Délibération n° 2021-004 du 14 janvier 2021 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

(demande d'avis n° 210000315)

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 (RGPD) ;

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 modifiée 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 la loi n° 2020-1379 du 14 novembre 2020 autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise 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 le décret n° 2020-1385 du 14 novembre 2020 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 le décret n° 2020-1387 du 14 novembre 2020 fixant la liste des professionnels de santé habilités à renseigner les systèmes d'information mentionnés à l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions ;

Vu le décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la covid-19 ;

Vu l'arrêté du 10 juillet 2020 modifié 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 et notamment son article 30 ;

Après avoir entendu Mme Marie-Laure DENIS, présidente, en son rapport, et M. Benjamin TOUZANNE, commissaire du Gouvernement, en ses observations ;

Emet 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[1]. Ces traitements de données à caractère personnel sont encadrés par un décret en Conseil d'Etat du 12 mai 2020 récemment modifié et qui précise leurs modalités de création et de mise en œuvre.

2. Au côté de ces fichiers, l'application mobile « STOPCOVID », dont le traitement est encadré par le décret n° 2020-650 du 29 mai 2020, a été déployée. Celle-ci est aujourd'hui remplacée par l'application mobile « TOUSANTICOVID ».

3. Dans un contexte exceptionnel de crise sanitaire et d'urgence, la Commission a été amenée à se prononcer à plusieurs occasions sur le cadre normatif encadrant ces traitements : auditionnée à six reprises et ayant rendu neuf avis depuis mai 2020[2], elle a ainsi utilement éclairé les débats parlementaires autour des enjeux fondamentaux liés au respect de la vie privée et des données à caractère personnel. La Commission a également procédé à vingt-cinq contrôles depuis la mise en œuvre de ces dispositifs. Ses préconisations et constats ont été détaillés dans son premier avis, en date du 10 septembre 2020, relatif au fonctionnement de ces systèmes d'information[3].

[1] Voir la description des dispositifs en annexe 1

[2] Voir annexe 2

[3] 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)

4. Ce deuxième avis de la Commission, rendu sur le fondement de l'article 11 de la loi du 11 mai 2020 modifiée, complète le second rapport trimestriel du Gouvernement qui sera adressé au Parlement et dont la Commission n'a pas encore eu connaissance. Cet avis s'attachera, notamment au regard des préconisations qu'elle a émises dans ses avis sur les projets de texte qui lui ont été soumis depuis août 2020 et de ses constatations lors des divers contrôles effectués, à rappeler les récentes évolutions du cadre normatif et à évaluer :

    - 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.

I- ÉVOLUTIONS DU CADRE NORMATIF ET AVIS DE LA CNIL

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

o L'avis de la Commission sur les modifications apportées aux systèmes d'information SI-DEP et CONTACT COVID

6. La Commission avait, dans son avis du 10 septembre 2020 sur le fonctionnement des systèmes d'information, rappelé qu'elle devrait être saisie de toute modification qui y serait apportée.

7. La Commission a ainsi été saisie, en urgence, le 3 novembre 2020, d'un projet de décret modifiant le décret n° 2020-551 du 12 mai 2020 fixant les modalités dans lesquelles les systèmes d'information prévus à l'article 11 de la loi n° 2020-446 du 11 mai 2020 prorogeant l'état d'urgence sanitaire peuvent être mis en œuvre.

8. Le décret prévoyait notamment :

    - la prolongation de la durée de mise en œuvre des systèmes d'information « CONTACT COVID » et « SI-DEP » jusqu'à la date mentionnée à l'article 11 de la loi n° 2020-546 du 11 mai 2020, soit au plus tard jusqu'au 1er avril 2021 ;

    - l'allongement de la durée de conservation des données pseudonymisées traitées à des fins de surveillance épidémiologique et de recherche sur le virus jusqu'à la date mentionnée à l'article 11 de la loi n° 2020-546 du 11 mai 2020, soit au plus tard jusqu'au 1er avril 2021[4] ;

[4] Pour rappel, la durée de conservation des données collectées par ces systèmes d'information avait été initialement fixée par la loi à trois mois après leur collecte. Une durée de conservation spécifique aux données traitées à des fins de recherche sur le virus a ensuite été ajoutée à la loi afin de permettre leur conservation jusqu'à six mois après la fin de l'état d'urgence sanitaire, soit jusqu'au 11 janvier 2021 dans un premier temps.

- l'extension de la remontée des résultats à tous les examens de dépistage (sérologique ou virologique) réalisés par des professionnels de santé figurant sur une liste prévue par décret et habilités à la réalisation de ces tests.

9. Dans son avis du 5 novembre 2020[5], la Commission a réitéré certaines remarques émises dans son avis du 8 mai 2020, s'agissant notamment :

   - du 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 ;

   - de l'atteinte portée à la vie privée par ces traitements, qui n'est admissible que si cette politique constitue une réponse nécessaire et appropriée pour ralentir la propagation de l'épidémie, impliquant que leur nécessité soit périodiquement réévaluée au vu de l'évolution de l'épidémie et des connaissances scientifiques ;

   - des garanties suffisantes qui doivent être apportées, quel que soit le contexte d'urgence, au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel.

10. Elle a également rappelé que :

   - des garanties doivent être mises en œuvre s'agissant du recours par les organismes nationaux et locaux d'assurance maladie, de la Caisse nationale militaire de sécurité sociale et des autres organismes de protection sociale à des sous-traitants et à des intérimaires pour l'enregistrement et la consultation de l'ensemble des données collectées. Elle a notamment pris acte de ce que le ministère s'est engagé à établir une liste exhaustive des sous-traitants auxquels il sera fait appel et a demandé que le responsable de traitement ait recours, pour le traitement des données, à des sous-traitants relevant exclusivement des juridictions de l'Union européenne et qu'aucun transfert de données ne soit effectué en dehors de l'Union européenne ;

   - pour les personnes pouvant consulter, enregistrer ou être destinataires des données :

     - des instructions claires et uniformes – reprenant les consignes des autorités sanitaires – devront être données à l'ensemble des intervenants et leurs sous-traitants quant à la définition des différentes notions utilisées dans le projet de décret qui justifient la collecte de données. La formation et la sensibilisation régulières des personnels qui sont amenés à intervenir sont en effet essentielles ;

[5] Délibération n° 2020-108 du 5 novembre 2020 portant avis sur un projet de décret 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

- il est nécessaire de définir une politique de gestion des habilitations adéquate et de mettre en œuvre des mesures d'authentification forte afin que seuls ceux qui ont besoin d'en connaître accèdent aux systèmes d'information, le ministère ayant été appelé à la vigilance sur ce point ;

- l'ensemble des supports d'information relatifs aux traitements devra être modifié afin de tenir compte des modifications apportées et que l'ensemble des personnes concernées devra en être informé.

11. Dans son avis, la Commission s'est également interrogée sur la compatibilité de la durée légale de conservation des données pseudonymisées issues de « CONTACT COVID » et de « SI-DEP » transmises à des fins de surveillance épidémiologique et de recherche sur le virus[6], avec l'hypothèse d'une intégration de ces dernières au système national des données de santé, dont la durée de conservation est de vingt ans en application de l'article L. 1461-1-IV-4° du code de la santé publique, ou de leur conservation dans un entrepôt pérenne au sein de la Plateforme des données de santé[7].

12. Enfin, elle a demandé à ce que les analyses d'impact relatives à la protection des données (AIPD) réalisées en application de l'article 35 du RGPD et actualisées en conséquence lui soient transmises.

13. A ce titre, la Commission rappelle qu'en application de l'article 67 de la loi « informatique et libertés » modifiée (LIL), les traitements de données à caractère personnel mis en œuvre dans le domaine de la santé par les agences régionales de santé (ci-après ARS) et ayant pour seule finalité de répondre à une alerte sanitaire et d'en gérer les suites, doivent faire l'objet d'une AIPD.

14. Elle rappelle également que les dérogations prévues par l'article 67 de la LIL précitée, qui permettent à certains responsables de traitement de mettre en œuvre des traitements de données de santé sans effectuer de formalités préalables auprès de la Commission, notamment les ARS dans le cadre de l'activité de suivi de contacts (« *contact tracing* ») de niveau 3 du dispositif « CONTACT COVID », prennent fin un an après la création des traitements. Des formalités devront donc être effectuées auprès d'elle dans l'hypothèse où les traitements de données seraient mis en œuvre durant plus d'une année.

15. Certaines observations de la Commission relatives au traitement « CONTACT COVID » ont été suivies, s'agissant des garanties apportées au recours aux sous-traitant par les organismes de protection sociale ainsi que la suppression de l'accès par l'ensemble des professionnels de santé et personnels habilités d'un établissement de santé ou social et médico-social aux données des personnes prises en charge par l'établissement, afin de limiter l'accès aux données des personnes effectivement prises en charge par ces professionnels et personnels.

---

[6] Jusqu'à la date mentionnée à l'article 11 de la loi n° 2020-546 du 11 mai 2020, soit au plus tard jusqu'au 1er avril 2021

[7] Pour rappel, la Commission s'est prononcée le 20 avril 2020 sur la centralisation de certaines données de santé des fichiers « CONTACT COVID » et « SI-DEP » 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. La Commission a également pris acte de ce que la liste des données pseudonymisées transmises à des fins de surveillance épidémiologique et de recherche a été précisée, répondant ainsi aux demandes formulées dans ses avis du 8 mai 2020 et du 23 juillet 2020.

17. Elle relève toutefois que certaines remarques concernant le traitement « SI-DEP » n'ont pas été prises en compte, et plus particulièrement s'agissant de l'ajout de la durée de conservation des données par le Service public d'information en santé (SPIS) et de la précision que la collecte du code postal du lieu dans lequel la personne envisage de séjourner pendant les sept jours suivant la réalisation du dépistage est nécessaire afin de déterminer l'ARS territorialement compétente pour procéder aux enquêtes sanitaires et pour permettre à l'Agence nationale de santé publique France d'effectuer des statistiques géographiques précises.

- **Le système d'information « VACCIN COVID »**

18. La Commission a été saisie pour avis le 30 novembre 2020 par le ministère des solidarités et de la santé d'un projet de décret en conseil d'Etat autorisant la création d'un système d'information (SI) pour la mise en œuvre, le suivi et le pilotage des campagnes vaccinales contre la covid-19 dénommé « VACCIN COVID » (SI « VACCIN COVID »).

19. Ce traitement de données, mis en œuvre sous la responsabilité conjointe de la direction générale de la santé et de la Caisse nationale d'assurance maladie (CNAM), a pour finalités d'identifier les personnes éligibles à la vaccination au regard des recommandations du ministre de la santé, la gestion de la campagne vaccinale, la mise à disposition de données à des fins de calcul d'indicateurs et de recherche, la délivrance d'une information aux personnes concernées en cas de risque nouveau et leur orientation vers un parcours de soins adaptés, la prise en charge financière des actes liés à la vaccination.

20. La CNIL a, dans son avis du 10 décembre 2020, relevé que ce SI n'est pas fondé sur les dispositions applicables dans le cadre de l'état d'urgence et qu'il n'a pas vocation à s'étendre à d'autres vaccinations que celle contre le coronavirus SARS-CoV-2. Elle a également relevé qu'à terme, lorsque la campagne vaccinale sera étendue à l'ensemble de la population adulte tel qu'envisagé par le ministère, le SI « VACCIN COVID » comportera certaines données de santé d'une majeure partie de la population française. En effet, ce traitement sera alimenté, au fur et à mesure de l'extension de l'éligibilité à la vaccination, par des versements successifs de données issues des bases des régimes d'assurance maladie obligatoire et complétés par des professionnels de santé.

21. Elle a ainsi rappelé :

- que les dispositions du code de la santé publique relatives au secret médical s'appliquent aux données traitées dans le cadre de ce SI et que seules les personnes habilitées et soumises au secret professionnel pourront y accéder dans les strictes limites de leur besoin d'en connaître pour l'exercice de leur mission ;
- qu'une AIPD doit être effectuée avant la mise en œuvre du traitement.

22. Elle a invité le Gouvernement à préciser notamment :

- les autres systèmes d'information avec lesquels le SI « VACCIN COVID » serait mis en relation et l'éventuel recours à une sous-traitance. Le cas échéant, la Commission invitait le ministère à diffuser ces informations, par exemple en les rendant publiques sur son site web ;
- à des fins de transparence, la liste des données pseudonymisées pouvant être transmises aux destinataires identifiés ;
- qu'aucune donnée traitée dans le cadre de ce SI ne serait transférée hors de l'UE ;
- que le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) serait traité en tant qu'identifiant national de santé.

23. Si ces précisions n'ont pas été apportées au décret n° 2020-1690 publié le 25 décembre 2020, des modifications ont toutefois été apportées s'agissant de l'information des personnes concernées. Dans son avis, la Commission avait insisté sur la parfaite information des personnes, notamment concernant l'exercice de leurs droits. Le décret a été précisé s'agissant de l'information qui sera apportée aux personnes invitées à se faire vacciner, à celles ayant consenti à la vaccination et aux professionnels de santé participant à la vaccination.

24. La Commission a également été suivie s'agissant de la possibilité pour les personnes d'exercer leur droit d'opposition jusqu'à l'expression d'un consentement à la vaccination, ainsi que pour l'utilisation de leurs données à des fins de recherche. En pratique, le droit d'opposition pourra être exercé par les personnes concernées après la réception des bons de vaccination et, le cas échéant, jusqu'au recueil du consentement à la vaccination par un professionnel de santé. Une fois le consentement à la vaccination exprimé, les personnes concernées pourront uniquement s'opposer à la transmission de leurs données à la CNAM et à la Plateforme des données de santé à des fins de recherche. La Commission considère en effet qu'une fois la vaccination réalisée, le traitement des données répond à un objectif important d'intérêt public, notamment dans le cadre de la pharmacovigilance.

25. La Commission a précisé qu'elle sera vigilante quant aux conditions de mise en œuvre du SI « VACCIN COVID » et qu'elle exercera son pouvoir de contrôle.

- **L'application mobile « TOUSANTICOVID »**

26. Le Gouvernement a déployé, le 22 octobre 2020, une nouvelle version de son application de traçage des cas contacts pour lutter contre la propagation de la covid-19 en France.

L'application a fait l'objet d'évolutions.

27. L'application « TOUSANTICOVID », qui vient remplacer « STOPCOVID »[8], a connu des évolutions successives suite aux annonces du Gouvernement le 22 octobre 2020.

[8] Pour rappel, la CNIL s'est prononcée à plusieurs reprises sur l'application « STOP COVID » dans ses avis en date du 24 avril et 25 mai 2020.

28. L'application de traçage des contacts fournit désormais des informations actualisées sur la circulation du virus et des liens vers d'autres dispositifs numériques du Gouvernement (MesConseilsCOVID, DépistageCovid, etc.). Depuis le 3 novembre 2020, l'application permet également de générer, sur le téléphone de l'utilisateur, une attestation de déplacement dérogatoire et permet à ce dernier de sélectionner une option afin de sauvegarder localement certaines de ses données (nom, date et lieu de naissance, adresse) pour faciliter de futures générations de l'attestation.

29. Par ailleurs, au-delà d'une communication renforcée autour de l'application « TOUSANTICOVID », le Gouvernement fait évoluer sa « doctrine d'usage » à destination de ses utilisateurs afin de sensibiliser sur son utilisation dans des situations à risque, lorsque ces derniers ne sont pas en mesure de s'assurer du respect des gestes barrières (port du masque, respect des distanciations sociales, etc.).

30. Toutefois, les éléments structurants du dispositif ne sont pas impactés par les évolutions de l'application. Ainsi, le protocole « ROBERT », conçu dans une logique de minimisation des données et de protection dès la conception, reste celui utilisé par l'application « TOUSANTICOVID ». Tout comme « STOPCOVID », l'application repose sur une démarche volontaire des personnes et permet la « recherche de contacts » (« *contact tracing* »), grâce à l'utilisation de la technologie « Bluetooth », sans recorir à une géolocalisation des individus.

Une vigilance particulière de la CNIL

31. Si la CNIL considère qu'il n'est pas opportun de règlementer les nouvelles fonctionnalités de l'application « TOUSANTICOVID » présentées ci-dessus[9], elle restera vigilante quant aux éventuelles évolutions d'un dispositif qui a posé des questions inédites en termes de protection des données à caractère personnel et de respect de la vie privée.

32. Elle rappelle notamment qu'elle peut diligenter de nouveaux contrôles, si nécessaire, et qu'elle devrait se prononcer, à nouveau, si le traitement de données venait à faire l'objet de modifications substantielles.

33. La Commission a notamment rendu un avis en urgence le 17 décembre 2020 sur un projet de décret modifiant le décret n° 2021-650 du 29 mai 2020 relatif au traitement de données dénommé « STOPCOVID », qui ne pourra être publié qu'après publication du décret précité.

---

[9] D'une part, l'administration les a déjà mis en œuvre dans le cadre de l'application « TOUSANTICOVID » et certains sites web d'administrations proposent, par ailleurs, des fonctionnalités similaires (notamment pour permettre de générer des justificatifs), sans être pour autant prévus par des textes règlementaires. D'autre part, les données à caractère personnel étant stockées et traitées uniquement localement sur le terminal de l'utilisateur, à sa discrétion et pour son compte, il ne semble pas que les autorités publiques soient responsables de ces traitements, la seule mise à disposition d'un logiciel au public ne constituant pas la mise en œuvre d'un traitement de données à caractère personnel.

II- SUR LE MAINTIEN DES DISPOSITIFS AU REGARD DES PRINCIPES DE NÉCESSITÉ ET DE PROPORTIONNALITÉ

34. L'article 11 de la loi du 11 mai 2020 a été modifié par la loi du 14 novembre 2020 afin de permettre le maintien des systèmes d'information « CONTACT COVID » et « SI-DEP » pour la durée strictement nécessaire à l'objectif de lutte contre la propagation de l'épidémie de covid-19 ou, au plus tard, jusqu'au 1er avril 2021. Pour rappel, la durée maximale de maintien de ces traitements avait été initialement fixée par la loi au 11 janvier 2021.

35. La CNIL a rappelé, dans son avis du 10 septembre 2020 sur le fonctionnement des systèmes d'information Covid-19, le caractère dérogatoire des différents traitements mis en œuvre, qui ne peut être justifié que si leur utilité est suffisamment avérée au regard de l'évolution sanitaire du pays.

36. Elle rappelait également 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.

37. Elle avait ainsi regretté 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 de l'époque. Elle a donc demandé à « *disposer d'indicateurs de performance des systèmes d'information déployés, afin de pouvoir mesurer leur efficacité au regard des objectifs poursuivis* » et d'une grille d'analyse établie au regard d'indicateurs d'efficacité sanitaire.

38. La demande de la Commission a été prise en compte lors de la modification de l'article 11 de la loi du 11 mai 2020 par la loi du 14 novembre 2020 qui précise que le rapport trimestriel du Gouvernement adressé au Parlement sur l'application de ces mesures doit comprendre : « *des indicateurs d'activité, de performance et de résultats quantifiés adaptés aux priorités retenues* ».

39. S'agissant de l'utilité et de l'efficacité de l'application « TOUSANTICOVID » sur la stratégie sanitaire globale, la Commission rappelle qu'elle avait demandé, dans son avis du 25 mai 2020, 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. A ce titre, elle avait invité le Gouvernement, dans son avis trimestriel du 10 septembre 2020, à établir une grille d'analyse au regard d'indicateurs d'efficacité sanitaire.

40. **En premier lieu**, au-delà d'une augmentation du nombre de téléchargements de l'application depuis la sortie de la version « TOUSANTICOVID », la Commission relève que le nombre d'utilisateurs se déclarant comme dépistés ou diagnostiqués à la covid-19 ainsi que celui des utilisateurs notifiés ont connu une croissance significative[10]. Par ailleurs, elle prend acte du fait que l'impact du changement des paramètres de notification des contacts à risque (critères de distance et de durée du contact au regard du risque de contamination[11]) sur le nombre d'utilisateurs notifiés est particulièrement important.

41. **En deuxième lieu,** la Commission observe que l'application a été enrichie de nouvelles fonctionnalités : information des utilisateurs sur la circulation du virus au niveau national et local ainsi que sur les mesures ou actions de promotion, de prévention et d'éducation pour la santé, orientation des utilisateurs vers d'autres outils numériques mis en œuvre pour la gestion de l'épidémie, etc. Elle considère que l'augmentation de l'adhésion de la population à l'application est susceptible de participer au renforcement de son utilité sanitaire, sous réserve de son activation.

42. **En troisième lieu**, interrogé sur ce point lors des contrôles de novembre 2020, le ministère des solidarités et de la santé a indiqué qu'une étude intitulée « *COVID-19 : identification des attentes en matière de numérique, les leviers au téléchargement et à l'utilisation de l'appli STOPCOVID* » a été publiée par la société KANTAR au mois d'août 2020. En outre, la Commission note que l'application a fait mention, à travers la fonctionnalité récente de fils d'actualités, d'une étude de l'Institut national de la santé et de la recherche médicale (INSERM) relative à l'efficacité de l'application dans la stratégie sanitaire globale publiée en octobre 2020.

43. La Commission en prend note et estime qu'il est indispensable de développer des initiatives et des indicateurs permettant d'évaluer pleinement l'effectivité sanitaire du dispositif dans le cadre de la lutte contre l'épidémie de covid-19**.** A cet égard, elle considère notamment que les métriques de l'application relatives à son efficacité (nombre d'utilisateurs déclarés positifs ainsi que ceux notifiés *via* l'application) pourraient être comparés avec celles des systèmes d'information « CONTACT COVID » et « SI-DEP » afin d'apprécier l'utilité du dispositif sur la stratégie sanitaire globale. En outre, il pourrait notamment être envisagé l'ajout d'une mention dans « CONTACT COVID » permettant d'identifier si la personne a été informée uniquement par l'application « TOUSANTICOVID », ou à la fois par l'application et par les méthodes manuelles de suivi de contact.

---

[10] Au 14 janvier 2021, plus de douze millions de personnes ont téléchargé et activé l'application, plus de cinquante mille personnes ont été notifiées par l'application suite à une exposition à la covid-19 et plus de quatre-vingt-douze mille utilisateurs se sont déclarés comme des cas de covid-19 dans l'application.

[11] L'application envoie dorénavant une alerte aux utilisateurs ayant été récemment en contact avec une personne ayant volontairement déclaré avoir été testée positive au coronavirus durant 5 minutes à moins d'1 mètre ou durant 15 minutes entre 1 et 2 mètres, contre une durée de 15 minutes à moins d'un mètre auparavant.

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

44. Conformément à ce qui avait été développé dans le cadre de la délibération du 10 septembre 2020[12], la Commission a continué à mener de nombreuses investigations autour des dispositifs « SI-DEP » et « CONTACT COVID » et de l'application « TOUSANTICOVID ».

45. Ces vérifications des conditions concrètes de mise en œuvre ont été effectuées dans le cadre de contrôles en ligne, sur audition, sur pièces et sur place. Ce sont en tout vingt-cinq **opérations de contrôle** qui ont été menées entre mai et novembre 2020 : six concernant « SI-DEP », douze concernant « CONTACT COVID », sept concernant « TOUSANTICOVID » (en incluant celles réalisées sur « STOPCOVID »).

46. Le présent avis comporte des éléments synthétiques issus des constatations opérées par la Commission dans le cadre de la seconde phase de vérifications qui s'est déroulée de septembre à novembre 2020. Il fait également état des échanges réguliers qui ont eu lieu avec le ministère des solidarités et de la santé, la CNAM et les ARS au cours de cette période.

A. Le contrôle des fichiers « SI-DEP » et « CONTACT COVID »

47. Les investigations des traitements « SI-DEP » et « CONTACT COVID » continuent à être menées simultanément depuis le mois de septembre 2020.

48. Pour le traitement « SI-DEP », un contrôle sur place et des investigations supplémentaires ont eu lieu depuis la publication du premier avis de la Commission, auprès de l'Assistance publique des hôpitaux de Paris (AP-HP) qui assure la mise en œuvre opérationnelle du traitement « SI-DEP ».

49. Pour le traitement « CONTACT COVID », des contrôles sur audition, en ligne et sur place ont eu lieu auprès de la CNAM, d'une caisse primaire d'assurance maladie (CPAM) et de deux ARS. Des contrôles sur pièces auprès du Conseil national de l'ordre des médecins (ci-après « CNOM ») et du Conseil national de l'ordre des pharmaciens (ci-après « CNOP ») ont également été menés.

50. Les points de vérification ont principalement porté sur :

- les modalités d'information des personnes ;
- la sécurité des systèmes d'information ;
- les flux de données et les destinataires ;
- les modalités de conservation des données.

[12] 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)

- **LE FICHIER « SI-DEP »**

51. Pour rappel, le fichier « SI-DEP » est un système d'information national de dépistage dont le responsable est le ministre chargé de la santé (direction générale de la santé). Le fichier « SI-DEP » permet la centralisation des résultats des tests au coronavirus SARS-CoV-2 réalisés par des laboratoires publics ou privés ou des professionnels de santé habilités, afin de les mettre à disposition des organismes chargés de déterminer les personnes ayant été en contact avec des personnes infectées, de réaliser des enquêtes sanitaires en présence de cas groupés pour rompre les chaînes de contamination, d'orienter, de suivre et d'accompagner les personnes concernées, et de faciliter le suivi épidémiologique aux niveaux national et local et la recherche sur le virus de même que les moyens de lutter contre sa propagation.

52. Les opérations de contrôle du traitement « SI-DEP » effectuées en octobre et novembre 2020 ont principalement eu pour objet de vérifier le respect de la durée de conservation des données fixée par le décret précité, ainsi que les modalités de transmission à la plateforme des données de santé visée à l'article L. 1462-1 du code de la santé publique (dite « *Health Data Hub* »).

53. Dans la continuité de ses précédentes observations, la Commission a de nouveau constaté l'importance des efforts mis en œuvre par le ministère des solidarités et de la santé et l'AP-HP pour assurer la conformité du traitement « SI-DEP » aux dispositions applicables. Ces efforts doivent être analysés à la lumière du volume important des données traitées (plus de 16 millions de tests réalisés entre mai et octobre 2020), en provenance de nombreuses sources, et à destination de plusieurs acteurs tels que la CNAM, Santé publique France, chacun ayant une modalité spécifique de réception des fichiers.

54. La délégation a ainsi constaté **un niveau de conformité satisfaisant** s'agissant du respect des durées de conservation des données.

55. Les échanges avec la direction générale de la santé ont également permis de constater que **les remarques effectuées par la Commission à l'issue de la première phase de contrôle en septembre ont été prises en compte** par les services concernés. Un plan d'action a été défini et est en cours de déploiement concernant la gestion de certains comptes utilisateurs et la traçabilité des accès.

56. Enfin, la transmission de données vers la plateforme des données de santé ayant été reportée par le Gouvernement, elle n'était pas encore effective lors des vérifications sur place menées par la Commission en octobre. Il a néanmoins été constaté que les modalités techniques de cette transmission sont déjà configurées et, à ce stade, apparaissent assurer un niveau de confidentialité des données suffisant avant que celles-ci soient communiquées à la CNAM, en charge du téléversement des données vers la plateforme.

57. **En l'état actuel des vérifications, la Commission considère que les conditions de mise en œuvre du fichier « SI-DEP » n'appellent pas de mesure particulière de sa part.**

- **LE FICHIER « CONTACT COVID »**

58. Comme annoncé par la Commission dans le cadre de son précédent avis, les contrôles opérés entre septembre et novembre 2020 ont porté sur les modalités de mise en œuvre du portail d'accès au traitement « CONTACT COVID » à destination des partenaires ne disposant pas d'un compte « amelipro » et sur l'information délivrée aux patients par les médecins et les pharmaciens sur ce fichier.

59. Pour rappel, le traitement « CONTACT COVID » permet :

- aux médecins de ville/établissements de santé/centres de santé d'initier une fiche de suivi des « patients zéro » et de leurs cas contacts (**niveau 1**) ;
- au personnel habilité de l'assurance maladie (ou aux personnes auxquelles cette mission est déléguée par les textes) (**niveau 2**) :
  - de compléter et d'affiner, si nécessaire, la fiche des « patients zéro » et la liste de leurs cas contacts ;
  - d'informer les cas contacts des consignes relatives à l'isolement, de tests et autres conduites à tenir ;
  - d'assurer le suivi, depuis septembre 2020, des chaînes de transmission en milieu scolaire ou dans une université ;
- aux ARS d'assurer (**niveau 3**) :
  - leurs missions de suivi des cas contacts ;
  - la gestion des situations nécessitant une prise en charge spécifique. Il s'agit par exemple des chaînes de transmission, notamment dans les entreprises ou les crèches.

Sur les traitements effectués par la CNAM dans le cadre de « CONTACT COVID »

60. A titre liminaire, il convient de souligner la bonne coopération entre la CNIL et la CNAM, et la réactivité de cette dernière. Par exemple, la CNAM a supprimé, à la demande de la CNIL, le recours jugé problématique au dispositif « reCaptcha ». Les vérifications effectuées ont permis de constater **le déploiement d'un plan d'action qui a amélioré les modalités de mise en œuvre du traitement et corriger les mauvaises pratiques** qui avaient été relevées par la Commission dans son précédent avis.

61. Tout d'abord, la CNAM a modifié en profondeur **les conditions d'accès au portail** et mis en place plusieurs profils permettant la gestion des droits au sein de l'application « CONTACT COVID ». L'utilisation de ces profils (super- administrateurs, administrateurs locaux et utilisateurs) est formalisée au sein d'un diaporama, dans des modes d'emploi et des guides méthodologiques à destination de chacun des profils utilisateurs.

62. Ensuite, **s'agissant de l'information délivrée aux « patients zéro » et aux « cas contacts »**, la CNAM a organisé une réunion auprès des fédérations hospitalières afin notamment de leur rappeler que les mentions d'information relatives à « CONTACT COVID » devaient être affichées au public au sein des établissements de santé. Pour aller plus loin, des affichettes d'information mises à jour devaient être adressées, au cours du mois de décembre 2020, par la CNAM aux fédérations hospitalières.

63. Sur ce point, tout en rappelant ne pas être responsable du traitement « CONTACT COVID » et donc pas tenus à une obligation d'information des personnes, **le CNOP et le CNOM ont tous deux procédé à une information des médecins et des pharmaciens** à travers des articles diffusés sur le site web des conseils de l'ordre (renvoyant notamment aux guides pratiques présents sur le web *ameli.fr*). Ces contenus ont été relayés soit par l'intermédiaire des lettres électroniques d'actualité des ordres, soit au travers des réseaux sociaux des ordres (Facebook, Twitter et Linkedln).

64. Enfin, la CNAM a en parallèle pris les mesures suivantes :

- les **guides méthodologiques** à destination des acteurs intervenant à chaque niveau du dispositif ont été mis à jour à la suite de la création de comptes partenaires pour les établissements de santé et les ARS ;
- les CPAM **recourent systématiquement aux messageries sécurisées** de santé pour transmettre des fichiers aux ARS ;
- la CNAM a rappelé aux fédérations hospitalières que les fichiers de tableurs (au format « Excel ») créés par les établissements de santé à destination des CPAM locales avant l'accès au portail « CONTACT COVID » devaient être supprimés ;
- les listes des cas contacts et patients zéro identifiés au sein d'établissements scolaires de l'éducation nationale et de l'enseignement supérieur sont directement transmises aux CPAM par l'intermédiaire d'une plateforme sécurisée (sans que l'ARS serve d'intermédiaire). Les délégations de contrôle ont pu à ce titre constater au sein d'une CPAM la suppression immédiate de ces fichiers sur la plateforme ainsi que sur le répertoire réseau destiné à recevoir les fichiers précédemment mentionnés, après leur intégration dans l'outil CONTACT COVID ;
- depuis le 28 juillet 2020, un système de suppression automatique des données de plus de trois mois contenues dans l'outil « CONTACT COVID » est mis en œuvre chaque jour. Les délégations de contrôle ont d'ailleurs pu constater l'effectivité de cette suppression lors d'un contrôle au sein d'une CPAM.

65. **En deuxième lieu,** malgré ces mesures, les vérifications effectuées ont révélé **de nouvelles mauvaises pratiques.**

66. Sur ce point, il convient au préalable de souligner que certains des dysfonctionnements constatés sont liés à l'augmentation brutale de la propagation de la covid-19 et aux adaptations qu'il a fallu effectuer en urgence pour y faire face.

67. En effet, entre le 10 octobre et le 9 novembre 2020, les agents de la CNAM et des CPAM locales ont en moyenne procédé à la création d'environ 120 000 fiches par jour, ce qui a nécessité la mise en œuvre dans les plus brefs délais de nouveaux modes de contact des personnes à risques et, notamment, l'information des cas contacts par l'envoi de SMS contenant un lien URL.

68. Parmi ces mauvaises pratiques, il a été relevé que :

- les conditions d'authentification à l'outil « CONTACT COVID » de certains profils « utilisateurs » ne constituent pas une authentification forte au sens de la Politique générale des systèmes d'information de santé (PGSSI-S)[13]. Néanmoins, dans l'attente de la généralisation de l'authentification forte, des mesures techniques et organisationnelles ont été mises en place pour renforcer le mode d'authentification actuellement mis en œuvre pour ces profils ;
- de manière isolée, certains comptes utilisateurs étaient des comptes génériques partagés par plusieurs utilisateurs, rendant plus difficile la traçabilité au sein de l'application ;
- la CNAM a pris l'initiative de procéder à l'envoi d'un SMS identique aux cas contacts n'ayant pas pu être joints dans la journée de la création de leur fiche dans l'outil « CONTACT COVID ». Ce SMS contenait une URL raccourcie entraînant la transmission de données à caractère personnel à un tiers (la société BITLY) non habilité à héberger des données de santé. Cette pratique ponctuelle n'a duré que du 23 octobre au 2 novembre 2020.

69. Compte tenu de ce qui précède, la présidente de la Commission a décidé d'adresser un courrier rappelant la CNAM à ses obligations et faisant état d'une part, des mauvaises pratiques relevées et, d'autre part, des mesures à mobiliser pour y remédier.

Sur les traitements effectués par les ARS dans le cadre de « CONTACT COVID »

70. A titre liminaire, il convient de rappeler que les ARS sont des établissements publics, autonomes moralement et financièrement, placés sous la tutelle du ministère des solidarités et de la santé[14].Il a été constaté de nombreuses disparités concernant les pratiques des ARS dans le cadre de l'activité de suivi de contacts (« *contact tracing* ») de niveau 3.

71. Ainsi, les vérifications effectuées auprès d'une des ARS contrôlées **ont permis de constater la mise en œuvre de nombreuses mesures pour garantir de façon optimale le respect des données des personnes** par l'intermédiaire d'un outil approprié à la gestion de l'épidémie (outil hébergé par un hébergeur de données de santé sur initiative de l'ARS en question, suppression automatique des données signalées depuis plus de trois mois, etc.).

72. A l'inverse, la Commission a constaté plusieurs manquements à l'égard d'un logiciel de suivi des « patients zéro » et des cas contacts développé spécifiquement par une ARS. Cet outil a pour finalité l'investigation et le suivi épidémiologique des cas confirmés de covid-19 et des cas contacts, en vue d'identifier les chaînes et cas groupés de contamination et de prendre les mesures destinées à limiter la propagation de l'épidémie. Ce traitement utilise des données à caractère personnel

[13] La PGSSI-S est un corpus documentaire conforme au cadre juridique de la santé numérique et à la politique de sécurité du système d'information du ministère chargé des Affaires Sociales. Conformément à l'article L. 1110-4-1 du code de la santé publique, les référentiels de sécurité élaborés par l'ANS peuvent être rendus opposables par arrêté du ministre de la santé.

[14] Articles L. 1432-1 et suivants du code de la santé publique

provenant de « CONTACT-COVID » et des données issues de l'entretien téléphonique avec la personne concernée.

73. Si le décret n° 2020-551 du 12 mai 2020 modifié a implicitement autorisé l'ensemble des traitements, mis en œuvre notamment par les ARS, aux fins de lutter contre la propagation de l'épidémie de covid-19, ce décret ne les réglemente pas en détail et vise essentiellement la mise en œuvre du système d'information « CONTACT COVID », résultant de l'adaptation d'amelipro. Dès lors, s'il doit être regardé comme autorisant la mise en œuvre de traitements de données à caractère personnel aux fins d'enquêtes sanitaires par les ARS, le décret n° 2020-551 du 12 mai 2020 modifié ne réglemente pas le traitement mis en œuvre spécifiquement par l'ARS via son logiciel de suivi des « patients zéro » et des cas contacts.

74. Cet outil est défini et mis en œuvre sous la seule responsabilité de cette ARS et est donc soumis aux dispositions du RGPD, de la loi « informatique et libertés » et de la loi n° 2020-546 du 11 mai 2020 modifiée qui l'autorise. Comme l'indique l'article 14 du décret n° 2020-551 du 12 mai 2020, les traitements mis en œuvre par les ARS le sont sur le fondement de l'article 67 de la loi du 6 janvier 1978, qui dispense d'autorisation préalable les traitements de données de santé mis en place par certains organismes pour répondre à une situation d'urgence sanitaire.

75. S'agissant de cet outil, la délégation a constaté certains manquements :

- Un manquement à l'obligation de respecter une durée de conservation des données proportionnée à la finalité du traitement : s'il ressort du contrôle sur place qu'une politique de durées de conservation des données est en cours d'élaboration par l'ARS, il a néanmoins été constaté en pratique qu'elle conserve sans restriction de durée les données contenues dans le logiciel spécifiquement développé depuis la date de la mise en œuvre de l'activité de suivi de contacts de niveau 3. L'ARS a également indiqué ne pas procéder à un archivage intermédiaire des données.

  La CNIL a également observé que les informations recueillies par l'investigateur à la suite de l'appel téléphonique à un « patient zéro » afin d'identifier ses cas contacts sont renseignées dans un tableur. Ce fichier est ensuite adressé à la CNAM par une messagerie sécurisée de santé pour qu'elle reporte les données dans le téléservice « CONTACT COVID ». La Commission relève que cette pratique est prévue par les circulaires MINSANTE n° 99 et n° 155. Elle considère cependant qu'elle entraîne une dispersion des données dans les messageries. Les fichiers sont ensuite, au moins en partie, conservés dans les serveurs. Cette pratique n'est pas, faute de précaution suffisantes, de nature à garantir l'effectivité du respect de durées de conservation raisonnables. La Commission demande, par exemple, soit de cesser de transmettre des tableurs via des messageries sécurisées de santé et d'alimenter les données relatives aux cas contacts du patient zéro dans le logiciel « CONTACT COVID » prévu à cet effet, soit de procéder à la suppression immédiate des courriels contenant les tableurs à la suite de leur envoi via les messageries sécurisées de santé, soit de procéder à un archivage régulier des courriels contenant ces tableurs.

- Un manquement à l'obligation d'assurer la sécurité des données : l'outil développé spécifiquement par l'ARS est accessible depuis un dossier partagé à accès restreint administré et hébergé par cette dernière. Aucune authentification supplémentaire n'est nécessaire pour accéder à cette application. Cette absence d'authentification ne permet pas de retracer finement les événements en cas d'accès à cette application par un tiers non autorisé, ni de déterminer par l'intermédiaire de quelle personne ce tiers y a eu accès.

- Au sein de cette ARS, il a également été relevé un manquement à l'obligation de réaliser une AIPD : conformément à l'article 67 de la loi « informatique et libertés » modifiée, les traitements de données à caractère personnel mis en œuvre dans le domaine de la santé par les ARS et ayant pour seule finalité de répondre à une alerte sanitaire et d'en gérer les suites, doivent faire l'objet d'une AIPD.

76. A la lumière des constatations effectuées, **la présidente de la Commission a adressé une mise en demeure de se conformer** aux exigences du RGPD dans un délai d'un mois à cette ARS.

77. Enfin, la Commission souhaite faire part de certaines recommandations à l'ensemble des ARS s'agissant de mauvaises pratiques relevées lors des contrôles.

78. Tout d'abord, s'agissant de l'information des personnes, l'information qui est délivrée aux personnes concernant la réutilisation des données issues de « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible. La Commission invite les ARS à veiller à faire preuve de vigilance sur ce point. En particulier, la délégation a relevé dans une des ARS contrôlés que, lors de l'entretien téléphonique, les « patients zéro » ou cas contacts ne sont pas mis en mesure d'être redirigés vers une information exhaustive sur le traitement de leurs données à caractère personnel, alors même qu'un courriel leur est systématiquement adressé sur les consignes sanitaires à respecter. Dès lors, la Commission recommande dans un premier temps de procéder à l'information des « patients zéro » et cas contacts lors des appels téléphoniques, par exemple, dans le cas d'un serveur vocal, par une mention orale automatisée en début de conversation intégrant un renvoi vers le site web ou vers une touche du téléphone pour la délivrance de l'ensemble des mentions d'information prescrites. Dans un second temps, la Commission recommande de prévoir un accès immédiatement à la suite de l'appel téléphonique à l'information délivrée sur le site, par exemple, en intégrant un lien hypertexte dans les courriels adressés à la suite de chaque appel téléphonique aux « patients zéro ».

79. Ensuite, les délégations ont relevé la présence de champs commentaires au sein des outils utilisés dans le cadre de la gestion de l'épidémie de covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. La CNIL recommande de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.

80. S'agissant de l'ARS au sein de laquelle les dysfonctionnements sont plus mineurs, la Commission a adressé un courrier lui rappelant ses obligations et les mesures à prendre pour se mettre en conformité.

81. **En parallèle, des courriers ont été envoyés simultanément au ministère des solidarités et de la santé afin de l'alerter sur les mauvaises pratiques précitées.**

82. Des courriers ont également été envoyés par la Commission à toutes les ARS afin de leur rappeler les mesures nécessaires à la protection des données des personnes concernées issues de l'outil « CONTACT COVID ».

B. Le contrôle de l'application TOUSANTICOVID

83. Le 2 juin 2020, l'application « STOPCOVID » a été déployée par le ministère des solidarités et de la santé dans les magasins d'applications mobiles (iOS et Android) accessibles au grand public.

84. Une première phase de contrôle a eu lieu au mois de juin 2020. A la suite de ces contrôles, la présidente de la Commission a mis en demeure le 15 juillet 2020 le ministère des solidarités et de la santé de mettre en conformité le traitement des données en lien avec l'application « STOPCOVID » au RGPD et à l'article 82 de la loi du 6 janvier 1978 modifiée. Le ministère s'étant mis en conformité dans le délai imparti, la présidente de la Commission a prononcé la clôture de cette mise en demeure le 3 septembre 2020.

85. Le 22 octobre 2020, le ministère des solidarités et de la santé a publié une nouvelle version de l'application « STOPCOVID », désormais dénommée « TOUSANTICOVID ».

86. La Commission a effectué de nouvelles vérifications sur cette application auprès du ministère des solidarités et de la santé, responsable de ce traitement, ainsi qu'auprès des 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.

87. Ces vérifications, effectuées en octobre et novembre 2020, ont notamment porté sur la pérennité des mesures suite à la mise en demeure du 15 juillet 2020 et sur la conformité des nouvelles fonctionnalités de l'application au RGPD et à la loi du 6 janvier 1978 modifiée.

S'agissant des mesures de mise en conformité suite à la mise en demeure

88. Dans sa mise en demeure telle que reprise dans son précédent avis, la Commission avait relevé plusieurs mauvaises pratiques liées au fonctionnement de l'application « STOPCOVID » dans sa version v1.0.

89. Il a été constaté qu'il n'est plus possible d'utiliser l'application dans cette version v1.0.

90. Les filtres de l'historique des contacts au niveau du téléphone de l'utilisateur ont été activés. Sur ce point, le ministère s'est mis en conformité en forçant la mise à jour de l'application vers la version v1.1.

91. Il a également été constaté que la technologie reCaptcha de la société Google mise en œuvre dans la version v1.0. n'est plus utilisée. L'arrêt de l'utilisation de cette technologie est mentionné dans l'AIPD.

92. Le ministère s'est par ailleurs mis en conformité en ajoutant dans sa politique de confidentialité son sous-traitant INRIA comme destinataire des données. La délégation a constaté, lors du contrôle, que cette mention y figurait.

93. Le ministère s'est mis en conformité en complétant les clauses relatives au RGPD dans le contrat de sous-traitance le liant à INRIA.

94. Dorénavant, conformément à l'article 35 du RGPD, il est mentionné dans l'AIPD 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 visant à empêcher les attaques par déni de service distribué (« anti-DDoS ») de la société ORANGE.

S'agissant de la nouvelle version de l'application dénommée « TOUSANTICOVID »

95. Le 22 octobre 2020, le ministère des solidarités et de la santé a déployé une mise à jour de l'application « STOPCOVID », dénommée « TOUSANTICOVID ».

96. L'application « TOUSANTICOVID » propose de nouvelles fonctionnalités en plus de la fonctionnalité principale de suivi de contacts, telles que l'accès à des informations sur l'épidémie et un accès facilité à l'attestation dérogatoire de déplacement.

97. Cette dernière fonctionnalité s'est d'abord matérialisée par un lien renvoyant vers le site du ministère de l'intérieur, puis une nouvelle version a été déployée le 3 novembre 2020 permettant de générer directement l'attestation dans l'application et de la conserver dans le terminal de l'utilisateur.

98. Il a été constaté qu'aucune des données traitées dans le cadre de ces nouvelles fonctionnalités, telles que mises en œuvre à date des contrôles de novembre 2020, ne fait l'objet d'un traitement sur le serveur central, dans une logique de minimisation des données et de protection des données dès la conception et par défaut.

99. Au cours des contrôles du mois de novembre 2020, le ministère des solidarités et de la santé a indiqué que le développement de nouvelles fonctionnalités était à l'étude, dont une permettant à l'utilisateur de filtrer les informations sanitaires en fonction d'un code postal de son choix. Ces nouvelles fonctionnalités ont fait l'objet d'une saisine de la Commission, telle que décrite au paragraphe 33 du présent avis.

C. Autres contrôles – les cahiers de rappel

100. Outre les contrôles effectués sur les principaux systèmes d'information « SI-DEP », « CONTACT COVID » et « TOUSANTICOVID », la Commission procède également à des vérifications sur des fichiers du quotidien liés au suivi de de la pandémie.

101. Elle a ainsi procédé à des contrôles concernant la tenue de « cahiers de rappel » mis en œuvre à partir du mois d'octobre 2020, par certains établissements de restauration et de débits de boisson situés dans les zones d'alerte maximale pour respecter le protocole sanitaire renforcé. Ces établissements collectaient les coordonnées de leurs clients afin de les communiquer, sur demande, aux autorités sanitaires pour les aider dans leurs recherches de « cas contacts ». La CNIL a notamment publié sur son site des exemples de cahiers de rappels à l'attention des professionnels[15].

102. Les investigations menées à la suite de plusieurs signalements sur les réseaux sociaux ont permis de constater plusieurs manquements au RGPD, dont le détournement de finalité (certains organismes se réservaient la possibilité d'utiliser les données collectées à des fins de prospection), la collecte de données non pertinentes et l'absence de mentions d'information sur les formulaires de collecte de données.

103. Les organismes concernés ayant indiqué avoir supprimé les données collectées et ne pas les avoir utilisées des fins commerciales, la CNIL a décidé de les rappeler à l'ordre tout en les invitant à se mettre en conformité à l'avenir dans l'hypothèse où la tenue de « cahiers de rappel » serait de nouveau nécessaire.

D. Une procédure de contrôle continue

104. La Commission rappelle 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.

105. Elle réitère également que les vérifications menées donnent toujours lieu à des échanges très réguliers et approfondis avec le ministère des solidarités et de la santé pour le dispositif « SI-DEP », mais également avec les autres organismes administrateurs et utilisateurs de l'application « CONTACT COVID » (CNAM, ARS, établissements de santé, etc.). Le présent avis ne constitue ainsi qu'une synthèse de ces échanges et des constatations effectuées lors de la deuxième phase de contrôle.

106. A cet égard, **une troisième phase de contrôles** est d'ores et déjà prévue et débutera dès le mois de janvier 2021. Elle portera principalement sur les points ci-dessous.

[15]https://www.cnil.fr/fr/cahier-de-rappel-exemples-de-formulaire-de-recueil-de-donnees-et-mentions-dinformation-rgpd

107. Concernant le traitement « SI-DEP », outre toute modification technique apportée au traitement, les points suivants feront l'objet d'une attention particulière :

- la mise en œuvre effective des transmissions à la plateforme des données de santé ;
- les potentielles évolutions du décret encadrant le traitement, tenant notamment compte de l'intégration à « SI-DEP » des résultats des tests antigéniques et tenant compte de l'évolution des données collectées ;
- le respect des durées de conservation ;
- la mise en œuvre du plan d'action défini par la direction générale de la santé.

Concernant le traitement « CONTACT COVID » :

- l'accès au portail « accès partenaires » « CONTACT COVID » de nouveaux utilisateurs (pharmaciens, universités, sous-traitants de la CNAM, etc.) ;
- la délivrance des tests antigéniques ;
- l'effectivité des mesures prévues pour l'exercice des droits des personnes concernées, en particulier au sein des universités et des établissements scolaires ;
- l'utilisation des données issues de « CONTACT COVID » par d'autres ARS dans le cadre de leur mission de suivi de contacts de niveau 3.

Concernant le traitement « TOUSANTICOVID » :

- les potentielles évolutions du décret encadrant le traitement, tenant notamment compte de l'intégration dans l'application « TOUSANTICOVID » des fonctionnalités liées à l'attestation dérogatoire de déplacement ;
- les mesures visant à évaluer l'efficacité et l'utilité de l'application dans le cadre de la lutte contre l'épidémie ;
- le cas échéant, la conformité des potentielles nouvelles fonctionnalités.

Concernant le traitement « VACCIN COVID » :

- des contrôles seront conduits dans les prochaines semaines pour s'assurer des conditions de mise en œuvre du traitement.

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

109. Enfin, **une ultime campagne 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.

110. Ce dernier point concerne également l'application « TOUSANTICOVID ».

La Présidente

Marie-Laure DENIS

ANNEXE 1 : Description des traitements « SI-DEP », « CONTACT COVID » et « TOUSANTICOVID »

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 ou des professionnels de santé habilités. 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) :
    - de compléter et d'affiner, si nécessaire, la fiche du « patient 0 » et la liste de ses « cas contacts » ;
    - d'appeler les « cas contacts » pour leur communiquer les consignes relatives aux mesures d'isolement, de tests et autres conduites à tenir ;
- aux Agences régionales de santé (ARS) d'assurer (niveau 3) :
    - leurs missions de suivi des « cas contacts » ;
    - la gestion des situations nécessitant une prise en charge spécifique. Il s'agit par exemple des chaines de transmission en milieu scolaire, dans un établissement de santé ou dans un foyer de jeunes.

L'application « STOPCOVID », remplacée par l'application « TOUSANTICOVID » 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 2 : 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 ;
25 novembre 2020 : audition devant la mission d'information de la commission des lois de l'Assemblée nationale relative au régime juridique de l'état d'urgence sanitaire ;

Liste des avis rendus sur les quatre traitements SIDEP, CONTACT COVID, VACCIN COVID et STOPCOVID/TOUSANTICOVID :

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 ;

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) ;

Délibération n° 2020-108 du 5 novembre 2020 portant avis sur un projet de décret 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 ;

Délibération n° 2020-126 du 10 décembre 2020 portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre le coronavirus SARS-CoV-2 ;

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 modifiée 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. **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 ;

3. **Loi n° 2020-1379 du 14 novembre 2020 autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise sanitaire et modifiant la loi n°2020-546 du 11 mai 2020 :** autorise la prolongation de la durée de mise en œuvre des systèmes d'information « CONTACT COVID » et « SI-DEP » jusqu'au 1er avril 2021 au plus tard ; Allonge la durée de conservation des données pseudonymisées traitées à des fins de surveillance épidémiologique et de recherche sur le virus jusqu'au 1 er avril 2021 ; La finalité des SI covid-19, relative à l'identification des personnes infectées et à la prescription et la réalisation des examens de biologie, est étendue à la prescription et à la réalisation d'examens de dépistage sérologique ou virologique, afin de prendre en compte l'évolution des modalités de réalisation des examens de dépistage par des professionnels de santé habilités (liste fixée par décret) ;

4. **Décret n° 2020-551 du 12 mai 2020 modifié relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 modifiée prorogeant l'état d'urgence sanitaire et complétant ses dispositions :** création des traitements « SI-DEP » et « CONTACT COVID » ;

5. **Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « STOPCOVID » :** institue l'application « STOPCOVID » ;

6. **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 ;

7. **Décret n° 2020-1385 du 14 novembre 2020 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 :** prolongation des SI covid-19 jusqu'au plus tard au 1 er avril 2021 ; extension de la remontée des résultats à tous les examens de dépistage (sérologique ou virologique) réalisés par des professionnels de santé figurant sur une liste prévue par décret et habilités à la réalisation de ces tests ; ajout de données collectées, de personnes accédant et enregistrant les données, de destinataires des données, etc.

8. **Décret n° 2020-1387 du 14 novembre 2020 fixant la liste des professionnels de santé habilités à renseigner les systèmes d'information mentionnés à l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions :** médecins, biologistes médicaux, pharmaciens et infirmiers.

9. **Décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la covid-19 :** porte création du système d'information « SI VACCIN » visant à permettre le déroulement et le suivi de la campagne de vaccination contre le coronavirus SARS-CoV-2.

10. **Arrêté du 10 juillet 2020 modifié 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).

11. **Arrêté du 9 octobre 2020 modifiant 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 ;**

12. **Arrêté du 16 octobre 2020 modifiant 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 :** 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 des dispositions prises en application de l'article 41 de la loi du 24 juillet 2019 susvisée (décret SNDS) - suppression de la date limite du 30 octobre 2020 pour traiter les données.

13. **Arrêté du 26 octobre 2020 modifiant l'arrêté du 10 juillet 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 depuis mai 2020

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 » :

La Caisse nationale de l'Assurance Maladie (CNAM) ;
Un établissement de santé recevant des malades en consultation ;
Des Caisses Primaires d'Assurance Maladie (CPAM) ;
Des agences régionales de santé (ARS) ;
Le Conseil national de l'Ordre des médecins (CNOM) ;
Le Conseil national de l'Ordre des pharmaciens (CNOP).

Traitement « STOPCOVID » / « TOUSANTICOVID » :

Le ministère des solidarités et de la santé ;
L'Institut national de recherche en sciences et technologies du numérique (INRIA) ;