ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

Mercredi
29 avril 2026
Séance de 16 heures 30

Compte rendu n° 33

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à seize heures trente.

M. le président Philippe Latombe. Le cycle d'auditions de notre commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France, nous amène à recevoir la nouvelle directrice générale de la Plateforme des données de santé (PDS), Mme Hela Ghariani. Je rappelle qu'au début de nos travaux, nous avions reçu le directeur par intérim de la PDS, M. Laurent Vilbœuf.

Mme Ghariani, je vous remercie d'avoir répondu à notre invitation. Nous avons plusieurs questions à vous poser, mais avant cela, nous souhaitons vous entendre sur votre vision de la PDS et sur vos priorités d'action. Nous souhaitons également faire le point sur le projet de migration des données de santé vers une solution d'hébergement souveraine, qui sera bientôt une réalité.

Avant de vous céder la parole, je vous demande de déclarer au préalable tout intérêt public ou privé de nature à influer sur vos déclarations. Je rappelle également que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission de prêter le serment de dire la vérité, toute la vérité, rien que la vérité.

(Mme Hela Ghariani prête serment).

Mme Hela Ghariani, directrice générale de la Plateforme des données de santé. Je me présente devant vous en tant que nouvelle directrice générale de la Plateforme des données de santé. J'ai pris mes fonctions il y a tout juste deux semaines. Auparavant, j'étais responsable de la délégation ministérielle au numérique en santé, où j'ai notamment porté, aux côtés de nos collègues de l'assurance maladie, la mise en place de Mon espace santé, le carnet de santé numérique des Français, un service public souverain, universel et gratuit, qui permet à chacun d'avoir la main sur ses données les plus sensibles. Avant cela, j'ai travaillé sous la direction d'Henri Verdier, que vous avez auditionné, à la mise en œuvre du programme beta.gouv.fr, qui a été l'un des premiers espaces dans lesquels nous avons internalisé des compétences numériques au cœur des services publics.

Je pense que vous m'interrogerez, au cours de cette audition, sur notre choix de retenir un hébergeur français, Scaleway, pour la PDS. Ce choix est avant tout le résultat d'un travail engagé dès 2019, destiné, d'une part, à garantir techniquement la réversibilité de la plateforme, c'est-à-dire notre capacité effective à changer d'hébergeur, et, d'autre part, à suivre assidûment l'évolution de l'offre de cloud française et européenne.

La PDS a pour vocation de permettre à des centaines, et je l'espère un jour à des milliers, d'acteurs d'accéder selon des standards de sécurité très élevés à des espaces de travail élastiques, c'est-à-dire capables de s'adapter à leurs besoins pour traiter des volumes massifs de données intrinsèquement sensibles. Pour réaliser cette mission, nous devons disposer d'une architecture technique avec un niveau d'exigence très élevé en termes d'élasticité et de sécurité.

Le choix dont nous allons discuter aujourd'hui est en réalité la rencontre entre ces besoins, particulièrement exigeants, et la maturité de l'offre aujourd'hui disponible. Nous avons annoncé notre choix la semaine dernière, mais je tiens à remercier l'ensemble des fournisseurs de cloud qui ont participé à la démarche et qui ont fait preuve d'un niveau d'engagement à la

hauteur de nos attentes, permettant de créer les conditions d'un travail serein et de grande qualité. Si vous avez des questions sur le détail de ces offres, je me permettrai de vous adresser mes réponses par écrit, car un certain nombre d'informations sont couvertes par le secret des affaires.

La Plateforme des données de santé est devenue un projet emblématique des questions de souveraineté liées à l'hébergement et au cloud, et nous en sommes parfaitement conscients. Mais notre mission est avant tout de permettre aux acteurs qui préparent l'avenir de notre système de santé de travailler dans les meilleures conditions, de concevoir des projets, des études, des évaluations et des thérapies sur la base de données qui ressemblent à nos populations et qui nous appartiennent. Si nous contribuons humblement aux enjeux de souveraineté numérique, j'espère que nous contribuerons aussi activement à poser les bases d'une souveraineté sanitaire, dans le contexte de l'arrivée du règlement relatif à l'espace européen des données de santé (EHDS).

M. le président Philippe Latombe. Pourriez-vous préciser le calendrier prévu pour la migration, avec la marge d'incertitude inhérente à un projet informatique ? Cette intégration se fera-t-elle uniquement sur des ressources propres, de votre part et de celles du prestataire, ou bien comptez-vous recourir à un intégrateur ? Si oui, s'agira-t-il de celui qui était déjà présent au sein de la plateforme, à savoir Capgemini ?

Mme Hela Ghariani. Nous avons prévu de construire les infrastructures nécessaires pour héberger la base principale des données de remboursement de l'assurance maladie, d'ici la fin de l'année 2026 ou le début de l'année 2027. Ce rétroplanning intègre des enjeux réglementaires importants, notamment l'audit de la sécurité des systèmes d'information (Passi), et la demande d'autorisation auprès de la Commission nationale de l'informatique et des libertés (Cnil) pour opérer la copie de la base principale du système national des données de santé (SNDS).

Le projet sera mené essentiellement par des équipes internes à la PDS. Nous avons demandé aux acteurs qui ont participé à la procédure de nous présenter des propositions d'accompagnement. L'offre que nous avons retenue, celle de Scaleway, prévoit la mobilisation de deux de leurs experts qui seront accueillis en immersion chez nous le temps du développement. Il n'y a pas d'intégrateur tiers prévu dans le projet. Je tiens toutefois à indiquer qu'une partie des équipes de développement de la plateforme sont des prestataires externes, mais il s'agit généralement de freelances qui interviennent directement au sein de notre équipe.

Mme Cyrielle Chatelain, rapporteure. Vous l'avez souligné, la Plateforme des données de santé est devenue un objet emblématique de la question de la souveraineté. Vous avez également indiqué que la PDS avait suivi l'évolution de l'offre de cloud. Quels sont les éléments déterminants dans l'évolution de cette offre, au-delà de la volonté politique, qui vous ont conduit à choisir une offre française ?

Mme Hela Ghariani. Il convient dans un premier temps de rappeler la nature de nos besoins. Nous avons une architecture nativement sécurisée, pour laquelle nous avons choisi des mécanismes de défense en profondeur. Cela signifie que pour chaque risque de sécurité susceptible de compromettre l'intégrité et la disponibilité de nos données, nous avons une, deux, voire trois mesures de sécurité. Cette stratégie s'appuie sur des services cloud et des options de configuration exigeants, ce qui explique notre capacité à offrir des conditions de sécurité très poussées.

Ce niveau d'exigence a été régulièrement mesuré au regard de la disponibilité des offres. La PDS avait établi un rapport dès 2019, renouvelé en 2020, puis une nouvelle étude en 2022. J'ai moi-même participé au suivi d'une étude menée en 2023 à la demande de la Cnil sur le projet EMC2, et plus récemment à l'analyse des offres. Ce que j'ai pu observer, notamment entre 2023 et ce nouvel exercice de comparaison, c'est d'abord l'apparition de nouvelles offres sur le marché, mais aussi, au sein de ces offres, de nouvelles fonctionnalités. Je pense à la gestion des identités et des accès, aux systèmes de gestion des clés et de chiffrement, ou encore à la brique Kubernetes, qui était pour nous un élément très attendu. Ces options sont aujourd'hui disponibles et présentent des niveaux de service et de configuration qui nous permettent de mettre en œuvre notre stratégie de défense en profondeur.

Nous avons passé plus de vingt-huit heures en audition avec les huit fournisseurs de cloud qui ont bien voulu nous présenter une offre depuis le mois de février. Eux-mêmes ont constaté, lors de ces auditions, une évolution certaine de l'offre disponible qui nous permet aujourd'hui d'amorcer cette bascule. Nous avons adressé aux fournisseurs un cahier d'exigences très fourni, comportant plus de 350 points. Aucune des offres ne satisfaisait l'intégralité de ces exigences, ce qui montre le niveau de notre cahier des charges. Néanmoins, nous avons collectivement estimé – je dis « collectivement » car nous étions accompagnés par des collègues de l'Institut national de recherche en sciences et technologies du numérique (Inria), de la direction interministérielle du numérique (Dinum) et du ministère de la santé – que, malgré les fonctionnalités manquantes, nous étions capables de mettre en place avec le partenaire retenu des mesures de contournement raisonnables en termes de délai et de sécurité.

Mme Cyrielle Chatelain, rapporteure. Je retiens de votre propos que, même si aucune offre ne répondait aux 350 exigences, les huit offres que vous avez étudiées étaient globalement solides.

Avez-vous une idée du coût de la migration ? Le recours à une offre française entraîne-t-il un surcoût par rapport à une solution non souveraine ?

Mme Hela Ghariani. Concernant le coût de la migration, l'essentiel des travaux relève du développement, qui sera en grande partie à la charge de la PDS. Il s'agit donc simplement d'une question de priorisation de nos ressources de développement internes, et on peut dire qu'il n'y a pas de surcoût entraîné par la migration en tant que telle.

Néanmoins, il convient de garder à l'esprit que, dans notre stratégie, nous serons amenés à maintenir notre infrastructure actuelle, hébergée chez Microsoft Azure, pendant douze à dix-huit mois. En effet, plus de 250 projets y sont hébergés, et il n'est pas question de les arrêter tant que la nouvelle infrastructure n'est pas capable de les accueillir. Le surcoût est donc plutôt lié à cette période de transition, durant laquelle nous opérerons deux plateformes simultanément.

Nous vous transmettrons par écrit le détail des offres financières. L'offre que nous avons retenue faisait partie des moins chères. Pour autant, cela ne nous permet pas d'établir qu'elle nous coûtera moins cher sur le long terme. Quand on fait les simulations, sur un modèle où l'on paie à la consommation (« pay as you go »), nous ne devrions pas avoir de différence substantielle d'un point de vue financier. Toutefois, nous n'en sommes qu'au début des échanges techniques avec le partenaire retenu et nous ne sommes pas encore entrés dans les subtilités des mécanismes de réservation de capacité. Nous pourrons donc établir un bilan financier plus précis dans un second temps.

M. le président Philippe Latombe. Concernant la copie du SNDS, vous comptez demander la rédaction et la prise d'un décret uniquement à la fin du processus. Aujourd'hui, la Cnil conserve son rôle d'autorisation des recherches. Il a été envisagé, à un moment, de ne plus avoir à passer par le filtre de la Cnil. Le fait de basculer vers une solution souveraine, répondant ainsi à la demande formulée par la Cnil, signifie-t-il pour vous que nous pourrons évoluer vers un système ne nécessitant plus le recours à son avis préalable ?

Ma deuxième question porte sur l'espace européen des données de santé. Le choix, très significatif, de retenir un fournisseur de cloud français, permettant ainsi de solder une partie des difficultés passées, pourrait-il constituer un signal envoyé à l'Union européenne ? Comment comptez-vous promouvoir ce choix stratégique français au niveau européen ? Je note que, le jour même où la PDS a annoncé son choix de confier l'hébergement à Scaleway, cela ne vous a pas échappé, l'Union européenne annonçait que parmi les quatre fournisseurs de cloud qu'elle retenait pour accompagner les agences de la Commission européenne, figurait ce même acteur. Mon propos n'est pas de vous inciter à promouvoir la même solution, naturellement, mais ce mouvement commence à trouver des échos en Europe. Pensez-vous que l'espace européen des données de santé permettra d'éviter les mêmes errements que nous avons connus autour de la PDS, et de s'orienter directement vers une solution souveraine européenne ?

Mme Hela Ghariani. Concernant l'impact de notre projet de bascule sur le rôle réglementaire de la Cnil dans l'autorisation des projets, il convient de rappeler que notre objectif est de récupérer une copie de la base principale des données de l'assurance maladie afin d'accélérer la mise à disposition des données dans des bulles sécurisées. Cependant, toute la phase réglementaire en amont, c'est-à-dire l'avis de la Cnil et celui du Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (Cesrees), ne sera pas affectée par la bascule. En d'autres termes, un projet s'appuyant sur les données du SNDS devra toujours prouver son respect de l'intérêt public après avis du Cesrees, et sa conformité au règlement général sur la protection des données (RGPD) après avis de la Cnil. Ainsi, la récupération d'une copie de la base principale ne déroge en rien au cadre réglementaire existant.

En revanche, et je tiens à saluer le travail des équipes de l'assurance maladie qui opèrent un portail de gestion des demandes d'accès depuis 2019, cette bascule permettra à nos équipes, qui préparent aujourd'hui l'appariement et les jeux de données, de le faire dans les conditions offertes par notre plateforme technologique, plutôt que d'avoir à envoyer des codes à l'assurance maladie pour que celle-ci réalise les extractions. C'est donc toute cette phase, en aval du processus réglementaire, que nous ambitionnons d'accélérer.

Le règlement européen prévoit de généraliser partout en Europe le régime des permis, qui est très calqué sur le modèle français. Il nous incombe donc désormais, en associant les parlementaires, de définir par la loi un processus d'accès aux données de santé qui soit à la fois simple pour les porteurs de projets, afin d'accélérer la recherche et l'innovation, tout en garantissant les droits des personnes et les libertés individuelles.

Dans ce contexte, le rôle de la PDS sera de mettre à disposition les infrastructures techniques et de faciliter la recherche des données d'intérêt via son catalogue des métadonnées. Pour ce qui est du régime des autorisations, des permis, des contrôles et des audits, je pense que ce travail se fera en lien étroit avec la Cnil. C'est cette répartition des missions au sein de l'organisme responsable de l'accès aux données (Orad) que nous devons encore définir, puis entériner par la loi.

Pour en venir à votre question sur les modalités de sécurisation de l'hébergement des données prévues par le règlement européen, je peux vous dire qu'en 2021-2022, lorsque nous abordions ces questions avec nos homologues européens, nos préoccupations recevaient un faible écho. Je me souviens avoir bataillé pour que des exigences sur l'hébergement des données par les Orad soient inscrites dans le règlement, et que tous les *Health Data Hubs* européens soient soumis à un même niveau d'exigence.

Nous avons réussi, avec le soutien de quelques États membres, à obtenir que les données soient hébergées sur le territoire européen, ce qui constituait une victoire symbolique. En revanche, nous n'avons pas réussi à obtenir un équivalent de ce que prévoit la loi visant à sécuriser et à réguler l'espace numérique, dite loi Sren, avec des exigences de cloud spécifiques. Aujourd'hui, le règlement impose que tous les acteurs chargés de l'accès aux données veillent à ce que celles-ci soient hébergées sur le territoire européen. Il prévoit une dérogation permettant à certains États d'héberger ces données chez des acteurs dépendants de législations étrangères disposant d'une décision d'adéquation avec le RGPD, ce que la France ne fera pas, la loi Sren ayant déjà fixé notre cadre. Le règlement établit donc un socle, la localisation, mais ne nous interdit pas d'être plus exigeants.

Enfin, des exigences de sécurité supplémentaires doivent encore être affinées avec les États membres, et il ne nous sera bien évidemment pas interdit de pousser pour élargir au maximum ce niveau d'exigence. Vous pouvez compter sur moi pour le faire.

M. le président Philippe Latombe. Comment concilier les exigences françaises très élevées, issues de la loi Sren et d'une décision du Parlement, avec la nécessité de mutualiser des données avec des pays qui n'appliqueront que le socle minimum, à savoir la localisation ? Un conflit de normes apparaîtra sur ce sujet. Comment le gérerez-vous ? Vous allez devoir partager des données avec la Hongrie ou d'autres pays qui auront choisi de n'utiliser que le socle minimum, alors que la loi Sren vous interdit de transférer les données de nos concitoyens vers des solutions qui ne sont pas certifiées SecNumCloud.

Mme Hela Ghariani. Je pense qu'une jurisprudence devra s'établir. Dans les discussions que nous avons aujourd'hui avec les autorités nationales dans le cadre de la mise en œuvre du règlement européen, il est évident que l'Orad français devra indiquer qu'il ne souhaite pas partager de données avec des acteurs dont les niveaux d'exigence sont inférieurs aux siens. Je pense qu'il y aura des recours contre ces décisions et qu'une jurisprudence se constituera avec le temps. Cependant, il nous reste une fenêtre de négociation : les actes d'exécution qui, comme je le disais, fixeront les exigences de sécurité applicables aux conditions d'hébergement. Je pense que, dans ce cadre, nous pourrons établir que des États ayant choisi des niveaux de sécurisation supérieurs seront en droit de refuser d'envoyer des données à des États dont les niveaux d'exigence sont inférieurs.

M. le président Philippe Latombe. Avez-vous une idée du calendrier de publication de ces actes d'exécution ?

Mme Hela Ghariani. Pour le moment, la Commission européenne annonce un calendrier qui nous amène jusqu'à la mi-2027. Ces sujets sont donc en cours de discussion. Nous ne sommes pas encore entrés dans le détail des exigences de sécurité, mais nous commençons déjà à discuter avec la Commission des actes d'exécution portant, par exemple, sur le contenu des demandes de permis et d'accès.

Mme Cyrielle Chatelain, rapporteure. La Plateforme des données de santé, vous l'avez dit, recense un grand nombre de données de santé, ce qui lui confère une expertise sur leur caractère sensible. Nous savons qu'il existe également des acteurs privés. Pouvez-vous nous dire si, pour vous, les données de santé présentent une sensibilité particulière ? Dans votre approche, distinguez-vous différents niveaux de sensibilité ou considérez-vous que toute donnée de santé est, par nature, sensible ?

Mme Hela Ghariani. J'ai passé les six dernières années de ma vie à traiter des données de santé à caractère personnel et, à mon sens, elles sont particulièrement sensibles. L'une des raisons pour lesquelles j'ai choisi de m'investir sur ces questions est que je considère qu'elles représentent une forme de dernière frontière. Leur caractère particulièrement sensible nous permet de prévoir un cadre distinct de celui qui s'applique aux autres données personnelles – cadre qui est certes très bien encadré par le RGPD, mais sur lequel on observe une forme de cannibalisation par les géants du numérique extracommunautaires.

Sur les données de santé, nous conservons une sorte de pré carré. Si l'on regarde les données de santé utilisées dans le contexte du soin, on constate que beaucoup d'acteurs européens sont encore présents sur ces marchés. Cela fait partie, à mon sens, des derniers espaces sur lesquels nous pouvons exercer une forme de souveraineté réelle, c'est-à-dire disposer des moyens de garantir à la fois la sécurité et l'usage de ces données pour la pérennité de notre système de sécurité sociale et de nos systèmes de santé européens.

Les données de santé pseudonymisées et anonymisées destinées à un usage secondaire restent, à mon sens, tout aussi sensibles, ne serait-ce que parce que, dans le contexte de la PDS, nous parlons de données massives. Autant l'opinion est malheureusement de plus en plus habituée aux cyberattaques, autant je pense qu'il ne faut pas s'y accoutumer. Nous devons continuer à nous indigner et à considérer qu'il est inacceptable que ces données soient utilisées à d'autres fins que celles autorisées et encadrées par la loi.

L'une des missions de la PDS est de garantir cette sécurité, depuis les phases de pseudonymisation jusqu'à la vérification des finalités d'usage. Je pense notamment, en tant que secrétaire du Cesrees, à la nécessité de s'assurer que la finalité d'intérêt public soit toujours vérifiée au moment où l'on autorise l'usage de ces données.

M. le président Philippe Latombe. Votre réponse me permet d'évoquer un arrêt récent de la Cour de justice de l'Union européenne, qui considère que les données personnelles anonymisées et transférées à un tiers ne sont plus personnelles. Cette définition a été reprise par la Commission européenne dans son projet Omnibus. Quel regard portez-vous sur cette nouvelle définition et qu'est-ce que cela pourrait changer concrètement en termes d'obligation pour la plateforme qui, en France, est soumise à la loi Sren ? Je rappelle que d'après cette loi, les données, même pseudonymisées, restent des données personnelles et donc d'une sensibilité particulière.

Mme Hela Ghariani. Le ruissellement de cette décision n'impacte pas encore nos activités ni le cadre légal qui les encadre. Pour le moment, la situation reste inchangée. À la PDS, nous avons commencé à travailler avec les acteurs de l'écosystème sur la notion de données synthétiques. Nous considérons que, dans le champ de la santé, il serait préférable d'établir des méthodologies scientifiques nous permettant de garantir la production de jeux de données parfaitement anonymisés car synthétiques, c'est-à-dire ne reflétant aucune situation individuelle réelle. Nous pensons que cette approche nous protégera bien plus que de considérer que les données pseudonymisées et anonymisées ne sont pas retraçables. Il nous semble

préférable de travailler à la généralisation de l'usage des données synthétiques plutôt que d'essayer d'alléger le cadre réglementaire qui encadre les données qui ont été personnelles à un moment de leur cycle de vie.

M. le président Philippe Latombe. Un acteur français, Doctolib pour ne pas le nommer, a accès à une quantité très importante de données de santé. L'hébergement de ces données est certifié Hébergeur de données de santé (HDS), alors que vous êtes soumis à la certification SecNumCloud, comme la loi vous l'impose.

Une convergence entre HDS et SecNumCloud est-elle, selon vous, nécessaire ? Si oui, comment y parvenir ? La plupart des personnes que nous avons interrogées nous disent qu'imposer SecNumCloud immédiatement nuirait à la capacité à héberger des données de santé. Comment peut-on continuer à expliquer à nos compatriotes qu'il existe une telle divergence dans la sécurisation des données, avec d'un côté HDS et de l'autre SecNumCloud ?

Mme Hela Ghariani. L'hébergement des données de santé constitue l'un des premiers actes de régulation de l'hébergement de données sensibles dans l'histoire du droit numérique français. Les questions qui se posaient à l'époque n'étaient pas les mêmes qu'aujourd'hui. L'accent était mis sur la qualité et la sécurité des mécanismes liés à la gestion de l'hébergement et aux fonctions de cloud, davantage que sur les questions de souveraineté, au sens de la nationalité des entreprises qui assurent ces services. Cet historique explique qu'aujourd'hui, nous comptions 302 acteurs certifiés HDS, contre seulement neuf acteurs, sauf erreur, certifiés SecNumCloud. Il serait donc compliqué, sur le plan industriel, d'établir une correspondance immédiate entre HDS et SecNumCloud.

Néanmoins, lors de la dernière révision du référentiel HDS, qui date de 2023 ou 2024, il a été établi dans le préambule de l'arrêté, qui est public, qu'une nouvelle révision devrait certainement avoir lieu en 2027. Cette échéance tient compte des discussions européennes sur la certification européenne de cybersécurité pour les services cloud (EUCS), discussions qui ont connu des avancées plus ou moins heureuses. Dans le cadre de mes précédentes fonctions, j'ai pu échanger sur ces questions avec les collègues du ministère de l'économie et des finances, qui suivent ces discussions à l'échelle européenne, afin d'établir une trajectoire industrielle lisible pour les acteurs du cloud.

Des paliers ont été définis, comme l'obligation d'inscrire de manière systématique dans les contrats des hébergeurs HDS la transparence sur leur exposition à des lois extracommunautaires, et de rendre cette information publique sur le site de l'Agence du numérique en santé (ANS), qui liste l'ensemble des 302 hébergeurs de données de santé. Je sais que cette transparence ne suffit pas, mais elle envoie un signal aux acteurs qui produisent et achètent ces services. À titre personnel, j'estime que la convergence entre la certification HDS et SecNumCloud doit relever d'une décision industrielle prise avec mesure.

Mme Cyrielle Chatelain, rapporteure. Sur les 302 acteurs certifiés HDS, avez-vous une idée, même approximative, du nombre d'entre eux qui sont soumis à des lois extraterritoriales ? Il nous a été rapporté que la certification SecNumCloud comporte un volet de protection contre les lois extraterritoriales, mais aussi des volets de protection physique très étendus. Envisager un SecNumCloud légèrement moins strict en termes de protection physique, maximale dans le référentiel actuel, mais davantage exigeant sur la protection contre les lois extraterritoriales, constituerait-il une approche plus progressive pour les industriels ?

Mme Hela Ghariani. J'entends l'idée de créer une forme de gradation entre le référentiel HDS actuel et SecNumCloud. En toute sincérité, je n'ai pas d'opinion arrêtée sur la question. Je pense que les collègues de l'Agence nationale de la sécurité des systèmes d'information (Anssi), du ministère de la santé et bien sûr de la direction générale des entreprises (DGE) ont très certainement un avis beaucoup plus éclairé que le mien sur le sujet.

Je ne suis pas en mesure de vous dire aujourd'hui combien des 302 acteurs sont soumis à des lois extraterritoriales. Cependant, avec l'entrée en vigueur de la nouvelle version du référentiel, tous les acteurs certifiés HDS devront le déclarer. Nous pourrons donc à terme en établir un diagnostic clair, et cette information sera publique.

Enfin, nous avons établi une forme de correspondance entre HDS et SecNumCloud, en annexe du référentiel, pour bien identifier les exigences communes et distinctes, et ainsi mesurer précisément les écarts. C'est à partir de là que nous pourrons établir une sorte d'éventail des options de sécurité.

M. le président Philippe Latombe. Avez-vous une idée du budget que la PDS va consacrer à la cybersécurité ? Les fuites de données irritent beaucoup nos concitoyens et posent une question de confiance vis-à-vis de l'État.

Mme Hela Ghariani. La PDS a retenu une stratégie d'architecture de défense en profondeur. Par conséquent, toutes nos dépenses liées au développement de notre plateforme et à son maintien en condition de sécurité sont pour nous des dépenses de cybersécurité, même si notre comptabilité analytique ne les étiquette pas comme telles.

En revanche, nous aurons des dépenses spécifiques. Dans le cadre de l'audit Passi pour obtenir l'homologation SNDS, nous devrons réaliser un test d'intrusion. Ce sera très clairement une des dépenses à réaliser au cours de l'année 2026 pour vérifier le niveau de sécurité de l'infrastructure de Scaleway. De plus, nous allons provisionner, l'année prochaine, des crédits pour organiser des exercices de crise en situation réelle afin de nous préparer à différents scénarios d'attaques et de fuites possibles. Si nous avons bien appris quelque chose dans le secteur de la cybersécurité, c'est que la meilleure manière d'éviter une attaque, au-delà de toutes les actions de prévention, c'est aussi d'être prêt le jour où elle survient, afin de limiter le niveau de divulgation, de diffusion et de compromission des données que nous gérons.

M. le président Philippe Latombe. Nous arrivons au terme de cette audition. Nous vous remercions, madame Ghariani, d'avoir fait le point sur le calendrier et les perspectives de la Plateforme des données de santé.

La séance s'achève à dix-sept heures trente.

Membres présents ou excusés

Présents. – M. Nicolas Bonnet, Mme Cyrielle Chatelain, M. Philippe Latombe, Mme Isabelle Rauch