CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

AUDITION DE LA PRESIDENTE DE LA CNIL SUR LES TRAITEMENTS DE DONNEES DANS LE CADRE DE LA LUTTE CONTRE LA PROPAGATION DE L'EPIDEMIE DE COVID-19

Le 9 mars 2021

> Lien vers l'audition

Marie-Laure DENIS, présidente de la Commission nationale de l'informatique et des libertés (CNIL), était auditionnée, le 9 mars 2021, par la commission des Affaires sociales de l'Assemblée nationale **sur les traitements de données dans le cadre de la lutte contre la propagation de l'épidémie de covid-19**.

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. Ces systèmes d'information regroupent des données de santé sur les personnes atteintes de la covid-19 et les personnes ayant été en contact avec elles, recueillies sans leur consentement.

La mise en place de ces systèmes d'information par le Gouvernement a été encadrée de **plusieurs garanties afin de protéger les libertés publiques** :

- la mise en place d'un comité de contrôle et de liaison covid-19 ;
- l'information régulière du Parlement sur les mesures prises par le Gouvernement.

Dans le cadre de ses missions, **la CNIL a analysé plusieurs traitements d'information** :

- SI-DEP ;
- Contact Covid ;
- Vaccin Covid ;
- Tous Anti Covid.

Cette audition fait suite à la **publication du deuxième avis trimestriel, le 21 janvier 2021**, sur le fondement de l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire, à la suite du premier avis en date du 10 septembre 2020.

CE QUE L'ON RETIENT DE L'AUDITION

La présidente a rappelé que **la CNIL rend un avis tous les 3 mois** à compter de la promulgation de la loi prorogeant l'état d'urgence sanitaire, **jusqu'à la disparition des systèmes d'information** et la suppression des données qu'ils contiennent.

❖ L'encadrement des systèmes d'information créés dans le cadre de la lutte contre la Covid-19

La CNIL a agi :

- **en amont** : avant la mise en œuvre des traitements,
  - 13 avis relatifs à la gestion de la crise sanitaire ont été rendus depuis mars 2020, principalement au Gouvernement ;
  - un avis sur le traitement de l'information relatif aux vaccins ;
- **en aval** : pour contrôler leur mise en œuvre par les organismes en charge, par le biais de contrôles sur place, sur pièce ou en ligne.

La présidente considère que la CNIL peut *« être exigeante, comme sur l'anonymisation des données ou de la sécurité informatique »* mais que ces exigences sont *« nécessaires et attendues »* par les citoyens.

Elle a fait un **bilan des contrôles effectués sur les différents systèmes d'information** mis en place :

- **Contact Covid**

Il est mis en œuvre par la Caisse nationale d'assurance maladie (CNAM). Il recueille des informations sur les personnes identifiées comme contact à risque de contamination, cas contact des personnes exposées, et les chaines de contamination.

11 contrôles ont été réalisés en 1 an auprès de la CNAM ou des agences régionales de santé (ARS).

La CNIL a constaté une **amélioration des modalités de mise en œuvre du traitement**, et la correction des mauvaises pratiques relevées lors du premier avis de septembre.

Certaines **mauvaises pratiques résiduelles relatives aux conditions d'authentification, à la traçabilité, à la transmission des données à un tiers non habilité à héberger des données de santé ont été identifiées.** La présidente de la CNIL a envoyé un courrier pour rappeler la CNAM à ses obligations, et les mesures à mettre en place pour y remédier.

De **nombreuses disparités ont été observées dans les pratiques de suivi de contacts par les ARS**. La présidente de la CNIL a donc :

- envoyé une mise en demeure à une ARS ;
- écrit à l'ensemble des ARS pour les informer de pratiques contraires au RGPD relevées lors des contrôles ;
- écrit au ministère des Solidarités et de la Santé afin de le tenir informé.

La CNIL a été **saisie début janvier 2021, sur un projet de décret** visant à :

- renforcer le dispositif de traçage des chaines de transmission du virus en **élargissant le champ d'action du fichier Contact Covid aux personnes co-exposées**, se retrouvant dans *« un même lieu où les gestes barrières n'ont pas été pleinement respectés les 14 derniers jours »* afin de faciliter la réalisation des enquêtes sanitaires ;
- **collecter de nouvelles catégories de données comme la participation à des activités ou des rassemblements de plus de 6 personnes**, et des **données relatives au retour d'un voyage à l'étranger ou en outre-mer**.

L'avis a été publié le 19 janvier dernier.

- **SI-DEP**

Il est mis en œuvre par le ministère des Solidarités et de la Santé. Il permet de centraliser les résultats des tests.

7 contrôles ont été réalisés auprès du ministère des Solidarités et de la Santé, de l'Assistance publique-hôpitaux de Paris (APHP), dans deux laboratoires d'analyse médicale réalisant des tests PCR. Les remarques faites à l'issue du premier avis ont bien été prises en compte et la CNIL a ***constaté « un niveau de conformité satisfaisant »*** **s'agissant de la durée de conservation des données**.

- **Tous Anti Covid**

C'est l'application de suivi de contacts basée sur le volontariat et utilisant la technologie du bluetooth et non la géolocalisation.

Elle permet d'alerter les utilisateurs d'un risque de contamination lorsqu'ils ont été à proximité d'un autre utilisateur ayant été diagnostiqué positif. Il devrait également permettre, au moment venu, l'**enregistrement des visites dans des lieux recevant du public grâce au scan de QR codes**, facilitant ainsi l'alerte des personnes ayant fréquenté ces lieux sur une plage horaire similaire d'une personne diagnostiquée positive.

7 contrôles ont été réalisés, à la suite de ceux déjà faits en juin 2020. Une mise en demeure a été émise, et rendue publique, à l'encontre du ministère des Solidarités et de la Santé. Le ministère s'est mis en conformité dans les délais. **Dès la mise à jour du nouveau système de QR codes mis en place, de nouveaux contrôles seront faits**. La présidente de la CNIL considère néanmoins que l'**alternative des cahiers de rappel doit être subsister**, et le ministère des Solidarités et de la santé a confirmé le recours aux deux possibilités : numérique et non numérique.

La CNIL a recommandé que l'**obligation d'enregistrement des visites dans les lieux recevant du public soit limitée à ceux qui présentent un risque élevé, ou ceux où il n'est pas possible de porter de masques**. Elle a également **alerté sur l'enregistrement de visites dans certains lieux pouvant porter atteinte aux libertés fondamentales** (ex : lieux de culte, réunions syndicales…).

La présidente a souligné la volonté de la CNIL de **préciser dans le décret qu'un utilisateur peut supprimer son historique des lieux visités**. Elle appelle également à l'élaboration et au suivi des critères d'évaluation.

- **Vaccin Covid**

Il est mis en œuvre sous la direction conjointe de la Direction générale de la santé et de la CNAM. Il permet la mise en œuvre, le suivi, et le pilotage de la campagne vaccinale.

Des contrôles sont prévus.

La CNIL procède également à des vérifications *« sur des fichiers du quotidien liés au suivi de la pandémie »*, comme les cahiers de rappel, mis en place dans les lieux recevant du public, en octobre 2020. Deux rappels à l'ordre ont été émis à ce titre.

La présidente de la CNIL a souligné **leur vigilance sur *« l'information des personnes et l'exercice de leurs droits, sur le respect du principe de minimisation des données, à l'encadrement de la dérogation au principe de 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 ».*

Dans ses avis trimestriels, le collège de la CNIL a rappelé que :

- l'**atteinte portée à la vie privée** n'est admissible que *« **si cette politique constitue une réponse nécessaire et appropriée pour ralentir la propagation de l'épidémie**, impliquant que la nécessité de ces systèmes d'information soit **périodiquement réévaluée** au vu de l'évolution de l'épidémie »* ;
- des **garanties doivent être apportées** en matière de respect des *« principes fondamentaux ».*

Le prochain avis de la CNIL portera sur l'état des lieux des contrôles, et en particulier ceux réalisés sur le système d'information Vaccin Covid.

Concernant la **pérennisation de ces systèmes d'information**, la présidente de la CNIL a indiqué que des échanges ont eu lieu avec le Parlement sur la question de l'instauration d'un potentiel régime pérenne de gestion des urgences sanitaires.

Le 17 décembre dernier, le collège de la CNIL a rendu un avis en urgence sur un PJL qui instituait un régime pérenne de gestion des urgences sanitaires, qui autorisait notamment le Gouvernement à créer par décret des systèmes d'information à des fins de gestion et de suivi des situations sanitaires exceptionnelles en dehors de l'état d'urgence sanitaire. Le PJL a été abandonné.

La présidente de la CNIL considère que :

- la **notion de *« situation sanitaire exceptionnelle »* doit être précisément définie** afin de s'assurer que l'atteinte portée à la vie privée **ne revêt pas un caractère systématique** ;
- **seuls des faits *« d'une particulière ampleur ou gravité »*** doivent pouvoir justifier la mise en œuvre immédiate de ces traitements.

De manière générale, la présidente de la CNIL estime qu'***« il faut veiller à ne pas banaliser le recours à ces techniques, à ces systèmes d'information, qui restent très intrusifs et consommateurs de données personnelles »***.

❖ L'hébergement et la protection des données de santé par des entreprises

o Le Health Data Hub

La présidente de la CNIL a rappelé le choix de Microsoft Azur pour l'hébergement des données de santé.

Elle estime que ce hub est *« une bonne idée pour la recherche médicale »*, mais il faut tout de même être vigilant *« sur l'accès direct des données par les autorités des pays tiers éventuels »*. Pour cette raison, **la CNIL a fait part de son souhait que l'hébergement des données de santé et les services liés à sa gestion soient réservés exclusivement à des juridictions de l'Union européenne**.

Elle souligne qu'un arrêt de la Cour de justice de l'Union européenne, datant de juillet 2020, a invalidé l'accord Privacy Shield de transfert de données notamment vers les Etats-Unis, et que le Conseil d'Etat a reconnu, en octobre 2020, dans une ordonnance, l'existence d'un risque de transfert de données issues de cette plateforme vers les Etats-Unis. En cause : la soumission de Microsoft au droit américain. **La CNIL a donc demandé que des garanties supplémentaires soient prises, et obtenu du ministère**

« un engagement de changer la solution technique permettant de supprimer ce risque dans un délai de 12 à 18 mois et ne devant pas dépasser 2 ans ».

La présidente a annoncé que la CNIL sera auditionnée par la CNAM sur l'avis rendu sur le décret *« système national des données de santé »* (SNDS) et le recours à Microsoft pour l'hébergement des données de cette plateforme. Le **conseil d'administration de la CNAM s'est opposé, en février dernier, au transfert de copies du système national des données de santé sur la solution Microsoft Azur**.

- **Le développement des pratiques numériques en santé**

La présidente de la CNIL constate *« un essor spectaculaire »* de la télémédecine ces derniers mois.

Ce **développement soulève plusieurs problématiques** selon la présidente de la CNIL :

- des **enjeux en matière de centralisation des données de santé** par des acteurs privés et des **risques de sécurité** ;
- un **enjeu d'inclusion numérique** : cela révèle des inégalités sociales, 12% des français ne disposant pas de connexion internet (selon l'INSEE).

La CNIL a publié un **référentiel relatif au traitement de données à destination des personnels médicaux et paramédicaux** et a **émis des recommandations à destination des prestataires de services** chargés de développer, assurer la maintenance de l'outil, du logiciel ou des postes de travail.

- **Le partenariat entre le Gouvernement et Doctolib**

L'utilisation de la plateforme Doctolib pour la prise de rendez-vous dans le cadre de la vaccination pose notamment un **problème en matière de protection des données**. En effet, il est reproché à Doctolib de **mettre en danger les données des patients en confiant l'hébergement à Amazon Web Services**, soumis au droit américain et son programme de surveillance.

La présidente de la CNIL a néanmoins indiqué ne pas avoir été saisie par le Conseil d'Etat sur la requête visant à interdire la prise de rendez-vous par Doctolib dans le cadre de la politique vaccinale, et a précisé qu'un collectif a déposé un référé liberté devant le Conseil d'Etat visant à obtenir l'annulation du partenariat entre le Gouvernement et Doctolib.

❖ Le partage des données médicales

La présidente de la CNIL estime nécessaire de *« concilier l'ouverture des données et la protection des données ».*

La CNIL a par ailleurs publié un **référentiel permettant l'accès aux données de l'échantillon généralisé des bénéficiaires** pour certains traitements qui ne nécessitent pas d'autorisation de la CNIL.

La présidente de la CNIL a précisé que l'**interopérabilité des systèmes d'information n'est pas prévue** par le décret sur lequel un avis a été rendu par la CNIL, et qu'elle n'est pas non plus prévue entre SI-DEP et Contact Covid. Elle estime qu'il **faut *« respecter un principe de finalité précis inscrit dans le RGPD et plutôt inscrit dans une logique de silo »***, en séparant les systèmes d'information en fonction de leur objectif.

La CNIL n'est **pas opposée au principe d'interopérabilité** *« tant qu'elle est encadrée mais dans le* ***respect de la minimisation des données et de la sécurité****, et non pas dans une logique d'interconnexion généralisée des systèmes d'information ».*

❖ L'utilisation des données pour la recherche en santé

La présidente de la CNIL souligne le **caractère « capital » de la recherche en santé**, et assure plus particulièrement que la CNIL a priorisé l'accompagnement des recherches sur la covid-19.

La CNIL s'appuie sur un **régime d'autorisation pour le traitement des données de santé**. Ce régime résulte d'un *« choix fort du législateur français »* en 2018 de maintenir des autorisations sur la recherche en santé, conscient des enjeux en matière de protection des données :

- une majorité des projets peuvent être mis en œuvre sans autorisation lorsqu'ils sont conformes à *« une* ***méthodologie de référence*** *»*, et nécessitent une simple déclaration à la CNIL ;
- pour les projets nécessitant une autorisation, une **procédure accélérée d'instruction** a été mise en place pour les projets nécessitant une autorisation :
  - 101 autorisations ont été délivrées spécifiquement sur la recherche sur la Covid depuis 1 an ;
  - 91 autorisations délivrées en 2020 ;
  - 10 depuis le début de l'année 2021 ;
  - ¼ des décision d'autorisation de recherche médicale prononcée en 2020.

Quelques chiffres sur les **délais d'autorisation de recherche médicale** :

- 45% des autorisations sont délivrées en moins de 2 jours en matière de recherche sur la Covid ;
- 2/3 des autorisations en matière de Covid sont délivrées en moins d'une semaine.

❖ La mise en place d'un passeport vaccinal

La présidente de la CNIL affirme qu'ils n'ont pas été saisis sur le sujet. Néanmoins, **le cas échéant, la CNIL sera amenée à se prononcer sur sa mise en œuvre**.

A ce sujet, la CNIL sera attentive :

- à la **sécurité des données de santé et sensibles** ;
- au **caractère volontaire** de l'utilisation d'un dispositif numérique et au fait de ne pas conditionner l'accès à des services à l'usage de ce dispositif numérique ;
- à l'**articulation avec d'autres dispositifs** mis en place en vue de la réouverture des lieux recevant du public pour *« éviter les risques de multiplication et de superposition de ces dispositifs »*.

La présidente de la CNIL a précisé que des **discussions sont en cours au niveau européen**. Elle a d'ailleurs participé à une réunion du comité européen de la protection des données, qui réunit les CNIL européennes, le 9 mars 2021. **La présidente de la Commission européenne a annoncé qu'une proposition législative serait présentée ce mois-ci sur un *« digital green pass »*** dont le but est de

prouver la vaccination et les tests PCR négatifs ou la présence d'anticorps. Le comité, ainsi que l'EDPS (la CNIL des institutions européennes), devraient être saisis pour avis *« dans des délais très courts ».*

La CNIL n'a pas été saisie concernant les compagnies aériennes qui testent des certificats sanitaires, ces projets ne nécessitant pas d'autorisation. Elle est néanmoins vigilante sur :

- la **collecte uniquement des données nécessaires** ;
- l'**information des personnes** et le **recueil de leur consentement** ;
- la **sécurité des données** et leur **stockage local** à la main de l'utilisateur ;
- l'**accès à ces données en répartissant le rôle et les responsabilités** ;
- le **respect du caractère volontaire** et le fait de proposer des **alternatives**.

❖ Les cyberattaques contre des hôpitaux

Récemment, plusieurs attaques de rançongiciels, qui chiffrent les données et demandent une rançon pour pouvoir y accéder de nouveau, ont visé certains hôpitaux.

La présidente de la CNIL juge important de ***« conjuguer les actions des différents intervenants »***, car la sécurité des données concerne également le secrétaire d'Etat au numérique et la déléguée au numérique du ministère des Solidarités et de la Santé.

Elle estime que ces attaques **soulèvent les problématiques** du :

- **pourcentage du budget des hôpitaux consacré à la protection des données** : à ce jour estimé à 1,6%, et qui mériterait de passer à 3% pour des actions en profondeur ;
- **recrutement d'experts informatiques** : elle pense par ailleurs que France relance *« pourrait permettre d'orienter les choses vers la bonne direction ».*

Selon elle, la CNIL ne dispose pas des ressources nécessaires pour accompagner tous les hôpitaux.

La présidente de la CNIL a rappelé que les hôpitaux doivent notifier à la CNIL les violations des données constatées dans les 48h, et que **2 médecins ont été sanctionnés d'une amende** afin de rappeler que les données des patients ne doivent pas se trouver en accès libre sur internet.

Elle considère que le **RGPD** est le **seul texte qui comporte des obligations en matière de sécurité et de protection des données**, **et des obligations pouvant entrainer des sanctions** de la part de la CNIL.

La CNIL est particulièrement sensible à la sécurité des données de santé et est **très active** en :

- éditant des guides ;
- émettant des recommandations sur les mots de passe ;
- éditant une application qui permet de réaliser facilement des études d'impact des traitements sur la protection des données lors d'un risque élevé ;

En 2021, 2 des 3 thèmes prioritaires de la CNIL portent sur la cybersécurité et les données de santé.

Concernant les violations de données, la présidente de la CNIL observe :

- une **augmentation de 24% des notifications de violation de données en 2020** par rapport à 2019, avec un peu moins de 3 000 notifications de violations de données par an, chiffres que la présidente de la CNIL considère *« sous-estimés »* ;

- une *« **multiplication par 3 des violations liées à des attaques par cryptolocker sur des établissements de santé** entre 2019 et 2020, passant de 12 à 36 violations »* ;
- **2/3 des sanctions de la CNIL concernent des manquements à la sécurité des données**.

La présidente de la CNIL a souligné qu'ils ont essayé d'être le plus réactif possible sur la fuite des données qui a affecté près de 500 000 patients de 28 laboratoires :

- en diligentant des contrôles sur pièce et sur place ;
- en saisissant le tribunal judiciaire de Paris pour que le fournisseur d'accès internet bloque le site hors Union européenne qui rendait disponible les bases de données ;
- en s'assurant que les victimes soient informées ou vont l'être de façon à instruire les notifications de violations de données.

La **cybersécurité dans la santé est un *« gros sujet »*** pour la CNIL.