

Délibération n° 2020-087 du 10 septembre 2020 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 (mai à août 2020)

(demande d'avis n° 20014534)

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, notamment son article 11 ;

Vu la loi n° 2020-856 du 9 juillet 2020 organisant la sortie de l'état d'urgence sanitaire ;

Vu le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions ;

Vu le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé STOPCOVID ;

Vu le décret n° 2020-1018 du 7 août 2020 pris en application de l'article 3 de la loi n° 2020-856 du 9 juillet 2020 organisant la sortie de l'état d'urgence sanitaire et modifiant le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions ;

Vu l'arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de COVID-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé ;

Sur la proposition de Marie-Laure DENIS, présidente, et après avoir entendu les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

— RÉPUBLIQUE FRANÇAISE —

3 Place de Fontenoy, TSA 80715 – 75334 PARIS CEDEX 07 – 01 53 73 22 22 – www.cnil.fr

*Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif.
Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données (DPO)
de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.*

Émet l'avis suivant :

1. Dans le cadre de la stratégie de « déconfinement progressif », la loi du 11 mai 2020 de prorogation de l'état d'urgence sanitaire a autorisé la création temporaire de deux fichiers nationaux : SI-DEP et CONTACT COVID. Ces traitements de données à caractère personnel sont encadrés par un décret en Conseil d'État du 12 mai 2020 qui précise leurs modalités de création et de mise en œuvre.
2. Ces fichiers doivent permettre d'identifier les personnes infectées par la COVID-19, les personnes qu'elles sont susceptibles d'avoir contaminées et les chaînes de contamination. Ils visent à assurer la prise en charge sanitaire et l'accompagnement des personnes atteintes du virus ou susceptibles de l'être, ainsi que la surveillance épidémiologique.
3. Au côté de ces fichiers, s'ajoute le déploiement de l'application mobile STOPCOVID.
4. Ce traitement, encadré par le décret n° 2020-650 du 29 mai 2020 et mis en œuvre par le ministre chargé de la santé, vise à informer les personnes utilisatrices qu'elles ont été à proximité de personnes diagnostiquées positives à la COVID-19 disposant de la même application.
5. Les fichiers SI-DEP et CONTACT COVID comprenant des nombreuses données à caractère personnel, y compris des données de santé et pouvant être consultés par un grand nombre d'acteurs, notamment par les enquêteurs sanitaires au bénéfice desquels la loi a expressément autorisé la levée du secret médical, le législateur a souhaité encadrer leur mise en œuvre.
6. Il a ainsi, d'une part, instauré un Comité de contrôle et de liaison COVID-19 et, d'autre part, prévu que le Gouvernement adresse au Parlement un rapport détaillé de l'application de ces mesures tous les trois mois à compter de la promulgation de la loi du 11 mai 2020 et jusqu'à la disparition des systèmes d'information. Enfin, le législateur a souhaité compléter ces rapports par un avis public de la Commission nationale de l'informatique et des libertés, objet de la présente délibération.
7. Dans un contexte exceptionnel de crise sanitaire et d'urgence, la Commission a intensifié les relations qu'elle entretient de façon régulière avec le Parlement au titre de sa mission d'accompagnement des pouvoirs publics (avis sur les projets de textes ; auditions). La Commission a ainsi répondu aux nombreuses sollicitations de ce dernier (ANNEXE 1), dans des délais particulièrement courts, compte tenu du calendrier d'adoption des projets de loi. Elle a ainsi été auditionnée à cinq reprises aux mois d'avril et mai 2020. Par ailleurs, cinq avis rendus par la Commission dans ce contexte d'urgence sanitaire ont pu contribuer utilement aux débats parlementaires autour des enjeux fondamentaux liés au respect de la vie privée et des données personnelles.
8. Le présent avis de la Commission rendu sur le fondement de l'article 11 de la loi du 11 mai 2020 s'attachera, notamment au regard des préconisations qu'elle a émises dans ses avis, à rappeler le cadre normatif dans lequel s'inscrivent ces traitements, et, à évaluer pour la période de mai à août 2020 :

- l'intérêt de ces traitements au regard de la situation sanitaire telle que décrite par le Gouvernement ;
- les conditions opérationnelles de mise en œuvre de ces traitements au regard des constatations faites dans le cadre de ses pouvoirs de contrôle.

I – RAPPEL DU CADRE NORMATIF ET DES PRÉCONISATIONS DE LA COMMISSION

9. Conformément à la loi, l'avis de la Commission a été sollicité par le Gouvernement sur l'ensemble des textes encadrant la mise en œuvre des traitements liés à la crise sanitaire.

- **L'avis de la Commission sur les systèmes d'information SI-DEP et CONTACT COVID**

10. Dans **son premier avis sur le projet de décret portant création des traitements SI-DEP et CONTACT COVID en date du 8 mai 2020**, la Commission a estimé que le dispositif présenté était globalement conforme au règlement général sur la protection des données (RGPD), un certain nombre de garanties étant apportées (caractère temporaire de ce dispositif, limitation des données de santé traitées ou encore caractère volontaire de la participation aux enquêtes).

11. Cependant, elle avait considéré nécessaire que le projet de décret soit complété et appelait à ce que certaines garanties juridiques, techniques et organisationnelles soient renforcées.

12. Plus particulièrement ses remarques ont porté sur :

- la nécessité d'encadrer plus précisément **l'accès aux données**, en fonction des catégories d'utilisateurs, afin que celui-ci ne puisse s'effectuer que dans la stricte limite de leurs missions ;
- la suppression dans le projet de texte du recueil, sans autre précision, **d'informations sur les « liens » existants entre un « patient 0 »¹ et un « cas contact »**. Le décret a supprimé cette mention et prévoit uniquement la collecte d'informations précises et circonscrites sur ce point (le fait de se connaître ou non, l'existence d'une cohabitation, la date du dernier contact) ;
- la mise en place de formations adaptées à l'utilisation de ces outils pour les **enquêteurs** et les autres personnes concernées (personnels des laboratoires d'analyse, médecins et autres professionnels de santé, pharmaciens, chercheurs, etc.) ;
- la mise en place d'un **dispositif de traçabilité** des consultations de façon à repérer les abus et à pouvoir les sanctionner ;
- la nécessité de mener une réflexion plus fine sur **les durées de conservation des données**. Des garanties ont été apportées sur ce point dans la loi du 11 mai 2020 ;

¹ Désigne une personne testée comme positive ou confirmée positive par l'établissement de santé qui a posé le diagnostic, aussi appelée « cas index ».

- **le droit d'opposition**, qui était écarté dans le projet, sauf pour permettre au « patient 0 » **que son nom ne soit pas révélé** à ses « cas contacts » et pour certaines transmissions de ses données pour des finalités de recherche. La Commission a demandé que la restriction du droit d'opposition aux fichiers soit réduite au minimum. En ce sens, un droit d'opposition a été ouvert par le décret aux « cas contacts » pour le traitement de leurs données dans CONTACT COVID et le « patient 0 » doit avoir donné son consentement pour que son identité soit révélée aux « cas contacts ».
13. **Son second avis, rendu le 23 juillet 2020, portait sur un projet de décret portant à six mois après la fin de l'état d'urgence sanitaire la durée de conservation des données pseudonymisées collectées dans le cadre de ces systèmes d'information** à des fins de surveillance épidémiologique et de recherche sur le virus de la COVID-19, comme l'avait préalablement autorisé **la loi du 9 juillet 2020**. En effet, la loi du 11 mai 2020 avait apporté de fortes garanties sur les durées de conservation des données en limitant la conservation des données dans les systèmes d'information à trois mois à compter de leur collecte.
14. Les observations de la Commission ont été majoritairement suivies par le Gouvernement dans le décret n° 2020-1018 du 7 août 2020 notamment s'agissant :
- de l'amélioration des modalités d'information des personnes concernées ;
 - de l'accès par les agences régionales de santé (ARS) aux données de CONTACT COVID à des fins de surveillance épidémiologique et de recherche, qui n'était pas prévu par le décret du 12 mai ;
 - de la limitation de l'ajout d'autres numéros d'identification uniquement si le numéro d'inscription au répertoire d'identification des personnes physiques (NIR ou numéro de sécurité sociale) ne peut être collecté.
15. La proposition de la Commission de rédaction d'une liste limitative des données permettant la finalité de suivi épidémiologique et de recherche sur le virus n'a cependant pas été reprise.
- **L'avis de la Commission sur la centralisation de certaines données de santé au sein de la Plateforme des données de santé (PDS ou Health Data Hub) et à la Caisse nationale de l'assurance maladie (CNAM)**
16. Dès le mois d'avril, le Gouvernement, dans le contexte d'urgence lié à la gestion de la crise sanitaire, a souhaité, par arrêté, organiser le regroupement de certaines données à caractère personnel, comprenant des données de santé et des données issues du Système national des données de santé (SNDS), afin de permettre leur utilisation en vue de suivre et projeter les évolutions de l'épidémie, de prévenir, de diagnostiquer et de traiter au mieux la pathologie et d'organiser le système de santé pour combattre l'épidémie et en atténuer les impacts. Pour ce faire, il a souhaité modifier les circuits traditionnels de remontée d'information portant notamment sur l'activité médicale, et permettre la centralisation des données utiles au sein de la Plateforme des données de santé (PDS), puis ultérieurement en incluant certaines données issues des fichiers SI-DEP et CONTACT COVID (décret du 12 mai 2020).

17. La Commission, dans **son avis rendu en urgence le 20 avril 2020**, a attiré l'attention du Gouvernement notamment sur :
- les risques liés aux conditions de démarrage anticipé de la solution technique de la PDS dans un contexte où celle-ci devait, pour garantir la sécurité des données, accomplir en quelques semaines des opérations, dont certaines structurantes, qui étaient prévues pour s'étaler sur plusieurs mois ;
 - le recours par la PDS à des prestataires d'hébergement informatique des données qui transfèrent des données hors de l'Union européenne et les éventuels risques matériels et juridiques en matière d'accès direct par les autorités de pays tiers. En effet, le contrat conclu entre la Plateforme et son hébergeur mentionne l'existence de transferts de données en dehors de l'Union européenne dans le cadre du fonctionnement courant de la Plateforme, notamment pour les opérations de maintenance ou de résolution d'incident. Dans son arrêt du 16 juillet 2020 dans l'affaire dite « Schrems II » la Cour de justice de l'Union européenne (CJUE) a estimé que le droit des Etats-Unis d'Amérique ne permet pas d'assurer un niveau de protection essentiellement équivalent à celui garanti par le droit de l'Union.
La PDS a toutefois transmis récemment à la Commission un avenant conclu avec l'un de ses prestataires, au travers duquel celui-ci apporte des garanties supplémentaires relatives au stockage et au traitement de données. Ces garanties devront être analysées en détail afin de déterminer si elles permettent de conclure à l'absence de transfert hors de l'Union européenne. La Commission sera en outre attentive aux conséquences de l'analyse de la législation des États-Unis d'Amérique, par la décision « Schrems II » de la CJUE, sur la situation de la PDS ;
 - l'importance des mesures de pseudonymisation : la pseudonymisation est une mesure de sécurité qui permet de limiter les risques pour les personnes dont les données seront traitées.
18. L'arrêté du 21 avril 2020 autorisant la centralisation de certaines données de santé au sein de la PDS pour la gestion de l'urgence sanitaire et l'amélioration des connaissances sur la COVID-19 a fait l'objet d'un recours en référé auprès du Conseil d'Etat. Par une ordonnance rendue le 19 juin 2020, le Conseil d'État a pour l'essentiel rejeté le recours et a ordonné à la PDS de fournir à la Commission tous éléments relatifs aux procédés de pseudonymisation utilisés. Les éléments transmis sont actuellement en cours d'instruction.
19. Cette centralisation et les usages possibles de ces données sont aujourd'hui encadrés par l'article 30 de l'arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de COVID-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé, venu remplacer l'arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020.
20. Cet arrêté prévoit que les données ne peuvent être traitées que pour des projets poursuivant une finalité d'intérêt public en lien avec l'épidémie actuelle de COVID-19 et jusqu'à l'entrée en vigueur du décret SNDS et au plus tard le 30 octobre 2020.
21. La Commission sera amenée à se prononcer prochainement sur le projet de décret SNDS qui encadrera les rôles respectifs des responsables de traitement et précisera les catégories de données réunies en son sein.

○ **L'avis de la Commission sur l'application mobile STOPCOVID**

22. Depuis le début de l'épidémie de SARS-Cov-2, plusieurs États dans le monde ont choisi de recourir à des dispositifs de "suivi des contacts" automatisés dont l'implémentation pratique, à géométrie variable, s'avère plus ou moins respectueuses des droits et libertés fondamentaux et notamment du respect de la vie privée de ses utilisateurs. Très tôt, la Commission s'est penchée sur le développement de ces outils ce qui lui a permis d'échanger, très rapidement, avec ses homologues européens afin de travailler à l'élaboration d'exigences communes pour ce type de dispositif.
23. Dans ce contexte, le comité européen à la protection des données (CEPD) a publié, le 21 avril 2020, des lignes directrices relatives à l'utilisation de données de géolocalisation et d'outils de "suivi des contacts" dans le cadre de la pandémie de COVID-19.
24. Ces lignes directrices viennent notamment clarifier le cadre juridique applicable aux applications de "suivi des contacts" et émettre des recommandations à destination des États membres désireux d'utiliser de tels dispositifs dans le cadre de leur stratégie sanitaire. Ainsi, les lignes directrices s'accompagnent d'un guide technique s'adressant aux développeurs d'applications de « suivi des contacts ». Sans être exhaustif, le guide dresse une liste de recommandations techniques concrètes ayant vocation à intégrer le principe de « protection des données dès la conception » consacré par le RGPD. Les recommandations portent principalement sur la nature de données traitées, les fonctionnalités ainsi que les mesures de sécurité. Elles sont le résultat d'une vision européenne harmonisée quant aux garanties qui doivent être mises en œuvre dans le cadre du recours à de tels dispositifs : utilisation basée sur le volontariat des personnes, recours à la technologie *Bluetooth*, utilisation de données à caractère personnel pseudonymisées (identifiants pseudonymes), publication du code source du dispositif, etc.
25. C'est sur la base de cette grille d'analyse européenne que la Commission a rendu ses avis dans le cadre des saisines du Gouvernement sur l'application STOPCOVID.
26. **Le premier avis, adopté le 24 avril 2020**, portait sur l'éventuelle mise en œuvre de l'application STOPCOVID. À ce stade, le déploiement de cette application et ses modalités exactes de mise en œuvre n'étaient pas encore arrêtés.
27. Dans son avis, la Commission :
- a insisté sur la nécessité de démontrer que l'utilité de l'application pour la gestion de la crise est suffisamment avérée et que les garanties appropriées sont apportées (recours à des données pseudonymisées, mesures techniques de sécurité, limitation du dispositif dans le temps, durée de conservation limitée des données, etc.) ;
 - est venue confirmer que l'application traiterait bien des données à caractère personnel (notamment des données concernant la santé) sous une forme pseudonymisée (donc bien soumise au RGPD) et non anonymisée comme cela a parfois pu être avancé ;

- a accueilli favorablement le caractère volontaire de l'utilisation d'un tel dispositif et a demandé qu'aucune conséquence négative ne puisse être attachée au choix de ne pas recourir à l'application (accès aux tests et aux soins, accès à certains services, etc.) ;
- a émis une série de recommandations sur les mesures de sécurité complémentaires à apporter.

28. Suivant la recommandation de la Commission de disposer d'un fondement juridique explicite et précis dans le droit national, sur lequel elle serait préalablement consultée, le ministère en charge de la santé a saisi la Commission, le 15 mai 2020, d'une demande d'avis concernant un projet de décret relatif à l'application mobile dénommée STOPCOVID.

29. Cette nouvelle saisine a permis à la Commission, d'une part, de constater que les principales recommandations formulées dans son précédent avis avaient été prises en compte et, d'autre part, d'émettre plusieurs observations tant sur le projet de décret que sur les conditions opérationnelles de déploiement de l'application :

- la Commission a estimé dans un **deuxième avis en date du 25 mai 2020**, que l'application pouvait être légalement déployée dès lors qu'elle apparaît être un instrument complémentaire du dispositif de suivi des contacts manuels et qu'elle permet des alertes plus rapides en cas de contact avec une personne contaminée, y compris pour des contacts avec des personnes inconnues. La Commission a cependant mis en avant la nécessité d'évaluer, de manière dynamique, l'impact effectif du dispositif sur la stratégie sanitaire globale afin de s'assurer de son utilité au cours du temps. La durée de mise en œuvre du dispositif devra ainsi être conditionnée aux résultats de cette évaluation régulière ;
- compte tenu de la sensibilité de l'application, la Commission a formulé plusieurs recommandations parmi lesquelles :
 - l'amélioration de l'information fournie aux utilisateurs, en particulier s'agissant des conditions d'utilisation de l'application et des modalités d'effacement des données personnelles ;
 - la nécessité de délivrer une information spécifique pour les mineurs et les parents des mineurs ;
 - la consécration, dans le décret à venir, d'un droit d'opposition et d'un droit à l'effacement des données pseudonymisées enregistrées tant sur l'ordiphone de l'utilisateur que sur le serveur central ;
 - l'opportunité de développer une technologie alternative à celle utilisée pour vérifier que l'application est bien utilisée par une personne physique. En effet, le recours à un système de "captcha" fourni par un tiers était non seulement susceptible d'entraîner la collecte de données à caractère personnel non prévues dans le décret, mais également d'entraîner le transfert de données hors de l'Union européenne ainsi que des opérations de lecture/écriture qui nécessiterait un consentement de l'utilisateur ;
 - le libre accès à l'intégralité du code source de l'application mobile et du serveur.

30. La publication du décret n° 2020-650 du 29 mai 2020 a permis à la Commission de constater que de nombreuses observations ont été suivies par le gouvernement : la liste des données collectées a été complétée, le droit d'opposition et le droit à l'effacement ne sont plus écartés par le texte, les sous-traitants ont été mentionnés au titre des accédants ou destinataires des données à caractère personnel dont ils auront besoin de connaître, la notion de « code informatique » a été remplacée par la notion de « code source ».

II - SUR LE MAINTIEN DES DISPOSITIFS AU REGARD DES PRINCIPES DE NECESSITE ET DE PROPORTIONNALITE

31. Comme souligné par la Commission dans ses différents avis, le caractère dérogatoire des différents traitements mis en œuvre ne peut être justifié que si leur utilité est suffisamment avérée au regard de l'évolution sanitaire du pays.

32. La gravité de la crise liée à la situation sanitaire créée par l'épidémie de COVID-19, d'une ampleur exceptionnelle, a conduit le Gouvernement à ne laisser de côté aucun outil permettant de lutter contre l'épidémie. Cette lutte, qui relève de l'objectif à valeur constitutionnelle de protection de la santé, constitue un impératif majeur de nature à justifier, dans certaines conditions, des atteintes au droit à la protection de la vie privée et des données à caractère personnel.

33. La Commission rappelle néanmoins que les protections constitutionnelle et conventionnelle du droit au respect de la vie privée et à la protection des données à caractère personnel, assises notamment sur la Charte des droits fondamentaux de l'Union européenne et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, imposent que les atteintes portées à ces droits par les autorités publiques soient non seulement justifiées par un motif d'intérêt général, comme cela est le cas en l'espèce, mais soient également nécessaires et proportionnées à la réalisation de cet objectif.

34. En outre, elle rappelle le caractère sensible, par nature, de la mise en œuvre de tels dispositifs qui permettent notamment le traitement et le partage de données de santé, pouvant être consultées par un grand nombre d'acteurs et nécessitant une protection supplémentaire.

35. Le principe de proportionnalité implique également de ne porter atteinte aux droits à la vie privée et à la protection des données à caractère personnel que pendant la durée strictement nécessaire à l'atteinte de l'objectif poursuivi. À cet égard, la Commission a pris acte du caractère temporaire de ces dispositifs, dont le terme de mise en œuvre est fixé par les décrets encadrant leur création, à six mois à compter de la fin de l'état d'urgence sanitaire, soit au 11 janvier 2021.

36. Si l'évaluation de la nécessité de maintenir ces dispositifs n'appartient pas à la Commission au titre de ses missions, elle a conscience que l'appréciation de leur utilité est délicate et qu'elle doit pouvoir tenir compte, le cas échéant, de possibles périodes de recrudescence de l'épidémie. Elle estime pour autant cette évaluation essentielle dès lors que ces dispositifs ne sont admissibles que s'ils contribuent utilement à la politique sanitaire et demande au Gouvernement d'y veiller.

37. À cet égard, la Commission souscrit à la demande du Comité de contrôle et de liaison COVID-19 dans son rapport annexé au rapport du Gouvernement adressé au Parlement, de disposer d'indicateurs de performance des systèmes d'information déployés, afin de pouvoir mesurer leur efficacité au regard des objectifs poursuivis. Elle estime qu'une grille d'analyse devrait être établie au regard d'indicateurs d'efficacité sanitaire.
38. En outre, la Commission avait demandé, dans son avis du 25 mai 2020 relatif à l'application mobile STOPCOVID, que l'impact effectif du dispositif sur la stratégie sanitaire globale soit étudié et documenté par le Gouvernement de manière régulière pendant toute sa période d'utilisation.
39. Il a cependant été constaté, au jour des contrôles, que l'évaluation formelle de l'effectivité de l'application n'avait pas encore débuté et que le calendrier du travail d'évaluation n'avait pas encore été établi par le ministère.
40. À ce titre, et sans à ce stade remettre en cause l'utilité de ces dispositifs, la Commission regrette que le rapport du Gouvernement adressé au Parlement le 9 septembre 2020 ne fasse pas état d'éléments plus précis justifiant de la nécessité de maintenir ces traitements au regard du contexte sanitaire actuel. La Commission a conscience que le déploiement de ces dispositifs est récent et que le Gouvernement dispose de peu de recul sur leur fonctionnement. Elle a également conscience que ces dispositifs ont été mis en œuvre au moment où l'épidémie diminuait et qu'un regain est actuellement en cours. Toutefois, elle estime que cette évaluation est indispensable et urgente au regard notamment des risques inhérents à ces traitements pour les droits et libertés des personnes.
41. A titre d'exemple, si le rapport mentionne le nombre de téléchargements de l'application mobile STOPCOVID, il ne permet pas d'apprécier suffisamment l'impact effectif de ce dispositif dans la lutte contre l'épidémie (absence d'analyse relative aux statistiques d'usage, aux résultats d'éventuelles enquêtes menées auprès des utilisateurs, professionnels ou grand public, au nombre de cas identifiés grâce à l'application).
42. La Commission rappelle que ces fichiers sont mis en œuvre aux fins de lutter contre la propagation de l'épidémie de COVID-19 pour la durée strictement nécessaire à cet objectif ou, au plus, pour une durée de six mois à compter de la fin de l'état d'urgence sanitaire déclaré par l'article 4 de la loi n° 2020-290 du 23 mars 2020. Toute prorogation de ces systèmes d'information au-delà du 11 janvier 2021 ne pourra donc être autorisée que par la loi.
43. En outre, la Commission rappelle qu'elle devra être saisie de toute modification apportée au décret relatif aux systèmes d'information SI-DEP et CONTACT COVID.
44. De même, les données à caractère personnel collectées par ces systèmes d'information ne peuvent être conservées à l'issue d'une durée de trois mois après leur collecte à l'exception des données collectées à des fins de surveillance épidémiologique aux niveaux national et local, pour la recherche sur le virus et les moyens de lutter contre sa propagation, pour lesquels une durée de conservation maximale de six mois à compter de la fin de l'état d'urgence sanitaire a été fixée par le décret n° 2020-1018 du 7 août 2020.

III- APPRÉCIATION DE LA COMMISSION SUR LES CONDITIONS OPÉRATIONNELLES DE MISE EN ŒUVRE DES TRAITEMENTS

45. En parallèle de sa mission de conseil et d'accompagnement à la conformité, la Commission peut contrôler les organismes afin de vérifier les conditions concrètes de mise en œuvre de tout traitement des données personnelles. Ces contrôles peuvent s'effectuer en ligne, par des auditions, sur pièces ou sur place.

46. Ainsi, conformément à ce qu'elle avait annoncé lors de son audition publique devant l'Assemblée nationale le 5 mai 2020, la présidente de la Commission a décidé de faire procéder à une série de contrôles des dispositifs SI-DEP et CONTACT COVID et de l'application STOPCOVID².

47. La campagne de contrôles menée par la Commission a vocation à s'effectuer en plusieurs étapes, à différents moments de la mise en œuvre des trois dispositifs précités. Le présent avis comporte des éléments synthétiques issus des constatations opérées par la Commission lors de la première phase de vérifications ainsi que des échanges réguliers qui ont lieu avec le ministère des solidarités et de la santé et les autres acteurs impliqués, notamment la CNAM et les agences régionales de santé (ARS).

○ Le contrôle des fichiers SI-DEP et CONTACT COVID :

48. Les investigations sont menées simultanément sur les traitements SI-DEP et CONTACT COVID depuis le mois de juin 2020 et donnent lieu à des réunions, des auditions et des contrôles sur place et sur pièces auprès des différents acteurs.

49. Pour le traitement SI-DEP, des contrôles sur pièces et sur place ont eu lieu auprès du ministère des solidarités et de la santé, de l'Assistance Publique des Hôpitaux de Paris (AP-HP), qui gère la mise en œuvre opérationnelle du traitement SI-DEP et des laboratoires privés afin d'opérer des vérifications relatives à l'accueil des patients.

50. Pour le traitement CONTACT COVID, des contrôles sur pièces, sur audition et sur place ont eu lieu auprès d'un établissement de santé, d'une caisse primaire d'assurance maladie (CPAM), d'une ARS, du Conseil national de l'ordre des médecins (CNOM) et du Conseil national de l'ordre des pharmaciens (CNOP).

51. Les points de vérification ont principalement porté sur :

- les modalités de recueil de consentement et d'information des personnes ;
- la sécurité des systèmes d'information ;
- les flux de données et les destinataires ;
- le respect des droits d'accès ou d'opposition des personnes.

² Une description de ces trois dispositifs figure en annexe 2 du présent avis.

○ **LE FICHER SI-DEP**

52. À ce stade des vérifications opérées par la Commission, et sous réserve de la finalisation de l'instruction de la procédure, les missions de contrôle menées auprès de l'AP-HP et de laboratoires de biologie médicale **ont permis de constater un niveau global de conformité satisfaisant.**
53. Les services ont relevé le soin porté au respect de la réglementation relative à la protection des données en dépit du contexte de crise sanitaire mobilisant fortement les ressources hospitalières, ainsi que d'un calendrier de mise en œuvre très court au vu de l'ampleur du projet (plus de 4 500 laboratoires connectés, 4,2 millions de tests enregistrés à la fin juillet).
54. Les équipes de contrôle ont constaté la mise en œuvre des bonnes pratiques suivantes :
- **les catégories de données collectées sont limitées à ce que prévoit le décret** portant création du traitement. L'AP-HP a défini les champs à renseigner obligatoirement afin d'assurer l'uniformité des fiches patient et le traitement de données fiables malgré la multiplicité d'intervenants dans le traitement ;
 - **un effort très important a été fourni afin de sensibiliser l'ensemble des acteurs** de la chaîne du traitement aux enjeux de protection des données concernant le traitement (diffusion de guides adaptés aux différents logiciels de gestion interconnectés avec SI-DEP utilisés par les laboratoires, collaboration étroite avec les éditeurs des logiciels en vue de leur évolution) ;
 - **les destinataires des données correspondent à ceux prévus par les textes.** Chaque organisme accédant au fichier a désigné un administrateur local, en charge de délivrer les habilitations aux utilisateurs de la solution au sein de son organisation. Ce principe de délégation d'habilitations attribuées aux utilisateurs de l'outil permet d'assurer un cloisonnement et une granularité des accès aux données à caractère personnel garantissant leur confidentialité ;
 - la mise en œuvre de moyens importants **permettant d'assurer l'information des personnes concernées** du traitement de leurs données et ce pour les différents points de contact possibles avec les patients ;
 - enfin, **la documentation des traitements** exigée en vertu des dispositions du RGPD (registre des activités de traitement, analyse d'impact sur la protection des données, registre des violations de données, etc.) est mise à jour dès que nécessaire.
55. S'agissant de la sécurité des données, le niveau atteint dans le cadre du dispositif SI-DEP est **globalement satisfaisant**, notamment en raison de l'utilisation de solutions logicielles déjà éprouvées et maîtrisées par l'AP-HP. En particulier, la procédure permettant aux patients d'accéder au résultat de leur test repose sur une authentification forte, évitant la divulgation de leurs données de santé à travers des canaux non sécurisés. En outre, une veille est menée sur les incidents de sécurité, pouvant entraîner une violation de données à caractère personnel, et les anomalies détectées sont tracées avec attention. Toutefois, quelques améliorations restent à apporter concernant la gestion des comptes d'administration et de la traçabilité des accès.

56. **En l'état actuel des vérifications, la Commission se rapprochera dans les tous prochains jours du ministère des solidarités et de la santé afin d'attirer son attention sur les pratiques à améliorer et les mesures à prendre en conséquence.**

○ **LE FICHER CONTACT COVID**

57. Lors des contrôles, les équipes de la Commission ont constaté que le téléservice CONTACT COVID, expressément conçu et développé par la CNAM pour assurer le suivi des cas « contact », bénéficie d'évolutions régulières pour répondre aux demandes d'amélioration des différents utilisateurs (ARS, professionnels de santé exerçant en libéral, établissements de santé, etc.).

58. Le traitement CONTACT COVID permet aux médecins de ville/établissements de santé/centres de santé (niveau 1), au personnel habilité de l'assurance maladie (niveau 2) et aux ARS (niveau 3) de recueillir des informations sur les cas contact et les chaînes de contamination. Les équipes de contrôle ont constaté des niveaux de maturité en matière de protection des données à caractère personnel différents en fonction des organismes.

59. D'une manière générale, il ressort des contrôles que **ces organismes ont mené des actions pour prendre en compte les exigences liées à la protection des données**. Ils ont, pour la plupart, bien pris conscience que ce dispositif impliquait la collecte de données de santé, qui sont des données sensibles par nature et qui nécessitent dès lors une protection supplémentaire.

60. À cet égard, certaines bonnes pratiques, mises en œuvre dans un délai contraint et des conditions sanitaires exceptionnelles, doivent être soulignées :

- **l'élaboration par la CNAM, de guides méthodologiques** à destination des acteurs intervenant à chaque niveau du dispositif (médecins pour le niveau 1, personnels habilités de l'assurance maladie pour le niveau 2, ARS pour le niveau 3 ainsi que les laboratoires et pharmaciens). Ces guides permettent aux acteurs impliqués dans le téléservice de comprendre le contexte de mise en œuvre du traitement et les fonctionnalités du service ;
- **la réalisation**, par certains organismes contrôlés, **d'analyses d'impact** relatives à la protection des données et la mise à jour en conséquence du registre des activités de traitements relatifs à CONTACT COVID ;
- **l'accès sécurisé** au téléservice par les acteurs engagés dans le dispositif de « contact tracing » **au moyen d'un mécanisme d'identification et d'authentification forte est satisfaisant** (ex : accès par les agents de l'assurance maladie au moyen d'une carte à puce).

61. Des mauvaises pratiques ont également été relevées :

- **dans le cadre des vérifications effectuées auprès d'un établissement de santé, il est apparu que les informations délivrées aux « patients O » et aux « cas contacts » sur les traitements** (finalité, durée de conservation des données, destinataires des informations, etc.) **sont parfois parcellaires, en l'absence de remise d'un support d'information**

délivré par la CNAM. Or, une information incomplète ne permet pas aux « patients 0 » et aux « cas contacts » de prendre pleinement connaissance du traitement qui est opéré sur leurs données et des droits qu'ils détiennent à cet égard (droit d'accès ou d'opposition le cas échéant). Au 25 juin 2020, il a cependant été relevé que 42% des « patients 0 » qui ont déclaré des « cas contacts » ont exercé leur droit d'opposition à la communication de leur identité à au moins un contact et que 21% d'entre eux en ont refusé la diffusion à l'ensemble de leurs contacts ;

- **dans une ARS, les équipes de contrôle de la Commission ont constaté qu'aucune procédure d'exercice des droits « informatique et libertés » à destination des « patients 0 » et des « cas contacts » n'a été formalisée ;**
- **il a été constaté que des CPAM ont adressé des données de santé par courriels à destination d'une ARS sans avoir recours à une messagerie sécurisée ;**
- **il a été constaté dans un établissement hospitalier que, sur instruction de la CNAM, il a été procédé à l'envoi occasionnel de données de santé inscrites dans des fichiers distincts du système d'information principal** ce qui conduit à l'éparpillement de fichiers et ne permet pas une gestion satisfaisante de la durée de conservation des données.

62. Des premiers échanges ont eu lieu entre la CNAM et la Commission sur les différentes pratiques constatées lors de cette première phase de contrôle. La Commission est consciente de la difficulté, à ce stade, pour le responsable de traitement de s'assurer de la correcte application des règles de protection des données personnelles par l'ensemble des organismes appelés à participer au traitement dans un très grand nombre de lieux. Elle souligne également que les contrôles ont été effectués au tout début de la mise en œuvre des traitements encore en cours d'évolution. Il a été décidé d'adresser dans les prochains jours, une demande de mise en conformité dans les plus brefs délais à chaque organisme impliqué (CNAM, ARS, ministère de la santé). À défaut de se conformer aux exigences du RGPD, il appartiendra à la Présidente de la Commission de déterminer si l'adoption d'une mesure correctrice est nécessaire.

○ **Le contrôle de l'application STOPCOVID :**

63. Le 2 juin 2020, l'application STOPCOVID a été déployée par le ministère des solidarités et de la santé dans les magasins d'applications accessibles au grand public.

64. Des vérifications sur cette application ont alors été diligentées auprès du ministère des solidarités et de la santé, responsable de ce traitement, mais également auprès d'autres organismes impliqués dans sa mise en œuvre dont notamment l'Institut national de recherche en sciences et technologies du numérique (INRIA), qui a conçu le protocole sur lequel repose l'application et qui agit en tant qu'assistant à maîtrise d'œuvre.

65. Les points de vérification ont notamment porté sur :

- les modalités de recueil de consentement et d'information des personnes ;

- la sécurité des systèmes d'information ;
- les flux de données et les destinataires ;
- le respect des droits d'accès ou d'opposition des personnes et organismes impliqués dans la mise en œuvre des traitements.

66. **Les contrôles réalisés ont permis de constater que le fonctionnement de l'application mobile STOPCOVID respecte pour l'essentiel les dispositions applicables relatives à la protection des données à caractère personnel** et que la plupart des préconisations formulées par la Commission dans ses avis des 24 avril et 25 mai 2020 ont été pris en compte par le ministère des solidarités et de la santé.

67. Lors des contrôles, **certains manquements aux dispositions du RGPD et de la loi « informatique et libertés »** ont été constatés dans la première version de l'application dite v1.0. Concomitamment au contrôle de la Commission, le ministère a rapidement déployé une deuxième version de l'application dite v1.1 afin d'apporter des changements sur la manière dont les données sont traitées.

68. **Au regard des manquements constatés, le ministère des solidarités et de la santé a été mis en demeure le 15 juillet 2020, dans le délai d'un mois, de :**

- **cesser de transmettre les données de toutes les personnes avec lesquelles l'utilisateur a été en contact au serveur central**, par exemple en forçant la mise à jour de l'application STOPCOVID vers la nouvelle version v1.1 par le blocage de l'application dans sa version v1.0 ;
- **compléter l'information fournie aux utilisateurs de l'application STOPCOVID**, en fournissant aux utilisateurs une information complète sur les destinataires ou catégories de destinataires des données à caractère personnel issues de l'application ;
- veiller à ce que **les contrats de sous-traitance conclus dans le cadre de l'exploitation de l'application STOPCOVID contiennent les mentions prévues à l'article 28 du RGPD** ;
- **compléter l'AIPD** issue de l'application STOPCOVID conformément à l'article 35 du RGPD :
 - o en mentionnant la collecte de l'adresse IP de l'équipement mobile de l'utilisateur de l'application dans le cadre des mesures de sécurité du système reposant sur la solution DDOS de la société ORANGE ;
 - o en mentionnant la collecte des informations présentes sur l'équipement mobile de l'utilisateur dans le cadre de la technologie reCaptcha de la société GOOGLE déployée dans le cadre de la version v1.0 de l'application, dans l'hypothèse où ces données seraient encore collectées ;
- veiller, le cas échéant, à **informer et recueillir le consentement des personnes** concernées aux actions de lecture et d'écriture des informations présentes sur les terminaux de communication électronique par la société GOOGLE dans le cadre de la technologie reCaptcha (version v1.0 de l'application), conformément aux dispositions de l'article 82 de la loi « informatique et libertés ». Cette injonction vise le cas des utilisateurs ayant téléchargé la version v1.0 de l'application et ne l'ayant pas encore activée pour la première fois.

69. Compte tenu du nombre de personnes concernées (environ deux millions trois cent mille téléchargements au jour du présent avis) et du caractère sensible des données personnelles utilisées dans l'application STOPCOVID, qui portent sur l'état de santé de certains des utilisateurs, **la Commission a décidé de rendre publique cette mise en demeure.**
70. Par un courrier en date du 14 août 2020, le ministère des solidarités et de la santé a adressé à la Commission des éléments de réponse et des documents relatifs aux mesures prises pour se conformer à la mise en demeure adoptée par la Présidente de la Commission. Les mesures prises par le ministère ont notamment consisté à techniquement forcer les utilisateurs à avoir recours à une nouvelle version de l'application (v1.1) dans le cadre de laquelle le préfiltrage de l'historique des contacts s'effectue au niveau du téléphone. Avec cette version, il est désormais impossible que l'intégralité de l'historique des contacts de l'utilisateur soit transmise au serveur central, sans préfiltrage au niveau du téléphone. De même, le ministère n'a plus recours au système de « reCaptcha » proposé par la société Google. Il n'y a donc plus d'opérations de lecture et d'écriture sur le terminal en lien avec cette technologie, même pour les utilisateurs de la première version de l'application (v1.0).
71. Après examen des réponses du ministère et des pièces justificatives associées (copies d'écran, code source des différentes versions de l'application, contrats mis à jour, etc.), il apparaît que l'ensemble des demandes exprimées par la Présidente de la Commission dans la mise en demeure du 15 juillet 2020 ont été satisfaites.
72. Les traitements mis en œuvre étant désormais conformes aux exigences du RGPD, la Présidente de la Commission a prononcé la clôture de cette mise en demeure le 3 septembre 2020. En cas d'évolution de l'application, la Commission pourra toujours, le cas échéant, procéder à de nouvelles vérifications.
- **Une procédure de contrôle continue :**
73. La Commission souligne que les contrôles se poursuivront tout au long de la période d'utilisation des fichiers, jusqu'à la fin de leur mise en œuvre et la suppression des données qu'ils contiennent.
74. Elle rappelle également que les vérifications menées donnent lieu à de nombreux échanges avec le ministère des solidarités et de la santé mais également avec d'autres organismes (CNAM, ARS, laboratoires, CNOM, etc.). Le présent avis ne constitue ainsi qu'une synthèse de ces échanges et des constatations effectuées lors de la première phase de contrôle.
75. À cet égard, **la seconde phase de contrôles** est d'ores et déjà prévue et débutera avant la fin du mois de septembre 2020. Elle portera principalement sur les points suivants :
76. Concernant le traitement SI-DEP :
- l'interconnexion de la Plateforme des données de santé avec le fichier SI-DEP, non opérationnelle à la date des premiers contrôles ;

- le transfert des données à des organismes tiers (remontées de données pour le suivi épidémiologique (données pseudonymisées) auprès de la DREES ou de Santé publique France ;

77. Concernant le traitement CONTACT COVID :

- les modalités de mise en œuvre du portail d'accès au traitement CONTACT COVID à destination des partenaires ne disposant pas d'un compte « ameli pro » ;
- l'information délivrée aux patients par les médecins et les pharmaciens sur le traitement CONTACT COVID.

78. Pour ces deux traitements, les investigations porteront également sur l'effectivité des mesures prévues pour l'exercice des droits des personnes concernées.

79. Le prochain avis public de la Commission fera état des résultats de ces contrôles.

80. Enfin, **une troisième vague de contrôles** sera effectuée à l'issue de la mise en œuvre des traitements. Des contrôles sur place seront ainsi réalisés auprès des organismes concernés, afin de vérifier notamment la suppression effective des données. Les vérifications devraient porter sur les durées de conservation des données, leur suppression et/ou leur anonymisation éventuelle.

81. Ce dernier point concerne également l'application STOPCOVID. Les vérifications effectuées par la Commission à cette occasion pourront également porter sur des aspects visés dans la mise en demeure du 15 juillet 2020.

La Présidente

Marie-Laure DENIS

ANNEXE 1 : Liste des auditions Parlementaires et des avis rendus par la Commission

Liste des auditions de la Commission :

8 avril 2020: auditions devant la commission des lois de l'Assemblée Nationale et devant les deux rapporteurs de la commission des affaires économiques de l'Assemblée Nationale ;

15 avril 2020: audition devant la commission des lois du Sénat ;

1er mai 2020 : audition devant le rapporteur de la commission des affaires sociales du Sénat sur le projet de loi de prorogation de l'état d'urgence ;

5 mai 2020 : audition devant la commission des lois de l'Assemblée Nationale sur le projet de loi de prorogation état d'urgence ;

Liste des avis rendus sur les trois traitements SIDEP, CONTACT COVID et STOPCOVID :

Délibération n° 2020-044 du 20 avril 2020 de la CNIL portant avis sur un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de COVID-19 dans le cadre de l'état d'urgence sanitaire ;

Délibération n° 2020-046 du 24 avril 2020 de la CNIL portant avis sur un projet d'application mobile dénommée «StopCovid» ;

Délibération n° 2020-051 du 8 mai 2020 portant avis sur un projet de décret relatif aux systèmes d'information mentionnés à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire ;

Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée «StopCovid» ;

Délibération n° 2020-083 du 23 juillet 2020 portant avis sur un projet de décret pris en application de l'article 3 de la loi n° 2020-856 du 9 juillet 2020 organisant la sortie de l'état d'urgence sanitaire relatif à la durée de conservation des données pseudonymisées collectées à des fins de surveillance épidémiologique et de recherche sur le virus de la COVID-19

ANNEXE 2 : Description des traitements SI-DEP, CONTACT COVID et STOPCOVID

Le traitement SI-DEP est un système d'information national mis en œuvre par le ministère de la santé qui permet la centralisation des résultats des tests au SARS-CoV-2 réalisés par des laboratoires publics ou privés. Ces résultats sont transmis à SI-DEP soit automatiquement (4500 laboratoires connectés) soit manuellement. Cette centralisation permet ensuite une transmission des données à différents destinataires, notamment :

- aux agences régionales de santé (ARS) et à la Caisse primaire d'assurance maladie (CPAM), en vue de la réalisation des investigations relatives aux cas contacts, dans le cadre du téléservice CONTACT COVID.
- à la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES) et à Santé publique France sous une forme pseudonymisées, à des fins de surveillance épidémiologique et de diffusion des informations statistiques.
- à la Plateforme des données de santé (PDS) et à la Caisse nationale d'assurance maladie (CNAM) aux seules fins de faciliter l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le virus.

Le traitement CONTACT COVID mis en œuvre par la Caisse nationale d'assurance maladie (CNAM) recueille des informations sur les cas contact et les chaînes de contamination et vise à détecter les cas contacts à trois niveaux différents.

Il permet :

- aux médecins de ville/établissements de santé/centres de santé d'initier une fiche de suivi du « patient 0 » et de ses « cas contacts » (niveau 1) ;
- au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) (niveau 2) :
 - o de compléter et d'affiner, si nécessaire, la fiche du « patient 0 » et la liste de ses « cas contacts » ;
 - o d'appeler les « cas contacts » pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir ;
- aux Agences régionales de santé (ARS) d'assurer (niveau 3) :
 - o leurs missions de suivi des « cas contacts » ;
 - o la gestion des situations nécessitant une prise en charge spécifique. Il s'agit par exemple des chaînes de transmission en milieu scolaire, dans un établissement de santé ou dans un foyer de jeunes.

L'application STOPCOVID est une application mobile de suivi de contact, basée sur le volontariat des personnes et utilisant la technologie *Bluetooth*, mise à disposition par le Gouvernement dans le cadre de sa stratégie globale de « déconfinement progressif ».

Elle permet d'alerter les utilisateurs d'un risque de contamination lorsqu'ils ont été à proximité d'un autre utilisateur ayant été diagnostiqué ou dépisté positif à la COVID-19. Pendant son utilisation, le smartphone stocke une liste de pseudonymes

temporaires des appareils qu'il a « croisés » pendant 14 jours (c'est ce qu'on appelle l'« historique de proximité »).

Quand un utilisateur est diagnostiqué ou dépisté positif à la COVID-19, il peut choisir de se déclarer dans l'application et, ainsi, faire remonter les données de ses contacts (les « cartes de visite » pseudonymes) vers un serveur central. La transmission de ces données au serveur ne sera possible qu'avec un code à usage unique remis par un professionnel de santé suite à un diagnostic clinique positif ou un QR Code remis à la personne à l'issue de son test. Le serveur traite alors chacun des contacts remontés dans l'historique de proximité et calcule pour chacun le score de risque de contamination au virus. L'application d'un utilisateur interrogera périodiquement ce serveur pour voir si l'un des identifiants qui lui est rattaché a été remonté par une personne diagnostiquée ou dépistée à la COVID-19 et si le score de risque associé atteint un certain seuil. Une fois notifiée qu'elle est un « contact », donc à risque, la personne est notamment invitée à consulter un médecin.

ANNEXE 3 : Liste des textes et de leurs principaux apports en matière de protection des données personnelles

1. **Loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions** : autorise aux seules fins de lutter contre l'épidémie de COVID-19, le traitement et le partage de données de santé à caractère personnel dans le cadre de systèmes d'information créés par décret en Conseil d'État ;
2. **Décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions** : création des traitements SI-DEP et CONTACT COVID ;
3. **Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé STOPCOVID** : institue l'application STOPCOVID ;
4. **Loi n° 2020-856 du 9 juillet 2020 organisant la sortie de l'état d'urgence sanitaire** : autorise la prolongation de la durée de conservation des données pseudonymisées collectées dans le cadre des systèmes d'information SI-DEP et CONTACT COVID à des fins de surveillance épidémiologique et de recherche sur le virus de la COVID-19 ;
5. **Décret n° 2020-1018 du 7 août 2020 pris en application de l'article 3 de la loi n° 2020-856 du 9 juillet 2020 organisant la sortie de l'état d'urgence sanitaire et modifiant le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions** : porte à six mois après la fin de l'état d'urgence sanitaire la durée de conservation des données pseudonymisées collectées dans le cadre de ces systèmes d'information à des fins de surveillance épidémiologique et de recherche sur le virus de la COVID-19
6. **Arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de COVID-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé** : encadre la centralisation des données des fichiers SI-DEP et CONTACT COVID au sein de la Plateforme des données de santé et de la CNAM et leur utilisation (remplace et abroge l'arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de COVID-19 dans le cadre de l'état d'urgence sanitaire).

ANNEXE 4 : Liste des organismes contrôlés dans le cadre de ces dispositifs

Traitement SI-DEP :

Le ministère des Solidarités et de la Santé ;
L'Assistance Publique des Hôpitaux de Paris (AP-HP) ;
Des laboratoires privés de biologie médicale ;

Traitement CONTACT COVID :

Un établissement de santé recevant des malades en consultation ;
Une Caisse Primaire d'Assurance Maladie (CPAM) ;
Une agence régionale de santé (ARS) ;
Le Conseil national de l'Ordre des médecins (CNOM) ;
Le Conseil national de l'Ordre des pharmaciens (CNOP).

Traitement STOPCOVID :

Le ministère des Solidarités et de la Santé ;
L'Institut national de recherche en sciences et technologies du numérique (INRIA) ;
Autres organismes.