ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Mission d'information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Jeudi
18 février 2021
Séance de 14 heures

Compte rendu n° 30

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Jean-Luc Warsmann, *président*

ASSEMBLÉE NATIONALE

Audition commune, ouverte à la presse, de M. Adrien Parrot, médecin-ingénieur, président, et de Me Juliette Alibert, avocate, membre de l'association InterHop

La séance est ouverte à 14 heures.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Bonjour à toutes et à tous. Je souhaite la bienvenue à Maître Juliette Alibert et à M. Adrien Parrot. Nous poursuivons avec vous des échanges très nourris, depuis ce matin, sur la thématique des données de santé et de la souveraineté numérique. InterHop est une association qui promeut et développe l'utilisation de logiciels libres et *open source* pour la santé – vous nous en direz plus tout à l'heure. Je crois savoir que vous prônez une utilisation autogérée des données de santé à l'échelle locale. Vous souhaitez en quelque sorte « dégoogliser » la santé numérique en proposant des hébergements de données décentralisés, transparents et éthiques. Vous œuvrez également en faveur du respect du Règlement général sur la protection des données (RGPD). Enfin, je dois noter que vous avez participé aux activités du comité SantéNathon à l'origine du recours intenté devant le Conseil d'État contre le choix effectué par « Health Data Hub » (HDH) en faveur du *cloud* de Microsoft pour l'hébergement de ces données. Nous sommes très heureux de pouvoir échanger avec vous aujourd'hui. La protection des données nous intéresse, évidemment, tout comme le recours à des logiciels libres et la question des communs numériques. Je vais laisser la parole à notre rapporteur afin qu'il introduise nos échanges.

M. Philippe Latombe, rapporteur. Je voudrais, en guise d'introduction, vous interroger sur trois points qui occupent nos travaux et qui ont été esquissés par M. le président. J'aimerais d'abord que vous nous présentiez votre association, InterHop, ainsi que votre combat en faveur des logiciels libres et de l'interopérabilité des systèmes d'information. Ces questions entrent en effet dans le champ des travaux de notre mission d'information. Ils suscitent un intérêt croissant et des discours parfois très tranchés. Nous sommes donc particulièrement intéressés par votre avis sur ces sujets que vous connaissez bien. Je résumerai ici mon propos au travers des questions suivantes : quel logiciel libre pourrait être utilisé ou substitué, selon vous, à des solutions propriétaires ? Quels seraient les avantages de cette approche ? Quels en sont également les limites et les risques ? Enfin, comment, selon vous, la question des communs numériques peut-elle nourrir aussi nos réflexions sur la souveraineté numérique ?

Le second point sur lequel je souhaiterais échanger avec vous concerne le HDH et l'hébergement des données de santé. InterHop, comme l'a rappelé M. le président, fait partie des membres du collectif SantéNathon, qui a attaqué en Conseil d'Etat le choix du HDH de recourir au *cloud* de Microsoft pour héberger les données de santé. Le ministre des Solidarités et de la Santé, M. Olivier Véran, s'est engagé à ce que le transfert du HDH vers un autre hébergeur que Microsoft intervienne dans un délai compris entre 12 et 18 mois. J'aimerais savoir quel regard vous portez sur la situation actuelle, quelle leçon il est possible, selon vous, d'en tirer pour les autres projets numériques portés par les pouvoirs publics. J'aimerais également vous entendre, dans le prolongement de cette réflexion, sur l'initiative européenne GAIA-X, qui doit permettre à l'Europe de retrouver une forme de souveraineté sur le segment du *cloud*. Enfin, mon dernier sujet ne vous étonnera pas au regard de l'actualité très récente, à savoir la vague de cyberattaques sur les systèmes d'information d'établissements de santé. Face à la sophistication de la menace cyber, comment pensez-vous qu'il soit possible de

garantir un niveau de protection maximale de nos infrastructures numériques, en particulier dans le domaine de la santé qui est un domaine critique par nature ?

M. Adrien Parrot, président de l'association InterHop. Je suis médecin anesthésiste-réanimateur et informaticien. J'ai travaillé deux ans aux Hôpitaux de Paris, à l'entrepôt de données de santé – une plateforme qui regroupe l'ensemble des données des hôpitaux à des fins de recherche essentiellement. En guise de préambule, je souhaite souligner que l'association InterHop n'est en aucun cas opposée à la recherche en santé. J'en veux pour preuve que j'ai travaillé à l'entrepôt de données de santé de l'AP-HP, qui fait de la recherche. La question n'est pas là. De la même manière, en ce qui concerne le traitement des données, nous sommes conscients de la nécessité que les données ne soient pas accaparées, mais au contraire partagées. InterHop est le diminutif d'« interopérabilité », avec un H pour « hôpitaux ». L'interopérabilité des systèmes d'information est au centre de notre démarche. L'interopérabilité des informations permet d'échanger des informations, au besoin, entre systèmes d'informations différents. La problématique du HDH et de notre combat, par exemple au Conseil d'État, réside dans la protection des libertés fondamentales. Nous agissons exclusivement sur ce terrain. Encore une fois, nous ne sommes pas opposés à un projet de recherche, comme pourrait l'être le HDH. Le HDH est emblématique d'une problématique systémique, avec plusieurs composantes : une centralisation extrême des données, qui s'oppose par exemple au Ouest Data Hub dont vous a entretenu le Pr Marc Cuggia. Dans ce modèle, les projets peuvent être centralisés mais ils le sont au cas par cas, projet par projet, sans que cela ne devienne la norme : autrement dit, toutes les données ne sont donc pas stockées au même endroit, sur une même plateforme. Enfin, ce sont avant tout les problématiques de Microsoft et de l'extraterritorialité du droit américain qui nous ont alertés.

Concernant les alternatives, outre le Ouest Data Hub ou l'AP-HP, centre dans lequel j'ai travaillé, il existe également des entrepôts de données de santé à Marseille, Toulouse, Bordeaux, Lille, Grenoble – et j'en oublie. Les alternatives sont multiples. Pour revenir à l'exemple de l'AP-HP, son entrepôt de données de santé traite plusieurs millions de données de patients (10 à 11 millions sur le site de l'entrepôt de données de santé) avec une plateforme issue des logiciels *open source*. Quand je faisais encore partie de l'équipe, l'autonomie numérique était pensée grâce au logiciel *open source*, celui-ci permettant d'être autonome et de protéger au maximum les données confiées.

L'AP-HP a par ailleurs plusieurs dizaines de projets en cours, sur le Covid -19 actuellement. Si nous voulons aller vite et que nous partons du principe – ce qui est vrai – que le traitement des données et la recherche vont améliorer la qualité de vie et le soin, alors autant renforcer l'existant, que ce soit avec l'AP-HP ou Ouest Data Hub – je n'ai pas de parti pris sur une plateforme en particulier. D'autres alternatives existent. En dehors du secteur public, le Pr Marc Cuggia a parlé du TeraLab tout à l'heure. Le Centre d'accès sécurisé aux données (CASD), qui est homologué au Système national des données de santé (SNDS) et qui possède la certification Hébergeur de Données de Santé (HDS), va jusqu'à proposer des boîtiers physiques où l'utilisateur doit mettre son empreinte digitale pour accéder aux données. Ce système a la qualité de ne pas déporter la sécurité sur le poste utilisateur, celui-ci étant par ailleurs également sécurisé *via* l'infrastructure. Le boîtier se connecte ensuite à une plateforme, qui peut être une plateforme *big data*.

Pour finir, je dirai que les critiques sont nombreuses. Elles ne sont pas propres à notre association : la Commission nationale de l'informatique et des libertés (CNIL) et la Caisse nationale de l'assurance maladie (CNAM) ont également émis de telles critiques.

Lorsque j'étais encore en poste aux Hôpitaux de Paris, un courrier rédigé par M. Martin Hirsch et révélé par Mediapart avait en outre pointé les risques de perte de confiance des citoyens, des citoyennes et des patients en cas de doute sur l'extraterritorialité, par exemple du droit américain.

Me Juliette Alibert, avocate, membre de l'association InterHop. Je voulais revenir, puisque vous nous posez la question, M. le rapporteur, sur le contexte autour du contentieux qui englobe le HDH. Vous avez rappelé qu'InterHop était membre de SantéNathon et avait porté ce contentieux devant le Conseil d'État. Pour rappeler le contexte, cela me paraît important, le projet HDH est né fin 2018 et a été mis en place début 2019. Nous avons très tôt su que le choix de la solution technique serait porté sur Microsoft, et ce, sans qu'un appel d'offres ne soit réalisé comme Mme Stéphanie Combe l'a rappelé lors de l'audition de ce matin. Un décret devait normalement permettre de régir le traitement des données au sein du SNDS – le périmètre historique de celui-ci étant modifié. Nous étions dans l'attente de ce décret réglementaire pour procéder à la mise en place et au traitement des données au sein du HDH. Cependant, le contexte sanitaire lié à la crise du Covid -19 et l'état d'urgence ont permis, au regard d'un cadre dérogatoire, de « pousser » le droit commun et de mettre en place les projets et les bases au sein du HDH, alors même que le décret réglementaire n'était pas sorti. Une logique inverse s'est mise en place. Je tiens à rappeler que, normalement, les données de santé d'ores et déjà présentes sur le HDH devront être supprimées à l'issue de l'état d'urgence sanitaire, sauf si le décret d'application venait – lors de sa sortie – à les rendre légales et utilisables à l'issue de cette période.

Dans ce contexte, l'association InterHop s'est saisie de la jurisprudence *Schrems* II de juillet 2020. Cet arrêt a fait valoir que le droit américain n'assurait pas, en l'état, un niveau de protection équivalent au RGPD, ce qui a donné lieu à la fin du *Privacy Shield*. Au-delà, l'intérêt de cette jurisprudence réside dans le fait qu'elle a permis l'appréciation concrète, par le juge européen, des pratiques de renseignement des services américains, sur le fondement notamment de deux bases légales intéressantes : la section 702 du *Foreign Intelligence Surveillance Act* (FISA), qui permet l'obtention immédiate et rapide, par le gouvernement, d'informations très larges, sans aucune notification et sans garantie pour les citoyens européens, et, plus attentatoire aux libertés fondamentales et au droit à la protection des données personnelles, *l'Executive Order 12333*. Ce décret présidentiel autorise, à des fins de renseignement, des techniques d'interception sur les signaux en transit, mais également en dehors des États-Unis, par les câbles sous-marins, ce qui n'est pas sans faire écho aux révélations d'Edward Snowden de 2013.

L'existence de cette collecte large, massive, soumise à la discrétion du gouvernement, sans aucun ciblage et sans autorité indépendante, sans même de droit opposable pour les citoyens européens, s'avère totalement en inadéquation avec le RGPD. Je tiens à le rappeler car, lors des différentes auditions que vous avez pu mener, le *Cloud Act* est souvent évoqué, alors que ces deux bases légales ne le sont pas. Microsoft y est pourtant soumis, en tant que personne morale soumise au droit américain. Il serait donc contraint de transmettre des données si elles lui étaient demandées au titre du *FISA* ou de l'*Executive Order 12333*, et ce, bien que ces données soient conservées sur le territoire européen.

Dans le référé-liberté porté par SantéNathon, dont InterHop est membre, nous avons essayé de faire valoir l'atteinte à cette liberté fondamentale que constitue le droit à la protection des données et à la vie privée, en faisant reconnaître du juge administratif que les risques étaient avérés au regard du *FISA* ou de l'*Executive Order* et que cela constituait une violation des libertés fondamentales. Entre le moment où nous avons déposé le référé et le

moment où l'ordonnance a été rendue, un arrêté émanant du ministre de la Santé a été pris le 10 octobre pour interdire le transfert des données vers le territoire des États-Unis. Cependant, nous voulions faire valoir que, indépendamment de ce transfert-là, les données étaient, quoi qu'il en soit, mises en péril de par ces deux textes dont je viens de vous parler. La CNIL l'a très clairement rappelé. Un mémoire en observation a été produit lors de l'audience. Nous sommes donc dans une situation où ces risques ont été reconnus à la fois par le Conseil d'État, puisque le juge des référés a admis qu'il y avait effectivement des risques, par la CNIL et par le juge de l'Union Européenne, dans l'arrêt *Schrems* II. C'est un élément important qui mérite, je pense, d'être rappelé. Le ministre de la Santé a d'ailleurs lui-même reconnu qu'il existait des risques dans un échange de courriers avec la CNIL. Ces risques existent et sont donc avérés. Dans ce contexte, il nous semble essentiel de défendre les données personnelles des citoyens français comme européens.

Cette audience a également été l'occasion d'aborder les enjeux de sécurité, en particulier la centralisation des données de santé. Il est question ici des données de santé de plus de 67 millions de Français, ainsi que de celles des personnes étrangères soignées sur le territoire français. Il a été rappelé que les clés de chiffrement étaient détenues par Microsoft. Il semblerait d'ailleurs que cette information n'ait pas été démentie dans l'audition que vous avez menée, ce matin. Nous sommes dans une situation où la société Microsoft conserve elle-même les clés de chiffrement. C'est un peu comme si on avait un prisonnier à qui l'on remettait les clés de la cellule. Selon nous, dès lors que les *data scientists* – qui fondent la recherche au sein du HDH – ont besoin d'utiliser ces données, et que Microsoft a accès aux clés de chiffrement, cela signifie que Microsoft déchiffre les données pour permettre la recherche. Or, même si ces données sont pseudonymisées, elles sont ré-identifiables en les croisant entre elles.

M. Adrien Parrot. On voit bien que les enjeux sont moins liés au *Cloud Act,* qu'aux autres textes, de portée extraterritoriale, des États-Unis. On pourrait aussi se poser la question des répercussions, et si cela ne reste qu'un risque. Sur ce terrain, il faut déjà dire que cela ne concerne pas uniquement le terrorisme. J'en veux pour preuve M. Frédéric Pierucci, ancien cadre d'Alstom, qui s'est fait arrêter aux États-Unis et a passé plusieurs mois dans un quartier de haute sécurité, parce que l'État américain avait eu accès à des données provenant de ses mails. C'est bien la portée extraterritoriale du droit américain qui a des répercussions et qui fait pression sur les entreprises – françaises, en l'occurrence. Nous ne parlons pas que du terrorisme, mais de l'intelligence économique au sens large. Il ne faut pas être naïf : les données de santé constituent aussi des enjeux économiques importants. À titre d'exemple, l'investissement sur les données de santé compte pour un tiers du budget « santé » d'Alphabet, la maison-mère de Google.

Concernant les enjeux autour des données de santé, plus précisément, le logiciel libre a pour principe central l'autonomie des utilisateurs et des utilisatrices. Ces derniers peuvent lancer le logiciel directement sur leur poste de travail. Avec l'arrivée du *cloud* et des serveurs distants, cette autonomie s'effrite progressivement, heurtant de plein fouet les enjeux liés aux données de santé. L'un des principes fondateurs de la médecine réside dans le serment d'Hippocrate, autrement dit dans le secret médical. On sait qu'il n'y a pas de confidence sans confiance, et que le secret permet de créer une relation de confiance entre le médecin et le patient. En parallèle, les données doivent être utilisées à des fins de recherche. Les données constituent en quelque sorte l'or du 21ème siècle, dans la mesure où les algorithmes d'intelligence artificielle, les réseaux de neurones, apprennent grâce aux données. Nous avons donc besoin de traiter des données. Cela n'est pas nouveau : la recherche les utilise depuis plusieurs années. Nous sommes confrontés à une balance bénéfices/risques, où

il faut faire de la recherche tout en conservant un cadre de sécurité pour ne pas faire peur, pour garder la confiance millénaire, pluri-centenaire, de la relation médecin-malade. Cet enjeu de confiance est central.

Je vais citer une phrase, relative au développement des plateformes, du rapport de la mission présidée par M. Éric Bothorel : *« les infrastructures nécessaires à la donnée sont de plus en plus exposées à des formes de dépendance logicielles, ce qui soulève un enjeu d'autonomie stratégique. Il ne faut surtout pas que le patient ou la patiente soit pris dans des enjeux d'autonomie et perde confiance dans le système. Les retentissements en termes de santé publique peuvent aussi être importants sur ce terrain-là ».*

Me Juliette Alibert. Pour compléter ces propos, je pense qu'il faut aussi parler des risques majeurs en termes de mise à mal de la Sécurité sociale. On voit bien, aujourd'hui, que les GAFAM – Google, Apple, Facebook, Amazon et Microsoft – et d'autres entreprises privées ont compris l'intérêt financier majeur que les données représentent. L'exemple de la maison mère de Google, Alphabet, qui investit plus de 30 % de son budget dans les données de santé, illustre bien cette prise de conscience. Or, les pratiques des entreprises privées pourraient mettre à mal le système actuel de la Sécurité sociale, qui repose sur une collectivisation des risques. Les pratiques de ces sociétés et les outils connectés pourraient en effet permettre aux GAFAM, demain, de cibler très spécifiquement les individus et d'identifier ceux porteurs de risques, au regard de leur profil, menant ainsi à une forme de médecine prédictive. Ce type de pratiques pourrait progressivement mettre à mal le système actuel en faisant reposer le risque sur l'individu et non plus sur la solidarité et le collectif, dans le même esprit que le principe « pollueur payeur ». Nous pensons que le risque de délitement de la Sécurité sociale constitue l'un des enjeux majeurs des données de santé.

M. Adrien Parrot. Nous avons vu le cadre, à savoir la portée extraterritoriale du droit américain ainsi que les enjeux autour des données et de la santé numérisée. Nous souhaitons maintenant enchaîner sur les solutions que nous espérons modestement apporter. Concernant la gouvernance, nous pensons que l'erreur originelle du HDH est d'avoir fondu la technique et la gouvernance. Nous sommes d'accord pour avoir plutôt une gouvernance centralisée. Nous partageons le constat de la complexité de l'accès aux données et sommes favorables à un guichet unique d'accès, comme se propose de l'être le HDH, avec des facilitations d'accès pour les chercheurs et des publications de cahiers des charges pour que les acteurs du numérique, par exemple, puissent être au courant de ce qui est en train de se passer. Nous ne sommes pas non plus opposés à une plateforme centralisée de gestion des consentements. Des améliorations méritent effectivement d'être apportées à ce niveau. Sur la gouvernance, et pour partir de l'existant, nous pensons qu'il faut créer le plus rapidement possible un comité de pilotage indépendant et multipartite, avec des utilisateurs publics et privés – les pouvoirs publics et les acteurs du numérique – pour engager ces travaux de réversibilité. J'ai appris ce matin que la direction interministérielle du numérique (DINUM) a réalisé une étude sur le sujet. Au titre de nos actions, nous avons demandé l'accès aux rapports de réversibilité. À ce jour, nous avons uniquement pu voir le premier rapport, datant de novembre 2019, mais pas le deuxième. Je pense que ce rapport doit être public et « auditable » par les experts comme par les citoyens.

D'un point de vue technique, c'est un petit peu plus compliqué. Nos propositions consistent à centraliser le développement de codes. Ce mouvement est d'ores et déjà à l'œuvre avec l'existence des forges logicielles (GitLab, GitHub, etc.), qui permettent le regroupement des codes et la collaboration des développeurs sur ces codes. Cette plateforme peut être française ou européenne. Elle permet uniquement de développer des logiciels qui utiliseront

les données, sans qu'elle n'ait jamais accès à ces données. Il s'agit donc seulement de développement de code, sur ce principe plutôt centralisé – français ou européen. Par contre, nous sommes radicalement opposés – et nous sommes rejoints, je pense, par le Ouest Data Hub sur ce point – à la centralisation dans les données ou à la centralisation *a minima*, projet par projet. Nous sommes favorables en revanche à la fédération d'acteurs. Cela représente, pour nous, l'application du RGPD. La décentralisation permet de restreindre l'accès aux données à des finalités – une plateforme n'a pas accès à tout, en permanence – et la fédération permet de répondre aux enjeux d'interopérabilité et de portabilité des données. Ainsi, nous répondons très bien au RGPD avec cette décentralisation technique.

Dernière chose, nous proposons un réseau de fédérations d'ingénieurs avec Inter-CHU, qui regroupe les ingénieurs des hôpitaux français. Ces derniers se réunissent dans ce cadre pour échanger autour de leurs pratiques. Il ne s'agit en aucun cas d'échanger des données, évidemment, mais bien des pratiques – autour du code, par exemple.

Me Juliette Alibert. Nous voulions aussi vous présenter rapidement des propositions davantage tournées vers le volet juridique. Dans la lignée de la loi pour la République numérique, qui prône le recours, pour les administrations, au logiciel libre, nous pensons que le logiciel libre répond, de la meilleure manière possible, à l'intérêt général et au service public, si l'on se réfère aux lois de Rolland par exemple. Nous pensons que le législateur a un rôle important à jouer, dans la mesure où la philosophie du logiciel libre est celle qui « colle » le mieux à la philosophie du service public. Nous pensons que le législateur doit augmenter la part de logiciels libres, peut être en imposant une part obligatoire dans différents secteurs et notamment en matière de santé. Nous souhaitons une exigence particulière dans ce domaine et que tout ce qui relève de la santé soit principalement porté par des acteurs du logiciel libre. Cela permet aussi une protection efficace des données de santé, qui sont des données particulièrement sensibles.

Nous pensons aussi qu'il faut renforcer la certification HDS. Alors que nous étions sous une forme d'agrément, nous sommes récemment passés sous la forme « certification », avec plusieurs niveaux. Dans les différentes auditions menées par votre mission d'information, certains intervenants ont émis des propositions de label. Nous pensons au contraire que le label n'a pas une valeur juridique assez contraignante. Nous souhaiterions plutôt renforcer l'existant en introduisant, par exemple, des clauses spécifiques restreignant le traitement et la sous-traitance des données de santé – parce que c'est ce qui nous intéresse et qu'il s'agit de données particulières, sensibles, prisées – à des acteurs européens *a minima*, permettant d'exclure de fait tous les acteurs hors de l'Union Européenne. Par contre, il serait nécessaire de mener une analyse comparée, notamment au niveau européen, en matière de droit de la concurrence. Bien que cela demande un peaufinage un peu plus important, nous espérons que des travaux seront conduits dans ce sens. Et cela ne peut pas se faire, de notre point de vue, par un label qui n'a pas assez de force coercitive pour garantir l'ensemble de ces conditions.

La troisième proposition juridique que nous souhaitons formuler consiste à renforcer les pouvoirs de la CNIL. Nous voyons aujourd'hui que son budget est largement moins important que celui de la CNIL allemande. Il s'agit donc de la renforcer dans ses moyens, mais également dans ses avis. Aujourd'hui, la CNIL rend des avis, dans le cadre d'un « droit souple ». Autrement dit, ces avis sont de l'ordre de la recommandation et de la préconisation en matière réglementaire, mais n'ont pas de force contraignante. Il ne s'agit pas d'avis conformes. Or, s'agissant de terrains particulièrement sensibles, comme celui les

données de santé, il serait peut-être nécessaire d'imposer un cadre d'avis conformes pour ces données. Cela fait partie de nos recommandations.

Enfin, nous sommes persuadés que l'enjeu se joue au niveau européen. Le *Privacy Shield* a fait l'objet d'une annulation par l'effet de la jurisprudence *Schrems* II en juillet dernier. Nous pensons que les négociations doivent être menées de façon particulièrement stricte au niveau européen pour ne pas avoir un nouveau *Safe Harbor* ou un nouveau *Privacy Shield*. Nous voudrions que la gouvernance européenne se saisisse bien de ces enjeux, au regard de ce qui a pu être mis en exergue par le juge européen sur les pratiques actuelles des renseignements américains. Il est important de se rendre compte qu'il n'y a pas de protection équivalente et qu'on ne peut pas s'en remettre simplement à une nouvelle habilitation de la Commission européenne.

M. Philippe Latombe, rapporteur. Je souhaiterais vous demander quelques précisions dans la mesure où cette audition est publique et doit permettre d'éclairer les gens qui nous écoutent, qui ne sont pas forcément experts du domaine. Aujourd'hui, vous avez mélangé – parce que c'est votre avis – la souveraineté, avec le HDS et le fait que le *cloud* de Microsoft soit utilisé par le HDS, et le logiciel libre. Si nous avions une solution qui ne relève pas du logiciel libre, mais qui soit une offre possible de *cloud* souverain, cela vous conviendrait-il quand même ? Si le HDH n'avait pas utilisé Azure mais OVH, par exemple, seriez-vous allés au Conseil d'État de la même façon ?

Ensuite, et c'est ma deuxième question, le logiciel libre nous assure-t-il de ne pas passer à côté des innovations dans l'avancée technologique, notamment de l'intelligence artificielle, du *machine learning* ou des réseaux neuronaux ? Sommes-nous sûrs que cette solution permettrait d'aller le plus vite possible tout en étant en permanence au bon niveau de l'état de l'art ? Je voudrais séparer les deux questions parce que vous les avez liées. Peut-on les prendre une par une ?

Me Juliette Alibert. Nous avons fait valoir une atteinte au droit à la protection des données devant le Conseil d'État. Si le choix ne s'était pas porté sur une solution technique américaine, je pense que nous n'en serions effectivement pas arrivés là. Pour autant, nous ne sommes pas en faveur d'une hypercentralisation des données. Au contraire, nous sommes favorables à un système reposant sur l'existant – sur les entrepôts de données de santé – et fédérant davantage les acteurs, dans la mesure où nous pensons que la centralisation des données fait reposer sur les données des enjeux de sécurité. En effet, en cas de faille de sécurité, l'ensemble des données de santé des citoyens – Français, Françaises et citoyens étrangers sur le sol français – peuvent devenir accessibles. Nous ne sommes donc pas favorables à ce type de solution et d'organisation du traitement des données de santé en matière de recherche. Nous pensons plutôt qu'il faut fédérer et travailler à des échelons décentralisés. À l'évidence, les risques sont moindres dans le cadre d'une solution européenne portée par un acteur français ou par un acteur européen.

M. Adrien Parrot. Une étude d'IBM pointe le fait que le *hacking* provient, pour 60 %, des organisations en interne. Évidemment, plus on concentre des données dans un point et plus il y a de risques. Ce risque existe vraiment. Ce qui peut être fait, au final, en matière de centralisation, c'est peut-être d'avoir une plateforme pour centraliser certains projets. C'est ce que fait aussi le Groupement de Coopération Sanitaire Hôpitaux Universitaires du Grand Ouest (HUGO). Certaines données sont parfois centralisées à Nantes, sans que cela ne devienne pour autant la norme. Ce qui nous dérange clairement, c'est la dépendance au droit américain. Pour moi, en tant que médecin et au regard du secret médical, les révélations

d'Edward Snowden, l'affaire Pierucci ou le FISA sont autant d'éléments qui scellent un *« no go »* absolu.

Concernant la deuxième question, je dirais que les logiciels libres et *open source* nous permettent d'atteindre l'état de l'art. C'est uniquement grâce au logiciel *open source* que nous sommes à l'état de l'art. Toute la plateforme technique de l'AP-HP repose sur des logiciels *open source*. Microsoft en utilise aussi. Il y a deux différences : qui exécute ce code ? – s'il s'agit de serveurs que l'on possède, cela change tout – et est-ce qu'il y a des interfaces de programmation (API), des couches qui englobent le logiciel *open source* ? Par exemple, Microsoft enveloppe un logiciel développé par la communauté, parfois même en partie par lui-même, au sein d'API propriétaires qui emprisonnent l'utilisateur. Aujourd'hui, les projets sont énormes et mondialisés et, pour collaborer, ceux qui fonctionnent sont presque essentiellement liés au logiciel *open source*.

M. Philippe Latombe, rapporteur. Je reviens sur l'audition précédente des représentants du Ouest Data Hub. Ils nous ont expliqué qu'ils rencontraient une difficulté assez particulière quant aux données et à la certitude que les données soient de bonne qualité et que les mêmes référentiels soient utilisés d'un entrepôt à l'autre – ils citaient par exemple les données de biologie –, dans la mesure où ils ont pu constater des problèmes d'harmonisation. Ils ont indiqué être parvenus à le gérer en raison de leur taille suffisamment importante, mais également grâce à leur histoire et grâce à un mode de fonctionnement très collaboratif entre eux, entre CHU de l'Ouest qui se connaissaient bien. On peut l'entendre aussi au niveau de l'AP-HP, où un certain nombre de discussions ont lieu entre les différents hôpitaux. Le fait de fonctionner de façon décentralisée, avec des entrepôts dans chacun des CHU, qui soient ensuite regroupés sous une forme régionale, avec l'équivalent d'un Ouest Data Hub pour chacune des régions, puis sous une couche nationale et éventuellement une couche européenne, ne générerait-il pas des difficultés sur la qualité de la donnée ?

M. Adrien Parrot. La qualité de données passera nécessairement par la localité, et donc les hôpitaux, peut-être même le cabinet du médecin généraliste. Si on veut faire des traitements de données de qualité, on est obligés d'être très proches du contexte de recueil des données et de comprendre comment les informations sont saisies. Parfois, les systèmes d'information sont tellement mal faits que le médecin entre la donnée où il peut dans son système, mais elle n'est pas forcément au bon endroit. Nous avons donc besoin d'être très proches des chercheurs qui veulent avoir accès aux données. Nous devons savoir à quoi ils ont besoin d'avoir accès. Le chercheur pourra se diriger vers les soignants, à l'endroit où les données sont stockées, regarder sous quel format elles le sont et poser des questions. C'est ce dialogue local, au plus proche de la recherche, des patients et des soignants, qui permettra d'atteindre une recherche de qualité. Il est indispensable que les données soient qualifiées – et 80 % du travail consistant précisément à la qualification des données. En effet, le fait d'envoyer des données brutes en dehors du lieu de production serait tout de suite beaucoup moins pertinent.

Me Juliette Alibert. Cette question se pose sans doute de la même manière si tout est directement centralisé. Si les données sont mal renseignées à la source, le HDH ou les projets hypercentralisés seraient confrontés aux mêmes difficultés de qualité.

M. Philippe Latombe, rapporteur. Sur la partie juridique, il y a deux aspects dans ce que vous dîtes. On nous dit aujourd'hui, assez fréquemment, que l'utilisation d'un *cloud* américain n'est pas problématique dans la mesure où tout est pseudonymisé, où tout est chiffré, et où l'utilisateur est le seul à détenir les clés de chiffrement. Vous avez dit que, dans

l'audition, vous aviez compris que les clés de chiffrement étaient chez Microsoft. Pourtant, d'autres organismes qui utilisent des *clouds* américains avancent qu'il n'y a pas de risque parce qu'ils ont leur propre clé de chiffrement et que, au-delà, le transfert a été interdit et les données sont stockées en Europe. En quoi ces éléments ne vous paraissent-ils pas suffisants ? Ce point fait partie des oppositions que vous avez eues lors de la discussion au Conseil d'État notamment.

Me Juliette Alibert. C'est ce que j'essayais d'expliquer tout à l'heure. Effectivement, les données sont pseudonymisées. Cependant, plusieurs études – nous pourrons vous communiquer les références – démontrent que, dès lors qu'on croise les données, même si celles-ci ne sont pas directement ré-identifiantes, il est en réalité très facile de ré-identifier des personnes, lorsqu'on dispose d'informations telles que la localisation, l'âge, le sexe, etc.

Sur l'aspect chiffrement, je tiens à rappeler que nous nous sommes appuyés sur un avis de la CNIL, datant du 20 avril 2020. La CNIL a avancé, dès le début, qu'il y avait plusieurs risques de sécurité importants, notamment sur ces clés de chiffrement détenues par Microsoft. Il nous a été confirmé ce matin – et cela l'avait été lors de l'audience devant le juge du référé – que Microsoft détient bien ces clés. Un système de *« customer lockbox »* permet en théorie un système d'accès sécurisé. Cependant, peut-on remettre les clés à un prisonnier dont on ne veut pas qu'il sorte de sa cellule, et lui dire de ne pas y toucher ? Techniquement, il n'y a aucune modalité qui empêche l'accès aux données par Microsoft. Par ailleurs, dès lors que ces données sont utilisées à des fins de recherche, d'intelligence artificielle – et, encore une fois, nous le rappelons, nous ne sommes pas contre la recherche –, cela signifie qu'elles sont à un moment déchiffrées. Pour permettre à ces *data scientists* de faire leur travail, il faut bien qu'elles soient déchiffrées. Elles leur sont délivrées de façon déchiffrée. La problématique reste donc pleine et entière.

Enfin, concernant l'interdiction des transferts de données vers les États-Unis, nous étions heureux de savoir que, dans l'instruction de notre recours devant le Conseil d'État, le ministre avait effectivement décidé d'empêcher les transferts. C'est une première garantie. Cependant, cela ne modifie pas en substance les risques des citoyens, quant à l'accès à leurs données personnelles sensibles, qui sont les données de leur sphère la plus intime, et vis-à-vis desquelles ils peuvent être victimes de discrimination (par exemple s'ils ont le VIH). Ces risques sont toujours présents, comme l'ont souligné le juge de l'Union européenne, la CNIL ainsi que d'autres acteurs. En tout état de cause, les pratiques du droit américain et ses effets extraterritoriaux ne sont pas conformes, dans le sens qu'ils ne remplissent pas les critères minimums de la protection telle qu'elle est aujourd'hui exigée par le RGPD. Elle ne l'est pas en raison des deux actes que je présentais tout à l'heure : l'*Executive Order*, ce fameux décret présidentiel, et la section *702 du FISA*. Ces deux fondements juridiques permettent aux services de renseignement d'avoir accès, de façon massive, discrétionnaire et indiscriminée, aux données, sans que les citoyens ne puissent s'y opposer d'aucune manière. Aujourd'hui, en tant que citoyen, nous sommes dans un système que nous avons *a minima* choisi : nous avons choisi nos représentants légaux, nos députés, etc. Nous avons accepté d'avoir tout cet ensemble et d'être régis par le RGPD. Cela fait partie du contrat social. Le problème réside dans le fait que des États tiers puissent, en méconnaissance de nos droits et du droit à la protection de nos données, accéder à ces données sensibles. Cela nous semble absolument insuffisant en termes de garantie. Ces pratiques s'inscrivent aujourd'hui en violation du RGPD et, plus largement, du droit à la protection des données, tel qu'il est garanti au niveau européen.

M. Adrien Parrot. Les arrêtés sont protecteurs et nous avons confiance dans la gouvernance du HDH. Cependant, en l'occurrence, Microsoft sera contraint – à son corps défendant – de donner accès aux données, si son supérieur hiérarchique le lui demande, en raison du *FISA* et de l'*Executive Order*. C'est vraiment sur ce point que les garanties sont insuffisantes. Dans ce contexte, nous devons nous interroger : est-il techniquement possible pour Microsoft d'avoir accès à ces données ? Où sont réalisées les analyses ? Le stockage est chiffré. C'est une garantie. Sur quel processeur les analyses sont-elles réalisées ? Est-ce sur un processeur soumis au droit américain ? Ce processeur est-il détenu par Microsoft ? Si le processeur – et c'est le cas – est soumis au droit américain, alors les données ne sont plus protégées.

Quant à la pseudonymisation, on peut toujours, en effet, ré-identifier un individu. Il existe deux techniques principales d'appariement entre bases de données. La première consiste à lier des bases de données à partir d'un même numéro présent dans deux bases différentes (par exemple un numéro de sécurité sociale). En l'absence d'un tel numéro, et si l'on dispose uniquement d'informations telles que l'âge ou le sexe, d'autres techniques permettent de lier des bases de données entre elles. Ce sont des techniques qui existent, qui sont utilisées en routine. Il est possible de ré-identifier des données de cette manière.

M. Philippe Latombe, rapporteur. Pensez-vous que le recours en Conseil d'État ait pu jouer un rôle dans la position de la CNAM quant à l'interdiction de transférer les données au HDH ? Par ailleurs, percevez-vous des risques équivalents dans d'autres domaines que les données de santé ? Existe-t-il, selon vous, une sorte de « HDH » dans d'autres domaines, pour lesquels le HDH pourrait servir de jurisprudence, d'exemple, si nous devions intervenir ?

Me Juliette Alibert. Je pense effectivement que les réserves de la CNAM sont en lien avec cette mobilisation autour de la protection des données et le recours en Conseil d'État. Le collectif SantéNathon représente de nombreuses personnes de la société civile, des associations de patients, des syndicats de médecins mais également des personnalités ayant travaillé sur la santé. Ces personnes ont soutenu le recours dans la mesure où les enjeux en présence sont importants. En effet, sous couvert d'urgence en lien avec le Covid, et pour aller vite, une solution technique comme Microsoft – qui était présentée comme la plus avantageuse et la seule solution – a été choisie, alors qu'elle met en péril les données de santé. Cela a donné lieu à de nombreux articles de presse et à de nombreuses prises de position dans les médias. Le collectif et le recours ont permis de mettre en lumière l'importance des risques, même s'ils avaient déjà été préalablement dénoncés par plusieurs personnes. Nous restons modestes dans notre démarche. Il est clair que plusieurs personnalités avaient pris position pour dénoncer ces risques importants. Cependant, cette mobilisation du collectif et ce recours ont – je pense – contribué à nourrir les inquiétudes, à faire émerger l'idée que nous étions peut-être allés trop vite, que nous n'avions peut-être pas vérifié si des solutions plus sécurisées étaient possibles, si la gouvernance ne pouvait pas être revue, ce qui a donné lieu à ses réserves de la part de la CNAM, mais également de la CNIL et d'autres autorités indépendantes qui se sont positionnées.

M. Philippe Latombe, rapporteur. Dans le collectif, vous qui avez porté ce recours devant le Conseil d'État, comment percevez-vous l'avenir du HDH ? Pensez-vous que la CNAM va obtempérer et transmettre ses données à terme ? Cela signifie-t-il que les données doivent être transférées très rapidement vers un *cloud* souverain ?

M. Adrien Parrot. La CNAM est historiquement très proche du SNDS. J'ai plutôt confiance dans les prises de position de la CNAM, dans les prochains jours et les prochaines semaines. En effet, l'idée consiste à ne pas bloquer le système ni la recherche. Je pense que tous les travaux qui ont été engagés sur la gouvernance, les travaux légaux, la loi de 2019 sur l'extension du SNDS, doivent être poursuivis et repris. C'est un travail indéniable, qui est tout à fait respectable. Par contre, en ce qui concerne l'hébergeur, notre souhait est que Microsoft s'arrête au plus vite. Les alternatives existent. Si nous ne voulons surtout pas d'interruption, nous pouvons nous tourner vers le CASD, vers Ouest Data Hub pour centraliser un projet de recherche dans les infrastructures – ils savent le faire –, vers l'AP-HP ou encore vers des industriels. En tout état de cause, le savoir de traitement des données est déjà actif, au moins au sein des hôpitaux. La CNAM sait aussi traiter des données. Je suis sûr que, si nous demandons de l'aide à l'existant pour centraliser les données sur certains projets, nous pourrons rentrer dans un cadre protecteur, en l'espace de deux secondes, sans que l'activité ne soit interrompue. Il est important d'avoir conscience que nous sommes dans un *no man's land* juridique, dès lors que nous faisons appel à des sociétés de droit américain. Actuellement, la jurisprudence *Schrems* est en cours, et on n'en mesure pas encore toute la portée. Dans ce contexte, il me paraît déraisonnable de faire courir un risque important aux personnes alors que de nombreuses alternatives existent.

M. Philippe Latombe, rapporteur. Selon vous, la réversibilité est donc faisable rapidement : cette réversibilité pourrait être accomplie, certes en mode peut-être un peu dégradé, dans le sens où elle « n'embarque pas » la totalité de ce qui était prévu au départ par le HDH, mais plus rapidement que le délai annoncé de dix-huit à vingt-quatre mois.

M. Adrien Parrot. Oui. Pour moi, il suffit de décider. Les plateformes fonctionnent. Si on décide de renforcer l'existant, l'existant existe. C'est presque de l'instantané. La sécurité nécessite effectivement d'être renforcée. Cependant, les travaux de sécurité ont d'ores et déjà été initiés. Les hôpitaux n'ont pas attendu le HDH pour renforcer la sécurité, surtout dans les entrepôts de données de santé qui sont des concentrateurs, à leur niveau, de données. L'exemple que je le connais le mieux est celui des hôpitaux de Paris. Sur la sécurité, la plateforme libre de l'AP-HP a subi des audits de sécurité et des tests de pénétration de plate-forme. Tout cela est déjà en cours.

Me Juliette Alibert. Nous avions posé la question lors de l'audience devant le Conseil d'État. Nous avions demandé quel était l'état des travaux et des bases implémentées au sein du HDH. À ce moment, je crois que seules trois bases étaient implémentées et qu'aucun projet de recherche n'était versé. En tout état de cause, il s'agit uniquement des données de santé de recherche en lien avec le Covid. En termes d'opportunité de favoriser une réversibilité rapide, je pense donc que nous sommes justement dans le bon *timing*. Il est nécessaire de se saisir de l'occasion avant que d'autres bases ne soient versées sur la plateforme.

M. Philippe Latombe, rapporteur. Ce n'est pas ce qui a été dit ce matin lors de l'audition du HDH. La CNIL a par ailleurs annoncé qu'un délai de 18 à 24 mois serait nécessaire, en ligne avec le ministère de la Santé. Une divergence en terme de temporalité apparaît ici nettement.

M. Adrien Parrot. Il est certain qu'une plateforme centralisée, comme peut la faire Microsoft actuellement et le HDH, nécessite des développements et du temps. Par contre, si l'idée consiste à ne pas bloquer la recherche, il est possible de la poursuivre dans des solutions un peu dégradées, en attente de cette infrastructure. Le CASD ou le TeraLab

constituent d'excellents exemples de plateformes « clés en main », qui sont disponibles pour faire des tests et pour avancer. Je pense que c'est le bon moment pour enclencher la réversibilité avant que les projets ne soient trop avancés, en utilisant l'existant. Pour moi, les délais annoncés sont trop importants.

M. Philippe Latombe, rapporteur. Au-delà des données de santé, d'autres domaines sont-ils selon vous confrontés aux mêmes problématiques ?

Me Juliette Alibert. Je pense que la problématique se pose dans tous les domaines faisant appel à des données sensibles au regard des publics qu'elles touchent. On peut, par exemple, penser à l'Éducation nationale. On peut penser à des données relatives à des personnes qui peuvent être exposées à des discriminations importantes, par exemple, des données sur des personnes qui sont en prison. Dans le secteur de l'éducation, le même niveau d'exigence devrait être appliqué, dès lors qu'il s'agit de données portant sur des mineurs.

M. Adrien Parrot. Il s'agit en effet d'un problème systémique. Encore une fois, la portée de la jurisprudence *Schrems* n'est pas encore dévoilée en entier. Nous savons cependant qu'elle concerne les données personnelles de façon large et que tous les secteurs sont touchés. Les enjeux d'intelligence économique sont très larges. Ils s'étendent, par exemple, à la R et D de nos entreprises pharmaceutiques et au développement des vaccins. Ce problème doit être traité dans une dimension systémique, qui dépasse largement la santé.

M. Philippe Latombe, rapporteur. Quelles seraient ou quelles sont vos attentes vis-à-vis du législateur dans le domaine des données de santé ? Certaines choses sont-elles aujourd'hui insuffisamment claires ? Certaines choses nécessiteraient-elles que l'on puisse légiférer ? Est-ce d'abord du domaine du législateur ? Vous avez dit tout à l'heure qu'il faudrait que la CNIL puisse rendre des avis conformes sur un certain nombre de sujets. Certainement, cela relève du législateur. C'est à nous de pouvoir l'imposer. Souhaitez-vous attirer notre attention sur d'autres sujets appelant, selon vous, des évolutions ?

Me Juliette Alibert. Le fait de permettre à la CNIL de rendre les avis conformes sur des données particulièrement sensibles fait effectivement partie de nos propositions. L'une de nos propositions consistait à interdire le traitement des données sensibles – et notamment des données de santé – par des acteurs extra-européens. Nous ne souhaitons pas que le traitement des données s'effectue dans le cadre d'un label, parce que nous sommes convaincus que la sécurité et la force contraignante d'un label n'offrent pas des garanties suffisantes. Il s'agirait plutôt d'un cadre de certification/agrément, ce qui relève en l'occurrence du pouvoir réglementaire. Cela pourrait donc éventuellement passer par une loi, en faisant valoir le caractère spécifique de ces données. Par contre, il faudrait effectivement croiser cette approche avec le droit de la concurrence au niveau de l'Union européenne.

Nous avons également émis une proposition consistant à imposer davantage de logiciels libres dans les administrations, et notamment dès lors que des données de santé sont en jeu. Il est possible, dans ce domaine, d'aller au-delà de la loi pour une République numérique de 2016, avec peut-être des quotas plus importants. En tout état de cause, on sent bien qu'un changement philosophique important est actuellement à l'œuvre. Une mairie – Échirolles, je crois – s'est récemment engagée à mettre en place des solutions de logiciels libres. Je pense vraiment que les services publics et les administrations ont tout intérêt à reposer sur ce type de solution beaucoup plus éthique, où effectivement les données sont protégées (personne n'a accès en clair aux données) mais où une transparence est faite sur le code. Le citoyen peut savoir dans quel cadre ses données sont sécurisées ou non. La lisibilité

du code donne énormément d'informations. Ces solutions offrent donc un cadre éthique à la fois très protecteur et très transparent. C'est pour cette raison que nous souhaitons que le législateur légifère en ce sens.

M. Philippe Latombe, rapporteur. Des annonces ont été faites la semaine dernière concernant la création d'une mission sur le logiciel libre au sein de la DINUM, issue de la mission Bothorel. Nous suivrons ce qui en découle. Je souhaite maintenant vous poser la même question que la précédente, mais au niveau européen. Qu'est-ce qui, selon vous, relève du domaine du législateur ou du domaine réglementaire national, et qu'est-ce qui relève – ou pourrait être amélioré – au niveau européen ?

Le combat que vous avez porté auprès du Conseil d'État est issu d'une jurisprudence de la Cour de justice de l'Union européenne, qui invalide le *Privacy Shield* par *Schrems* II. Vous proposez une solution qui serait *« RGPD by design »* et donc décentralisée, en affirmant que cette solution est la plus proche de l'esprit du RGPD, qui constitue lui-même une réglementation d'origine européenne. Que faudrait-il changer, que faudrait-il améliorer au niveau européen sur les données de santé ? Pensez-vous qu'il manque un cadre ?

Me Juliette Alibert. Je pense que le législateur européen doit effectivement réfléchir à aller éventuellement au-delà du cadre du RGPD, notamment sur des données particulièrement sensibles. Un cadre existe et il est très protecteur. Cependant, dans la perspective d'un éventuel futur *Privacy Shield*, les négociations empêchent peut-être la reconnaissance d'un niveau de protection équivalente. En ce qui nous concerne, nous sommes plutôt opposés à ce type d'accord. Il s'agit de notre positionnement militant. Cependant, il me semble indispensable que le législateur européen travaille sur ses aspects.

M. Adrien Parrot. Tant que les services de renseignement américains sont ce qu'ils sont, et tant que le droit américain dispose de cette portée extraterritoriale, l'Europe doit rester très vigilante face à l'émergence de futurs textes et se méfier d'un éventuel *Privacy Shield* ou d'un *Safe Harbor III*.

Me Juliette Alibert. Peut-être faudrait-il imaginer, au-delà du RGPD, des directives européennes spécifiques permettant de laisser à chacun des États des marges de manœuvre pour protéger certaines données particulièrement sensibles. En tout état de cause, je pense qu'il y a énormément à faire au niveau européen. L'enjeu que constitue la protection des données personnelles ne peut s'affranchir de cet échelon-là.

M. Philippe Latombe, rapporteur. Concernant la protection cyber des données, vous avez, dans votre propos liminaire, avancé que le fait d'avoir un système centralisé pouvait générer des risques plus importants, dans la mesure où une faille pourrait mener à l'ensemble des données. Un système décentralisé permettrait à l'inverse de ne pas « mettre tous ses œufs dans le même panier ». Comment expliquez-vous les attaques qui surviennent actuellement et comment s'en prémunir ? Faut-il créer un écosystème spécialement dédié aux données de santé, qui soit à la main des directions des systèmes d'information (DSI) dans chacun des CHU – si je prends votre modèle décentralisé ? Faut-il recourir à des solutions privées ?

M. Adrien Parrot. Les DSI ne disposent pas de moyens financiers suffisamment importants pour répondre aux besoins. Elles peinent à obtenir des ingénieurs de qualité en quantité suffisante. La difficulté est en partie liée à cette situation, et c'est typiquement ce que le logiciel *open source* peut faire et peut apporter. L'État – et il s'agit peut-être de l'une des

prochaines missions de la DINUM – devra, dans un premier temps, recenser les logiciels existants, mettre en avant un catalogue de logiciels et s'appliquer à « mettre de la glu » entre ces différentes briques logicielles. Cela permettra ensuite de proposer des briques, unifiées dans un tout cohérent, aux hôpitaux et aux professionnels de santé. Ces derniers pourront aider localement à l'installation des logiciels, qui peuvent être certifiés. Le fait d'initier une gouvernance qui fournit du code et du logiciel libre – pour le secteur public, en l'occurrence – semble être une très bonne idée. C'est aussi reprendre ce que pourrait faire Framasoft et ce qui est partiellement fait par l'État, avec son ébauche d'annuaire. Il faut renforcer ces actions, créer des forges logicielles et embaucher des développeurs qui créent des logiciels prêts à être utilisés directement dans les hôpitaux. Ce travail est tout à fait nécessaire. Notre association s'efforce d'œuvrer dans cette direction afin de pallier le manque que nous observons sur ce terrain. Nous essayons ainsi de « mettre de la glu » entre plusieurs logiciels et de les proposer aux professionnels de santé.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder certains sujets que nous n'aurions pas traités, qu'il s'agisse des données de santé ou de la souveraineté ?

Me Juliette Alibert. En ce qui concerne la souveraineté, je préciserai simplement que nous nous attachons plutôt à une notion d'« autonomie numérique » que de « souveraineté numérique ». En effet, les enjeux de souveraineté relèvent à notre sens de l'autonomisation des acteurs – au sens de la capacité de ces derniers à avoir la maîtrise de leurs données et de leur sphère numérique. Selon nous, les enjeux se situent à tous les niveaux : à l'échelle individuelle, à l'échelle départementale, à l'échelle régionale, au niveau de l'État et, enfin, entre les États eux-mêmes. La souveraineté nous semble trop rattachée à la notion souverainiste des États-nations face aux États tiers, alors même qu'une collaboration est à l'œuvre au niveau européen entre les membres de la Communauté européenne. Pour nous, cette notion de souveraineté ne fait donc pas nécessairement sens. C'est pour cette raison que nous préférons la notion d'autonomie numérique.

M. Adrien Parrot. C'est en construisant que nous avancerons. Il est nécessaire de coconstruire localement pour produire des données de qualité, ces dernières étant ensuite utilisées par les algorithmes. Il faut donc repartir de la localité et coconstruire des logiciels, peut-être grâce à l'appui de la puissance publique. En tout état de cause, un travail de coconstruction entre les hôpitaux doit clairement être favorisé et animé.

Nous devons par ailleurs bien nous rappeler que le principe du secret médical est au centre de la question du traitement des données de santé. Ce principe est pluri-centenaire et cela me semblerait déraisonnable de renier le serment d'Hippocrate. Nous nous devons de sécuriser les données, et particulièrement les données de santé, sans quoi une perte de confiance des patients est à craindre.

Me Juliette Alibert. Concernant le risque de perte de confiance des patients, il est indispensable de démontrer un niveau d'exemplarité et de transparence important, lors de l'implémentation de projets tels que le HDH. Par exemple, il nous a été dit qu'aucun appel d'offres n'avait été conduit car une solution existait et que les autres solutions n'étaient pas envisageables. Il faudrait pourtant que le citoyen ait accès, de façon transparente, à l'ensemble des documents qui montrent que toutes les solutions existantes ont été auditées, et qui expliquent pour quelle raison le choix s'est porté sur cette entreprise plutôt qu'une autre. Il est nécessaire que le choix soit *a minima* expliqué. Il a été indiqué ce matin que le choix se porterait de nouveau sur Microsoft si un marché public venait à être reconduit. Or, nous n'avons pas les moyens de comprendre ce choix en tant que citoyens. Nous avons pourtant

besoin de comprendre les décisions politiques pour y adhérer, notamment lorsque ces décisions mobilisent des enjeux de sécurité importants. Je pense qu'il est indispensable de donner les clés de lecture aux citoyens. L'association InterHop a en outre soumis des demandes d'informations concernant plusieurs documents annoncés comme « publics » sur le site de la DINUM. Or, nous peinons à y accéder. Je ne dis pas que nous nous heurtons à une mauvaise volonté de l'État de nous fournir ces documents, mais simplement qu'il sera difficile de comprendre les choix qui sont faits en l'absence d'une plus grande transparence. Cette lisibilité est cruciale dans la mesure où nous ne pouvons pas transiger avec les libertés individuelles, ni avec le droit au secret médical. Il est clair qu'on ne peut pas avoir recours à ces solutions en méconnaissance des libertés fondamentales, et d'autant plus quand aucune explication n'est fournie et quand l'accès à certains documents clé qui permettraient de comprendre et de réfléchir de façon concertée – en réunissant, en terme de gouvernance, des associations de patients – n'est pas communiqué. Je pense que les choses ont été très rapidement exécutées, alors qu'on avait peut-être le temps pour prendre des décisions. Ces dernières ont été rapidement mises en place, et ce, alors même que nous n'étions pas encore dans l'urgence du Covid. En effet, le choix de Microsoft a été opéré en amont de la crise sanitaire, et non pour y répondre.

M. Philippe Latombe, rapporteur. En tant que rapporteur, je serais preneur de la liste des documents publics auxquels vous avez demandé d'avoir accès, mais que vous n'avez pas obtenus. Cela m'intéresserait, en tant que parlementaire, que vous puissiez me la faire parvenir dans la note écrite que vous nous transmettrez.

Me Juliette Alibert. Bien sûr.

La séance est levée à 15 heures 15.

Membres présents ou excusés

Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Réunion du jeudi 18 février 2021 à 14 heures

Présents. - M. Philippe Latombe, M. Jean-Luc Warsmann