Délibération CNIL n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (demande d'avis n° 20008032)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre des solidarités et de la santé d'une demande d'avis concernant un projet de décret relatif à l'application mobile dénommée StopCovid ,

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, notamment son article 6-III ;

Vu la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, notamment son article 4 ;

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

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, notamment son article 9 ;

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

Vu la 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 ;

Après avoir entendu Mme Marie-Laure DENIS, présidente, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;

Emet l'avis suivant :

La Commission nationale de l'informatique et des libertés (ci-après la Commission) a été saisie en urgence par le ministre des solidarités et de la santé (ci-après le ministère), le 15 mai 2020, d'une demande d'avis concernant un projet de décret relatif à l'application mobile

dénommée StopCovid , en application des dispositions du III de l'article 6 de la loi n° 78-17 du 6 janvier 1978 susvisée (ci-après la loi Informatique et Libertés). Conformément à ces dispositions, le présent avis devra faire l'objet d'une publication avec le décret correspondant.

Cette saisine intervient dans le contexte de l'épidémie de covid-19, et plus particulièrement de la stratégie dite de déconfinement . Dans ce cadre, le Gouvernement envisage de mettre en œuvre une application, dénommée StopCovid , disponible sur ordiphones (smartphones) et, le cas échéant, sur d'autres équipements mobiles. Elle vise à informer les personnes utilisatrices qu'elles ont été à proximité de personnes diagnostiquées positives à la covid-19 et disposant de la même application, cette proximité induisant un risque de transmission du virus SARS-CoV-2.

La Commission s'est prononcée, dans son avis du 24 avril 2020, sur la conformité générale aux règles de protection des données à caractère personnel d'un dispositif de suivi de contacts tel qu'envisagé alors par le Gouvernement. La présente saisine sur un projet de décret relatif à l'application dénommée StopCovid , accompagnée de l'analyse d'impact sur la protection des données (ci-après AIPD) relative au dispositif envisagé, précise les conditions de mise en œuvre projetées de l'application de suivi de contacts. Ce traitement de données à caractère personnel, qui doit être conforme aux dispositions applicables du règlement (UE) 2016/679 du 15 avril 2016 susvisé (ci-après le RGPD) et de la loi Informatique et Libertés , appelle les observations suivantes de la part de la Commission.

Sur la nécessité et la proportionnalité du dispositif

La Commission souligne en premier lieu qu'elle a pleinement conscience de la gravité de la crise liée à la situation sanitaire créée par l'épidémie de covid-19, d'une ampleur exceptionnelle. La mise en œuvre du traitement StopCovid s'inscrit dans le cadre de l'action du Gouvernement pour lutter contre l'épidémie et traduit le souhait de ne laisser de côté aucun outil permettant de lutter contre l'épidémie, et notamment de gérer au mieux la période de déconfinement.

La lutte contre cette épidémie, 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 transitoires au droit à la protection de la vie privée et des données à caractère personnel. Elle a ainsi justifié l'autorisation, par la loi du 11 mai 2020 susvisée, de dispositifs reposant sur le traitement de données à caractère personnel, d'une particulière sensibilité et d'ampleur nationale. Les traitements Contact Covid et SI-DEP , qui visent à permettre l'identification des chaînes de contamination du virus SARS-CoV-2 et à assurer le suivi et l'accompagnement des personnes concernées, ont été autorisés à ce titre par le décret du 12 mai 2020 susvisé, pris après l'avis de la Commission en date du 8 mai 2020.

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.

En outre, elle rappelle le caractère sensible, par nature, de la mise en œuvre d'un dispositif de suivi automatique des contacts des utilisateurs d'une application mobile mise à disposition par les autorités publiques. Si la Commission reconnaît que l'application projetée respecte le concept de protection des données dès la conception, une telle collecte, qui a vocation à s'appliquer à la plus grande partie de la population possible, doit en tout état de cause être envisagée avec prudence. Elle renvoie sur ce point à son avis du 24 avril 2020.

En deuxième lieu, en ce qui concerne l'utilité du traitement StopCovid , la Commission avait rappelé, dans son avis du 24 avril 2020, que le dispositif projeté ne serait admissible que si le Gouvernement disposait d'éléments suffisants de nature à établir son utilité pour la gestion de la crise, notamment dans le cadre du déconfinement. En particulier, elle avait insisté sur la nécessaire insertion de ce dispositif dans une politique sanitaire globale.

A cet égard, la Commission relève que le ministère entend compléter, par la mise en œuvre du traitement, le dispositif de traçage des contacts autorisé par le décret susvisé du 12 mai 2020 et ainsi contribuer plus efficacement à la réduction des chaînes de contamination. Le traitement vise ainsi à permettre une information et une alerte plus rapides des cas contacts quant aux risques d'exposition au virus, notamment lorsqu'il s'agit de cas contacts que les personnes contaminées ou exposées ne connaissent pas nécessairement, comme par exemple les personnes croisées dans les transports en commun ou dans les commerces. Il permet également d'alerter certains cas contacts de personnes qui ne souhaiteraient pas répondre aux enquêteurs sanitaires.

Elle relève en outre que le ministère a fait état de plusieurs études scientifiques et épidémiologiques, y compris étrangères, démontrant l'intérêt, pour les autorités sanitaires, de pouvoir disposer d'applications de suivi de contacts , en appui du suivi manuel de propagation des chaînes de transmission, aux fins d'identifier le plus rapidement et largement possible les contacts des cas détectés. Le ministère a précisé que certaines de ces études conduisent à estimer qu'une telle application est utile à la réduction des chaînes de contamination, y compris lorsqu'elle n'est téléchargée que par une partie limitée de la population. Il fait également référence aux positions favorables du conseil scientifique covid-19 et de l'Académie nationale de médecine.

Il y a lieu par ailleurs de tenir compte du caractère incertain des informations dont dispose le ministère en cette matière au début du déploiement de cet outil et de la difficulté de comparer le traitement projeté à ceux déjà expérimentés ou envisagés dans d'autres pays, notamment au sein de l'Union européenne.

L'utilité de l'application vient enfin de ce que le traitement projeté s'articulera avec le dispositif de prise en charge sanitaire des personnes exposées au virus, dès lors que la personne alertée via l'application StopCovid et qui déciderait, à la suite et conformément à cette notification, de consulter un professionnel de santé serait alors enregistrée dans les traitements Contact Covid ou SI-DEP précités.

Au regard de ces éléments, l'utilité de l'application et la nécessité du traitement projeté pour accomplir la mission d'intérêt public ainsi confiée à l'autorité publique, au sens des règles de protection des données, sont suffisamment démontrées en amont de la mise en œuvre du traitement.

En troisième lieu, en ce qui concerne la proportionnalité du dispositif projeté, de nombreuses garanties sont prévues par le ministère afin de limiter les atteintes à la protection des données susceptibles d'être portées par un tel dispositif.

Plusieurs garanties substantielles étaient prévues dès le projet initial du Gouvernement, telles que le choix de stocker dans le serveur central des identifiants pseudonymes de personnes exposées à la maladie et non de personnes contaminées, l'utilisation de la technologie de communication de proximité Bluetooth pour évaluer la proximité entre deux ordiphones et non le recours à une technologie de géolocalisation, le choix d'un dispositif fondé sur le volontariat ou encore le recours à des pseudonymes minimisant les possibilités d'identification des personnes concernées.

En outre, la Commission prend acte que plusieurs des garanties complémentaires qu'elle a demandées dans son avis du 24 avril 2020 ont été intégrées dans le projet du gouvernement. Il en est ainsi, notamment, de la définition précise des finalités du traitement projeté, du fait que la responsabilité du traitement est confiée au ministère en charge de la politique sanitaire ou encore de la mise en œuvre de certaines mesures techniques de sécurité. De même, si les alertes générées par l'application s'articuleront avec le reste du dispositif sanitaire, le ministère a confirmé qu'il n'envisage pas d'attacher des conséquences juridiques défavorables au fait de ne pas avoir téléchargé l'application et qu'aucun droit spécifique ne sera réservé aux personnes qui l'utiliseront. Enfin, la recommandation de la Commission de disposer d'un fondement juridique explicite et précis dans le droit national, sur lequel elle serait consultée préalablement, pour en permettre la mise en œuvre, a été suivie par le ministère, comme en témoigne sa saisine sur un projet de décret en Conseil d'Etat concernant le traitement fondé sur les articles 6.1.e et 9.2.i du RGPD.

La Commission considère que ces éléments sont de nature à réduire les risques que fait peser le traitement de données sur les droits et libertés fondamentaux des personnes concernées et rendent l'atteinte proportionnée à l'utilité estimée du dispositif.

Elle rappelle en quatrième lieu que 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.

A cet égard, la Commission prend acte du caractère temporaire de l'application projetée, dont le terme de la mise en œuvre est fixé à six mois à compter de la fin de l'état d'urgence sanitaire par le projet de décret. Cette durée correspond à celle prévue pour les traitements Contact Covid et SI-DEP , l'application n'ayant d'utilité qu'en lien avec le cadre plus général de conduite des enquêtes sanitaires.

La Commission estime qu'il s'agit là d'une durée maximale. Elle demande que l'impact effectif du dispositif sur la stratégie sanitaire globale soit, indépendamment du rapport

d’évaluation prévu par le décret après l’arrêt global du traitement StopCovid , étudié et documenté de manière régulière pendant toute la période d’utilisation de celui-ci, afin de s’assurer de son utilité au cours du temps.

Elle a conscience que cette appréciation de l’utilité sera délicate et doit pouvoir tenir compte, le cas échéant, de possibles périodes de recrudescence de l’épidémie. Elle estime pour autant cette évaluation essentielle, dès lors qu’un outil automatisé de suivi de contacts automatique, mis à disposition par les autorités publiques et installé sur les ordiphones des personnes physiques, n’est admissible, ainsi qu’elle l’a souligné dans son avis du 24 avril dernier, que s’il contribue utilement à la politique sanitaire. La Commission demande que ces rapports de suivi lui soient communiqués au fur et à mesure de leur établissement.

Le projet de décret appelle dès lors les observations suivantes de la part de la Commission.

Sur les finalités et la responsabilité de traitement

Sur les finalités du traitement

L’article 1er du projet de décret précise que le traitement a pour finalités :

— l’information d’une personne utilisatrice de l’application qu’elle s’est trouvée à proximité d’au moins un autre utilisateur de cette même application ayant ultérieurement été diagnostiqué positif à la covid-19, de sorte qu’il existe un risque qu’elle ait été contaminée à son tour ;

- la sensibilisation des utilisateurs de l’application, identifiés comme contact à risque d’avoir été contaminés par le SARS-CoV-2, sur les symptômes de la maladie, les gestes barrières et la conduite à adopter pour lutter contre la propagation du virus ;

- l’orientation des contacts à risque vers les acteurs de santé compétents pour leur prise en charge et l’accès aux examens de dépistage ;

- l’amélioration de l’efficacité du modèle utilisé par l’application pour la définition des cas contacts grâce à l’utilisation de données statistiques anonymes au niveau national.

En premier lieu, s’agissant de l’orientation des contacts à risque vers les acteurs de santé compétents, la Commission prend acte de ce que le projet de décret sera modifié afin de préciser que la prise de contact entre l’utilisateur et le professionnel de santé sera recommandée mais demeurera à la discrétion de l’utilisateur.

En deuxième lieu, la Commission prend acte des précisions apportées par le ministère selon lesquelles la finalité d’amélioration de l’efficacité du modèle de santé utilisé par l’application sur la définition des cas contacts vise à l’amélioration des performances de l’application et non à la mesure de son utilité sanitaire. La Commission comprend que d’autres méthodes, de type statistiques ou par sondages, permettront de répondre à cette dernière nécessité.

En troisième lieu, sont expressément exclues des finalités poursuivies par le traitement : les opérations de recensement des personnes infectées, d'identification des zones dans lesquelles ces personnes se sont déplacées, de prise de contact avec la personne alertée ou de surveillance du respect des mesures de confinement ou de toute autre recommandation sanitaire. Le traitement ne doit pas non plus permettre de réaliser le suivi des interactions sociales des personnes.

En quatrième lieu, compte tenu du caractère sensible des données collectées et des finalités poursuivies par le traitement, la Commission accueille favorablement le fait que, conformément à ce qu'elle avait recommandé dans sa délibération du 24 avril 2020, le ministère chargé de la santé soit désigné comme responsable du traitement. Elle considère qu'une telle désignation permet de contribuer à ce que tant le développement et le déploiement que les évolutions possibles du dispositif soient définies par ou en lien avec les autorités sanitaires nationales compétentes.

Une application fondée sur le volontariat des utilisateurs

Le Gouvernement a suivi les recommandations du Comité européen de la protection des données dans son avis n° 04/2020 du 21 avril 2020 et de la Commission dans son avis du 24 avril dernier en fondant l'application StopCovid sur une mission d'intérêt public, intégrée à la politique sanitaire. La Commission avait rappelé que le choix de cette base légale n'exclut pas que le téléchargement et l'utilisation de l'application soient fondés sur le volontariat.

L'article 1er du projet de décret consacre le principe selon lequel le téléchargement et l'utilisation de l'application StopCovid doivent reposer sur une démarche volontaire de l'utilisateur.

La Commission prend acte de ce que le volontariat se matérialise dans toutes les composantes du dispositif : installation de l'application, activation de la communication par Bluetooth, prise de contact avec un professionnel de santé, notification du caractère positif de son diagnostic ou résultat positif à un examen de dépistage à la covid-19 dans l'application, réalisation du dépistage suite à la réception d'une notification, désinstallation de l'application.

Sur les données collectées et traitées

Concernant les données collectées

A titre liminaire, la Commission relève que l'application StopCovid s'appuiera sur le protocole ROBERT, spécifié par INRIA. Elle relève que ce protocole a été conçu dans une logique de minimisation des donnés et de protection des données dès la conception. Elle relève également que ce protocole prend le parti de diffuser les identifiants des personnes exposées au virus plutôt que de diffuser les identifiants des personnes effectivement contaminées, et qu'il garantit qu'aucun lien ne sera conservé entre les personnes contaminées et la liste des personnes qu'elles auraient pu exposer. La Commission relève que ce choix est protecteur de la vie privée des personnes concernées.

L'article 2 du projet de décret énumère la liste limitative des données à caractère personnel qui pourront être collectées dans le cadre de l'application StopCovid .

Comme la Commission l'a déjà relevé dans sa délibération du 24 avril 2020, si le dispositif a vocation à traiter des données à caractère personnel au sens du RGPD, l'application ne collecte que des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, dans le respect du principe de minimisation des données posé par l'article 5.1.c du RGPD.

Par ailleurs, des données à caractère personnel concernant la santé seront traitées. Le traitement de ces données sensibles se fonde sur l'article 9.2.i du RGPD comme précédemment évoqué.

Toutefois, certaines données évoquées dans l'AIPD ne sont pas mentionnées à l'article 2 du projet de décret. La Commission prend acte de l'engagement du ministère de modifier le projet afin de mentionner la collecte des périodes d'exposition des utilisateurs à des personnes contaminées ainsi que les codes pays. Par ailleurs, eu égard aux particularités du traitement, elle recommande que la collecte des dates de dernière interrogation du serveur soit également mentionnée.

Concernant l'exactitude des données

La Commission rappelle qu'assurer l'exactitude et le maintien à jour des données est une obligation légale au titre de l'article 5.1.d du RGPD.

A cet égard, la Commission accueille favorablement le fait que la possibilité d'introduire intentionnellement des faux positifs dans les notifications transmises aux personnes afin de limiter les risques de ré-identification dans certains types d'attaques n'est plus envisagée.

La Commission prend acte de ce que l'algorithme permettant de déterminer la distance entre les utilisateurs de l'application reste à ce stade en développement et pourra subir des évolutions futures. A cet égard, l'échange de messages via la technologie Bluetooth servira également à estimer la distance entre deux appareils mobiles selon la puissance du signal reçu, tandis que l'horodatage de ces messages permettra d'estimer la durée de l'interaction. Il est nécessaire de prendre en compte de nombreux paramètres afin de pouvoir estimer correctement les distances via cette technologie. A cette fin, des tests de calibration actuellement en cours visent à proposer un modèle statistique adapté. La Commission relève ainsi que la détermination d'une interaction à risque sera effectuée de façon probabiliste, ce qui s'inscrit dans la logique générale de l'application de prévenir les utilisateurs d'un risque de contamination, et qu'en aucun cas la réception d'une alerte provenant de l'application ne signifiera que l'utilisateur a été effectivement contaminé.

La Commission relève qu'une application mobile de suivi des contacts ne permet pas de tenir compte du contexte dans lequel les personnes se trouvaient au moment où une exposition à une personne infectée a été enregistrée. Par exemple, un professionnel de santé ou un agent d'accueil seront particulièrement susceptibles d'être notifiés par l'application comme étant à risque d'avoir été contaminés par le SARS-CoV-2 alors même qu'ils étaient protégés (port

d'un masque, paroi séparatrice, etc.) au moment où le contact a été enregistré. Ainsi, l'absence de prise en compte par l'application du contexte des contacts est susceptible d'entraîner la génération de nombreux faux positifs.

En conséquence, la Commission s'interroge sur l'opportunité de prévoir à terme dans l'application la possibilité pour l'utilisateur de définir des plages de temps pendant lesquelles des contacts ne devraient pas être considérés comme potentiellement à risque.

En tout état de cause, afin de tenir compte de ces cas particuliers, la Commission recommande que l'information délivrée aux utilisateurs puisse intégrer des recommandations quant à l'usage de l'application dans des contextes précis. La présence d'un bouton de désactivation temporaire, aisément accessible, sur l'écran principal de l'application pourrait être de nature à réduire le nombre de fausses alertes correspondant à des moments où l'utilisateur n'est pas réellement exposé.

La Commission relève que le transfert de l'historique des identifiants pseudonymes des cas contacts d'une personne infectée, depuis une application mobile vers le serveur central, requiert l'utilisation d'un code à usage unique remis par un professionnel de santé suite à un diagnostic clinique positif ou un examen de dépistage positif à la covid-19. Par conséquent, un utilisateur ne pourra pas fausser la base de données du serveur central de l'application en se déclarant positif sans avoir été dépisté. En outre, la Commission prend acte de ce que la vérification du code à usage unique se limitera à sa validité, et ne fera pas intervenir de vérification de l'identité de la personne à laquelle il a été délivré. La Commission relève également que cette transmission se fera sans que l'historique de contacts transmis au serveur puisse être rattaché à la personne infectée.

Sur les destinataires et les accédants aux données

L'article 3 du projet de décret précise que les utilisateurs de l'application qui seront notifiés comme étant à risque d'avoir contracté la covid-19 sont destinataires de l'information selon laquelle ils se sont retrouvés à proximité d'un autre utilisateur diagnostiqué ou dépisté positif au virus.

Par ailleurs, la Commission relève que l'AIPD transmise liste plusieurs organismes agissant en qualité de sous-traitants pour le compte du responsable de traitement.

En premier lieu, la Commission recommande que le projet de décret soit complété afin de mentionner que des sous-traitants seront accédants ou destinataires des données à caractère personnel dont ils auront besoin de connaître.

En deuxième lieu, l'AIPD précise que les relations de sous-traitance entre le responsable du traitement et ses sous-traitants, notamment en qualité d'hébergeur, sont conclues ou sont prévues sous forme de convention, lors des différentes phases du projet d'application, à savoir les phases de développement, de production et d'exploitation. La Commission rappelle qu'une telle convention doit préciser les obligations de chaque partie, dans le respect des dispositions de l'article 28 du RGPD, notamment en matière d'exercice des droits des personnes concernées et de mesures de sécurité.

La Commission prend acte de ce que le fournisseur de service d'informatique en nuage (cloud computing) hébergeant l'infrastructure de l'application, agissant en qualité de sous-traitant, possède des centres de données localisés en France. Le contrat de sous-traitance le liant au responsable de traitement devra notamment préciser les zones géographiques depuis lesquelles les administrateurs accèdent à l'infrastructure.

En dernier lieu, elle relève que l'article 1er du projet de décret qualifie INRIA de sous-traitant et précise que la mise en œuvre du traitement par INRIA, pour le compte du ministère, se fait dans les conditions prévues à l'article 28 du RGPD. Elle s'interroge sur une telle qualification au regard de la définition du sous-traitant donnée par l'article 4.8 du RGPD.

Sur les transferts de données hors de l'Union européenne

Le projet de décret ainsi que l'AIPD mentionnent que les données à caractère personnel ne sont pas transférées hors de l'Union européenne. La Commission prend donc acte de ce que le traitement aura lieu exclusivement sur le territoire de l'Union.

Sur les durées de conservation

La Commission prend acte de ce que l'article 4 du projet de décret prévoit une conservation des clés et des identifiants associés aux applications pendant la durée de fonctionnement de l'application StopCovid et au plus tard six mois à compter de la fin de l'état d'urgence sanitaire, et une conservation des historiques de proximité des personnes diagnostiquées ou testées positives pendant quinze jours à compter de leur émission.

Conformément au principe de limitation de la conservation (article 5.1.e du RGPD), la durée de conservation des données doit être limitée à ce qui est strictement nécessaire au regard des finalités précédemment décrites. Par conséquent, les identifiants temporaires échangés entre les applications ainsi que les horodatages associés ne peuvent pas être conservés pour une durée supérieure à celle pendant laquelle ces données sont effectivement utiles pour déterminer si un contact a pu engendrer une contamination. Ainsi, cette période a été estimée à quinze jours, conformément à la recommandation de Santé publique France et du ministère.

La Commission prend acte que l'utilisateur de l'application peut à tout moment demander la suppression de ses données de son ordiphone et de la base centrale du serveur au moyen d'une fonctionnalité mise à sa disposition dans l'application, avant la désinstallation. En effet, si l'utilisateur peut désinstaller l'application à tout moment, cela entraînera une suppression de ses données de son ordiphone, mais sera sans effet sur les données stockées au niveau du serveur. La Commission considère que s'il apparaît techniquement impossible de supprimer les données sur le serveur après une suppression de l'application par l'utilisateur, les données relatives aux applications devraient être supprimées au bout d'une période d'inactivité, pour garantir que dans un tel cas de figure des données devenues inutiles ne soient pas conservées. Par ailleurs, il devrait être conseillé aux utilisateurs de l'application de supprimer leurs données du serveur central préalablement à une éventuelle désinstallation de l'application.

Sur l'information et les droits des personnes

Sur l'information des personnes

S'agissant du respect des obligations de transparence (articles 5.1.a et 12 à 14 du RGPD), l'article 5 du projet de décret précise, d'une part, que les personnes concernées sont informées des principales caractéristiques du traitement et de leurs droits au moment de l'installation de l'application StopCovid et, d'autre part, que des mentions d'information sont également mises à la disposition du public par l'intermédiaire du site web https://www.stopcovid.gouv.fr .

En outre, l'AIPD précise que des infographies complèteront l'information en permettant de vulgariser les concepts technologiques sous-jacents.

En premier lieu, la Commission attire l'attention du ministère sur le fait que l'intégralité des informations doit être mise à disposition de l'utilisateur au sein même de l'application. Une telle obligation ne fait cependant pas obstacle à la possibilité d'adopter une approche à plusieurs niveaux par laquelle le responsable de traitement choisit de faire figurer les principales caractéristiques du traitement dans un premier temps. En tout état de cause, une information conforme aux dispositions du RGPD doit être aisément accessible tant lors de l'installation de l'application que tout au long de son usage.

En deuxième lieu, la Commission insiste sur la nécessité de délivrer une information compréhensible par le plus grand nombre, dans la mesure où une partie importante de la population est susceptible d'être concernée par le dispositif. L'information devrait également être mise à disposition dans des modalités permettant aux personnes en situation de handicap d'en prendre connaissance.

Une attention particulière devrait, par ailleurs, être accordée aux mineurs, quand bien même l'information fournie sera identique pour tous les utilisateurs de l'application. Les mineurs équipés d'ordiphones par leurs parents sont en effet susceptibles de télécharger l'application, dans des conditions de droit commun. A leur intention, plus encore que pour les autres utilisateurs, une attention particulière doit être apportée à l'information fournie, afin que l'application soit utilisée à bon escient et que le message d'alerte susceptible de leur être adressé soit adapté et bien interprété. La Commission demande donc que soient intégrés dans l'information fournie aux utilisateurs des développements spécifiques à la fois pour les mineurs eux-mêmes mais aussi pour leurs parents.

Au regard de ces éléments, les exemples de mentions d'informations fournis dans l'AIPD devront faire l'objet de travaux complémentaires afin de répondre aux dispositions des articles 12 à 14 du RGPD.

Sur les droits d'accès, de rectification, le droit à la portabilité et le droit à la limitation du traitement

La Commission relève que l'article 5 du projet de décret a vocation à exclure les droits d'accès, de rectification ainsi que le droit à la limitation du traitement sur le fondement des articles 11 et 23.i du RGPD.

S’agissant du droit à la rectification et du droit à la limitation du traitement, la Commission considère qu’au regard des caractéristiques du traitement, ces derniers n’ont pas vocation à s’appliquer. Il en est de même pour le droit à la portabilité, étant donné que le traitement n’est pas fondé sur l’article 6.1.a ni sur l’article 6.1.b du RGPD.

Le droit d’accès pourrait théoriquement concerner la consultation par un utilisateur des clés et identifiants pseudonymes associés à l’application qu’il utilise. Eu égard au fait que la consultation de ces données ne présente en principe, compte tenu notamment de leur caractère pseudonyme, qu’une très faible utilité pour la personne concernée et que leur libre consultation par toute personne pouvant s’approprier l’ordiphone sur lequel l’application est installée serait de nature à fragiliser la sécurité du dispositif, la Commission estime qu’il résulte des dispositions 11, 15(4) et 23 du RGPD que le ministère peut écarter l’application du droit d’accès. L’application est en effet conçue dans un objectif de santé publique et la pseudonymisation est un élément important pour préserver la vie privée des personnes qui utiliseront ce dispositif.

Sur le droit à l’effacement et le droit d’opposition

La Commission relève que le ministère considère que le droit à l’effacement et le droit d’opposition ne sont pas applicables dans le cadre de la mise en œuvre du dispositif.

D’une part, le ministère estime que les dispositions de l’article 17.3.b et c du RGPD excluent l’application du droit à l’effacement et il entend, d’autre part, déroger au droit d’opposition sur le fondement de l’article 23 du RGPD.

La Commission considère que s’agissant d’un traitement basé sur le volontariat des personnes concernées, le droit à l’effacement et le droit d’opposition devraient être pleinement applicables. Par ailleurs, elle relève qu’en pratique l’AIPD prévoit bien la possibilité, pour l’utilisateur, d’exercer ces droits de manière effective.

En premier lieu, l’utilisateur peut demander l’effacement de ces données directement via l’application tant en ce qui concerne les données stockées sur le terminal que celles disponibles sur le serveur central.

En second lieu, le droit d’opposition se matérialise par la possibilité, pour l’utilisateur, de cesser, à tout moment, d’utiliser l’application en se désabonnant du serveur ou en désinstallant celle-ci du terminal. L’AIPD précise, à cet égard, que le désabonnement doit conduire à l’effacement des données tant en local que sur le serveur central et que la désinstallation conduira à l’effacement des données en local ; les données potentiellement présentes sur le serveur central ne pourront alors plus être rattachées à un utilisateur.

La Commission prend acte de l’engagement du ministère à modifier le projet de décret sur ces points.

Sur les mesures de sécurité

A titre liminaire, la Commission prend acte que le dispositif envisagé a fait l'objet de mesures complémentaires sur un certain nombre de points qu'elle avait relevés dans sa délibération du 24 avril 2020.

En premier lieu, concernant la sécurité du serveur chargé de la centralisation des identifiants des personnes exposées au virus, l'avis de la Commission attirait l'attention sur la nécessité de mettre en œuvre des mesures de sécurité organisationnelles et techniques permettant d'apporter les garanties les plus élevées possibles contre tout détournement de finalité, du fait de la nature centralisée du protocole mis en œuvre au sein de l'application StopCovid . A ce titre, la Commission prend acte de ce que le ministère aura recours à des modules de sécurité afin de protéger les clés de chiffrement permettant l'accès aux identifiants des personnes concernées.

Elle relève également que le responsable de traitement prévoit la mise en place d'un comité regroupant plusieurs entités auxquelles seraient confiés des fragments des clés de chiffrement, afin de garantir l'impossibilité pour un seul acteur d'opérer un détournement d'usage des données. Elle estime qu'une telle mesure est de nature à limiter les risques de détournement de la base centrale, et elle appelle le ministère à inclure dans ce comité des organismes de natures différentes et présentant un haut niveau d'indépendance, et relève que la participation de plusieurs organismes de recherche scientifique serait de nature à accroître encore le niveau de garantie apporté par le dispositif. Elle appelle toutefois le ministère à évaluer spécifiquement le niveau de garantie offert par une telle mesure dans l'AIPD, et à mettre en place des garanties supplémentaires le cas échéant.

En deuxième lieu, sur le recours à des mécanismes cryptographiques, la Commission rappelle s'être prononcée dans son avis sur la nécessité d'utiliser des algorithmes cryptographiques à l'état de l'art et conformes au référentiel général de sécurité édité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Elle note à cet égard que le protocole a évolué, l'algorithme de chiffrement 3DES ayant été remplacé par SKINNY-CIPHER64/192, tel que recommandé par l'ANSSI.

En troisième lieu, concernant la publication du code source, le projet de décret mentionne que certains éléments du code informatique de l'application ou du serveur central ne seront pas rendus publics, car cela mettrait en danger l'intégrité et la sécurité de l'application. Même si le paramétrage des logiciels utilisés et le détail des mesures de sécurité n'ont pas vocation à être rendus publics, il est important que l'intégralité du code source soit quant à lui rendu public. La Commission accueille favorablement l'engagement du ministère de rendre public l'intégralité du code source et suggère que le décret soit modifié en conséquence.

Par ailleurs, la Commission relève que l'utilisation du mécanisme de fixation du certificat (certificate pinning) sur les applications mobiles constitue une bonne pratique, permettant aux applications d'authentifier de manière sûre le serveur avec lequel elles communiquent et par là même de garantir la stricte confidentialité des données échangées avec le serveur.

La Commission prend acte que seules les personnes individuellement habilitées pourront accéder aux données enregistrées sur le serveur central. Elle rappelle que les modalités d'authentification de ces personnes devront être conformes à la délibération n° 2017-012 du

19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, et que compte tenu de la nature du traitement elle recommande que des mécanismes d'authentification forte soient mis en place.

La Commission prend acte de ce que le fournisseur de l'infrastructure hébergeant la plateforme StopCovid , agissant en qualité de sous-traitant, est qualifié SecNumCloud par l'ANSSI, qu'il est certifié hébergeur de données de santé (HDS) et qu'il met en œuvre des centres de données certifiés ISO/IEC 27001.

En outre, la Commission prend acte que, conformément au référentiel général de sécurité, une homologation de sécurité de StopCovid est prévue, préalablement à la mise en production de l'application. Elle relève également que l'ANSSI est impliquée dans la mise en œuvre de l'application, et qu'un certain nombre de recommandations ont été émises par cette dernière à destination du responsable de traitement.

De plus, la Commission accueille favorablement le fait que des audits de sécurité soient prévus par l'ANSSI tout au long du développement de l'application. La Commission prend acte également que des audits seront réalisés par des tiers.

La Commission prend acte de ce que le ministère prévoit d'avoir recours à un captcha lors de l'initialisation de l'application, afin de vérifier que celle-ci est bien utilisée par une personne physique. Elle relève que le captcha envisagé repose, dans un premier temps, sur l'utilisation d'un service assuré par un tiers. La Commission constate que le recours à ce service est susceptible d'entraîner la collecte de données personnelles non prévues dans le décret, des transferts de données hors de l'Union européenne, ainsi que des opérations de lecture/écriture qui nécessiteraient un consentement de l'utilisateur. La Commission relève également que l'utilisateur final devrait être informé de ces opérations de traitement conformément au RGPD et que la relation avec ce tiers devrait être encadrée par un contrat de sous-traitance. En conséquence, elle appelle le ministère à la vigilance et souhaiterait que des développements ultérieurs de l'application permettent rapidement l'utilisation d'une technologie alternative.

La Commission relève enfin qu'il est prévu que certaines opérations fassent l'objet de mesures de journalisation. Concernant les données relatives aux erreurs techniques, la Commission recommande que seul le minimum de données strictement nécessaire à la vérification du bon fonctionnement du système soit journalisé, et notamment que ces journaux soient exempts d'identifiants ou de clés cryptographiques relatives aux utilisateurs. Concernant la journalisation des actions réalisées par les administrateurs, la Commission recommande que celle-ci soit conservée pendant une durée de six mois dans des conditions permettant de garantir son intégrité, et que des mécanismes d'analyse automatiques soient mis en place afin de détecter toute opération anormale.

La Commission prend acte que des évolutions de l'application et du protocole de suivi des contacts, notamment afin de permettre une interopérabilité à l'échelle de l'Union européenne, sont susceptibles d'être développées à moyen terme. Elle prend également acte de l'intention du ministère de la saisir à nouveau, y compris de façon facultative, pour toute modification qui serait apportée au traitement.