A S S E M B L É E N A T I O N A L E

X V I^e L É G I S L A T U R E

Compte rendu

Commission des lois constitutionnelles, de la législation et de l'administration générale de la République

Mercredi
12 octobre 2022
Séance de 11 heures

Compte rendu n° 3

SESSION ORDINAIRE DE **2022-2023**

Présidence de M. Sacha Houlié, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 11 heures

Présidence de M. Sacha Houlié, président.

La commission auditionne Mme Marie-Laure Denis, présidente de la CNIL, sur les traitements automatisés mis en œuvre pour lutter contre la Covid-19.

M. le président Sacha Houlié. Nous recevons aujourd'hui Mme Marie-Laure Denis, présidente de la CNIL, déjà auditionnée à plusieurs reprises par notre commission.

Le 6 juillet dernier, nous avons examiné la prolongation jusqu'au 31 janvier 2023 des traitements automatisés dérogatoires utilisés dans la lutte contre l'épidémie de Covid, notamment SI-DEP. Lorsque nous avions adopté un amendement à l'unanimité en commission, je m'étais engagé à auditionner madame Denis avant le 1er novembre. C'est chose faite. Elle sera également auditionnée par la mission d'information de la commission des lois portant sur les images de sécurité, rapportée par Philippe Latombe et Philippe Gosselin, le 18 octobre.

La loi du 30 juillet 2022 a mis fin à la plupart des mesures exorbitantes du droit commun pour la gestion de la crise sanitaire. Elle a prorogé jusqu'au 31 janvier 2023 les systèmes d'information SI-DEP et Contact Covid, mis en œuvre sur le fondement de la loi du 11 mai 2020. Cette audition vise à dresser un bilan de leur utilisation par le gouvernement dans le contexte de sortie de crise, du moins d'un point de vue juridique.

Ensuite, si l'application TousAntiCovid ne relève pas directement de ces systèmes d'information, elle a aussi été mise en œuvre sur le fondement de la loi du 11 mai 2020. Son autorisation a été prorogée, notamment pour permettre l'enregistrement et l'émission, *via* SI-DEP des tests de dépistage. Dans un avis, vous recommandiez d'inciter les utilisateurs à n'activer la fonctionnalité de traçage que pendant les périodes de circulation active du virus.

Quel bilan tirez-vous de l'utilisation de cette application, sur laquelle nous sommes plusieurs à avoir émis des réserves ?

Ensuite, pouvez-vous nous dresser un bilan de tous les outils numériques mobilisés pour faire face à cette crise ? J'évoque ici les systèmes SI-DEP et contact covid, l'application TousAntiCovid, et les passes sanitaires et vaccinaux.

Vous avez publié cinq avis au Parlement. Dans celui d'octobre 2020, vous regrettiez que le gouvernement n'ait transmis aucun élément concret d'évaluation de l'efficacité de ces dispositifs. J'observe que le Conseil d'analyse économique a estimé que les passes avaient permis d'éviter 4 000 décès. Pouvez-vous corroborer cette information, et sur quel élément ?

À la veille de l'hiver, les cas épidémiques repartent à la hausse. Quelles perspectives donnez-vous à l'utilisation de ces différents systèmes d'information ? Quelles recommandations pouvez-vous émettre devant notre commission, qui pourrait éventuellement être saisie sur un texte à l'avenir ?

Mme Marie-Laure Denis, présidente de la CNIL. Je suis accompagnée par Hélène Guimiot-Breaud, cheffe du service de la santé, Nassera Bekhat, cheffe du service des affaires économiques, Benjamin Vialle, chef du service des contrôles sur la santé, les ressources humaines et les affaires publiques.

Notre commission s'est prononcée à de nombreuses reprises sur les systèmes d'information, tant dans le cadre de ses missions d'accompagnement des pouvoirs publics que de son pouvoir de contrôle a posteriori.

La gestion de cette crise a rendu nécessaire la création, souvent dans des conditions d'urgence, de nombreux nouveaux outils impliquant le traitement d'importants volumes de données à caractère personnel, et en particulier de données de santé, très sensibles. Leur conception et leur calibrage ont soulevé des questions inédites en matière de protection des données, en raison de leur ampleur. Certains systèmes d'information ont ainsi collecté les données d'une majorité de la population française. Une multitude de professionnels devaient accéder aux données de SI-DEP et du système d'information sur les vaccins, notamment.

Enfin, de nouvelles technologies ont été utilisées dans le cadre de l'application Stop Covid, devenu TousAntiCovid, et de la gestion du passe sanitaire.

Ensuite, cette situation exceptionnelle n'a pas fait obstacle à l'application de la réglementation sur la protection des données. Les principes posés par cette dernière ont démontré la grande robustesse du règlement général sur la protection des données (RGPD). Ils étaient suffisamment souples pour permettre le déploiement de divers outils de gestion de l'épidémie tout en offrant à la CNIL la possibilité de contrôler le respect des droits et des libertés fondamentales des personnes. Le cas échéant, elle a pu demander des corrections de mauvaises pratiques.

Ces deux dernières années ont mis en exergue la nécessaire prise en compte de la protection des données à caractère personnel, facteur déterminant pour contribuer à la confiance des concitoyens. Elle participe à la création de conditions d'acceptabilité sociale des solutions proposées, et garantit ainsi l'efficacité des mesures mises en place.

Pendant cette crise, la CNIL a veillé à la conformité des outils utilisés aux réglementations applicables en matière de droit au respect de la vie privée, et au respect d'autres libertés et droits fondamentaux qu'elle n'a pas pour vocation habituelle de protéger : liberté d'aller et venir, liberté d'entreprendre, égalité de traitement entre les personnes, liberté de consentir à un traitement médical ou de subir un acte médical. À cette fin, elle a fait appel à l'ensemble des pouvoirs lui étant dévolus par la loi, et a mobilisé toutes les ressources à sa disposition. À cet égard, le collège de la CNIL et ses agents ont fait preuve d'un engagement et d'une réactivité remarquables.

Cette crise a démontré toute la pertinence des équilibres organisés par la loi informatique et libertés.

La CNIL a conseillé les pouvoirs publics à de nombreuses occasions, souvent en urgence, sur la conformité des traitements mis en œuvre. À cet égard, je souligne la qualité de nos échanges avec les ministères compétents lors des phases d'élaboration des textes et de la conduite des études d'impact. Notre dialogue efficace a certainement contribué à une réelle prise en compte des principes fondateurs et protecteurs de la réglementation en matière de protection des données.

Depuis 2020, la CNIL a rendu 31 avis sur des projets de textes du gouvernement. La présente audition est la treizième devant le Parlement. Elle contribue à éclairer les débats sur les enjeux fondamentaux liés au respect de la vie privée et des données à caractère personnel.

Dans le même temps, nous avons instruit près de 170 demandes d'autorisations relatives à des projets de recherche en lien avec la crise sanitaire, dans des délais extrêmement courts, grâce à une procédure *ad hoc* s'appuyant sur la priorité des demandes.

Nous avons fréquemment rappelé au gouvernement la nécessité d'une évaluation régulière des dispositifs mis en œuvre dans le cadre d'une politique sanitaire, qui doit être observée dans sa globalité. Il s'agissait d'une part d'apprécier la proportionnalité des dispositifs au plus fort de la crise pour mettre fin, le cas échéant, à des mesures inutiles ou disproportionnées. D'autre part, nous devons aujourd'hui être à même de déterminer les systèmes les plus utiles pour gérer une crise sanitaire de cette ampleur, et les concevoir de façon à concilier les impératifs de protection de la santé et de la vie privée.

L'article 11 de la loi du 11 mai 2020 demandait un rapport détaillé pour l'application des systèmes d'information SI-DEP et Contact Covid. L'article 1er de la loi du 31 mai 2021 demandait la transmission au Parlement, par le gouvernement, d'un rapport sur l'impact des mesures prises et les indicateurs sanitaires justifiant le maintien de ces systèmes d'information. Plus récemment, l'article 5 de la loi du 30 juillet 2022 prescrivait la transmission d'une évaluation du cadre juridique en vigueur, y compris en matière de traitement de données à caractère personnel.

Dans ce contexte, l'application TousAntiCovid et le passe sanitaire ont fait l'objet de rapports d'évaluation *ad hoc*, transmis à la CNIL. Après analyse du rapport et sur la base de ses propres investigations, celle-ci a constaté que l'outil était particulièrement respectueux de la vie privée. Le traçage des contacts automatiques au moyen des téléphones était réalisé par la puissance publique, et générait légitimement des craintes parmi nos concitoyens. Il pouvait présenter des risques pour les libertés publiques. Le gouvernement a associé la CNIL à sa conception, et a tenu compte de ses conseils. Notre collège a considéré que l'application pouvait être maintenue en vigueur, compte tenu des garanties intégrées : volontariat, strict respect du principe de minimisation des données, absence de géolocalisation.

Cependant, l'évaluation a montré que l'application n'a eu qu'une utilité marginale dans le *contact tracing*. Nous devons en tirer des leçons pour l'avenir, en déterminant notamment le moment auquel un outil de ce type, à supposer qu'il soit nécessaire, est le plus utile. L'est-il au début de la circulation d'un virus particulièrement dangereux pour identifier un pic de contaminations et en tirer des conséquences ? Doit-il être utilisé lors de périodes particulièrement actives pour compléter les enquêtes réalisées manuellement, lorsqu'elles sont déjà fortement mobilisées ? Nous ne savons pas encore répondre à ces questions.

Il ressort des avis du Conseil d'État de juillet et décembre 2021 que les passes sanitaires et vaccinaux avaient pour objectifs principaux de réduire la probabilité de développer et de transmettre la covid-19 pour les personnes exerçant des activités à risque, et de limiter les formes graves de la maladie afin d'alléger la pression sur les systèmes hospitaliers. Faute d'outils pour distinguer la part de réduction des risques de transmission attribuable au passe sanitaire, et en l'absence de situations de référence comparables, l'évaluation révèle que le passe sanitaire a principalement participé à l'augmentation de la couverture vaccinale. Selon le rapport, c'est ce qui a contribué à réduire la propagation du virus et les formes graves, limitant ainsi la pression exercée sur les hôpitaux.

Si le bilan semble révéler leur utilité, je souligne que ces passes sanitaires, puis vaccinaux, sont particulièrement attentatoires aux libertés publiques. Ils ne doivent être

réservés qu'à des situations extrêmes, pour un temps limité. Le Parlement doit marquer qu'il n'y a pas d'effet cliquet de ce point de vue.

Enfin, l'évaluation des systèmes d'information SI-DEP et Contact Covid ou ceux des agences régionales de santé (ARS), et de Vaccin Covid n'a fait état que d'éléments factuels et chiffrés portant sur la mise en place de chacun de ces systèmes d'information et de traitement dans leur mise en œuvre individuelle.

La création de SI-DEP semble avoir été légitime, même si la CNIL n'est historiquement pas favorable à la centralisation des fichiers servant à l'administration des soins de santé. Cette doctrine a pour justification la protection des données de santé des Français, particulièrement sensibles. En effet, une telle centralisation, intrusive, peut présenter des risques de mésusage et de divulgation, notamment accidentelle, et n'est pas sans conséquence.

Nous devons tout de même resituer cette discussion dans un contexte de progression de la numérisation de la société. Par ailleurs, une centralisation a pu être justifiée au vu des caractéristiques d'une crise sanitaire d'une telle violence, nécessitant une forte réactivité pour traiter et transmettre un très grand nombre de données. Le collège de la CNIL a considéré que dans ces circonstances particulières, l'architecture centralisée des systèmes d'information était admissible.

Je reste en revanche sur ma faim concernant les évaluations de Contact Covid et des systèmes d'information des ARS, principalement utilisés pour les enquêtes sanitaires. Je ne nie pas le principe de ces traitements, mais ils présentent des risques particuliers en termes de protection de la vie privée. Ils ont conduit à collecter et brasser une quantité colossale de données. Leur utilisation continue, avec une telle intensité et une telle densité, était-elle indispensable ? Elle était sans nul doute légitime, mais si nous sommes de nouveau confrontés à cette situation, nous devrons nous interroger sur une possibilité de calibrage plus fin. Le traitement pourrait varier selon le contexte. Lors de périodes de circulation intense du virus, un tel traitement impose toutefois de disposer de moyens suffisants pour collecter et exploiter efficacement les données. Il faut pouvoir mobiliser un grand nombre d'enquêteurs à former, et mener des enquêtes dans des délais contraints pour conserver la pertinence de la notification. Il n'est pas certain que tel ait été le cas, notamment au plus fort de la crise.

Sans pouvoir porter un jugement définitif, une analyse de la complémentarité des dispositifs mis en œuvre me semble nécessaire, à plus forte raison avant d'envisager une éventuelle refonte du cadre juridique applicable en période de crise. Il ne s'agit nullement de remettre en cause la légitimité de l'action sanitaire mise en place dans l'urgence, mais d'apprendre de cette période.

Dès le début de la crise, j'ai annoncé que la CNIL contrôlerait en continu les fichiers liés à sa gestion pour répondre au caractère exceptionnel de la situation, et au vu de la sensibilité des données traitées. Ce contrôle a mobilisé énormément de ressources, mais a contribué à la confiance de nos concitoyens à l'égard des services publics. Ces vérifications ont principalement porté sur l'information des personnes, la sécurisation des données et leur durée de conservation. Ainsi, depuis 2020, la commission a procédé à 52 contrôles. De nouvelles vérifications seront diligentées au terme de l'alimentation de Contact Covid, prévue le 31 janvier 2023.

Plus globalement, les investigations ne s'achèveront qu'au terme de l'utilisation des fichiers. Nous nous attacherons notamment à vérifier que les différents systèmes d'information ne sont plus alimentés et que les données sont bien supprimées à l'issue de leur durée de conservation.

Cette démarche de contrôle continu des outils de gestion de l'épidémie est sans équivalent dans l'histoire de notre institution. Elle a permis de s'assurer de la mise en conformité des systèmes d'information en temps réel. Il en résulte un bilan globalement positif en matière de conformité RGPD. Comme l'a souligné le collège de la CNIL dans les cinq avis vous ayant été adressés, aucun dysfonctionnement structurel majeur des systèmes d'information créés pour lutter contre la crise sanitaire n'a été relevé.

Lorsque la CNIL a identifié des difficultés, notamment à la suite de violations de données, des modifications techniques ont été opérées, et les textes ont été ajustés. Etaient notamment concernés l'information des personnes, l'encadrement du recours à des prestataires privés ou l'amélioration des mesures de sécurité.

Cette crise a constitué un puissant accélérateur de la diffusion numérique dans le domaine de la santé. La place des plates-formes en ligne de prise de rendez-vous et l'essor considérable de la téléconsultation l'illustrent. Elle a également éclairé sous un jour nouveau les questions de souveraineté numérique, et les risques en matière de sécurité des systèmes d'information, tels que l'augmentation des cyberattaques ou la faiblesse de la culture numérique chez certains acteurs.

La CNIL n'est pas compétente pour dire si les dispositifs existants suffisaient pour lutter contre une pandémie. Pour autant, les nombreux textes adoptés pendant la crise ont témoigné de l'insuffisance ou de l'incomplétude du cadre juridique antérieur à cette période. Ils ont répondu à la nécessité, dans certains cas précis, de déroger au secret médical, et ont mis en exergue les besoins de transparence quant au fonctionnement de dispositifs nouveaux.

Par ailleurs, une évaluation globale de ces dispositifs semble s'imposer afin de s'assurer de leur complémentarité, à plus forte raison avant d'envisager toute éventuelle pérennisation.

À la lumière de ces trois dernières années, il convient de procéder à un état des lieux objectif de l'existant, et d'engager une réflexion sur le cadre juridique actuel et les évolutions nécessaires. Une telle évaluation s'impose avant la fin de ce mois, en application de l'article 5 de la loi du 30 juillet 2022, bien que celle-ci précise qu'elle ne concerne que les pandémies, et non les épidémies d'autres catastrophes sanitaires.

En outre, une réflexion sur l'opportunité de maintenir certains dispositifs en dehors des périodes de crise doit aussi être engagée. Ce débat permettra de cranter dans la loi un certain nombre de garanties assurant un équilibre entre l'objectif de protection de la santé publique et le respect des libertés fondamentales des personnes, l'accès au soin et la protection des données à caractère personnel. Il conviendra de prendre en compte les spécificités de chaque crise afin que les atteintes portées aux droits et libertés des personnes concernées constituent des mesures nécessaires et proportionnées. Par voie de conséquence, il s'agit de déterminer les critères spécifiques de création ou d'activation des systèmes d'information.

Cette vigilance plaide pour l'élaboration d'un dispositif à géométrie variable. En tout état de cause, seules des situations d'une ampleur ou d'une gravité particulières devraient autoriser la mise en œuvre de traitements spécifiques, a fortiori s'ils sont dérogatoires au droit commun et attentatoires aux droits et libertés.

Pour ces raisons, je demande que la CNIL soit saisie de tout projet de loi relatif à la protection des données à caractère personnel et à leur traitement, quand bien même la mise en œuvre des traitements en cause devrait être précisée par voie réglementaire.

Enfin, cette crise a confirmé qu'il était possible de mettre en œuvre des traitements de données de manière efficace, rapide et respectueuse de la vie privée. Loin de constituer des freins à la gestion de la crise sanitaire, le RGPD et la loi Informatique et libertés ont garanti la mise en œuvre effective de dispositifs respectueux des droits et libertés des personnes. Ils ont ainsi participé à une transparence de l'action de l'État, qui a contribué, je l'espère, à limiter la défiance de nos concitoyens à l'égard des systèmes d'information.

M. le président Sacha Houlié. Je réponds favorablement à votre demande de consultation préalable avant tout texte législatif ou délégant un pouvoir législatif au pouvoir réglementaire sur la question de la protection des données. J'ai par ailleurs cru comprendre que vous regrettiez qu'ait été rayé d'un trait de plume tout le dispositif législatif sur la question de l'état d'urgence sanitaire, qui figurait dans le Code de la santé publique. Je l'ai moi aussi déploré en commission mixte paritaire et lors de la lecture des conclusions de celle-ci.

M. Rémy Rebeyrotte, Renaissance (RE). Lors du débat et du vote sur le RGPD, dont j'étais responsable pour le groupe majoritaire, nous étions loin d'imaginer ce qui allait arriver. Nous avons beaucoup réfléchi au lien entre la protection des données et leur diffusion, notamment en matière scientifique, pour tirer des conclusions et chercher une amélioration des dispositifs. Un débat intense portait notamment sur l'anonymisation, la *cryptonomisation* ou la pseudonymisation des données.

Comment ressentez-vous cette situation ? Des améliorations peuvent-elles encore être apportées en matière de RGPD?

Par ailleurs, les moyens complémentaires donnés à la CNIL pour réaliser l'ensemble de ses tâches sont-ils suffisants ? Devons-nous en ajouter pour mieux réaliser ces politiques essentielles pour notre liberté et notre vie en société ?

M. Jean-François Coulomme, (LFI–NUPES). Comme tout système informatique, nous sommes confrontés à des flux de données. Qui les centralise ? Pouvez-vous nous donner des informations sur les types de serveurs, leur propriétaire et leur nationalité ? Qui décide à qui sont transmises ces données ? Existe-t-il une autorité supérieure indépendante, ou le propriétaire du logiciel s'en charge-t-il ? Quels sont les droits affectés au détenteur des données pour en décider le destinataire ou l'utilisateur ?

Des organismes sont censés assurer l'accompagnement social des agents de services préfectoraux, par exemple. Qui leur accorde les droits ?

Par ailleurs, de quelle manière la CNIL est-elle vigilante aux garanties ?

Enfin, comment disposer d'un système simple d'annulation, de suppression ou d'accès aux données par leurs propriétaires ?

M. Emmanuel Mandon, Démocrate (Dem). Depuis sa création en 1978, la CNIL s'attache à la défense de la protection de la vie privée et des libertés individuelles, et en particulier de la protection de nos données personnelles recouvrant des enjeux de plus en plus larges et complexes. Le Groupe démocrate a montré sa sensibilité vis-à-vis de cette protection lors de l'examen de différents textes relatifs à la crise sanitaire.

L'irruption continue de nouvelles technologies conjuguée à l'omniprésence des traitements de données personnelles dans tous les domaines de la vie constitue un défi permanent pour la CNIL et pour notre société. La combinaison du RGPD et de la CNIL fut fort heureuse dans le contexte que nous venons de vivre. Nous sommes conscients de l'importance de cette action. Le bilan vous paraît globalement positif. Aujourd'hui, que pouvez-vous dire des moyens dont vous disposez ?

Enfin, l'application TousAntiCovid, dont vous avez un peu mis en doute l'utilité, reste-t-elle indispensable pour la suite ?

Mme Edwige Diaz (RN). La CNIL a alerté à plusieurs reprises quant aux risques de dispositifs attentatoires à la vie privée, tels que le passe sanitaire. Dans une de ses délibérations, on peut lire « *il est essentiel que l'impact des différents dispositifs numériques sur la stratégie sanitaire globale soit étudié et documenté régulièrement à partir de données objectives afin de s'assurer que ce type de dispositif prenne fin dès que leur nécessité disparaîtra ».*

Vous avez mis en cause l'utilisation des données du passe sanitaire par mail, qui les rendait accessibles à tous de façon indéterminée. Vous avez également dû rappeler à l'ordre une fédération sportive à ce sujet, sans la sanctionner. Qu'est-il advenu des données insérées dans les passes sanitaires alors que celui-ci n'est plus en vigueur ? Où, comment et combien de temps sont-elles conservées ? Qui y a accès ?

M. Hervé Saulignac (SOC). Vous l'avez rappelé, la population française a consenti à la collecte d'une partie de sa vie pour lutter contre le virus. Pour autant, je ne crois pas qu'elle ait admis la pérennisation de ces dispositifs. Les Français s'interrogent aujourd'hui sur la nécessité de les maintenir, compte tenu de l'état sanitaire actuel. Même si l'outil est respectueux de la vie privée, il n'en demeure pas moins que nous avons créé un risque de violation de celle-ci.

Dans ce contexte, pouvez-vous décomposer les usages aujourd'hui faits de l'application TousAntiCovid, fondée sur le *contact tracing* qui a été marginal dans son usage. Ce dispositif garde-t-il du sens dès lors qu'il n'y a plus de passe sanitaire ? N'est-il pas temps d'éteindre ces dispositifs ?

M. Philippe Pradal (HOR). Je ne retiendrai que le bilan globalement positif de cet exposé très clair, bien qu'il ne rappelle pas que des souvenirs positifs à un certain nombre de personnes dont les cheveux sont blancs. Je ne ferai que prolonger la réflexion du Président Houlié sur le fait qu'un certain nombre de dispositifs ont disparu du Code de la santé publique.

Dans un monde où les crises vont probablement s'enchaîner, comment la CNIL pourrait-elle participer à l'élaboration d'une doctrine qui permettrait d'activer les systèmes avec un peu plus d'anticipation ? Ainsi, nous n'aurions plus à réagir au dernier moment, mais

plutôt à anticiper les crises grâce à un corpus doctrinal auquel vous pourriez contribuer, avec les autorités de l'Etat et le Parlement.

M. Jérémie Iordanoff (Écolo-NUPES). Nous comprenons grâce à votre état des lieux que les dispositifs en vigueur connaissent une amélioration, à la suite de votre contrôle et de vos avis. Je m'y associe parfois, notamment sur le risque d'accoutumance et de banalisation des dispositifs dérogatoires au droit commun. Ces mesures ne peuvent être justifiées que si elles sont efficaces et prouvées. À ce titre, vous notez que le passe sanitaire, particulièrement attentatoire aux libertés publiques, n'a pas eu d'effet direct proportionné sur la limitation de la propagation du virus, mais uniquement sur la couverture vaccinale.

Par ailleurs, les moyens financiers et d'investigation de la CNIL sont-ils suffisants au regard des enjeux en présence ? En termes de prérogatives, un principe d'autosaisine serait-il pertinent ?

Mme Elsa Faucillon (GDR-NUPES). Au-delà des auditions, les avis de la CNIL ont largement occupé nos débats lors du dernier projet de loi. Mon groupe et moi avons exprimé nos craintes quant aux dangers d'un fichier d'une telle ampleur, à des prorogations toujours bien trop longues, et aux dangers que pouvaient présenter ces différentes applications et ces recueils de traitement de données. Vous les exprimez peut-être moins maintenant qu'un travail a été réalisé, mais les premiers avis de la CNIL rejoignaient ces craintes.

Pouvez-vous nous donner des préconisations quant à la méthode d'extinction envisagée de ces données ?

Ensuite, dans une délibération du 19 mai 2022, vous invitiez les responsables des traitements Vaccin Covid et SI-DEP à relever le niveau de sécurité des systèmes et à mettre à jour leur analyse d'impact sur la protection des données. Cette sollicitation a-t-elle été prise en compte ? Quels sont les risques identifiés liés à la sécurité numérique des données de santé ?

Enfin, dans un avis sur la sécurité numérique des personnes, la Commission nationale consultative des droits de l'homme (CNCDH) alertait sur un effet cliquet du recours à ces dispositifs numériques, craignant une accoutumance. Vous avez également émis des craintes. Je relève à cet égard la tentative du ministère de l'économie d'accéder à des données bancaires des français. Pensez-vous que le gouvernement a suffisamment informé la population sur l'existence de ces différents traitements ?

Mme Marie-Laure Denis, présidente de la CNIL. Concernant l'état d'urgence sanitaire et une éventuelle pérennisation, je crois qu'il y avait un projet de loi en fin d'année 2020, mais qu'il n'a pas abouti.

Outre le fait que nous n'avons pas de compétences sanitaires ou scientifiques particulières, il nous est délicat de nous prononcer sur l'éventuelle pérennisation de certains de ces dispositifs en l'absence de texte et sans savoir quel système est prolongeable plutôt qu'un autre. En tout état de cause, nous devrons retenir un dispositif à géométrie variable, fondé sur la nécessité et la proportionnalité au cas par cas. Il ne s'agit pas de copier et coller l'ensemble d'un outil particulier et lié à des circonstances précises.

Le RGPD et la CNIL n'ont pas été un frein dans le domaine de la santé. Nous délivrons des autorisations en matière de recherche en santé si les projets ne sont pas conformes aux méthodologies de référence que nous avons nous-mêmes émises. 85 % des

demandes nous ayant été adressées pour de la recherche sur la covid-19 y étaient conformes. Dans les autres cas, nous avons délivré 170 autorisations, la plupart du temps en moins d'une semaine. Nous avions mis en place une adresse mail dédiée, accentué la disponibilité des équipes, dématérialisé des décisions, et commencé à traiter la pré-instruction des dossiers en amont avec des chercheurs. Ainsi, nous avons aidé les acteurs à trouver des solutions respectant les modalités de recueil du consentement des personnes dont les données faisaient l'objet de recherches. Nous nous sommes également attachés aux modalités d'information de celles-ci. Le processus tel qu'il existe n'est pas bloquant. Un article de la loi informatique et libertés permet à certains organismes listés par un arrêté de réaliser sans autorisation de la CNIL des traitements de données de façon temporaire dans le domaine de la santé. En tout état de cause, nous devons nous attacher à déterminer les catégories de données pouvant faire l'objet d'un traitement à des fins de suivi de recherche.

Vous avez évoqué les subtilités entre l'anonymisation et la pseudonymisation. Nous sommes notamment très sensibles à la réutilisation de données pseudonymisées. Les noms, prénoms, numéros de sécurité sociale, adresses et coordonnées de contact doivent à notre sens être exclus. Les fuites de données sont possibles dans le domaine de la santé. Ce sujet rejoint la préoccupation cyber, sur laquelle je reviendrai. Les individus prennent conscience des enjeux en matière de sécurité lorsque leurs propres données sont concernées.

La crise sanitaire et la réaction de la CNIL face à celle-ci ont probablement été déterminantes dans la prise de conscience des pouvoirs publics concernant nos moyens. À la fin de l'année prochaine, nos effectifs atteindront 290 personnes, ce qui correspond à une augmentation d'un tiers en l'espace de trois ou quatre ans. Ceci dit, la CNIL reste petite par rapport à des autorités de protection des données comparables. Notre homologue britannique, l'ICO, et l'autorité de protection des données allemande, certes dans un système fédéral, comptent respectivement trois et quatre fois plus d'agents que nous. De plus, une révolution réglementaire s'annonce. Le paquet numérique européen et tous les textes que vous connaissez, dont le DMA, le DSA ou le *digital governance act,* nous poussent à nous interroger sur celui qui dirigera concrètement ces dispositions. La CNIL a selon moi un rôle à jouer sur un certain nombre de ces textes, qui concernent largement les données à caractère personnel. Si de nouvelles compétences nous échoient, ce que nous souhaitons, nous devrons proportionner nos moyens en conséquence.

À ma connaissance, les serveurs des systèmes d'information Covid étaient bien français, puisque SI-DEP étaient hébergé à l'APHP. Sur le passe sanitaire, le ministère de la santé a pu envisager de faire appel à un acteur américain pour disposer de solutions permettant des mesures de sécurité. Après discussions, il a choisi de basculer chez un acteur français. De façon générale, notre collège est attentif à ce que les données soient hébergées par des structures exclusivement soumises au droit français et européen, quitte à ce que les opérateurs utilisent des technologies étrangères. Ainsi, nous limitons l'accès des données à des acteurs dont le niveau de garantie n'est pas le même.

Nous avons été très vigilants à la garantie des droits. Vous évoquez le droit d'opposition. Parfois, vous l'avez vous-même exclu, ce qui peut être compréhensible. Lorsque vous vous faites vacciner, votre nom apparaît dans un fichier. Vous n'avez pas le choix, pour des raisons de pharmacovigilance, entre autres. En revanche, la réglementation prévoit un ensemble de droits sur l'information aux données, le droit d'accès ou de rectification. Si certains droits peuvent être restreints en situation de crise sanitaire, ces limitations doivent être inscrites dans un texte pris après avis de la CNIL. Les individus doivent en être informés. Dans le même temps, le consentement du patient infecté doit être recueilli pour que son

identité soit communiquée à ses cas contacts, par exemple. Une vigilance particulière s'impose également pour les données couvertes par le secret médical. Dans la mesure du possible, seuls des professionnels de santé devraient y avoir accès, mais la loi a dû élargir cette catégorie d'acteurs. Il est nécessaire de pouvoir aménager des dérogations au secret médical. SI-DEP et Contact Covid en ont fait l'objet.

L'application TousAntiCovid a concentré de nombreux débats et interrogations pendant la crise sanitaire, puisqu'elle était la première application de traçage étatique. Nous avons travaillé en partenariat avec l'INRIA pour nous assurer qu'elle intègre dès sa conception des considérations de vie privée. Ce dispositif était basé sur le volontariat, ne faisait pas de géolocalisation, et traitait un minimum de données, a priori non identifiantes. Il nous a semblé qu'il pouvait être maintenu, mais nous avons demandé dans notre dernier avis que les gens n'activent pas la fonctionnalité de traçage lorsque la circulation du virus est faible. Par ailleurs, l'application présente de nombreuses autres fonctionnalités, dont le stockage de certificats et de passes, ou le recueil d'informations sur la vaccination et le dépistage. Ainsi, dans la balance entre son utilité marginale et la faible atteinte à la protection de la vie privée, il nous a semblé que cette application pouvait être maintenue, mais le moins longtemps possible. D'ailleurs, je crois savoir qu'elle doit disparaître le 31 janvier 2023. Nous y veillerons. Les données collectées par TousAntiCovid ne sont, en outre, pas conservées au-delà d'une quinzaine de jours.

La loi du 31 mai 2021 modifiée et son décret d'application interdisent la conservation des données du passe sanitaire. Elles ne sont utilisées que pendant son contrôle. Des garanties fortes ont été poussées par la CNIL sur ce sujet, et nous avons réalisé des contrôles. Nous avons beaucoup insisté en termes de pédagogie pour que seuls le « oui » ou le « non » apparaissent, et non l'ensemble des données, sauf pour le passe utilisé pour les déplacements hors de France, nécessitant davantage de données.

J'ai rappelé plus tôt le côté multifonctionnel de l'application TousAntiCovid : *contact tracing,* statistiques sur la crise sanitaire, stockage du passe – encore utilisé pour le passe européen en vigueur jusqu'en juin 2023. Cette application s'éteindra le 31 janvier 2023.

J'imagine que cette audition est en partie liée au fait que vous allez devoir réfléchir à la pérennisation de certains dispositifs. J'ai indiqué plus tôt que la CNIL n'était pas compétente sur le plan sanitaire et médical, et qu'il nous était difficile de nous prononcer. C'est d'ailleurs le collège de la CNIL qui prend des décisions sans pouvoir répondre sur un texte. Notre activité nous demande de concilier la protection de la vie privée avec d'autres impératifs importants, faisant souvent l'objet d'une protection constitutionnelle, tels que le droit à la santé ou la sécurité publique. Nous veillons à ce qu'il y ait des garanties pour les citoyens, que le droit à l'information soit respecté, que les traitements soient nécessaires et proportionnés, que l'on connecte le moins de données possible, et qu'elles soient conservées le moins longtemps possible. Nous vérifions la limitation du nombre d'accédants et le traçage de la donnée en cas de mésusage. Nous sommes capables de décliner les grands principes du droit de la protection des données.

Nous pensons que nous devons prendre en compte les spécificités de chaque crise et les critères spécifiques d'application des différents systèmes, mais aussi définir les termes. Quand allons-nous appliquer, s'ils sont nécessaires, des systèmes d'information dérogatoires au droit commun ? Qu'est-ce qu'une situation sanitaire exceptionnelle ou une crise ? Qui décide de cette activation : le législateur, le gouvernement, une agence, une autorité ? Nous devons définir les organismes concernés par ces dispositifs et la date de péremption des

systèmes d'information qui seraient mis en œuvre. Seule la loi permet de déroger au secret médical, bien que les conditions de celui-ci puissent être décidées en Conseil d'État après avis de la CNIL. J'imagine que le législateur a pour rôle de prévoir un cadre global et de déterminer les conditions de mise en œuvre qui doivent varier en fonction des caractéristiques de la crise, notamment.

Nous sommes assez sobres sur le plan budgétaire. Nous pourrions d'ailleurs investir davantage. Nous comptons une trentaine de contrôleurs répartis en binômes d'un juriste et un spécialiste des systèmes d'information ou informaticien pour contrôler toutes les entreprises et administrations de France. Nous réalisons des contrôles sur place, mais aussi en ligne. Lors d'un contrôle dans un domaine déterminé, nous pouvons espérer que les résultats, souvent rendus publics, impactent l'ensemble du secteur. Nous travaillons avec les têtes de réseaux pour qu'elles diffusent elles-mêmes les bonnes pratiques auprès de leurs administrés. La CNIL n'est pas qu'un gendarme de la protection des données, elle fait aussi de l'accompagnement. Nous recevons 14 000 plaintes clients, près du double de ce que nous recevions avant la mise en œuvre du RGPD. La prise de conscience de nos concitoyens n'a pas faibli en la matière.

L'année dernière, nous avons compté 135 mises en demeure. La formation restreinte de la CNIL a prononcé 18 sanctions, notamment prononcées à l'égard des GAFAM sur le sujet des cookies. C'est 3 fois plus qu'avant le RGPD, et les montants sont bien plus importants.

Le différentiel entre le nombre de plaintes et celui des sanctions illustre notre accompagnement envers les organismes ayant fait l'objet de ces plaintes. Nous aurions évidemment besoin de plus de contrôleurs.

Il nous arrive de nous autosaisir sur des contrôles. Rien ne nous empêche de prendre des positions publiques sur tel ou tel point. Vous nous y aidez en nous invitant dans ces commissions. Nous ne nous sentons pas limités de ce point de vue.

Tous les systèmes d'information sauf celui sur les vaccins ont une date d'extinction prévue entre le 31 janvier et le 30 juin 2023. Le passe sanitaire est déjà éteint. Il sera du rôle de la CNIL et de son service des contrôles de s'assurer qu'ils ne sont plus alimentés par des données, et qu'aucune d'entre elle n'a été conservée hors finalités de recherche, si cela était prévu et de façon pseudonymisée.

Vous posiez la question légitime de la sécurité. La CNIL en est un acteur majeur. À ce stade, le RGPD est un allié de la cybersécurité. C'est le seul texte imposant des obligations de moyens. Tous les responsables de traitement en France doivent embarquer un certain nombre de mesures. En 2021, au cœur de la crise, nous avons observé un pic de notifications des violations de données. 18 % d'entre elles concernaient la santé, contre 8 % l'année précédente. Parmi celles-ci, 66 % correspondaient à du piratage (rançongiciels et hameçonnage). Nous en comptions 40 points de moins en 2019. Ainsi, le secteur de la santé est particulièrement ciblé. L'attaque du CHU de Bordeaux ou les données compromises et envoyées dans la nature pour le non-paiement de la rançon de l'hôpital de Corbeil-Essonnes ne sont que les faces émergées de l'iceberg. En 2021, la hausse des cyberattaques, la fatigue des personnels et les nouveaux process mis en œuvre dans l'urgence ont pu contribuer à cette surchauffe en matière de risques de sécurité. Ceux-ci sont un peu retombés.

D'ailleurs, l'agence nationale de la sécurité des systèmes d'information (ANSSI) a fait des rançongiciels et du hameçonnage le thème annuel du *cyber-mois*. La CNIL, en parallèle des actions pédagogiques qu'elle mène sur la cybersécurité, accompagne le ministère de la santé sur les thèmes cyber. Ce sujet nous préoccupe, parce que nous devons faire progresser le niveau de sécurité de l'écosystème. Nous espérons y contribuer par nos actions d'accompagnement et de contrôle.

Enfin, concernant l'effet cliquet, l'accoutumance et le solutionnisme technologique, il ne faudrait pas que les systèmes dérogatoires mis en œuvre pendant la crise sanitaire soient banalisés.

M. Gilles Le Gendre (RE). Vous avez souligné le fait que les moyens avaient sensiblement augmenté à l'occasion des textes sur le RGPD. J'ai cru comprendre que vous aviez notamment amélioré et renforcé les capacités de la CNIL en matière de conformité, pour mieux aider les professionnels de toute nature à s'adapter à ces nouvelles règles complexes. En quoi ces démarches consistent-elles plus précisément ?

Vous avez également fait allusion au fait que les contrôles, voire les erreurs, vous donnaient l'occasion d'accompagner les différents acteurs. Un investissement est-il également réalisé en amont, accompagné d'un travail pédagogique, notamment à l'égard des petites ou moyennes entreprises ? La règle est souvent un casse-tête pour celles qui ne disposent pas des moyens humains et économiques nécessaires.

Enfin, nous évoluons dans un contexte d'explosion des normes et des règles. Que pouvons-nous tirer, à ce stade, de votre expérience dans le domaine, qui pourrait être mutualisée ?

Mme Julie Lechanteux (RN). Un récent décret a permis la prolongation de l'application TousAntiCovid jusqu'au 31 janvier 2023. La CNIL avait demandé la publication d'un rapport sur son fonctionnement pour janvier 2021. Il n'a été publié qu'un an plus tard, et n'a fait l'objet d'aucune information publique. On y lit que l'efficacité technique du dispositif a été sous-optimale dans le nombre de personnes testées positives à la covid-19 qui ne se sont pas déclarées à l'application. De plus, la fonction de suivi des utilisateurs, censée pouvoir retracer des chaînes de contamination pour stopper la propagation du virus, a été sous-utilisée, amenant l'application à n'être utile que pour stocker le passe sanitaire.

Par ailleurs, l'application a montré ses faiblesses à plusieurs reprises, notamment concernant la protection des données personnelles, puisque l'anonymat des utilisateurs n'était en aucun cas assuré.

Pour rappel, la création de ce dispositif usant des données personnelles de millions d'utilisateurs était conditionnée à la publication du rapport d'impact – cela n'a pas été le cas – et au fait qu'il démontre une réelle utilité. Il n'a manifestement pas fonctionné. Il a par ailleurs coûté 7 millions d'euros à nos concitoyens.

Qu'attendez-vous pour vous prononcer en faveur de l'arrêt de cette application ? Qu'adviendra-t-il des données personnelles de ces millions de français, et notamment de leur traçage collecté depuis le début de la pandémie ?

Mme Raquel Garrido (LFI-NUPES). Cet exposé très clair aurait été très utile avant nos travaux sur la loi de prolongation des systèmes d'information SI-DEP et Contact Covid.

Ce n'est pas de votre faute si vous n'avez pu être entendue plus tôt, le gouvernement ayant décidé en urgence de nous faire prolonger ces systèmes. À l'époque, la pression était très forte sur les responsables politiques que nous sommes, le gouvernement nous ayant transmis une sorte d'angoisse de l'écrasement de ces fichiers dans la maîtrise éventuelle d'une pandémie et de nouveaux variants.

Aujourd'hui, j'observe une tension très claire entre le concept de pérennisation et celui de limitation dans le temps. Ils entrent en contradiction. Certains collègues pensent que compte tenu de l'évolution climatique ou des zoonoses et risques de pandémies réels, nous ne pouvons nous passer de ces dispositifs, qui doivent être pérennisés. À l'inverse, vous dites que nous devons assumer la péremption des fichiers, quitte, le cas échéant, à en rouvrir un si besoin.

Dans le cas de SI-DEP et Contact Covid, nous devons reconnaître que les gens se sont eux-mêmes sortis du système en ne se faisant pas dépister et en ne communiquant pas le nom de leurs contacts. Ainsi, l'efficacité du dispositif était erronée.

Enfin, j'aimerais que vous rappeliez à nos collègues que le fichier le mieux protégé est celui qui n'existe pas.

Mme Cecile Untermaier (SOC). La clarté et l'éclairage que vous nous donnez après cette période extrêmement compliquée sont très utiles. Les propos ont évolué. Les orientations sont plus assurées et affirmées, c'est normal.

Le travail colossal réalisé au gouvernement avec la CNIL a démontré que notre organisation était capable de porter le sujet de la protection de la vie privée devant une crise sanitaire majeure à laquelle il fallait répondre. Pouvez-vous nous confirmer que la relation avec le gouvernement s'était relativement bien passée, et que vous n'avez pas rencontré d'obstacles?

Vous dites que cette page doit être tournée pour que nous en ouvrions une autre, si besoin. Sur ce point, nous sommes d'accord. Nous serons vigilants à la bonne fermeture de cette page, pour que les données soient protégées.

Comment réalisez-vous les contrôles ? J'imagine que vous n'avez pas recours à un cabinet de conseil.

Ensuite, la période de dix ans me paraît très longue. Avez-vous désormais une philosophie sur la question de la conservation des données sur cette période ?

Enfin, cette crise vous a-t-elle fait évoluer personnellement sur la question du secret médical ?

Mme Clara Chassaniol, Renaissance (RE). J'ai récemment été alertée en circonscription sur l'opportunité d'améliorer le traitement des données de personnes interpellées par la police afin de faciliter leur identification. Aujourd'hui, une personne placée en garde à vue peut avoir été enregistrée plusieurs fois dans le fichier de traitement des antécédents judiciaires sous une fausse identité. Les policiers sont donc incapables de connaître ses antécédents, puisqu'ils ne sont pas interconnectés avec les fichiers d'empreintes digitales et génétiques. En 2016, un rapport de la cour de comptes proposait de connecter ces deux fichiers avec une base commune pour améliorer la fiabilité des identités et repérer plus systématiquement les individus y étant signalisés.

Dans le même esprit, nos collègues Didier Paris et Pierre Morel-A-L'Huissier ont proposé dans un rapport publié en 2018 la mise en relation des trois fichiers sous la forme d'une base pivot. Même s'il existe aujourd'hui des freins juridiques, malgré les réticences politiques généralement invoquées, certains croisements sont déjà opérés dans le système d'information Schengen, par exemple.

Ainsi, sans remettre en cause la question des données personnelles et au regard de l'utilité que représenterait une meilleure identification des personnes mises en cause, vous paraîtrait-il envisageable que nous puissions avancer sur ces sujets et créer cette base pivot ? Dans le cas contraire, qu'est-ce qui s'y opposerait ?

Mme Élisa Martin (LFI–NUPES). Un certain nombre de nouvelles technologies et de nouveaux outils se développent. Leur recours paraît d'ailleurs occuper une place très importante dans le projet de loi d'orientation et de programmation du ministère de l'intérieur (LOPMI). Peu importe.

À la CNIL, disposez-vous des moyens techniques nécessaires pour évaluer les capacités de ces nouveaux outils à être faiblement protégés, utilisés dans d'autres contextes et pour d'autres utilisations ? S'ils n'existent pas au sein de votre commission, pouvez-vous les solliciter ailleurs ?

M. Jean Terlier (RE). La représentation nationale vous remercie du retour de la CNIL sur l'efficacité et la pertinence des systèmes d'information et de traitement de données mis en place pendant la crise sanitaire. Nous étions nombreux, lors des différentes auditions menées, à exprimer quelques doutes quant à la pertinence de leur mise en place. En effet, leur efficacité n'était pas avérée pour lutter contre la crise sanitaire, et des problématiques pouvaient se poser en termes de libertés publiques. Les avis de la CNIL ont orienté le choix du législateur sur la mise en place de ce type de dispositif, notamment dans les conditions d'urgence que nous avons connues.

Contrairement aux propos du Rassemblement National, vous avez clairement indiqué que l'application TousAntiCovid était respectueuse de la vie privée, nonobstant le traçage mis en place. Vous avez dit qu'il n'existait pas de risque majeur pour les libertés publiques, et qu'elle était conforme au RGPD. En revanche, vous avez évoqué les difficultés d'appréciation de son utilité selon le moment, avant l'existence d'une crise sanitaire, ou pendant celle-ci. Pourrais-je avoir plus de précisions à ce sujet ?

Mme Marie-Laure Denis, présidente de la CNIL. Nous avons rendu 31 avis dans le cadre de la crise sanitaire, et avons pris part à 13 auditions parlementaires, dont celle-ci. D'une façon plus générale, nous réalisons autant d'accompagnement que d'actions répressives, de traitement de plaintes ou de contrôle. Nous sommes convaincus du caractère indispensable de la pédagogie sur ces sujets, y compris auprès des plus jeunes. D'ailleurs, nous faisons beaucoup d'éducation au numérique sous le prisme de la protection des données. Nous animons le dispositif EDUCNUM et publierons prochainement des ressources pour les 8-10 ans en partenariat avec l'éducation nationale. Nous sommes, je crois, l'une des rares autorités administratives indépendantes (AAI) à répondre au téléphone. Certains députés ont d'ailleurs pu découvrir nos permanences téléphoniques, très instructives. Le dispositif *Besoin d'aide* permet également de poser des questions par email. Un service d'une dizaine de personnes est par ailleurs spécialisé dans l'accompagnement des délégués à la protection des données, aujourd'hui au nombre de 30 000 en France. Nous mettons aussi des outils à disposition, dont un *mooc* s'enrichissant depuis trois ans de divers modules, ayant fait l'objet

de 140 000 créations de comptes. Nous observons ainsi un réel besoin de pédagogie. J'espère surtout que nos concitoyens et le milieu entrepreneurial, qui a vu arriver le RGPD avec une certaine réticence, en voient l'intérêt. Aucun développement durable et serein de l'économie numérique ne sera possible sans cette confiance. J'identifie un risque de réputation, mais également un avantage concurrentiel distinctif pour certaines entreprises dans le fait de protéger les données de leurs concitoyens.

Nos 290 agents ne nous permettent pas de mener un accompagnement très individualisé. Nous le faisons donc à travers les têtes de réseaux, sauf pour les très gros acteurs ou certaines technologies pouvant occasionner des effets importants.

Nous faisons beaucoup de droit souple et de référentiels à destination des cabinets médicaux et paramédicaux ou des pharmacies, par exemple. Notre site a enregistré 11 millions de connexions l'année dernière. C'est autant que le ministère de la justice, ce qui illustre bien un besoin de contenu auquel nous essayons de répondre. Nous avons également publié un guide en lien avec BPIFrance concernant les exigences différant entre les très petites entreprises et les grands groupes. Nous nous rendons notamment à Station F pour « évangéliser » les start-ups à la protection des données.

J'ai essayé d'adopter des orientations projetables à l'extérieur de Paris. Nous allons faire le tour des régions. Nous nous sommes déjà rendus à Lyon, où nous étions réunis avec la plus grande association de délégués à la protection des données. Nous étions 300, pour 500 demandes, et avons évoqué le principe du RGPD.

L'année dernière, j'ai lancé le *Bac à sable* par lequel nous accompagnons chaque année, par le biais d'un appel à projets, une dizaine d'acteurs sur une thématique particulière : santé numérique, numérique dans l'éducation…. Nous tiendrons un colloque sur ce dernier sujet début novembre.

Nous n'avons pas la prétention de servir de modèle à qui que ce soit, mais l'accompagnement constitue l'un des fondamentaux de notre ADN. Nous essayons en permanence de nous adapter et de répondre aux préoccupations posées au plus près du terrain.

Les données de l'historique de proximité de TousAntiCovid sont conservées et tracées pendant quinze jours à compter de leur enregistrement par l'application. L'application sera en outre désactivée le 31 janvier prochain. Par ailleurs, la CNIL a obtenu des garanties en matière de vie privée sur ce dispositif dès le début de sa mise en œuvre.

Concernant l'angoisse possible vis-à-vis de l'écrasement des fichiers, je crois, comme le collège de la CNIL, que la plupart des dispositifs doivent avoir une date de péremption et être désactivés, sauf dans deux cas. Je pense à des raisons de pharmacovigilance, notamment concernant les vaccins, et aux besoins de recherche, dans des conditions assurant la protection de la vie privée des personnes dont les données sont utilisées, calibrées par nous-mêmes.

Ce sujet pose plus globalement la question de l'évaluation de ces dispositifs. Nous la réalisons en silo, système d'information par système d'information. Il nous paraît important de réaliser une évaluation plus globale de leurs interactions.

Effectivement, il pourrait être utile d'évaluer TousAntiCovid au regard de l'évaluation du système d'information Contact Covid. Quelles sont les interactions entre l'un

et l'autre ? Sont-ils utiles en même temps ? À quel moment de la propagation du virus ? L'utilité de TousAntiCOvid porte peut-être davantage sur l'identification de pics de contamination au tout début, en plus d'une complémentarité avec les actions d'enquêtes manuelles lorsque le virus circule davantage.

S'agissant de données de santé particulièrement sensibles, nous avons été accompagnés par un médecin. Nous avons également adopté des méthodes de contrôle qui n'empêchaient pas les équipes des organismes concernés de travailler, notamment au plus fort de la crise. Nous avons réalisé ces contrôles en temps réel, et avons obtenu des modifications très rapides sur un certain nombre de sujets, par un dialogue continu avec les responsables de traitement.

À ma connaissance, nous ne faisons pas appel à des cabinets de conseil. Je crois que nous n'en aurions pas les moyens.

Le secret médical est une notion fondamentale dans le cadre de la mise en œuvre de systèmes d'information tels que ceux-ci, raison pour laquelle le législateur doit en délimiter les contours et les éventuelles exceptions.

Madame Chassaniol, nous reviendrons vers vous concernant votre question, dont le lien avec l'objet de cette audition est ténu. La CNIL est très attentive aux modalités de mise en œuvre des fichiers régaliens d'une façon générale. Nous contrôlons régulièrement les fichiers des ministères de l'intérieur ou de la défense. Par exemple, le fichier des empreintes génétiques a fait l'objet d'une sanction de la CNIL et d'un rappel à l'ordre public il y a un an, ainsi que d'une injonction de mise en conformité, notamment sur les durées de conservation.

La CNIL est la seule autorité de protection des données de l'Union européenne à disposer d'un laboratoire d'innovation numérique, le LINC, adoptant une approche multidisciplinaire d'ingénieurs, de chercheurs, de sociologues. Ils travaillent entre autres sur les enjeux de régulation économique de la donnée, de nouveaux textes européens étant attendus sur le partage et l'ouverture des données ou l'intelligence artificielle. Nous disposons de nos propres ressources, bien qu'elles ne soient pas suffisantes.

Nous produisons des livres blancs, sur les assistants vocaux ou les données de paiement, par exemple.

Vous parliez de solliciter d'autres expertises. Le gouvernement a mis en place au ministère de l'économie le PEReN, service permettant de réaliser des études numériques. Un certain nombre d'AAI peuvent avoir accès ou définir en commun des études. Nous le faisons également.

*

* *

La séance est levée à 12 heures 40.

Membres présents ou excusés

Présents. – Mme Caroline Abadie, M. Jean-Félix Acquaviva, Mme Sabrina Agresti-Roubache, M. Pieyre-Alexandre Anglade, M. Erwan Balanant, M. Romain Baubry, Mme Pascale Bordes, M. Ian Boucard, M. Florent Boudié, M. Xavier Breton, Mme Blandine Brocard, Mme Émilie Chandler, Mme Clara Chassaniol, M. Jean-François Coulomme, Mme Mathilde Desjonquères, Mme Edwige Diaz, M. Philippe Dunoyer, Mme Elsa Faucillon, Mme Raquel Garrido, M. Yoann Gillet, M. Guillaume Gouffier-Cha, M. Sacha Houlié, M. Timothée Houssin, M. Jérémie Iordanoff, Mme Emeline K/Bidi, M. Gilles Le Gendre, Mme Julie Lechanteux, M. Didier Lemaire, Mme Marie-France Lorho, M. Benjamin Lucas, M. Emmanuel Mandon, Mme Élisa Martin, M. Didier Paris, M. Éric Pauget, M. Jean-Pierre Pont, M. Éric Poulliat, Mme Marie-Agnès Poussier-Winsback, M. Philippe Pradal, M. Rémy Rebeyrotte, Mme Béatrice Roullaud, M. Thomas Rudigoz, M. Hervé Saulignac, M. Raphaël Schellenberger, Mme Sarah Tanzilli, M. Jean Terlier, Mme Cécile Untermaier

Excusés. - M. Éric Ciotti, M. Philippe Gosselin, Mme Marie Guévenoux, M. Jordan Guitton, Mme Élodie Jacquier-Laforge, M. Mansour Kamardine, M. Ludovic Mendes, Mme Naïma Moutchou, Mme Danièle Obono, M. Stéphane Rambaud, M. Davy Rimane, M. Thomas Ménagé, M. Roger Vicot