ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 8454	De **Mme Anne Le Hénanff** (Horizons et apparentés - Morbihan)	**Question écrite**

Ministère interrogé > Transition numérique et télécommunications	**Ministère attributaire** > Santé et prévention

Rubrique >numérique	**Tête d'analyse** >Révision du référentiel HDS	**Analyse** > Révision du référentiel HDS.

Question publiée au JO le : **30/05/2023**
Réponse publiée au JO le : **12/12/2023** page : **11277**
Date de changement d'attribution : **21/07/2023**

Texte de la question

Mme Anne Le Hénanff appelle l'attention de M. le ministre délégué auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargé de la transition numérique et des télécommunications, sur la certification « hébergement des données de santé » (HDS). La certification HDS est une référence au niveau national qui permet d'attester de la capacité d'un opérateur à mettre en place un hébergement protecteur des données de santé à caractère personnel, particulièrement sensibles, et ainsi construire un environnement de confiance autour de la modernisation du système de santé français. Le 2 novembre 2022, l'Agence du numérique en santé (ANS) a officiellement mis en consultation la révision du référentiel HDS avec comme un des objectifs principaux le renforcement des exigences de protection des données personnelles, au regard des transfert de données hors de l'Union européenne. Le 14 décembre 2022, l'ANS a publié une révision de la feuille de route du numérique en santé qui érige la souveraineté numérique et la durabilité en valeurs cardinales. Cette feuille de route souligne la nécessité de renforcer la souveraineté numérique, *via* HDS, en mettant en place des mesures juridiques et techniques pour réduire le risque de transfert hors de l'Union européenne. Les données de santé des Français étant des données particulièrement sensibles et stratégiques, il est impératif de les protéger face aux risques de captation par des autorités étrangères. En effet, certaines législations extraterritoriales, comme le *Foreign Intelligence Surveillance Act* (dit FISA Act) ou le *Cloud Act* aux États-Unis d'Amérique, permettent à des autorités étrangères d'avoir accès à des données sans que les utilisateurs concernés ni les autorités compétentes des pays où ils sont établis n'aient à en être informés. La feuille de route du numérique en santé 2023-2027, « Mettre le numérique au service de la santé », présentée le 17 mai 2023, va dans ce sens et annonce que le cadre réglementaire sur l'hébergement devra être renforcé pour renforcer la souveraineté de la France. Ainsi, il est précisé que « dans un premier temps, la nouvelle certification "hébergement de données de santé" (HDS), évoluera en 2023 pour intégrer un hébergement systématique des données de santé dans l'Espace économique européen avec des mesures juridiques ou techniques de réduction du risque de transfert extraterritorial des données. À l'horizon 2027, dès qu'un consensus européen aura émergé sur les exigences du niveau 3 du futur schéma de certification européen sur les services en nuage (EUCS) et qu'une offre souveraine suffisamment large sera disponible, la certification HDS fixera de nouvelles exigences en matière de souveraineté. Les acteurs sont incités à anticiper, en commençant le plus tôt possible avec leurs nouveaux projets ». Aussi, Mme la députée souhaite savoir quelles évolutions du référentiel sont concrètement prévues afin de garantir une protection effective des données de santé. Elle aimerait également des précisions sur les mesures « juridiques ou techniques » afin de réduire le risque de transfert extraterritorial des données, annoncées dans la feuille de route. Enfin, elle souhaite savoir si ces mesures seront alignées sur les critères du chapitre 19.6 du

référentiel SecNumCloud.

Texte de la réponse

Afin de garantir une protection effective des données de santé à caractère personnel, la Délégation au numérique en santé (DNS) et l'Agence du numérique en santé (ANS) ont introduit, dans la version révisée du référentiel de certification des hébergeurs de données de santé (HDS), quatre nouvelles exigences concernant la souveraineté des données qui s'appliqueront à tout hébergeur de données de santé à caractère personnel et à ses sous-traitants. Ces exigences ont été élaborées en tenant compte de nombreux échanges avec les services de la Commission nationale de l'informatique et des libertés (CNIL) sur le référentiel de certification HDS, pour lequel celle-ci a rendu un avis le 13 juillet 2023. Elles portent sur la souveraineté des données de santé et visent à garantir le respect du règlement général sur la protection des données (RGPD) par les hébergeurs. La certification HDS apporte ainsi des garanties aux personnes quant à la protection de leurs données de santé, notamment vis-à-vis des législations extracommunautaires qui pourraient présenter un risque de divulgation des données et ne pas leur apporter les garanties reconnues par le RGPD quant à l'effectivité de leurs droits. Les 4 exigences, qui s'appliquent à l'hébergeur et à ses sous-traitants, peuvent être résumées ainsi : - obligation de stocker les données de santé à caractère personnel sur le territoire de l'Espace économique européen ; - transparence de l'hébergeur vis-à-vis de ses clients sur l'encadrement et les garanties prises en cas d'accès à distance depuis un pays tiers à l'Union européenne ne faisant pas l'objet d'une décision d'adéquation. L'hébergeur doit indiquer au client si les garanties appropriées mises en place permettent de garantir un niveau de protection des données équivalent à celui garanti par le droit de l'Union, et à défaut documente les mesures supplémentaires qu'il a prises pour garantir un tel niveau ; - obligation de transparence de l'hébergeur vis-à-vis de ses clients sur son éventuelle soumission à une loi extraterritoriale n'assurant pas un niveau de protection adéquat au sens du RGPD et sur les mesures mises en œuvre pour atténuer les risques d'accès non autorisés aux données induits par ces règlementations (mesures pouvant prendre des formes diverses : d'ordre juridique/contractuel, organisationnel ou technique, et dont l'appréciation relève de la compétence de la CNIL) ; - obligation pour l'hébergeur de rendre public sur son site internet et sur le site de l'ANS les transferts de données de santé vers un pays n'appartenant pas à l'Espace Economique Européen et les risques d'accès auxquels il est soumis. Lors de la révision du référentiel de certification HDS, le choix a été fait de ne pas aligner les exigences avec les mesures relatives à l'immunité extraterritoriale figurant dans le référentiel SecNumCloud (Version 3.2) de l'Agence nationale de la sécurité des systèmes d'information au paragraphe 19.6. En effet, parmi les 270 hébergeurs qui étaient certifiés « HDS » en juin 2023, un seul est certifié dans la version 3.2 du référentiel SecNumCloud et quatre sont certifiés sur la version précédente du référentiel SecNumCloud. Par conséquent, la quasi-totalité des hébergeurs n'auraient pas eu la capacité d'obtenir la qualification SecNumCloud dans le délai imparti, obligeant les éditeurs, les professionnels de santé ou les établissements de santé à migrer leur solution vers un autre hébergeur. Il s'agit d'une opération complexe et coûteuse, pouvant avoir un effet dissuasif et faisant courir un risque juridique majeur d'illégalité des hébergements de données de santé supportés par les responsables de traitement exerçant des activités médicales, paramédicales, médico-sociales et sociales. En définissant ces nouvelles exigences, la DNS a la volonté d'inciter les acteurs de l'hébergement de données de santé vers davantage de souveraineté, un sujet qu'elle porte également dans la négociation du texte européen relatif à l'espace européen des données de santé. Le référentiel HDS prévoit explicitement une clause de revoyure, indiquant que des exigences renforcées en terme de souveraineté européenne seront ajoutées au plus tard en 2027, en cohérence avec les futurs référentiels européens (EUCS – European Cybersecurity Certification Scheme for Cloud services).