immédiate%20de%20la%20plateforme.

CNIL, Mémoire en observations, Conseil d'Etat, Section du contentieux, référé L. 521-2 CJA, 8 octobre 2020. https://cdn2.nextinpact.com/medias/observations-de-la-cnil-8-octobre-2020-1---1-.pdf

CNIL « Invalidation du Privacy shield : les premières questions-réponses du CEPD », 31 juillet 2020 » https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-travaux-du-cepd

CNIL, 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. https://www.cnil.fr/sites/cnil/files/2023-06/deliberation_du_20_avril_2020_portant_avis_sur_projet_darrete_relatif_a_lorganisation_du_systeme_de_sante.pdf

- ANSSI :

ANSSI, « SecNumCloud pour les fournisseurs de services Cloud – Pourquoi et comment être qualifié SecNumCloud ? », Publié le 29 septembre 2023 mis à jour le 25 avril 2024. https://cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud

PREMIER MINISTRE ET ANSSI, « Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigence », Version 3.2 du 8 mars 2024. https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf

• **Textes américains**

- LOI FISA, section 702 (FISA Amendments Act of 2008).

- EXECUTIVE ORDER 12 333 (décret exécutif du Président des Etats-Unis).

VI - Jurisprudences

• CJUE

- CJUE, Décision d'exécution (UE) 2023/1795 de la Commission du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis. C/2023/4745.

- CJUE, Gr., Ch, du 16 juillet 2020. Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems. Demande de décision préjudicielle, introduite par la High Court (Irlande), C-311/18.

- CJUE, Arrêt de la Cour (grande chambre) du 6 octobre 2015, Maximillian Schrems contre Data Protection Commissioner. Demande de décision préjudicielle, introduite par la High Court (Irlande), C-362/14.

- CJUE, 6 nov. 2003, aff. C-101/1 Bodil Lindqvist et G29, 15 février 2007, WP131.

• Jurisprudences françaises

- CE, Juges des référés, 13 octobre 2020, 444937, Recueil Lebon.

- CE, 19 juil. 2010, n° 317182 Base Elèves et CE, 28 mars 2014, n°361042.

VII - Ressources internet

• Articles

- Publications de l'ANS :

ANS, « Certification des hébergeurs de données de santé ». https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante

ANS, « HDS ». https://esante.gouv.fr/produits-services/hds

ANS, « Publication de la doctrine du numérique en santé - Version 2023 », Communiqué de presse, 26 avril 2024. https://esante.gouv.fr/espace-presse/publication-de-la-doctrine-du-numerique-en-sante-version-2023

ANS, « Hébergement des données de santé (HDS) : évolution des référentiels de certification et d'accréditation », ANS Actualités, 27 décembre 2023. https://industriels.esante.gouv.fr/actualites/toutes-les-actualites/hebergement-des-donnees-de-sante-hds-evolution-des-referentiels-de-certification-et-d-accreditation

ANS, « Certification HDS – Référentiel d'accréditation, Version 1. 1 finale », mai 2018. https://esante.gouv.fr/sites/default/files/media_entity/documents/hds_referentiel_daccreditation_v1.1f_mai2018.pdf

- BASCOU Stéphanie, « EUCS : Les critères de souveraineté sont-ils mis au placard ? Le vote est reporté au mois de juin », 01net.com, 18 avril 2024. https://www.01net.com/actualites/eucs-les-criteres-de-souverainete-sont-ils-mis-au-placard-la-decision-sera-prise-dans-un-mois.html

- BASCOU Stéphane, « EUCS : L'Europe en passe d'abandonner ses critères de souveraineté ? », Actualités 01net.com, 5 avril 2024. https://www.01net.com/actualites/eucs-leurope-en-passe-dabandonner-ses-criteres-de-souverainete.html#:~:text=La%20dernière%20version%20du%20texte%20qui%20doit%20définir,clouders%20américains%20pour%20les%20données%20sensibles%20ou%20stratégiques.

- BERNELIN Margo, « Plateformes de données de santé : enjeux d'éthique, un avis du CCNE et du CNPEN à ne pas manquer », Dalloz Actualités, IP/IT Communications, 5 juin 2023. https://www.dalloz-actualite.fr/flash/plateformes-de-donnees-de-sante-enjeux-d-ethique-un-avis-du-ccne-et-du-cnpen-ne-pas-manquer

- BRAC DE LA PERRIÈRE Marguerite, « Hébergement de données de santé, décryptage des évolutions à venir », DSIH – L'actualité des systèmes d'information hospitaliers et de la e-santé, 8 janvier 2024. https://www.dsih.fr/article/5368/hebergement-de-donnees-de-sante-decryptage-des-evolutions-a-venir.html

- BRANDELA Hélène, « Projet européen de certification cloud (EUCS) : L'utopie d'un cloud souverain », *Village de la Justice,* 6 novembre 2023. https://www.village-justice.com/articles/certification-cloud-niveau-europeen-utopie-cloud-souverain,47738.html

- BRAS Pierre-Louis et LOTH André, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2023, p. 43. https://drees.solidarites-sante.gouv.fr/sites/default/files/2021-01/rapport-donnees-de-sante-2013.pdf

- BONFILLON Romain, « Nouveau référentiel HDS : ce qu'il va changer pour l'écosystème de la santé », MIND HEALTH, 6 mars 2024, mis à jour le 7 mars 2024. https://www.mind.eu.com/health/financement-et-politiques-publiques/nouveau-referentiel-hds-ce-quil-va-changer-pour-lecosysteme-de-la-sante/

- BOSSY MALAFOSSE Jeanne, « La Commission européenne valide le nouvel accord de protection des données entre l'Europe et les Etats-Unis », DELSOL Avocats, Blog Données personnelles, 11 juillet 2023. https://www.delsolavocats.com/La-Commission-europeenne-valide-le-nouvel-accord-de-protection-des-donnees-entre-l-Europe-et-les-Etats-Unis

- CARAVAGNA Léo, « Publication de la nouvelle version de la doctrine du numérique en santé », TICSANTÉ.com, 3 mai 2024. https://www.ticsante.com/story?ID=7204

- CARAVAGNA Léo, « Health Data Hub : la mission Marchand-Arvier propose de quitter Microsoft pour un hébergeur SecNumCloud d'ici deux ans », Ticpharma.com. 26 janvier 2024. https://www.ticpharma.com/story?ID=2485

- CIGREF, « EUCS, le déclin d'une ambition – Lettre ouverte à la Commission européenne », Communiqué de presse, 11 avril 2024. https://www.cigref.fr/wp/wp-content/uploads/2024/04/@Cigref_CP_EUCS-le-declin-dune-ambition_11042024.pdf

- CLOUD TEMPLE, « Fiche réglementaire : Le nouvel HDS », 22 avril 2024. https://ctwwwmedias.blob.core.windows.net/default/2024/04/Fiche-reglementaire_Nouvel-HDS.pdf

- DARNAULT Cécilia, « Les outils de transfert des données hors UE », Les outils de transfert des données hors UE, Observatoire de la Compliance, 19 août 2021. https://observatoire-compliance.univ-avignon.fr/2021/08/19/les-outils-de-transfert-des-donnees-hors-ue/

- DE GALZAIN JEAN-NOËL, « Certification cloud européenne (EUCS) : l'Europe est-elle en train de passer à côté de sa souveraineté numérique ? », La Tribune, 12 février 2024. https://www.latribune.fr/opinions/tribunes/certification-cloud-europeenne-eucs-l-europe-est-elle-en-train-de-passer-a-cote-de-sa-souverainete-numerique-990277.html

- DE MOTA Thomas, « Le référentiel HDS : l'évolution », Le Club Cyber, 15 décembre 2023. https://leclubcyber.com/referentiel-hds-evolution-certification/

- DEROUET Thierry, « La directive « cloud au centre » de l'Etat en péril », Itforbusiness.fr, 9 avril 2024. https://www.itforbusiness.fr/eucs-la-directive-cloud-au-centre-de-letat-en-peril-75277

- DERRIENNIC ASSOCIÉS, « Certification HDS : un nouveau « nouveau projet de référentiel » », 18 janvier 2024. https://derriennic.com/certification-hds-un-nouveau-nouveau-projet-de-referentiel/

- DESMARAIS Pierre, « HDSv2 : Les référentiels 2024 prennent de front la CJUE et le CE », Blog Desmarais-Avocats, 22 mai 2024. https://www.desmarais-avocats.fr/hdsv2-les-referentiels-2024-prennent-de-front-la-cjue-et-le-ce/

- DHURATA Jahiu, MAZZOLI Robert, « Hébergement de données de santé (HDS) », MICROSOFT AZURE, Article, France, 31 janvier 2024. https://learn.microsoft.com/fr-fr/compliance/regulatory/offering-hds-france

- DPO Partagé, « Évolution du cadre réglementaire de l'hébergement des données de santé et du marché de l'information en nuage en France », Blog DPO Partagé, 10 avril 2024. https://www.dpo-partage.fr/evolution-hebergement-des-donnees-de-sante/

- FILIPPONE Dominique, « La Cnil adoube Microsoft pour l'hébergement des données de l'Assurance Maladie », Actualités Données personnelles, Le Monde informatique, 31 janvier 2024. https://www.lemondeinformatique.fr/actualites/lire-la-cnil-adoube-microsoft-pour-l-hebergement-des-donnees-de-l-assurance-maladie-92839.html

- FRANCE RELANCE, « Stratégie nationale pour le cloud - Soutenir l'innovation dans le cloud », Dossier de presse, 2 novembre 2021. https://www.enseignementsup-recherche.gouv.fr/sites/default/files/2021-11/dossier-de-presse---strat-gie-nationale-pour-le-cloud-14677.pdf

- GALICHET Charlotte, « Nouvelles Clauses Contractuelles Types relatives au transfert de données vers un pays tiers : Quels changements ? », Données personnelles, 22 juin 2021. https://avocatspi.com/2021/06/22/nouvelles-clauses-contractuelles-types-relatives-au-transfert-de-donnees-vers-un-pays-tiers-quels-changements/

- HAAS AVOCATS, « Accord UE-US sur le transfert des données : un pastiche shield ? », Blog du cabinet HAAS Avocats, 4 septembre 2023. https://info.haas-avocats.com/droit-digital/accord-ue-us-sur-le-transfert-des-donnees-un-pastiche-shield

- INTERNET SOCIETY – France CHAPTER, « L'Internet Society France demande l'annulation de la délibération de la CNIL autorisant l'hébergement par Microsoft des données de santé des Français », Communiqué de presse, 13 avril 2024. https://cdn.isoc.fr/wp-content/uploads/2024/02/CP_ISOCFR_Donneesdesante.pdf

- ISSARNI Alain, « Pourquoi il faut renforcer la sécurité des données de santé avec le SecNumCloud », L'Usine Digitale, 11 avril 2024. https://www.usine-digitale.fr/article/pourquoi-il-faut-renforcer-la-securite-des-donnees-de-sante-avec-le-secnumcloud.N2206235

- KLABA Octave, Publication du directeur générale d'OVH Cloud sur le réseau LinkedIn, 8 février 2024. https://fr.linkedin.com/in/octave-klaba-3a0b3632

- LE FIGARO avec AFP, « Données de santé : OVH Cloud se positionne sur le Health Data Hub », Le Figaro Flash Eco, 9 janvier 2024. https://www.lefigaro.fr/flash-eco/donnees-de-sante-ovh-cloud-se-positionne-sur-le-health-data-hub-20240109

- LEFEBVRE DALLOZ, « Traitement des données de santé », Fiche thématique Droit des affaires - Protection des données personnelles (RGPD), 8 décembre 2023 https://open.lefebvre-dalloz.fr/droit-affaires/protection-donnees-personnelles/traitements-donnees-sante_a93474

- LOUYER Adriane « L'hébergement des données de santé : Un sujet enfin réglé ? ». Blog Houdars & Associés Avocats. 4 juillet 2023. https://www.houdart.org/lhebergement-souverain-des-donnees-de-sante-un-sujet-enfin-regle/

- MARTIAL-BRAZ Nathalie, « Souveraineté numérique – Souveraineté numérique en danger ! », Communication Commerce électronique n°5, mai 2024, repère 5, LexisNexis. https://www.lexis360intelligence.fr/revues/Communication_-_Commerce_%C3%A9lectronique/PNO_RCCE/document/PS_KPRE-678709_0KTB?doc_type=doctrine_revue&q=souverainet%C3%A9%20donn%C3%A9es%20de%20sant%C3%A9&sort=score&from=0&to=1715759217168&source=history&numero=11

- MICROSOFT – Documentation

MICROSOFT.COM, « Health Insurance Portability and Accountability Act (HIPAA) & Health Information Technology for Economic and Clinical Health (HITECH) Act », Document de conformité Microsoft Accessible en ligne, 31 janvier 2024. https://learn.microsoft.com/fr-fr/compliance/regulatory/offering-hipaa-hitech

MICROSOFT.COM, « Plan d'action RGPD Microsoft 365 - Principales priorités pour vos premiers 30 jours, 90 jours et au-delà », Document de conformité Microsoft accessible en ligne, 17 mars 2023. https://learn.microsoft.com/fr-fr/compliance/regulatory/gdpr-action-plan

- NOYB Association, « La Commission européenne soumet les transferts de données entre l'UE et les Etats-Unis à un troisième examen par la CJUE », News Noyb Data Transfers, 10 juillet 2023. https://noyb.eu/fr/european-commission-gives-eu-us-data-transfers-third-round-cjeu

- OVH CLOUD BLOG, « OVHcloud accélère sur sa stratégie SecNumCloud avec la qualification SecNumCloud 3.2 sur trois datacenters distincts », Communiqué de presse, 9 janvier 2024. https://corporate.ovhcloud.com/fr/newsroom/news/secnumcloud-strategy-acceleration/

- ROBERT Alice et FIEVEE Alexandre, « Un entrepôt de données de santé peut-il être hébergé par Microsoft ? », DSIH – L'actualité des systèmes d'information hospitaliers et de la e-santé, 26 février 2024. https://www.dsih.fr/article/5419/un-entrepot-de-donnees-de-sante-peut-il-etre-heberge-par-microsoft.html

- SCHMIEDT Morgan, « DATA PRIVACY FRAMEWORK – Le député et membre de la CNIL Phillipe Latombe dépose un recours à la CJUE pour obtenir l'annulation de la décision d'adéquation avec les États-Unis », Blog eWatchers.org, Information du 8 septembre 2023. https://ewatchers.org/info/2023-09-08-data-privacy-framework-le-depute-et-membre-de-la-cnil-phillipe-latombe-depose-un-recours-a-la-cjue-pour-obtenir-l-annulation-de-la-decision-d-adequation-avec-les-etats-unis-150

- VITARD Alice, « Les Etats-Unis renouvellent et étendent leur pouvoir de collecte de données sur les communications », L'Usine Digitale, 22 avril 2024. https://www.usine-digitale.fr/article/les-etats-unis-renouvellent-et-etendent-leur-pouvoir-de-collecte-de-donnees-sur-les-communications.N2211872

- VITARD Alice, « EUCS : Des fournisseurs européens, dont OVHCloud et Orange, appellent à protéger les données sensibles », L'Usine Digitale, 12 avril 2024. https://www.usine-digitale.fr/article/eucs-des-fournisseurs-europeens-dont-ovhcloud-et-orange-appellent-a-proteger-les-donnees-sensibles.N2211456

- VITARD Alice, « Les données de santé d'EMC2 hébergées chez Azure, le label SecNumCloud désavoué ? », L'Usine Digitale. 5 février 2024. https://www.usine-digitale.fr/article/les-donnees-de-sante-d-emc2-hebergees-chez-azure-le-label-secnumcloud-desavoue.N2207612

- VITARD Alice, « Le cloud souverain n'est-il qu'un fantasme ? », L'Usine digitale, 20 octobre 2021. https://www.usine-digitale.fr/article/le-cloud-souverain-n-est-il-qu-un-fantasme.N1151837

- ULYS, « Article 9 : Traitement portant sur des catégories particulières de données à caractère personnel », Article, GDPR.expert. https://www.gdpr-expert.eu/article.html?id=9#eu-regulation

- ZIRAR Wassinia, « Health Data Hub : la CNIL lâche temporairement du lest sur l'hébergement chez Microsoft », Ticpharma.com. 2 février 2024. https://www.ticpharma.com/story?ID=2491

- **Webinaires**

- CNIL, « Webinaire Transferts de données hors de l'UE : quelles sont les règles de base ? », 7 juin 2024 à 11h.

- CNIL, BOUCHER DE CREVECOEUR Erik, « Webinaire Etablissements de santé : les référentiels en santé et la « gouvernance » de la protection des données », 11 octobre 2022.