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

(demande d'avis n° 20006919)

La Commission nationale de l'informatique et des libertés,

Saisie par le secrétaire d'Etat chargé du numérique d'une demande d'avis concernant les conditions et modalités de l'éventuelle mise en œuvre de l'application « StopCovid » au regard des règles françaises et européennes de protection des données à caractère personnel ;

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 8-I-2°e) ;

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

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 a été saisie par le Secrétaire d'Etat chargé du numérique, le 20 avril 2020, d'une demande d'avis relative aux conditions et modalités de l'éventuelle mise en œuvre de l'application « StopCovid » au regard des règles françaises et européennes de protection des données à caractère personnel, sur le fondement de l'article 8-I-2°-e) de la loi n° 78-17 du 6 janvier 1978 susvisée (ci-après, la « loi Informatique et Libertés »).

Cette saisine intervient dans le contexte de l'état d'urgence sanitaire liée à l'épidémie de COVID-19, et plus particulièrement de la stratégie dite de « déconfinement ». Dans ce cadre, le Gouvernement envisage de développer et de proposer une application, dénommée « StopCovid », disponible sur ordiphones (smartphones) et autres équipements mobiles. Cette application permettrait d'informer les personnes l'ayant téléchargée du fait qu'elles ont été à proximité, dans un passé proche, de personnes diagnostiquées positives au COVID-19 et disposant de la même application, cette proximité induisant un risque de transmission du virus.

Il s'agirait d'une application de « suivi de contacts » (ou « *contact tracing* »), et non de suivi des personnes exposées ou diagnostiquées positives au virus, qui reposerait notamment sur l'utilisation de la technologie de communication de proximité « Bluetooth » pour évaluer la proximité entre deux ordiphones, sans recourir à une technologie de géolocalisation. Elle serait utilisée uniquement sur la base du volontariat et ses modalités de mise en œuvre viseraient à minimiser toute identification directe ou indirecte des personnes qui y auraient recours. Les documents annexés à la saisine, qui décrivent un protocole dit protocole ROBERT, fournissent des premiers éléments de réflexion sur l'architecture fonctionnelle et technique d'une telle application.

Dans ce contexte et sur la base de ces informations, le Gouvernement interroge la Commission sur l'existence ou non, dans le cadre de l'hypothèse de la mise en œuvre d'une telle application, d'un traitement de données à caractère personnel au sens du règlement (UE) 2016/679 du 27 avril 2016 susvisé (ci-après, le « RGPD ») et de la loi « Informatique et Libertés », sur l'identification de la base légale d'un tel traitement, au sens des mêmes dispositions, sur la conformité d'un tel dispositif aux règles de protection des données personnelles et, le cas échéant, sur les garanties supplémentaires qu'il conviendrait de prévoir.

Le présent avis de la Commission vise à apporter ces éléments de réponse et à éclairer le Gouvernement sur l'analyse d'une telle application du point de vue du droit de la protection des données à caractère personnel, étant précisé que le déploiement de cette application comme ses modalités exactes de mise en œuvre, sur les plans juridique, technique et pratique, ne sont pas encore arrêtés à ce stade. La Commission demande, après la tenue du débat au Parlement et s'il était décidé de recourir à un tel instrument, qu'elle soit à nouveau saisie pour se prononcer sur les modalités définitives de mise en œuvre du dispositif.

A titre liminaire, la Commission souligne qu'elle a pleinement conscience de la gravité de la situation sanitaire liée à l'épidémie de COVID-19, des décès et des souffrances qu'elle entraîne, ainsi que des difficultés liées au confinement des personnes résidant sur le territoire national. Le pays est confronté à une crise sanitaire d'une ampleur exceptionnelle et le gouvernement a le devoir de prendre les mesures de protection de la population nécessaires. Le projet du gouvernement s'inscrit dans son action pour lutter contre l'épidémie et traduit le souhait de ne laisser de côté aucun outil permettant d'endiguer la maladie et de gérer au mieux la période de déconfinement. En outre, la conception de l'application StopCovid témoigne du souci de protéger la vie privée des personnes, notamment en évitant que soit centralisée dans un serveur une liste des personnes qui se déclarent malades.

Pour autant, il est également du devoir de la Commission de souligner que ce projet pose des questions inédites en termes de protection de la vie privée. Certes, il ne consiste pas à suivre tous les mouvements géographiques des personnes : il ne s'agit pas de tracer les individus de façon continue. Néanmoins, il s'agit d'établir, par la collecte de traces pseudonymes, la liste des personnes dont chaque porteur de l'application a été physiquement proche, pendant une durée circonscrite, parmi tous les porteurs de l'application. Une telle collecte, qui a vocation à s'appliquer à la plus grande partie de la population possible, doit être envisagée avec une grande prudence.

La protection de la vie privée est garantie par la Constitution et d'autres sources de droit ; le fait de collecter les listes de personnes que les individus ont fréquentées y porte une atteinte forte, qui ne peut, le cas échéant, être justifiée que par la nécessité de répondre à un autre principe constitutionnel, à savoir la protection de la santé, qui découle du onzième alinéa du préambule de la Constitution de 1946. Le recours à des formes inédites de traitement de données peut en outre créer dans la population un phénomène d'accoutumance propre à dégrader le niveau de protection de la vie privée et doit donc être réservé à certaines situations exceptionnelles, Enfin, la Commission souligne que la conformité aux règles de protection des données à caractère personnel, et notamment la bonne information des personnes concernées, le respect de leurs droits et, plus généralement, des dispositions du RGPD et de la loi « Informatique et Libertés », est de nature à favoriser la confiance des utilisateurs de l'application et, par suite, l'effectivité du dispositif projeté.
C'est à l'aune de ces principes généraux qu'il y a lieu d'étudier le recours à l'application Stopcovid décrite dans la saisine.

L'existence de traitements de données à caractère personnel et notamment de données de santé

Le dispositif envisagé à ce jour se compose, d'une part, d'une application mobile qui sera mise à disposition sur les équipements mobiles (notamment ordiphones et tablettes) fonctionnant sous les systèmes d'exploitation Android et iOS et, d'autre part, d'un serveur central qui assurera le stockage et la transmission d'un certain nombre de données nécessaires au fonctionnement global du dispositif. Le gouvernement s'interroge sur l'existence de données à caractère personnel traitées dans le cadre du dispositif dès lors, d'une part, que le téléchargement et l'utilisation de l'application ne requerraient pas la fourniture de données directement identifiantes (telles que nom, numéro de téléphone, adresse électronique, etc.) et, d'autre part, que l'application téléchargée, et donc son utilisateur, ne serait identifiée par le serveur central que par un *pseudonyme,* c'est-à-dire une donnée non identifiante par elle-même. Le protocole décrit dans la saisine repose ainsi sur un système associant à chaque application téléchargée un identifiant aléatoire permanent (ci-après, le pseudonyme permanent) permettant ensuite de créer plusieurs identifiants aléatoires temporaires (ci-après, les pseudonymes temporaires).

En premier lieu, il faut souligner qu'afin de pouvoir informer un utilisateur d'une exposition possible au virus, le serveur central doit vérifier s'il existe une concordance entre les pseudonymes attribués, lors de son installation, à l'application de cet utilisateur et ceux ayant été transmis au serveur central par l'application d'une autre personne reconnue comme positive. Il en résulte que demeure un lien entre les pseudonymes et les applications téléchargées, chaque application étant elle-même installée sur un terminal, qui correspond généralement à une personne physique déterminée. Du fait de ce lien, la Commission estime que le dispositif traitera des données à caractère personnel au sens du RGPD. En outre, la collecte des pseudonymes temporaires des personnes avec lesquelles l'utilisateur a été en contact pourrait permettre de reconstituer l'ensemble des relations qu'il a eues avec d'autres utilisateurs de l'application. Au regard de ces éléments, la Commission estime que le dispositif projeté est soumis aux règles de protection des données à caractère personnel, tout en reconnaissant que les protections prises apportent un haut degré de garantie pour

minimiser le risque de ré-identification des personnes physiques associées aux données stockées, pour une durée nécessairement limitée, par le serveur central.

En deuxième lieu, le serveur central disposerait de l'information selon laquelle un utilisateur aura ou non reçu une notification lui indiquant qu'il a été exposé au virus. La Commission relève que toute l'architecture du dispositif envisagée tend à ne faire remonter au serveur central que les pseudonymes générés par les applications associées aux personnes avec lesquelles un individu infecté a été en contact, et non le pseudonyme de ce dernier. Elle souligne que ce procédé minimise le risque de réidentification de la personne infectée à l'origine d'une alerte, dans le plein respect des principes de protection des données personnelles.

En troisième lieu, la Commission observe que des données concernant la santé seront traitées par le dispositif. D'une part, le déclenchement d'une alerte par une personne infectée est directement lié à l'état de santé de celle-ci. D'autre part, l'information selon laquelle une personne présente un risque suffisamment élevé d'avoir contracté une maladie, et conduisant notamment à ce qu'elle en soit informée par l'application, est, selon l'analyse de la Commission, une donnée concernant la santé et bénéficiant du régime de protection spécifique de ces données sensibles prévu par le RGPD, éclairé par son considérant 35, par la loi « Informatique et Libertés », voire, en fonction des usages prévus, par les dispositions spécifiques du code de la santé publique relatives notamment au partage et à l'hébergement des données. Cette information sera présente dans le serveur central. En outre, si des précautions techniques sont prises pour minimiser la possibilité de réidentification de la personne infectée par les personnes qu'elle a côtoyées et qui ont reçu l'alerte, ce risque, qui sera fonction du contexte, et notamment du nombre de personnes côtoyées durant la période précédant l'alerte, peut subsister et est à prendre en compte.

Néanmoins, la Commission rappelle que la présence de données à caractère personnel ne fait pas obstacle, par principe, à la mise en œuvre du dispositif. Elle impose cependant de prévoir des garanties adaptées d'autant plus fortes que les technologies sont intrusives, garanties au titre desquelles l'atténuation des possibilités de ré-identification constitue une mesure essentielle.

Un dispositif fondé sur le volontariat

Une finalité limitée à l'alerte de personnes exposées au risque de contamination

La Commission rappelle que le principe de limitation des finalités, consacré par l'article 5(1) (b) du RGPD, est un principe cardinal de la protection des données à caractère personnel : celles-ci ne doivent être utilisées que pour un objectif précis et déterminé à l'avance. Toute autre utilisation des données est en principe interdite.

En l'espèce, ainsi qu'il a été dit, l'objectif de « suivi de contacts » poursuivi par le dispositif consiste à pouvoir informer un utilisateur de l'application que son téléphone (ou autre équipement mobile) s'est trouvé à proximité, au cours des jours précédents, de celui d'une personne ayant ultérieurement été diagnostiquée positive au COVID-19, de sorte qu'il existe un risque qu'il ait été contaminé à son tour.

L'application StopCovid n'a pas pour objet de surveiller le respect de mesures de confinement ou d'autres obligations sanitaires. La Commission prend également acte de ce que le traitement décrit dans la saisine n'a pas pour objet d'organiser une prise de contact avec la personne alertée, de réaliser un suivi du nombre de personnes infectées ou d'identifier les zones dans lesquelles ces personnes se sont déplacées. Un enrichissement des finalités de l'application nécessiterait de prendre en compte le juste équilibre entre ces nouveaux objectifs et la protection de la vie privée.

Une application fondée sur le volontariat des utilisateurs

La Commission prend acte de ce que le projet du gouvernement consiste à mettre à disposition de la population résidant sur le territoire national l'application StopCovid, dont le téléchargement et l'utilisation reposeraient sur une démarche volontaire. Elle considère à ce titre que le caractère volontaire de l'usage, conjugué à une transparence renforcée quant au mode de fonctionnement et aux finalités de traitement, est un élément déterminant pour assurer la confiance dans le dispositif et favoriser son adoption par une partie significative de la population. Ce volontariat devrait être explicitement prévu dans les textes juridiques régissant ce dispositif comme dans l'information du public.

A cet égard, il convient de souligner que le volontariat ne doit pas uniquement se traduire par le choix, pour l'utilisateur, de télécharger puis de mettre en œuvre l'application (installation de l'application, activation de la communication par Bluetooth, voire fait de se déclarer positif au COVID-19 dans l'application) ou la faculté de la désinstaller. Le volontariat signifie aussi qu'aucune conséquence négative n'est attachée à l'absence de téléchargement ou d'utilisation de l'application. Ainsi, l'accès aux tests et aux soins ne saurait en aucun cas être conditionné à l'installation de l'application. L'utilisation d'une application sur la base du volontariat ne devrait pas conditionner ni la possibilité de se déplacer, dans le cadre de la levée du confinement, ni l'accès à certains services, tels que par exemple les transports en commun. Les utilisateurs de l'application ne devraient pas davantage être contraints de sortir en possession de leurs équipements mobiles. Les institutions publiques ou les employeurs ou toute autre personne ne devraient pas subordonner certains droits ou accès à l'utilisation de cette application. Ceci constituerait en outre, en l'état du droit et selon l'analyse de la Commission, une discrimination. A ces conditions l'utilisation de StopCovid pourra être regardée comme réellement volontaire. Des choix différents, qui relèveraient du législateur et dont la stricte nécessité devrait alors être démontrée, porteraient une atteinte bien plus considérable au droit à la protection des données à caractère personnel et au respect de la vie privée. Toute l'analyse qui suit ne s'applique donc qu'à un projet d'application d'usage volontaire répondant aux caractéristiques précitées.

La base légale de l'application StopCovid

L'article 6 du RGPD et l'article 5 de la loi « Informatique et Libertés » prévoient que le traitement de données à caractère personnel n'est possible que dans certaines hypothèses et pour certains motifs limitativement énumérés, qui constituent les « bases légales » possibles du traitement. En l'espèce, le gouvernement s'interroge sur la possibilité de fonder l'application StopCovid sur la base légale du *consentement* de

ses utilisateurs ou, à défaut, sur l'existence d'une *mission d'intérêt public* de lutte contre l'épidémie de COVID-19.
A titre liminaire, la Commission rappelle qu'un usage volontaire de l'application est compatible en droit avec l'une ou l'autre de ces « bases légales ».

Elle rappelle que le droit de la protection des données à caractère personnel n'établit aucune hiérarchie entre les différentes bases légales et que la base légale appropriée doit être déterminée uniquement au cas par cas, de manière adaptée à la situation et au type de traitement. Chaque base légale obéit en effet à des conditions spécifiques et emporte des conséquences juridiques particulières pour l'organisme mettant en œuvre le traitement comme pour les personnes concernées par celui-ci. Le choix de la base légale peut donc être une opération délicate, qui n'appelle pas une réponse univoque. Pour autant, si plusieurs bases légales peuvent s'avérer appropriées pour un même traitement, il convient de n'en retenir qu'une seule, considérée *in fine* comme la plus appropriée au cas d'espèce.

La Commission relève que la lutte contre l'épidémie de COVID-19 constitue une mission d'intérêt général dont la poursuite incombe en premier lieu aux autorités publiques. En conséquence, elle estime que la *mission d'intérêt public*, au sens des articles 6.1.e) du RGPD et 5.5° de la loi « Informatique et Libertés », constitue la base légale la plus appropriée pour le développement par l'autorité publique de l'application StopCovid. Elle relève que le Comité européen de la protection des données a considéré, dans son avis n° 04/2020 du 21 avril 2020, que cette base légale est la plus appropriée pour ce type d'applications mises en œuvre par les autorités publiques. Le choix de cette base légale permet en outre de concilier en toute sécurité juridique le caractère volontaire de l'utilisation de cette application et les éventuelles incitations des pouvoirs publics à une telle utilisation, afin de promouvoir son utilisation la plus large possible. Le RGPD requiert néanmoins que les finalités du traitement en cause soient nécessaires à la mission d'intérêt public en cause et que celle-ci dispos d'une assise juridique suffisante dans une norme du droit national.

S'agissant du cas spécifique du traitement de données relatives à la santé des personnes concernées, le RGPD prévoit que le traitement de telles données peut notamment intervenir, comme en l'espèce, pour des motifs d'intérêt public « *dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé* », dès lors que ce traitement est nécessaire à ces fins et prévu par le droit de l'Union ou le droit national et que celui-ci prévoit « *des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée* » (article 9-2-i du RGPD). Sans préjudice de la possibilité juridique de fonder le traitement de ces données sur une autre exception prévue par l'article 9 du RGPD, la Commission estime que ces dispositions paraissent les plus adaptées à la situation de l'application StopCovid.

Dans ces conditions, la Commission recommande que le recours à un dispositif volontaire de suivi de contact pour gérer la crise sanitaire actuelle dispose d'un fondement juridique explicite et précis dans le droit national. Elle demande au gouvernement, le cas échéant et quel que soit le vecteur retenu, de la saisir à nouveau du projet de norme encadrant la mise en œuvre de l'application en cause lorsque la décision aura été prise et le projet précisé.

Enfin, il peut être relevé que le projet d'application StopCovid implique également l'accès à des informations stockées et l'inscription d'informations dans un équipement terminal de communications électroniques des personnes concernées, au sens de l'article 82 de la loi « Informatique et Libertés », à savoir dans l'équipement mobile des personnes mettant en œuvre l'application. A cet égard, la Commission considère que ces opérations sont strictement nécessaires à la fourniture du service de communication en ligne expressément demandé par la personne concernée et qu'elles sont donc licites.

L'admissibilité de l'atteinte à la vie privée par un dispositif de suivi de contacts

La Commission rappelle qu'en vertu de la protection constitutionnelle de la vie privée, qui résulte de l'article 2 de la Déclaration des droits de l'homme et du citoyen, des protections conventionnelles, 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, ainsi que des garanties spécifiques exigées par le RGPD, notamment pour ce qui concerne le traitement de données de santé dans le cadre d'une mission d'intérêt public, le gouvernement doit veiller à ce que l'atteinte portée à la vie privée demeure proportionnée à l'objectif poursuivi. Comme il a été indiqué, la protection de la santé constitue également un objectif à valeur constitutionnelle.

D'une part, le respect du principe de proportionnalité se traduira notamment par une collecte et une conservation des données limitées à ce qui est strictement nécessaire, afin de minimiser l'atteinte portée à la vie privée des personnes. Cette garantie fondamentale implique en l'espèce que la collecte et le traitement de données opérés par l'application revêtent un caractère temporaire, d'une durée limitée à celle de l'utilité du dispositif au regard des finalités précédemment décrites. Elle implique également que toutes les données soient supprimées dès le moment où l'utilité de l'application ne sera plus avérée. Dans l'hypothèse où une exploitation statistique ou à des fins de recherche scientifique se révélerait néanmoins nécessaire, celle-ci devra être réalisée en priorité sur des données anonymisées ou, à défaut, dans le strict respect des règles fixées par le RGPD et la loi « Informatique et Libertés ».

D'autre part, il apparaît à la Commission que l'atteinte portée à la vie privée ne sera en l'espèce admissible que si, en l'état des informations immanquablement lacunaires et incertaines dont il dispose pour affronter l'épidémie, le gouvernement peut s'appuyer sur des éléments suffisants pour avoir l'assurance raisonnable qu'un tel dispositif sera utile à la gestion de la crise, et notamment à la sortie du confinement de la population qui porte par lui-même une atteinte très forte à la liberté d'aller et venir. Or, si ce type de dispositif peut potentiellement aider les autorités publiques à surveiller et à contenir la pandémie de COVID-19, en complétant les méthodes traditionnelles de recherche de contacts utilisées pour contenir la propagation des épidémies, il n'en possède pas moins des limites, tant intrinsèques que liées à son insertion dans une politique sanitaire globale, qui sont susceptibles de porter atteinte à son efficacité.

En premier lieu, son efficacité dépend de certaines conditions techniques, notamment la possibilité pour une proportion suffisante de la population d'accéder à l'application et de l'utiliser dans de bonnes conditions. Cela signifie notamment qu'il serait souhaitable que cette application soit disponible sur suffisamment de magasins d'applications mobiles (« *appstores* », « *playstore* », etc.) et compatible avec la majorité des téléphones et autres équipements mobiles actuellement en circulation, tant d'un point de vue matériel que logiciel. La Commission relève en outre que la concurrence de plusieurs applications de suivi de contacts, qui doivent en tout état de cause respecter les dispositions applicables en matière de protection des données à caractère personnel et sont, à ce titre, soumises aux pouvoirs de contrôle de la Commission, est susceptible de nuire à l'efficacité du dispositif.

En deuxième lieu, la Commission souligne que l'effectivité du dispositif repose en partie sur une adoption large de celui-ci, alors qu'une partie significative de la population ne dispose pas d'équipements mobiles adéquats ou peut éprouver des difficultés pour installer et utiliser l'application. Or, certaines des personnes les plus vulnérables à la maladie, ainsi que les personnes les plus jeunes n'ayant pas de téléphone, qui pourraient jouer un rôle sensible dans la propagation de celle-ci, sont particulièrement concernées. En outre, certaines personnes qui utiliseront l'application sont susceptibles de contracter la maladie sans en présenter les symptômes, et pourraient donc ne pas déclencher l'alerte de leurs contacts. Toutefois, cet élément doit être relativisé par le fait que le dispositif envisagé pourrait aussi, du fait de l'éventuelle notification d'une alerte, inciter ces personnes à faire l'objet d'une mesure de dépistage.

En troisième lieu, la Commission souligne également que l'effectivité du dispositif envisagé repose sur le bon calibrage des algorithmes permettant d'identifier une interaction susceptible d'avoir engendré une contamination. Par ailleurs, la Commission recommande que le recours à toute forme d'automatisation de la décision d'informer des personnes exposées soit associé à la possibilité pour ces personnes d'échanger avec un personnel qualifié.

En quatrième lieu, un dispositif numérique de suivi individualisé des personnes ne peut être mis en place qu'à titre de mesure complémentaire dans le cadre d'une réponse sanitaire globale. En ce sens, la Commission considère que l'utilisation d'applications de suivi des contacts ne saurait être une mesure autonome et appelle, sur ce point, à une vigilance particulière contre la tentation du « solutionnisme technologique ». Aussi, il revient au gouvernement d'évaluer l'ensemble des différentes actions à mettre en place, telles que la mobilisation de personnels de santé et des enquêteurs sanitaires, la disponibilité de masques et de tests, l'organisation des dépistages, les mesures de soutien, les informations et le service délivrés aux personnes qui auront reçu l'alerte, la capacité à les isoler dans des lieux adéquats, etc. Ce déploiement doit s'inscrire dans un plan d'ensemble.

Sur ce point, la Commission accueille avec intérêt les précisions apportées par le Secrétaire d'Etat chargé du numérique, qui lui a indiqué que l'usage de l'application est envisagé dans une approche intégrée à la stratégie sanitaire globale pilotée notamment par le ministère de la santé et des solidarités.

La Commission souligne que l'ensemble de ces précautions et garanties est de nature à permettre la confiance du public dans ce dispositif, qui constitue un facteur important de son effectivité.

Enfin, elle recommande que l'impact du dispositif sur la stratégie sanitaire globale soit étudié et documenté de manière régulière, afin que l'efficacité de celui-ci au cours du temps puisse être évaluée. Cela permettra aux pouvoirs publics de décider de manière éclairée son maintien ou non au regard, notamment, des principes de proportionnalité et de nécessité. La Commission recommande que ces analyses lui soient, le cas échéant, communiquées, afin de lui permettre d'exercer sa mission de contrôle de la conformité de la mise en œuvre du dispositif projeté.

La configuration de l'application

La Commission rappelle qu'elle ne se prononce que sur le principe du déploiement d'une application telle que celle décrite dans la saisine, dont les modalités précises pourraient, le cas échéant, évoluer. Elle souhaite cependant apporter dès à présent au Gouvernement les précisions suivantes.

La responsabilité du traitement

L'identification du responsable de traitement permet d'établir qui est responsable du respect des règles en matière de protection des données à caractère personnel. Compte tenu de la sensibilité des données collectées, la Commission est d'avis que le dispositif devrait être conçu de telle manière que le ministère chargé de la santé ou toute autre autorité sanitaire impliquée dans la gestion de la crise sanitaire puisse assurer la responsabilité de traitement.

Sur la nécessité de réaliser une analyse d'impact sur la protection des données

La Commission attire l'attention du gouvernement sur le fait que, comme tout traitement susceptible de présenter des risques élevés (données de santé, usage à grande échelle, suivi systématique, utilisation d'une nouvelle solution technologique), une analyse d'impact sur la protection des données (AIPD) devra être réalisée avant toute mise en œuvre d'un tel dispositif. La publication de l'AIPD est recommandée à des fins de transparence et au regard du contexte actuel.

Sur l'exactitude des données

La Commission relève que, dans le protocole technique qui lui a été transmis, il est envisagé qu'on puisse introduire des faux positifs dans les notifications transmises aux personnes afin de limiter les risques de ré-identification dans certains types d'attaques. Elle considère que cette mesure ne peut ni ne doit être mise en œuvre, dès lors qu'elle aurait pour conséquence d'alerter faussement des personnes n'ayant pas eu de contact à risques, et qui seraient dès lors encouragées à se soumettre à des mesures de confinement volontaire consistant en une restriction auto-imposée de leurs libertés individuelles. Elle souligne que maintenir l'exactitude des données est une obligation légale impérieuse au titre du RGPD et de la loi « Informatique et Libertés » et qu'une telle mesure n'est pas envisageable, sous peine de remettre en cause la conformité du traitement au regard des textes applicables.

Sur la sécurité des données

La sécurité des données personnelles est une garantie indispensable, eu égard à la sensibilité de ce dispositif. Cette sécurité nécessite une prise en compte exhaustive des conditions de mise en œuvre du traitement et une amélioration continue des techniques, procédures et protocoles mis en place. Face au défi que représente la prise en compte de ces exigences dans un temps très court, la Commission attire l'attention du ministère sur ce point.

La Commission souligne que le présent avis s'appuie sur le corpus documentaire qui lui a été transmis, qu'il ne couvre pas l'ensemble des caractéristiques du traitement et que le protocole proposé est encore à ce jour en constante évolution. Elle estime néanmoins nécessaire d'attirer dès maintenant l'attention du Gouvernement sur les quatre points suivants.

En premier lieu, la Commission relève que le dispositif envisagé comprend un serveur chargé de la centralisation des identifiants des personnes exposées. Afin d'apporter les garanties les plus élevées possibles contre tout détournement de finalité lié à ce choix, elle estime nécessaire que des mesures de sécurité organisationnelles et techniques de très haut niveau soient mises en place, en accord avec un modèle de sécurité adapté prenant en compte tout acte malveillant. A ce titre, elle attire l'attention sur les clés de chiffrement permettant l'accès aux identifiants des personnes concernées, qui pourraient par exemple être protégées *via* des modules de sécurité matériels, ainsi que des tiers de confiance indépendants.

En deuxième lieu, la Commission estime nécessaire que des mesures soient mises en œuvre à la fois dans le serveur central et dans l'application pour éviter de pouvoir recréer un lien entre ces pseudonymes temporaires et des informations spécifiques au terminal liées à la technologie Bluetooth (comme le nom de l'équipement mobile ou son adresse MAC) permettant d'identifier les utilisateurs.

En troisième lieu, la Commission rappelle que seuls des algorithmes cryptographiques à l'état de l'art doivent être mis en œuvre, afin d'assurer l'intégrité et la confidentialité des échanges. Elle relève à cet égard l'usage de l'algorithme 3DES, envisagé à ce stade, et attire l'attention du ministère sur le fait que conformément au référentiel général de sécurité édité par l'Agence nationale de la sécurité des systèmes d'information cet algorithme ne devrait en principe plus être utilisé.

Enfin, en quatrième lieu, la Commission relève que le dispositif envisagé ne prévoit pas de mécanisme d'enrôlement des personnes lors de la première utilisation de l'application, ce qui permet de limiter les données personnelles collectées. Toutefois, il pourrait en résulter un risque d'attaque accru qui n'est acceptable que dans la mesure où un tel mécanisme d'enrôlement des personnes remettrait en question la logique de pseudonymat du traitement. Elle appelle donc le ministère à mettre en place des mesures appropriées afin de lutter contre ce risque.

Par ailleurs, la Commission accueille favorablement le fait que des éléments de documentation technique ont déjà été rendus publics. Elle souligne à cet égard l'importance d'assurer le libre accès aux protocoles utilisés ainsi qu'au code source de l'application, du serveur central et leur paramétrage. Il s'agit tant de permettre à la communauté scientifique de contribuer à l'amélioration constante du dispositif et à la correction des éventuelles vulnérabilités que de garantir une parfaite transparence vis-à-vis de l'ensemble des citoyens. Elle recommande par ailleurs, afin de maximiser la qualité de la solution, que les commentaires et débats de la communauté scientifique soient pris en compte.

Sur le respect des droits des personnes sur leurs données à caractère personnel

La maitrise de leurs données par les personnes concernées est une garantie essentielle pour garantir la confiance du public dans les mesures prises aux fins de gestion de la crise du COVID-19. Une information appropriée devra donc être fournie aux utilisateurs, dans le respect des articles 12 à 14 du RGPD. Dans la mesure où une partie importante de la population est susceptible d'être concernée par le dispositif, la Commission insiste notamment sur la nécessité de délivrer une information compréhensible par le plus grand nombre, dans des termes clairs et simples.

La Commission rappelle que des situations telles que l'épidémie actuelle de COVID- 19 ne suspendent ni ne restreignent, par principe, la possibilité pour les personnes concernées d'exercer leurs droits sur leurs données à caractère personnel conformément aux dispositions des articles 12 à 22 du RGPD. Des modalités appropriées pour l'exercice des droits devront également être définies si l'application est déployée.

La Présidente

Marie-Laure DENIS