ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission des affaires sociales

– Audition, en visioconférence, de Mme Marie-Claire Denis, présidente de la Commission nationale de l'informatique et des libertés, sur les traitements de données dans le cadre de la lutte contre la propagation de l'épidémie de covid-19 2

Mardi
9 mars 2021
Séance de 17 heures 15

Compte rendu n° 56

SESSION ORDINAIRE DE 2020-2021

Présidence de Mme Fadila Khattabi, ***Présidente***

ASSEMBLÉE NATIONALE

COMMISSION DES AFFAIRES SOCIALES

Mardi 9 mars 2021

La séance est ouverte à 17 heures 15.

———

La commission auditionne, en visioconférence, Mme Marie-Claire Denis, présidente de la Commission nationale de l'informatique et des libertés, sur les traitements de données dans le cadre de la lutte contre la propagation de l'épidémie de covid-19.

Mme la présidente Fadila Khattabi. Nous entamons une nouvelle semaine chargée, durant laquelle nous allons notamment poursuivre nos travaux de suivi de la crise sanitaire dans toutes ses dimensions. Demain matin, nous nous intéresserons à la question du télétravail avec les organisations syndicales de salariés et nous ferons le point l'après-midi avec la ministre déléguée chargée de l'autonomie, Mme Brigitte Bourguignon.

Aujourd'hui, je remercie Mme Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (CNIL), d'avoir bien voulu répondre à notre invitation.

Comme vous le savez, l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire, autorise le traitement et le partage, dans le cadre d'un système d'information, des données à caractère personnel concernant la santé relatives aux personnes atteintes par le virus de la covid-19 et aux personnes ayant été en contact avec elles, recueillies le cas échéant sans le consentement des personnes intéressées.

Cette compétence conférée au pouvoir exécutif en matière de libertés publiques a été entourée de garanties telles que la mise en place d'un Comité de contrôle et de liaison covid-19 et l'information régulière du Parlement sur les mesures prises par le Gouvernement.

Une importante garantie réside également dans les avis publics de la CNIL. L'autorité administrative indépendante que vous présidez, madame, a donc été amenée à examiner plusieurs traitements de données, désormais bien connus : SI-DEP, Contact Covid, Vaccin Covid et TousAntiCovid. Dès lors, il nous a paru utile que vous nous présentiez les avis rendus par la CNIL sur la mise en œuvre de ces traitements et les actions que vous entendez entreprendre dans ce domaine dans les mois à venir.

Mme Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (CNIL). Je vous remercie de votre invitation qui me donne l'occasion, pour la première fois depuis mon entrée en fonction à la CNIL, de venir échanger avec les membres de la commission des affaires sociales. Je suis accompagnée, bien que vous ne les voyiez pas, de M. Thomas Dautieu, directeur de la conformité, de Mme Marie Fromentin, juriste au service de la santé, et de M. Benjamin Vialle, chef du service des contrôles pour les secteurs RH, santé et affaires publiques.

Votre invitation fait suite à l'envoi au Parlement du deuxième avis trimestriel rendu public par la CNIL le 21 janvier dernier sur le fondement de l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire. La CNIL avait adressé un premier avis au Parlement le 10 septembre 2020.

Le thème proposé pour cette audition porte sur les traitements de données dans le cadre de la lutte contre la propagation de l'épidémie de covid-19. Ce titre, englobant, rejoint parfaitement la démarche suivie par la CNIL depuis que le législateur a souhaité qu'elle adresse un avis public, en complément du rapport détaillé du Gouvernement, tous les trois mois à compter de la promulgation de la loi du 11 mai 2020 et ce, jusqu'à la disparition des systèmes d'information.

En effet, le Gouvernement a mis en place de nombreux systèmes numériques dans le cadre de la lutte contre l'épidémie. Il a non seulement déployé SI-DEP et Contact Covid, qui font l'objet de l'article 11, mais aussi l'application mobile StopCovid, devenue TousAntiCovid, et le système d'information Vaccin Covid. C'est pourquoi la CNIL, dans le cadre de sa mission d'accompagnement des pouvoirs publics, a fait le choix d'inclure ces différents dispositifs dans ses avis trimestriels afin d'informer le Parlement et les citoyens quant au dispositif global de lutte contre l'épidémie de covid-19.

En préambule, je souhaiterais saisir l'occasion qui m'est offerte de partager avec vous quelques réflexions relatives au rôle dévolu à notre autorité au cours de cette période. Je me suis exprimée devant vos collègues de la commission des lois, le 8 avril 2020, alors que nous affrontions le début de la crise sanitaire, et je leur ai fait part de mes réflexions.

J'avais indiqué en premier lieu que les membres de la CNIL estimaient que les données personnelles seraient considérées comme une ressource permettant de répondre directement aux défis sanitaires, à la recherche en santé, à la protection des personnes vulnérables et à l'accompagnement des stratégies de confinement et de déconfinement.

En second lieu, j'avais rappelé aux membres de la commission des lois de l'Assemblée nationale que les textes qui protègent les données personnelles, ou à caractère personnel, ne s'opposent pas à la mise en œuvre de solutions de suivi numérique, individualisé ou non, visant à la protection de la santé publique. Cependant, ces textes imposent de prévoir des garanties adaptées.

Depuis un an, le collège et les services de la CNIL ont entrepris des actions de sorte à accompagner les innovations mises en œuvre dans le cadre de la lutte contre l'épidémie, dans le respect des droits fondamentaux.

Les données de santé font l'objet d'une protection renforcée en vertu du règlement général sur la protection des données (RGPD) et de la loi informatique et libertés, très substantiellement modifiée par la loi du 20 juin 2018, que vous avez votée à la suite de l'entrée en application du RGPD.

La CNIL fonde donc son action sur des textes récents qui tiennent compte des derniers développements technologiques et qui ont passé, si j'ose dire, le « test » de l'urgence sanitaire. Par ailleurs, le Parlement s'est appuyé sur la CNIL pendant l'année écoulée, comme en témoignent non seulement ce dispositif lié à l'avis trimestriel, mais également le nombre croissant de sollicitations que nous recevons de sa part. Pour la seule année 2020, la CNIL a répondu à une dizaine de questionnaires et participé à une vingtaine d'auditions, et huit d'entre elles présentaient un lien direct avec la crise sanitaire.

Autorité administrative indépendante, la CNIL a largement contribué à installer et à préserver un climat apaisé en regard de systèmes d'information potentiellement intrusifs, tout en exerçant la plénitude des pouvoirs qu'elle détient en vertu de la loi. En effet, l'efficacité des mesures de santé publique est interdépendante de l'adhésion du public, celle-ci requérant la confiance qu'une autorité administrative indépendante et experte peut contribuer à apporter.

Nous avons agi non seulement en amont de la mise en œuvre du traitement, mais également en aval, afin de contrôler cette mise en œuvre.

En amont, depuis mars 2020, le collège de la CNIL a rendu treize avis relatifs à la gestion de la crise sanitaire. Ils étaient essentiellement destinés au Gouvernement et émis souvent en urgence, comme ce fut le cas récemment encore, pour l'avis relatif au traitement du système d'information lié aux vaccins contre la covid.

En aval, la CNIL a mené des contrôles d'organismes chargés de la mise en œuvre et elle s'est fortement mobilisée sur l'accompagnement de l'ensemble des acteurs, non seulement le Gouvernement et le Parlement, mais également les collectivités territoriales, ainsi que l'ensemble des secteurs d'activité liés à la santé et à la recherche. La CNIL maintient par ailleurs un contact permanent avec les régions, les départements et les mairies, territoires avec lesquels d'ailleurs, elle a conclu des partenariats. La CNIL reste à l'écoute de leurs problématiques, notamment sur trois sujets : le partage des données issues des fichiers sociaux et médico-sociaux des collectivités, notamment des départements, à des fins d'accompagnement des personnes vulnérables ; la distribution des masques et les fichiers de données sur la base desquels les distribuer ; la participation des collectivités à la campagne de vaccination de la population, notamment en Corse.

Par ailleurs, en matière de recherche en santé, la CNIL a priorisé un accompagnement des recherches sur la covid-19. Nous agissons sur la base d'un régime d'autorisations pour le traitement des dossiers de santé qui résulte d'un choix fort du législateur français, en 2018, de maintenir des autorisations quant à la recherche relative à la santé, conscient des enjeux liés à la protection des données.

Certes, la majorité des projets peuvent être mis en œuvre sans autorisation, sous réserve qu'ils soient conformes à une méthodologie de référence, et il suffit alors de faire une simple déclaration à la CNIL.

Cependant, s'agissant des projets qui nécessitent une autorisation – par exemple des études pour lesquelles les patients ne peuvent pas être informés individuellement de l'usage de leurs données –, la CNIL a mis en place une procédure accélérée d'instruction. Dès que les dossiers sont complets, les autorisations peuvent être délivrées rapidement, parfois même en quelques heures.

Nous avons ainsi délivré cent une autorisations de recherche spécifiquement liées à la covid-19 depuis un an, soit quatre-vingt-onze autorisations en 2020 et dix autorisations depuis le début de l'année 2021. Elles représentent environ un quart des décisions d'autorisation de recherches médicales que nous avons prononcées en 2020. En outre, 45 % des autorisations liées, en 2020, à la recherche sur la covid-19 ont été délivrées en moins de deux jours lorsque les dossiers étaient complets et près des deux tiers de ces autorisations ont été délivrés en moins d'une semaine. Le délai moyen de traitement s'élevait à dix-sept jours.

Cette mobilisation a été réalisée dans le respect des droits des personnes et de la sécurité des données. Je reconnais et j'assume que la CNIL se montre parfois exigeante quant à certains aspects tels que l'anonymisation des données et la sécurité informatique. Toutefois, l'actualité récente – fuites de données de laboratoires, par exemple – démontre combien ces exigences sont nécessaires et attendues de nos concitoyens.

S'agissant des grandes lignes du deuxième avis trimestriel de la CNIL relatif aux systèmes d'information conçus en vue de lutter contre la covid-19, je rappelle très brièvement quels traitements sont concernés : Contact Covid, mis en œuvre par la Caisse nationale de l'assurance maladie (CNAM), recueille les informations relatives aux personnes identifiées comme contacts à risque de contamination, cas contacts ou personnes co-exposées, et les chaînes de contamination ; le système SI-DEP, créé par le ministère des solidarités et de la santé, permet la centralisation des résultats des tests ; TousAntiCovid, ancien StopCovid, est une application mobile de suivi des contacts, utilisant la technologie Bluetooth et fondée sur le volontariat des personnes. Elle est mise à disposition afin d'alerter les utilisateurs d'un risque de contamination, lorsqu'ils se sont trouvés à proximité d'un autre utilisateur ayant été diagnostiqué positif à la covid-19. Elle a récemment évolué de sorte à permettre, le moment venu, l'enregistrement des visites dans des lieux recevant du public, grâce à des codes QR, afin de faciliter l'alerte des personnes ayant fréquenté ces lieux, sur une plage horaire similaire à celle d'une ou plusieurs personnes ultérieurement diagnostiquées positives au virus ; le système d'information Vaccin Covid, mis en œuvre sous la responsabilité conjointe de la direction générale de la santé et de la CNAM, vise à organiser, suivre et piloter les campagnes vaccinales contre la covid-19.

Pour chacun de ces systèmes d'information, la commission a été particulièrement vigilante quant aux modalités d'information des personnes et à l'exercice de leurs droits, quant au respect du principe d'anonymisation des données, quant à l'encadrement de la dérogation au principe du secret professionnel, notamment en exigeant une gestion particulièrement fine des habilitations des personnes amenées à accéder aux données et une sensibilisation spécifique à ces questions, et quant au respect des principes de sécurité. Ces exigences sont liées non seulement à la sensibilité de ces données, mais également à l'ampleur des traitements susceptibles d'être consultés par un grand nombre d'acteurs.

Dans ses avis trimestriels, le collège de la commission a également rappelé que l'atteinte portée à la vie privée est admissible uniquement dans le cadre d'une politique constituant une réponse nécessaire et appropriée au ralentissement de la propagation de l'épidémie et qu'elle implique que la nécessité de ce système d'information soit périodiquement réévaluée, en fonction de l'évolution de l'épidémie. La CNIL a aussi insisté sur l'obligation, malgré le contexte d'urgence, d'apporter des garanties au respect des principes fondamentaux. Dans ce cadre, le deuxième avis que nous avons publié contient le détail des observations que nous avons formulées pour chacun des systèmes mis en œuvre.

Au début du mois de janvier 2021, la CNIL a été saisie d'un projet de décret visant à renforcer le dispositif de traçage des chaînes de transmission du virus, en élargissant le champ d'action du fichier Contact Covid, afin de faciliter la réalisation des enquêtes sanitaires. En pratique, cela se traduit notamment par une extension significative du nombre de personnes concernées par l'ajout de la possibilité de collecter les données relatives aux personnes co-exposées, à savoir des personnes qui se trouvaient au même moment qu'un patient diagnostiqué positif au virus en un lieu dans lequel il s'avérait impossible de respecter pleinement les mesures barrières et ce, au cours des quatorze derniers jours.

Dans l'avis que nous avons publié le 19 janvier 2021, nous avons noté que le projet de décret implique la collecte d'une nouvelle catégorie de données, notamment sur la participation à des activités ou des rassemblements de plus de six personnes ainsi que des données relatives au retour d'un voyage international ou dans l'outre-mer.

Les contrôles menés par la CNIL peuvent prendre plusieurs formes, à savoir sur place, sur pièces ou en ligne. En un an, nous avons réalisé onze contrôles de Contact Covid, soit auprès de la CNAM, soit auprès des agences régionales de santé (ARS).

Dans son deuxième avis, la CNIL a constaté le déploiement d'un plan d'action qui a amélioré les modalités de mise en œuvre du traitement des données et corrigé les mauvaises pratiques qui avaient été relevées dans le cadre de son premier avis, publié au mois de septembre 2020.

Toutefois, nous avons constaté certaines mauvaises pratiques résiduelles relatives aux conditions d'authentification, à la traçabilité et à la transmission des données personnelles à un tiers non habilité à héberger des données de santé. J'ai donc décidé d'adresser un courrier rappelant la CNAM à ses obligations et faisant état des manquements relevés et des mesures qu'il s'avère nécessaire de mobiliser pour y remédier.

La CNIL a également relevé de nombreuses disparités dans les pratiques des ARS pour ce qui concerne le suivi des contacts. Dans ce cadre, j'ai donc adressé une mise en demeure à l'une d'entre elles ainsi qu'un courrier de sensibilisation à l'ensemble des ARS afin de les informer de quelques pratiques contraires au RGPD, relevées lors des contrôles. J'ai également écrit au ministère des solidarités et de la santé afin de le tenir informé.

Pour ce qui concerne SI-DEP, nous avons réalisé sept contrôles non seulement auprès du ministère et de l'Assistance publique - Hôpitaux de Paris (AP-HP), mais également dans deux laboratoires d'analyses médicales réalisant des tests PCR. Dans notre deuxième avis, nous avons relevé que les remarques formulées à l'issue de la première phase de contrôle, au mois de septembre 2020, avaient bien été prises en compte et que le niveau de conformité était satisfaisant s'agissant du respect des durées de conservation des données. Ces constats posés, nous avons considéré qu'il n'était pas nécessaire de prendre des mesures particulières.

S'agissant de TousAntiCovid, anciennement StopCovid, nous avons également réalisé sept contrôles. À l'issue des contrôles que nous avons menés au mois de juin 2020, j'ai adressé une mise en demeure, qui a été rendue publique, à l'encontre du ministère de la santé. Le ministère s'étant mis en conformité dans le délai imparti, j'ai prononcé la clôture de cette mise en demeure le 3 septembre 2020. Dans la perspective de la réouverture de certains établissements recevant du public, le Gouvernement a souhaité poursuivre ces évolutions en introduisant un dispositif numérique d'enregistrement dans certains établissements par codes QR. De nouveaux contrôles seront planifiés dès que la mise à jour de l'application sera réalisée.

Pour ce qui concerne Vaccin Covid, des contrôles sont d'ores et déjà prévus.

Enfin, outre les contrôles effectués sur ces principaux systèmes d'information, la CNIL procède également à des vérifications sur les fichiers du quotidien liés au suivi de la pandémie. Elle a ainsi procédé à des contrôles relatifs, par exemple, à la tenue des cahiers de rappel, mis en œuvre à partir du mois d'octobre 2020, alors que les établissements étaient encore ouverts. Nous avons d'ailleurs publié sur notre site, à l'attention des professionnels, des exemples de cahiers de rappel qui protègent les droits des personnes et qui rappellent que ces données ne doivent pas être utilisées à des fins de prospection commerciale. Dans ce cadre, nous avons prononcé deux rappels à l'ordre à l'encontre d'organismes qui utilisaient ces cahiers de rappel sans respecter la procédure de protection des données.

En conclusion, sans remettre en cause la légitimité de poursuivre la lutte contre l'épidémie, il convient non seulement de concilier la protection de la santé et la protection des données, mais également de veiller à ne pas banaliser le recours à ces systèmes d'information qui demeurent très intrusifs et consommateurs de données personnelles.

Quoi qu'il en soit, les contrôles se poursuivront tout au long de la période d'utilisation des fichiers, jusqu'à la fin de leur mise en œuvre et jusqu'à la suppression des données qu'ils contiennent. Le prochain avis public publié par la CNIL fera état des résultats de ces contrôles, notamment pour ce qui concerne les contrôles liés à Vaccin Covid. Une ultime salve de contrôles sera effectuée jusqu'à la suppression effective des données.

Mme Annie Vidal. Je vous remercie, madame la présidente, pour votre disponibilité et pour les éclairages que vous nous avez apportés. Dans le contexte épidémique actuel, le numérique en santé offre aux citoyens un accès aux soins facilité et est devenu un outil incontournable de lutte contre la covid-19. La France avance à grands pas dans ce domaine et elle inscrira ses avancées dans la durée, notamment *via* le développement du dossier médical partagé (DMP). Si ce mouvement offre de réelles opportunités, il convient de rester très vigilant quant à la confidentialité et la sécurité des données de santé.

En octobre dernier, vous avez émis des réserves sur le rôle de l'entreprise américaine Microsoft dans la gestion du Health Data Hub, dont l'objectif consiste à compiler l'ensemble des données du système de santé français. Le Conseil d'État a rejoint votre jugement en invoquant le risque d'un transfert de données vers les États-Unis en raison de l'extraterritorialité du droit américain.

Par ailleurs, un nombre croissant d'acteurs privés utilisent les données de santé des Français afin d'offrir de nouveaux services aux patients. Certains éditeurs de logiciels de prise de rendez-vous utilisés en France travaillent avec des entreprises américaines. Nous savons, par exemple, que Doctolib a recours aux prestations d'une filiale d'Amazon, ce qui interroge quant à la confidentialité des données, naturellement indissociable du secret médical et essentielle afin de préserver la confiance des patients dans notre système de soins.

Dès lors, quels sont vos points de vigilance sur le rôle croissant des acteurs privés dans le traitement des données de santé ? Comment garantir la sécurité de ces données ?

M. Stéphane Viry. Madame la présidente, votre audition de ce jour devant notre commission est très importante ; en tout cas je la considère comme telle. En effet, vous êtes une autorité qui représente peut-être la véritable garantie sur laquelle nous appuyer en ce moment, dans le cadre des mesures d'urgence sanitaire. Votre regard sur les pratiques et vos contrôles de leur conformité à nos lois et principes fondamentaux sont, selon nous, véritablement essentiels.

Cet article 11, qui autorise le traitement et le partage de données d'informations à caractère personnel, interroge quant au droit individuel et aux libertés publiques. Bien que nous fonctionnions dans un contexte dérogatoire et exceptionnel, notre vigilance est nécessaire. Votre autorité administrative indépendante représente une garantie qui confirme l'importance de votre prise de parole aujourd'hui et des informations que vous nous livrez quant à votre réactivité, à la mobilisation de la CNIL, aux différents dispositifs que vous avez mis en place et aux contrôles que vous effectuez.

Cette autorité indépendante dispose-t-elle de moyens suffisants de sorte à assurer le rôle fondamental qui est le sien dans le cadre de notre démocratie sanitaire ?

Par ailleurs, au-delà de la crise sanitaire actuelle, nous sommes engagés dans un processus de création d'une filière numérique d'e-santé qui implique le recueil et le partage de données. Il est probablement nécessaire de mettre en place une forme de balisage.

Quel regard portez-vous sur cette nouvelle médecine, sur cette transformation de notre système de santé qui repose sur des données individuelles et sur des données qui relèvent du secret médical ? Serait-il nécessaire de légiférer afin de nous assurer que les fichiers et traitements informatiques soient conformes à nos principes fondamentaux ?

M. Cyrille Isaac-Sibille. Je confirme que cette audition est importante, car le rôle de la CNIL est essentiel. Dès lors, madame la présidente, quel est votre sentiment quant aux conditions de mise en œuvre d'un passeport sanitaire, d'un passeport vaccinal éthique ? Selon vous, à quelles conditions devrait-il répondre afin d'être efficace et d'assurer une équité de traitement des patients ?

Mme Agnès Firmin Le Bodo. Vous avez évoqué la nécessité de ne pas banaliser les données de santé. En effet, les moyens techniques mis à disposition et faciles d'accès ne doivent pas occulter qu'il s'agit de données de santé qu'il convient de protéger. Des hôpitaux, pourtant très protégés, ont été victimes de cyberattaques.

Que pensez-vous de la protection des données de santé détenues par les laboratoires et les pharmaciens, qui utilisent également SI-DEP ? Les médecins ont accès au système Vaccin Covid. Comment on peut réussir à protéger collectivement les praticiens de santé de cyberattaques ?

Enfin, il est question d'équiper le passeport sanitaire de codes QR. Pour autant, que pensez-vous de l'éventualité d'y intégrer les résultats de tests antigéniques PCR ou de tests antigéniques réalisés en pharmacie ?

Mme Valérie Six. Madame la présidente, depuis un an maintenant, nous devons renoncer à une part importante de nos libertés fondamentales afin de lutter contre l'épidémie. Les outils numériques jouent un rôle de facilitateur : dérogations en ligne durant le confinement, création de l'application TousAntiCovid visant à identifier les contacts, etc. Comme bien souvent, et en particulier dans un contexte de crise sanitaire, les outils numériques sont essentiels. Cependant, leur utilisation doit être strictement encadrée de sorte qu'ils ne contreviennent pas à nos libertés fondamentales.

Le partage des données médicales, non seulement entre professionnels de santé, mais également entre les organismes de sécurité sociale, nous semble très important dans la lutte contre la covid-19 et pour la protection de nos concitoyens. Toutefois, les outils existants sont dépourvus de lien entre eux. Je pense notamment au DMP pour les données de santé, à l'application TousAntiCovid pour le traçage des contacts, ou encore à Doctolib pour la prise de rendez-vous.

Selon vous, madame la présidente, un partage plus large de ses données de santé ne permettrait-il pas de proposer une offre de soins plus adaptée et, peut-être, plus efficace ?

Le RGPD ne constitue-t-il pas une garantie suffisante dans la préservation des libertés individuelles, notamment en imposant non seulement une proportionnalité dans l'usage des données collectées, mais également une durée de conservation de ces données ?

Mme Martine Wonner. La crise sanitaire a plongé notre pays dans une situation véritablement difficile non seulement dans le domaine de la santé, mais également parce qu'elle a considérablement atrophié nos libertés.

Aux côtés de la recherche de solutions médicales dans la lutte contre le virus, la tentation du solutionnisme technologique s'installe désormais dans les esprits. Cette tentation avait déjà fait l'objet de votre audition, en avril 2020, par la commission des lois. J'avais adhéré à vos alertes quant aux risques encourus dans cette posture. Il est tentant de recourir aux technologies, car elles offrent des opportunités réelles, mais elles présentent des risques en regard de notre identité et de nos libertés.

La question du passeport vaccinal, ou certificat vaccinal, interroge votre institution. Elle semble bien loin l'époque où un journal avait pu, dans un seul article, déstabiliser tout un Gouvernement lorsque celui-ci souhaitait mettre en place un mégafichier en croisant différents fichiers. C'était dans le journal *Le Monde* et c'était l'affaire « Safari » qui fut à l'origine de la création de votre autorité, la CNIL, en 1978. Comment en sommes-nous arrivés à imaginer très sérieusement la mise en place aujourd'hui d'un tel dispositif ? Nous avons le devoir de proportionner l'utilisation des technologies concernant les données personnelles des citoyens en fonction de l'intérêt de santé publique qu'elle représente. Cet équilibre entre intérêts santé et risques sur nos libertés est fondamental.

Madame la présidente, vous n'êtes pas sans savoir que de nombreux organismes privés ont déjà commencé ou projettent de poser le passeport vaccinal comme condition d'usage de leurs services. Je pense notamment à certaines compagnies aériennes.

Par ailleurs, j'ai appris ce matin – et j'en suis très inquiète – que certains confrères médecins commencent à établir des listes de personnes non vaccinées et qu'ils y sont encouragés par les agences régionales de santé. La CNIL envisage-t-elle de mettre en place des dispositifs visant à interdire au plus vite ces dangereux comportements ?

M. Pierre Dharréville. Certaines mesures prises dans ces circonstances exceptionnelles présentaient un caractère exorbitant du droit commun. S'agissant de leur installation dans la durée, en quelque sorte, avez-vous été amenés à vous interroger quant à leur pertinence réelle et aux risques auxquels elles exposent les libertés publiques ? Leur usage a-t-il fait évoluer vos points de vue ?

Vous avez évoqué la nécessité que ces mesures soient pertinentes et appropriées. Or depuis le début de cette crise, nous constatons que notre perception des choses a évolué. Qu'en pensez-vous ? N'existe-t-il pas une forme d'illusion dans la magie de la technologie qui, pour autant, ne suffit manifestement pas à régler nos problèmes ? L'usage demeure-t-il effectivement pertinent et proportionné ?

L'ensemble de ces dispositifs nécessite un recours à des acteurs privés, notamment pour ce qui concerne l'hébergement des données. N'existe-t-il pas un risque de levier de marchandisation ? La question a été notamment soulevée s'agissant du passeport vaccinal. Quel est votre avis à ce sujet ?

Au bout du compte, que restera-t-il de ces mesures pour des temps ordinaires de normalité retrouvée ? Avez-vous engagé une réflexion à long terme à ce sujet ?

Mme la présidente de la CNIL. S'agissant de la plateforme de données Health Data Hub, je tiens d'abord à souligner l'utilité d'une plateforme de données de santé, notamment pour la recherche médicale. Nous disposons, en France, d'un nombre considérable de données de santé qui peuvent être utilisées à des fins de recherche, sous réserve d'en préserver la sensibilité et d'assurer des conditions de sécurité maximales. Le collège de la CNIL se montre très vigilant quant à un éventuel accès direct à ces données par les autorités de pays tiers. C'est la raison pour laquelle il a très fermement fait part de son souhait que l'hébergement de la plateforme et des services qui sont rattachés à sa gestion puisse être réservé à des entités relevant exclusivement des juridictions de l'Union européenne.

Vous avez évoqué l'arrêt rendu par la Cour de justice de l'Union européenne au mois de juillet dernier qui a invalidé l'accord de transfert de données, notamment vers les États-Unis. Le Conseil d'État a reconnu, dans une ordonnance d'octobre dernier, le risque présenté par le transfert de données, notamment vers les États-Unis, en raison de la soumission de Microsoft au droit américain. Il a par ailleurs demandé que des garanties supplémentaires soient mises en place.

Le collège de la CNIL estime nécessaire d'éliminer ce risque. C'est la raison pour laquelle nous avons demandé et obtenu, de la part du ministère, l'engagement de modifier la solution technique de sorte à supprimer ce risque dans un délai déterminé, compris entre douze et dix-huit mois, et qui, en tout état de cause, ne devra pas excéder deux ans. La CNIL considère que ce délai est de nature à garantir un juste équilibre entre la préservation du droit à la protection des données et l'objectif qui consiste à favoriser la recherche et l'innovation dans le domaine de la santé. Dans notre esprit, il s'agit d'une période transitoire.

La CNIL sera d'ailleurs très prochainement auditionnée par la CNAM, notamment le membre du collège qui est en charge de la santé, au sujet non seulement de l'avis qu'elle a rendu relativement au décret, mais également du recours à Microsoft pour l'hébergement des données de cette plateforme. Je vous rappelle que le conseil d'administration de la CNAM s'est opposé, en février, au transfert d'une copie du système.

S'agissant des moyens dont dispose la CNIL, les pouvoirs publics sont conscients du périmètre couvert par ses missions. En effet, nous assurons des missions d'accompagnement non seulement des pouvoirs publics – notre échange en est l'illustration –, de millions d'entreprises, mais également des individus qu'il importe d'informer de leurs droits.

La CNIL compte actuellement deux cent vingt-cinq agents, effectif qui sera porté à deux cent quarante-cinq à la fin de l'année. Les pouvoirs publics sont donc conscients qu'il convient d'étoffer les ressources de la CNIL. En effet, la valeur de la CNIL réside exclusivement dans ses agents. Pour autant, le ratio entre le nombre d'agents de l'autorité de protection des données et la population est l'un des trois plus faibles de l'ensemble de l'Union européenne. En outre, notre effectif compte moitié moins d'agents que celui de notre homologue anglais. Pour autant, le nombre de plaintes que nous enregistrons augmente de 30 % par an depuis la mise en œuvre du RGPD : il atteint 14 000 plaintes par an. Nous réalisons des centaines de contrôles. Nous sommes très présents pour l'accompagnement des entreprises et des organismes. Nous sommes très impliqués à l'échelon européen et international afin de faire vivre cette coopération européenne qu'incarne le RGPD. Nous sommes très engagés pour la cybersécurité, qui nécessite également des moyens. C'est pourquoi je suis convaincue qu'il est impératif de renforcer les effectifs à temps plein de la CNIL.

Plusieurs d'entre vous m'ont interrogée quant au passeport vaccinal. La CNIL n'a pas été saisie à ce sujet. Dès lors, les informations dont je dispose sont issues des articles que je lis dans la presse. Pour autant, je vous confirme que, si la création de ce passeport se confirmait, la CNIL serait amenée à se prononcer quant à la mise en œuvre d'un tel traitement de données qui nécessiterait des modifications législatives ou réglementaires. Nous serions attentifs à la sécurité des données, notamment les données de santé et les données sensibles. Dans le cas échéant de la mise en œuvre d'un dispositif numérique, nous serions particulièrement attentifs à la préservation du caractère volontaire, d'une réelle liberté de choix et, par là même, à ce que l'accès à des services ne soit pas conditionné à l'utilisation de ce dispositif numérique. Nous serions également très vigilants quant à son articulation avec d'autres dispositifs qui ont été mis en place en vue de la réouverture de certains établissements recevant du public afin d'éviter les risques de multiplication et de superpositions de ces dispositifs et de confirmer leur réelle utilité dans la lutte contre l'épidémie et la covid-19.

Des discussions sont en cours au niveau européen, cet après-midi même, dans le cadre d'échanges au sein du Comité européen de la protection des données, qui réunit l'ensemble des CNIL européennes. Il est probable que cette instance européenne soit amenée, le cas échéant, à se prononcer sur le sujet. En effet, la présidente de la Commission européenne a annoncé très récemment que la Commission allait présenter ce mois-ci une proposition législative relative au *Digital Green Pass*, dont l'objectif consisterait à fournir non seulement la preuve de la vaccination, mais également celle du test PCR négatif ou la présence d'anticorps.

Les compagnies aériennes expérimentent différentes méthodes de test. Air France a mis à l'essai, à destination de l'outre-mer, un outil différent de celui qui est mis en place par l'Association internationale du transport aérien. La CNIL n'a pas été saisie de ces projets, ce qui n'est d'ailleurs pas anormal puisque le RGPD implique une responsabilisation des personnes en charge des traitements de données qui ne sont donc pas obligées de solliciter l'autorisation à la CNIL. En revanche, ils sont tenus de respecter l'ensemble des règles en matière de protection des données et de mobilisation de ces données. En effet, la collecte doit concerner uniquement des données nécessaires et ne peut intervenir qu'après avoir informé les personnes, recueilli leur consentement et s'être assuré de la sécurité de ces données. Il est également important que ces données soient stockées localement, à la disposition de l'utilisateur, et non pas dans une base centrale. Il convient également d'identifier les accès aux données et de répartir les rôles et les responsabilités entre un consortium, par exemple, réunissant les acteurs à l'origine de cette initiative, les professionnels de santé et les compagnies bénéficiant du dispositif. J'insiste sur le fait que le caractère volontaire du dispositif doit s'appliquer également aux compagnies aériennes. Il doit se traduire par une réelle liberté de choix et la proposition de solutions alternatives en cas de refus d'utiliser cette méthode sans que cette posture implique un refus d'accès au voyage.

Tels sont quelques-uns des points d'attention et de vigilance sur lesquels nous ne manquerions pas de nous prononcer, le cas échéant et le moment venu.

La question de la sécurité des données est bien entendu indissociable de la protection des données. Vous avez évoqué notamment les attaques dont ont été victimes certains hôpitaux *via* des logiciels qui chiffrent les données et réclament le paiement d'une rançon pour en libérer l'accès. Ces attaques n'impliquent pas uniquement des conséquences financières et de désorganisation. En effet, l'année dernière en Allemagne, une patiente est décédée à la suite attaque de ce type visant l'établissement dans lequel elle était hospitalisée.

Dès lors, dans le domaine de la sécurité des hôpitaux, il me paraît essentiel de conjuguer les actions de la CNIL à celles des différents intervenants. Je me suis récemment entretenue avec le secrétaire d'État chargé de la transition numérique et avec la déléguée ministérielle au numérique en santé, que vous avez d'ailleurs auditionnée récemment. La question repose concrètement sur la part de leur budget que les hôpitaux peuvent consacrer à la protection des données. Elle s'élève actuellement entre 1,6 et 1,8 % et l'engagement d'actions de fond nécessiterait de l'augmenter à environ 3 %. Ces actions impliqueraient d'engager, et de rémunérer au prix du marché, des experts informatiques en la matière. Je pense que le volet numérique du plan France Relance pourrait permettre des avancées dans ce cadre.

Le rôle de la CNIL réside dans de l'accompagnement, autant que possible. Cependant, elle ne dispose pas des ressources nécessaires à l'accompagnement de l'ensemble des hôpitaux. Dès lors son action se limite à prodiguer des conseils généraux, à entretenir des contacts avec les fédérations et les représentants du domaine hospitalier. Nous accompagnons également les hôpitaux par nos actions de contrôle. En effet, nous avons procédé à sept contrôles d'établissements français en 2020. Je rappelle que, conformément au RGPD, les hôpitaux, comme l'ensemble des acteurs, des entreprises et des organismes publics, sont tenus de notifier à la CNIL un constat de violation des données dans les soixante-douze heures qui suivent la prise de conscience de cette violation de sorte que nous puissions décider, si cela n'a pas encore été fait et en fonction de la nature de la violation et des données concernées, s'il convient d'en informer les utilisateurs et les personnes dont les données ont été violées.

La formation restreinte de la CNIL, c'est-à-dire sa commission des sanctions, a sanctionné deux médecins au mois de décembre dernier, bien que les sommes en jeu ne fussent pas importantes, et leur a rappelé qu'il était interdit de donner libre accès sur Internet aux données de leurs patients. À ma connaissance, le RGPD constitue le seul texte qui comporte des obligations en matière de sécurité et de protection des données sur lesquelles baser les sanctions de la CNIL.

Par ailleurs, nous sommes très actifs dans l'édition de guides, de recommandations relatives aux mots de passe, etc. Nous avons également édité une application qui permet de réaliser facilement des études d'impact des traitements sur la protection des données lorsqu'un risque élevé est identifié.

En 2021, le collège de la CNIL a décidé d'axer deux de ses trois thèmes prioritaires de contrôle sur la cybersécurité et les violations de données. Force est de constater que les notifications de violations de données ont augmenté de 24 % entre 2019 et 2020. Nous enregistrons un peu moins de trois mille notifications de violations de données chaque année et je pense que ce chiffre est sous-estimé. En outre, les violations liées à des attaques par CryptoLocker sur des établissements de santé ont triplé entre 2019 et 2020 – douze en 2019 contre trente-six en 2020 – et de nombreuses sanctions de la CNIL concernent des manquements à la sécurité des données. Nous suivons tout particulièrement ce sujet.

Comme vous avez pu le constater dans l'actualité, nous avons également essayé d'être les plus réactifs possible face à la fuite des données de santé qui a affecté simultanément près de cinq cent mille patients de vingt-huit laboratoires. Nous avons diligenté des contrôles sur pièces et sur place. Nous avons déjà réalisé des contrôles et nous poursuivons notre action dans ce domaine. Nous avons également saisi le tribunal judiciaire de Paris de sorte qu'il enjoigne les fournisseurs d'accès à Internet de bloquer le site, situé hors de l'Union européenne, qui rendait cette base de données accessible. Nous nous sommes assurés que les personnes dont les données ont été violées en avaient été informées ou étaient

sur le point de l'être par les laboratoires. Nous continuons à instruire les notifications de violations de données.

La cybersécurité constitue un sujet prégnant, notamment dans le domaine de la santé, compte tenu du volume des données concernées, de la sensibilité et de l'intimité qu'elles révèlent. La CNIL agit et continuera à agir massivement sur les problématiques liées à la cybersécurité.

S'agissant du partage des données médicales, d'une façon générale, il importe de concilier l'ouverture des données et leur protection. L'ouverture des données, notamment des données d'intérêt public – qui ne concernent pas exclusivement le domaine de la santé – constitue non seulement un facteur d'innovation, mais également un élément de la confiance entre l'administration, les pouvoirs publics et les administrés. Cette ouverture des données relève d'ailleurs de la loi pour une République numérique de 2016, qui oblige l'ouverture par défaut des données de l'administration.

La CNIL est en relation institutionnelle avec la Commission d'accès aux documents administratifs avec laquelle, à la fin de l'année 2019, elle a édité un guide de réutilisation des données publiques. Ce guide propose des fiches thématiques et il a fait l'objet de quatre mille cent téléchargements. Les collectivités territoriales, notamment, disposent de nombreuses données publiques qui peuvent être intéressantes. Cependant, le respect du principe d'anonymisation des données à caractère personnel constitue une des principales clefs de protection des données dans le cadre de l'ouverture des données publiques, par exemple patrimoniales ou financières. La protection des données fonde la condition d'un partage acceptable des données sur le plan social.

En ce qui concerne plus spécifiquement les données de santé, nous avons publié un référentiel qui permet un accès des bénéficiaires aux données de l'échantillon généraliste pour certains traitements qui ne font pas l'objet d'une autorisation de la CNIL.

Le décret sur lequel nous avons rendu un avis ne prévoit pas d'interopérabilité des systèmes d'information SI-DEP et Contact Covid parce que certaines catégories de personnes habilitées à consulter ou à accéder à ces fichiers sont identiques et peuvent donc procéder à un partage d'informations, notamment par exemple, afin d'augmenter l'efficacité des enquêtes d'identification des cas contacts. Quoi qu'il en soit, les systèmes d'information doivent respecter un principe de finalité précis, inscrit dans le RGPD, qui implique une logique en silos, une séparation des systèmes d'information en fonction de leur objectif, ainsi qu'une identification très précise des destinataires de données.

La CNIL ne s'oppose pas à l'interopérabilité des systèmes d'information dès lors qu'elle permet un échange de données contrôlé afin qu'elles puissent aisément être réutilisées dans un autre système, par exemple. Ces échanges doivent être réalisés dans le respect de l'anonymisation des données et de la sécurité, mais en aucun cas dans une logique d'interconnexion généralisée des systèmes d'information. Quoi qu'il en soit, cette interopérabilité devrait être traduite dans les textes.

Le collège de la CNIL a souvent recours à l'expression « solutionnisme technologique » non pas à des fins de stigmatisation de la technologie et des innovations technologiques, mais pour appeler l'attention sur le fait que ces technologies suscitent une sorte de facilité et de fascination qui conduisent à considérer que la faisabilité technologique exonère de l'étude des risques. Les algorithmes, par exemple, sont très utiles, mais il convient

d'être conscient des risques qu'ils sont susceptibles de générer. Il importe donc de ne pas tomber dans ce piège du solutionnisme technologique, sans pour autant, bien entendu, rejeter les opportunités d'innovations.

Lorsqu'il rend un avis sur un système d'information ou sur l'article 11 de la loi du 11 mai 2020, le collège de la CNIL garde constamment à l'esprit la nécessité et la proportionnalité des systèmes d'information. Il s'interroge quant aux bénéfices apportés par ces systèmes dans le cadre de la stratégie sanitaire globale. À titre d'exemple, nous souhaitons que l'application TousAntiCovid fasse l'objet de critères d'évaluation suivis. Je constate que les Britanniques ont récemment opéré des traçages numériques sur leur propre application.

Vous avez indiqué que les ARS encourageraient l'établissement de listes de personnes non vaccinées. Lorsque nous avons rendu notre avis sur le système d'information lié aux vaccins, nous avons constaté qu'il ne s'agissait pas d'un fichier listant les personnes non vaccinées, comme on avait pu entendre que l'Espagne, par exemple, l'envisageait. Si votre information est pertinente, je n'en ai pas été informée. Quoi qu'il en soit, nous avons prévu de contrôler des ARS et nous ne manquerons pas de vérifier précisément ce point.

Il me paraît très important de rappeler que lorsqu'il a examiné le système d'information sur les vaccins, le collège de la CNIL a demandé qu'un droit d'opposition soit possible et figure dans ce fichier et nous l'avons obtenu dans le cadre du décret qui a été publié. Cela signifie que lorsqu'une personne reçoit un bon de vaccination, elle est autorisée à s'opposer à figurer dans le système en formation sur les vaccins si elle refuse de se faire vacciner. En revanche, toute vaccination est consignée dans le fichier pour des raisons de traçabilité pharmacologique. Toutefois la CNIL a veillé à ce que toute personne vaccinée ait le droit de s'opposer à l'utilisation de ses données, même anonymisées, à des fins de recherche.

Dès que la CNIL étudie un système d'information relatif, notamment, à la crise sanitaire, elle est particulièrement attentive à faire respecter les droits de nos concitoyens, les droits dits « Informatique et libertés », dans l'élaboration de ses systèmes d'information.

Nous n'avons pas été saisis par le Conseil d'État à propos de la requête introduite contre la prise de rendez-vous *via* l'application Doctolib. Un collectif a déposé récemment un référé liberté devant le Conseil d'État visant à obtenir l'annulation du partenariat passé entre le Gouvernement et Doctolib pour la prise de rendez-vous. Il est reproché à Doctolib de mettre en danger les données personnelles des patients en confiant leur hébergement à Amazon Web Services, société soumise au droit américain et donc potentiellement aux programmes de surveillance qu'il autorise. Doctolib a publiquement contesté ces allégations. Les requérants demandent au Conseil d'État d'ordonner la suspension de ce partenariat. Cette affaire a été portée devant la justice, mais à ce jour, la CNIL n'a pas été sollicitée par le Conseil d'État à ce sujet.

S'agissant de la question de la pérennisation des systèmes d'information liés à la covid-19, la CNIL a échangé avec le Parlement quant à l'éventuelle instauration d'un régime pérenne de gestion des urgences sanitaires, lors d'une audition qui s'est déroulée au mois de novembre dernier devant la mission d'information de la commission des lois de l'Assemblée nationale relative aux aspects juridiques de l'état d'urgence sanitaire. Au mois de décembre dernier, le collège de la CNIL a également rendu en urgence un avis relatif à un projet de loi qui visait à instituer un régime pérenne de gestion des urgences sanitaires et qui autorisait le Gouvernement à créer par décret des systèmes d'information à des fins de gestion et de suivi

de situations sanitaires exceptionnelles, en dehors du régime de l'état d'urgence sanitaire. Ce projet de loi a finalement été abandonné. Dans l'avis qu'il a rendu, le collège a émis des réserves, considérant que la notion de situations sanitaires exceptionnelles devrait être précisément définie afin de s'assurer que l'atteinte portée à la vie privée par de tels traitements ne revête pas un caractère systématique. De tels systèmes peuvent être mis en œuvre uniquement s'ils constituent une réponse nécessaire et appropriée à la situation en cause. Nous avons estimé que seuls des faits d'une particulière ampleur ou gravité pouvaient justifier la mise en œuvre de tels traitements.

M. Bernard Perrut. Mes questions concernaient des sujets sur lesquels vous êtes déjà intervenue, notamment le passeport sanitaire et les modalités de réponse à ces évolutions qui posent des questions inédites quant à la protection des données à caractère personnel et au respect de la vie privée. Mes interrogations portaient également, bien sûr, sur la collecte d'informations pendant cette campagne de vaccination et sur les garanties à activer de sorte que ces informations soient correctement protégées par le secret médical et accessibles aux seules personnes habilitées et soumises au secret professionnel.

Je souhaite revenir sur le sujet très particulier – qui a déjà été évoqué – de l'hôpital et notamment de l'hôpital de Villefranche-sur-Saône, la ville où je suis élu, qui a été victime d'une attaque par un cryptovirus rançongiciel, le 15 février dernier. Cette attaque aurait pu avoir des conséquences considérables, voire dramatiques, en mettant des vies en danger. Grâce au travail des informaticiens et des techniciens, depuis ce matin, l'ensemble des services a retrouvé un fonctionnement normal et nous en sommes heureux.

Le nombre d'attaques de ce type augmente depuis 2020 et notamment depuis le début de la pandémie qui conduit plus facilement les hôpitaux à s'acquitter de la rançon en raison de la nécessité critique de continuité de l'activité.

Le nombre de procédures a également beaucoup augmenté : cent quarante-huit en 2019 contre quatre cent trente-six en 2020. Une quarantaine d'autres procédures ont été ouvertes devant le parquet de Paris pour le seul mois de janvier. Par conséquent, la situation est grave. Les interpellations pour des faits liés à ces actes, que je juge criminels, demeurent très rares et le nombre croissant de ces cyberattaques remet en cause l'efficacité de la lutte contre la cybermenace.

Par conséquent, madame la présidente, dans ce contexte sanitaire et compte tenu des enjeux toujours croissants liés à la numérisation de la santé, *via* notamment les plateformes de prise de rendez-vous médicaux en ligne, la gestion des violations de données personnelles dans les établissements de soins ne constitue-t-elle pas un véritable sujet de préoccupation ?

Comment la CNIL intervient-elle ? Comment contrôle-t-elle la sécurité des données de santé dans les établissements ?

Au-delà de la vérification de la conformité, les contrôles menés doivent permettre de continuer à augmenter le niveau de sécurité des données de santé des personnes.

Madame la présidente, quelles politiques publiques, non seulement de prévention et d'accompagnement, mais également de protection et de réponse à la cybercriminalité, la CNIL et vous-même pouvez-vous promouvoir ? Quelles mesures avez-vous initiées de sorte à nous rassurer ?

M. Philippe Vigier. Madame la présidente de la CNIL, je souhaite prolonger la question relative au passeport sanitaire, qui émerge progressivement en Europe. N'envisagez-vous pas de vous autosaisir et d'engager une discussion avec vos collègues européens à ce sujet ? Il serait peut-être souhaitable de créer un passeport standard européen, comme on a su le faire pour le vaccin. Cela me semble d'autant plus important que vous auriez ainsi la possibilité de formuler des préconisations. Avez-vous échangé avec le Conseil d'État à ce sujet ?

Je partage pleinement les propos de Stéphane Viry relatifs à l'usage des données. En tant que biologiste, j'ai été extrêmement inquiet de constater une large diffusion de données.

Disposez-vous de suffisamment de moyens de contrôle ?

Ne pensez-vous pas que les contrôles, sur pièces et sur place, des personnes auxquelles vous avez délivré des autorisations d'utilisation des données nécessiteraient un encadrement législatif ? Il me semble qu'une telle initiative sécuriserait non seulement le législateur, mais également les usagers.

M. Alain Ramadier. Madame la présidente de la CNIL, le 17 décembre dernier, la CNIL s'est prononcée sur un projet de décret modifiant les décrets du 29 mai 2020 relatifs au traitement de données dénommé « StopCovid ». Le projet de décret vise à introduire dans l'application TousAntiCovid un dispositif d'enregistrement des visites dans certains établissements recevant du public (ERP), dans la perspective de leur réouverture. La CNIL a considéré qu'au stade actuel de la lutte contre l'épidémie, l'utilité d'un dispositif complémentaire d'identification des contacts à risque de contamination était suffisamment démontrée. Si chaque Français a besoin et envie de retrouver une vie plus normale, le traçage des personnes représente une solution afin d'en terminer avec les restrictions engendrées par les mesures sanitaires.

Néanmoins sans y être opposé, je m'interroge quant aux conséquences de telles mesures qui touchent à nos libertés et à nos droits de vie privée. En effet, pour qu'un tel dispositif soit entièrement opérationnel, il conviendrait que chaque personne accepte de fournir ses informations personnelles avant d'accéder à un ERP. Que répondre aux personnes qui refuseraient ?

Comment, par ailleurs, assurer la confidentialité de ces données ? Comment faire accepter à la population qu'une application permette de suivre et d'enregistrer les allées et venues ? N'est-ce pas contraire au droit à la vie privée ?

C'est pourquoi j'estime qu'il convient de définir des restrictions temporelles pour l'application de telles mesures afin qu'elles ne perdurent pas après la pandémie.

M. Guillaume Chiche. Madame la présidente de la CNIL, je m'interroge au sujet de l'application TousAntiCovid. Cette application utilisant la technologie de traçage numérique est fondée sur la géolocalisation. Elle consiste à installer une application sur le téléphone portable afin de prévenir toutes les personnes, dans un périmètre défini par Bluetooth, qu'un individu est porteur de la covid-19. Le suivi des personnes infectées constitue à cet effet une réponse imparfaite. Outre le fait que le Gouvernement ne parvienne toujours pas à mettre en place un outil techniquement opérationnel et respectueux de nos libertés, cette application suscite des interrogations quant à la sécurité des données de santé. Je pense naturellement aux événements survenus dans différents laboratoires et à la fuite massive de données de santé,

qui s'est produite la semaine dernière, et sur laquelle vous avez été saisie. Non seulement les données de santé de cinq cent mille personnes, dont mille sept cents militaires, ont été diffusées sur des forums accessibles *via* des moteurs de recherche parmi les plus basiques, mais également leur numéro de sécurité sociale, leur adresse postale et encore leur numéro de téléphone portable. La mise en ligne de ces données constitue manifestement une violation de la vie privée, une atteinte grave aux droits des personnes concernées.

Bien que l'objectif de l'application TousAntiCovid consiste à limiter la propagation de la covid-19 et à maîtriser les chaînes de contamination, le dispositif ne doit pas conduire à mettre en danger nos libertés fondamentales. Pouvons-nous considérer que l'application TousAntiCovid est suffisamment protégée contre d'éventuelles cyberattaques ?

Par ailleurs, quels sont les acteurs qui interviennent dans le traitement et le stockage des données ?

Enfin, pouvons-nous considérer que la démarche d'installation d'une telle application est volontaire alors que le secrétaire d'État en charge du dossier, M. Cédric O, explique, à grand renfort d'interviews, que les personnes qui s'y opposent devront porter la responsabilité de l'accroissement du nombre de victimes de la covid-19 ?

Mme Josiane Corneloup. Madame la présidente de la CNIL, la crise sanitaire actuelle aura mis en lumière la dépendance absolue de notre pays à des technologies étrangères. Alors que nous ne cessons d'évoquer la résilience, il me semble important de nous réapproprier notre souveraineté économique et *a fortiori* numérique. La saga du Health Data Hub constitue un exemple emblématique de cette urgence.

Nul d'entre nous ne remet en question la nécessité de collecter les données médicales des citoyens afin de permettre un meilleur suivi médical et épidémiologique des patients. Cependant, nous devons être conscients qu'il s'agit de données particulièrement sensibles, dont la protection constitue une nécessité absolue.

Les données de santé des citoyens ont été confiées à un *cloud* américain. La CNIL et le Conseil d'État s'en sont émus et la CNAM a récemment exprimé ses réserves. Le recours à un *cloud* étranger a été justifié par une prétendue incapacité des acteurs français et européens dans ce domaine, alors que des solutions souveraines existent, comme en atteste la mise en œuvre réussie de l'Ouest Data Hub ou encore du système de l'AP-HP en logiciel libre.

Pouvez-vous nous éclairer quant à ces différentes possibilités ?

M. Jean-Pierre Door. Madame la présidente de la CNIL, il semble en effet que les données de santé aient été transférées à une société américaine, à savoir la société Microsoft. Nous confirmez-vous cette affirmation ? Dans l'affirmative, votre avis a-t-il été sollicité à ce sujet ? En effet, je pense qu'il existe des hébergeurs sérieux en France ou en Europe. Quelles sont les raisons du choix de Microsoft ?

Mme la présidente de la CNIL. S'agissant de l'attaque au rançongiciel qui a frappé l'hôpital de Villefranche-sur-Saône, de façon plus générale, la CNIL est particulièrement vigilante quant à la sécurité dans les hôpitaux face à d'éventuelles cyberattaques. En 2020, la CNIL a procédé à sept contrôles dans des établissements de santé et des hôpitaux. Elle poursuivra ces opérations de contrôle de sorte à s'assurer que la sécurité des données est préservée. Nous souhaitons traiter ce sujet non seulement par une approche répressive, mais

également, en complément des actions engagées par les ministères, dans une démarche d'accompagnement.

Le nombre d'attaques par des rançongiciels et cryptolockers sur les traitements de données dans les hôpitaux a triplé, ce qui génère des conséquences de désorganisation des soins et des risques encourus par les patients. Ainsi que je l'ai indiqué précédemment, la cybersécurité et la protection des données de santé constituent deux des trois thèmes prioritaires retenus par le collège de la CNIL pour l'année 2021.

S'agissant du système d'information relatif aux vaccins, nous nous assurons que les personnes sont correctement informées. Nous procéderons à des contrôles dans des centres de vaccination. Nous serons particulièrement vigilants quant au respect du secret médical et à l'habilitation des personnes qui ont accès au système d'information. Nous assurons également un accompagnement des collectivités locales au cours de la campagne de vaccination des populations. Nous avons publié une fiche pratique sur notre site.

Je profite de l'occasion qui m'est offerte pour indiquer que le site de la CNIL constitue une mine d'informations et il fait l'objet de plusieurs millions de visites chaque année.

Nous avons indiqué aux collectivités locales qu'elles étaient autorisées à cibler et à informer les publics prioritaires pour la vaccination, voire à mener des actions de transport en utilisant les données qu'elles ont à leur disposition de sorte à conduire des populations vers les centres de vaccination.

En revanche, s'agissant de la question de la prise de rendez-vous par exemple, la CNIL leur a indiqué qu'il n'y avait pas lieu de proposer des alternatives aux outils identifiés par l'État, voire de se préoccuper du suivi de l'administration des vaccins.

Nous sommes donc très attentifs à l'utilisation du système d'information sur les vaccins et nous veillons à ce que seules les personnes habilitées puissent y accéder.

S'agissant du développement de pratiques numériques en matière de santé, à savoir peut-être, plus indirectement, la télémédecine, il est vrai que la médecine à distance a connu un essor spectaculaire au cours des derniers mois. Au niveau mondial, nous avons atteint l'objectif fixé pour 2035. En France, nous sommes passés de quelques milliers de consultations par semaine avant le début du confinement à un million de consultations par semaine, au plus fort de la crise, au mois d'avril 2020, qui ont représenté un quart des consultations générales. Ce constat trouve une explication non seulement dans le contexte sanitaire, mais également dans l'ouverture de ces téléconsultations offertes par certaines plateformes aux médecins abonnés, dans la prise en charge à 100 % de ces consultations par l'assurance maladie, annoncée par le Gouvernement en mars dernier, et dans la possibilité d'y recourir avec un autre médecin que son médecin habituel.

Il n'en reste pas moins que cet essor du service de médecine à distance soulève des enjeux en matière de centralisation des données de santé par des acteurs privés et des risques inhérents en matière de sécurité. Dans ce cadre, au mois de juillet, la CNIL a reçu une notification émanant d'une entreprise de rendez-vous en ligne indiquant qu'elle avait subi une attaque informatique ayant permis d'accéder à un certain nombre de rendez-vous.

Nous prenons très au sérieux ces aspects de sécurité. Nous avons récemment publié un référentiel relatif au traitement de données, destiné à la gestion des cabinets médicaux et paramédicaux, dans lequel nous avons formulé des recommandations et abordé la question des mesures de sécurité à mettre en œuvre. Nous avons notamment insisté à ce sujet auprès des prestataires de service chargés de développer et d'assurer la maintenance des logiciels ou des postes de travail qui gèrent les dossiers des patients.

S'agissant de la télémédecine, nous sommes également très attentifs aux questions d'exclusion numérique parce que la télémédecine révèle également des inégalités sociales quant à l'accès à ces technologies. Je rappelle en effet que, selon une enquête de l'Institut national de la statistique et des études économiques menée à la fin de l'année 2019, 12 % des Français ne disposent pas de connexion à Internet.

Pour ce qui concerne le passeport sanitaire, la Commission européenne a confirmé aujourd'hui même aux membres du Comité européen de la protection des données, qui réunit l'ensemble des homologues européens de la CNIL, qu'elle solliciterait très prochainement à ce sujet l'avis de l'ensemble des autorités européennes réunies dans ce comité européen des données ainsi que celui du Contrôleur européen de la protection des données, qui est en quelque sorte la CNIL des institutions européennes.

S'agissant de TousAntiCovid, je voudrais battre en brèche l'idée selon laquelle cette application serait fondée sur la géolocalisation. Un des points d'attention extrêmement important de la CNIL a consisté à veiller à ce que l'application ne repose pas sur une géolocalisation. Elle utilise un protocole dit « Robert » en Bluetooth qui ne constitue pas une géolocalisation et ne permet pas de pister les personnes. La CNIL l'a vérifié lors de ses contrôles. Il en serait de même pour les informations recueillies par le flashage des codes QR à l'entrée d'un établissement recevant du public.

Au-delà du fait qu'elle opère des contrôles sur le déploiement des codes QR, la CNIL s'interroge régulièrement quant à la nécessité et à l'utilité de l'application TousAntiCovid. En outre, elle appelle de ses vœux – et c'est en partie le cas – une doctrine d'usage, à savoir que cette application soit utilisée dans des endroits où sont rassemblées des personnes qui ne se connaissent pas et qui sont susceptibles de présenter des risques de contamination, comme dans les transports en commun ou les ERP.

S'agissant des questions de proportionnalité, nous avons indiqué dans l'avis que nous avons rendu récemment que nous ne disposions pas encore de suffisamment d'éléments relatifs aux établissements recevant du public qui seraient concernés par ces conditions de réouverture. Il convient d'ailleurs de distinguer l'enregistrement obligatoire dans des lieux recevant du public de l'utilisation obligatoire de l'application TousAntiCovid. En effet, la CNIL a beaucoup insisté sur le fait que l'application repose sur un usage volontaire et je confirme qu'il ne peut pas y avoir de conséquences négatives au refus d'utiliser cette application. Il en serait de même des codes QR qui seraient mis à la disposition des ERP.

Il convient de proposer une alternative à l'utilisation de l'application TousAntiCovid, matérialisée tout simplement par des cahiers de rappel en version papier qui doivent également respecter les éléments relatifs à la protection des données. Lorsque nous avons déposé notre avis, le ministère nous a confirmé que deux dispositifs, l'un numérique et l'autre non numérique – cahier de rappel –, seraient mis à la disposition des personnes.

Par ailleurs, dans le cadre de notre avis, nous avons recommandé que le caractère obligatoire, non pas de l'utilisation de l'application, mais de l'enregistrement des visites dans des établissements recevant du public soit limité aux établissements à fort potentiel de risque, à savoir ceux dans lesquels le port du masque n'est pas possible – restaurants, salles de sport – ou ceux dans lesquels les mesures barrières ne sont pas efficaces.

Nous avons également attiré l'attention du Gouvernement et du Parlement sur le fait que, selon nous, il ne faut pas rendre ces enregistrements de visites obligatoires dans les lieux recevant du public dont la fréquentation relève de libertés fondamentales, comme les lieux de culte et les locaux syndicaux.

Nous avons obtenu que figure dans le décret la possibilité pour un utilisateur de supprimer de l'historique un lieu qu'il a visité.

Je vous rappelle que l'application TousAntiCovid a fait l'objet de nombreux contrôles de la CNIL. Nous avons réalisé sept contrôles et prononcé une mise en demeure contre StopCovid en juillet dernier qui a été clôturée en septembre. Pour autant, dès la conception de cette application, les préoccupations de protection de la vie privée ont été prises en compte et nous y avons veillé.

J'ai précédemment évoqué les actions que nous avons mises en œuvre à la suite de la fuite des données de santé de près de cinq cent mille patients de laboratoires. Nous nous sommes assurés que les personnes concernées avaient été informées ou le seront dans de très brefs délais. Nous avons obtenu le blocage de l'accès au fichier par le biais d'un référé d'heure à heure, déposé auprès du tribunal judiciaire de Paris, dès l'instruction des notifications de violations de données que nous avions enregistrées. Nous rappelons sans cesse la nécessité de protéger suffisamment les données de santé, thème prioritaire de nos contrôles.

Vous avez souligné la dépendance de certains de nos systèmes d'information aux technologies étrangères. Je confirme que l'hébergement des données de santé est assuré par Microsoft, société de droit américain. Je rappelle que la CNIL ne conteste absolument pas l'utilité et l'intérêt de cette plateforme de données de santé en matière de recherche. Cependant, en raison de la sensibilité et du volume des données en cause, elle a engagé un dialogue extrêmement nourri avec le ministère de la santé quant au risque éventuel présenté un hébergement de données par un opérateur qui n'est pas soumis à une juridiction européenne. Nous avons obtenu un engagement du ministère de la santé de remplacer cet hébergeur ou, en tout cas, de modifier les conditions de cet hébergement de sorte qu'il respecte davantage la souveraineté numérique française et européenne. Au mois de juillet dernier, la Cour de justice de l'Union européenne a annulé le traité permettant d'échanger des données entre l'Union européenne et les États-Unis, faute de garanties de protection suffisantes. Le Conseil d'État a également demandé la mise en œuvre de garanties supplémentaires à la fin de l'année dernière. Le collège de la CNIL sera particulièrement vigilant au respect du délai indiqué pour la mise en œuvre d'un hébergement conforme aux exigences françaises et européennes en matière de protection des données.

De nombreux responsables politiques nationaux et européens se montrent favorables, dans leurs discours et dans leurs actions, à la souveraineté numérique européenne.

Mme la présidente Fadila Khattabi. Je vous remercie, madame la présidente, pour l'ensemble de vos réponses.

La réunion s'achève à 18 heures 45.