Délibération 2020-135 du 17 décembre 2020

Commission Nationale de l'Informatique et des Libertés
Nature de la délibération : Avis
Etat juridique : En vigueur
Date de publication sur Légifrance : Mardi 16 février 2021
NOR : CNIX2105104V

Délibération n° 2020-135 du 17 décembre 2020 portant avis sur un projet de décret modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid » (demande d'avis n° 20020446)

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 modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé 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° 2020-1379 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° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé StopCovid ;

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 :

La Commission a été saisie en urgence, par le ministre des solidarités et de la santé, d'une demande d'avis relative à un projet de décret modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé StopCovid . Le projet de décret vise à faire évoluer les conditions de mise en œuvre des traitements de données nécessaires au fonctionnement de l'application désormais dénommée TousAntiCovid , notamment dans la perspective d'un nouveau déconfinement et de la réouverture de certains établissements recevant du public (ERP).

Les évolutions envisagées visent principalement à introduire dans l'application TousAntiCovid un dispositif numérique d'enregistrement des visites dans de tels lieux, afin de faciliter l'alerte des personnes les ayant fréquentés sur une plage horaire similaire à celle d'une ou de plusieurs personnes ultérieurement dépistées ou diagnostiquées positives à la COVID-19. Le projet de décret a également vocation à permettre la collecte et le traitement de nouvelles données nécessaires à la lutte contre l'épidémie et à intégrer les évolutions successives de l'application depuis le déploiement de sa version 2.0 en octobre dernier.

Prises dans leur ensemble, ces modifications ont pour effet de faire évoluer l'application vers un portail comprenant plusieurs fonctionnalités reposant, le cas échéant, sur des traitements de données poursuivant des finalités distinctes et dont les modalités de mise en œuvre sont propres à chacune d'entre elles. Le ministère souhaite, pour des raisons de transparence, encadrer l'ensemble des traitements de données susceptibles d'intervenir dans le cadre de l'utilisation de l'application, et non le seul traitement de données de santé ayant rendu nécessaire la prise d'un décret en Conseil d'Etat pris après avis de la Commission. Outre le fait qu'il semble que le décret pourrait gagner en lisibilité, cette saisine appelle les observations suivantes.

S'agissant du dispositif relatif aux codes-QR utilisés dans certains lieux

Ce nouveau dispositif disponible dans l'application TousAntiCovid a vocation à alerter les personnes utilisatrices qu'elles ont été présentes dans un lieu clos (ci-après dénommé lieu contact) permettant le rassemblement ou la réunion de plusieurs personnes et sur une période pendant laquelle elles auraient pu être contaminées par une ou plusieurs personnes ultérieurement diagnostiquées ou dépistées positives à la COVID-19. Il repose sur un protocole dénommé TAC-WARNING (ci-après TAC- W), distinct du protocole ROBERT et de la fonctionnalité de suivi des contacts.

En pratique, il repose sur la mise à disposition, par les responsables des ERP, de codes-QR que les personnes sont invitées à scanner, à l'entrée ou à l'intérieur de ces locaux, avec l'application TousAntiCovid . Ces codes-QR et la plage d'horaire concernée sont enregistrés dans l'application. Lorsqu'un utilisateur se signale comme positif au virus, l'application adresse au serveur central TAC-W la liste des codes-QR scannés, qui représente donc la liste des ERP qu'il a fréquentés. Cette liste de lieux contacts est enregistrée sur le serveur. Par ailleurs, l'application de chaque utilisateur interroge régulièrement ce

serveur central en lui envoyant la liste des codes-QR scannés par celui-ci et, lorsque le serveur TAC-W identifie une concordance entre un des lieux remontés et un lieu contact déjà enregistré, il notifie l'utilisateur qu'il a pu être exposé dans un des lieux qu'il a fréquentés.

La nature de la notification reçue pourra varier en fonction du risque de contamination encouru, calculé par le serveur TAC-W sur la base de préconisations à venir des autorités sanitaires. Ainsi, les personnes ayant fréquenté un lieu pendant la même plage horaire qu'une ou plusieurs personnes déclarées positives seront notifiées en tant que contact à risque modéré. Au-delà d'un certain seuil permettant d'identifier la présence d'un cluster, les utilisateurs pourront être notifiés comme contact à risque élevé comme dans le protocole ROBERT.

Sur la nécessité et la proportionnalité du dispositif

L'introduction d'une telle fonctionnalité doit contribuer à renforcer l'utilité sanitaire de l'application en permettant à un plus grand nombre d'utilisateurs d'être informés des contacts à risques qu'ils ont croisés. Elle a ainsi vocation à compléter la fonctionnalité de suivi des contacts reposant sur l'utilisation de la technologie de communication de proximité Bluetooth pour évaluer la proximité entre deux ordiphones, de manière à tenir compte des risques particuliers de contamination liés à la fréquentation des ERP et autres lieux accueillant plusieurs personnes.

Conformément aux recommandations de Santé Publique France, ces lieux sont en effet susceptibles de présenter un risque élevé d'exposition au virus, lorsque les personnes qui les fréquentent ne sont pas en mesure de s'assurer du respect des gestes barrières (salles de sport, restaurants, bars, etc.), ou un risque modéré lorsque ces mesures barrières doivent être mises en œuvre mais qu'une rupture de cette protection y est possible (transports publics, lieux culturels, lieux de culte, etc.).

Au regard de ces éléments, la Commission estime que l'utilité, au stade actuel de la lutte contre l'épidémie, d'un dispositif complémentaire d'identification des contacts à risque de contamination est suffisamment démontrée.

Elle rappelle toutefois que les atteintes aux droits au respect de la vie privée et à la protection des données à caractère personnel doivent non seulement être nécessaires à la poursuite d'un intérêt général, comme cela est le cas en l'espèce, mais également être proportionnées à cet objectif. Elle souligne en outre que l'enregistrement des lieux fréquentés par les personnes révèle des informations relevant de leur vie privée, voire des données sensibles bénéficiant d'un régime de protection spécifique prévu par le règlement général sur la protection des données (RGPD) dans certains cas, comme par exemple en cas de fréquentation de lieux de culte. Le traitement de ces informations, et en l'espèce par les pouvoirs publics, doit donc faire l'objet de la plus grande vigilance.

A cet égard, la Commission relève que l'architecture technique et fonctionnelle du dispositif apporte plusieurs garanties substantielles, de nature à en assurer la proportionnalité. En particulier, le dispositif ne recourt pas à une technologie de géolocalisation ni n'implique le suivi des déplacements des utilisateurs de l'application. Il repose sur la seule conservation dans le serveur central TAC-W de la liste des lieux contacts, sans lien avec un quelconque identifiant d'utilisateur, minimisant ainsi le risque de rattacher l'ensemble des lieux fréquentés à l'utilisateur et de pouvoir ainsi reconstituer un historique de certains de ses déplacements.

En outre, si l'interrogation du serveur central nécessite que l'application d'un utilisateur lui transmette la liste des lieux qu'il a fréquentés associés à un horodatage, cette interrogation ne fait pas intervenir, d'après les éléments fournis par le ministère, d'identifiant de l'application, de la personne ou de son terminal. La Commission relève également que les modalités de stockage et de comparaison des lieux fréquentés font l'objet de mesures visant à limiter les risques d'identification de ces lieux par des tiers. Enfin, la collecte et le traitement de données opérés pour cette fonctionnalité revêtent un caractère temporaire et ces données sont strictement séparées de celles traitées dans le cadre du protocole ROBERT (aucun identifiant commun et des serveurs centraux distincts pour les deux fonctions).

Le ministère a ainsi fait le choix d'une architecture dans laquelle l'application interroge le serveur en envoyant régulièrement l'historique des lieux fréquentés et enregistrés par l'application, et non celui d'une architecture dans laquelle les codes-QR des lieux contacts seraient diffusés par le serveur à tous les utilisateurs, permettant la comparaison, en local, des lieux contacts sur chaque application. Néanmoins, au regard de l'ensemble des éléments, la Commission estime que le dispositif projeté est 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 dans le contexte de la crise sanitaire actuelle.

Elle relève en revanche que l'étendue de la collecte et du traitement de données dont les utilisateurs de l'application feront l'objet est conditionnée à certains choix qui n'ont pas pu être portés à sa connaissance, sur la liste précise des ERP concernés, sur le caractère obligatoire ou non, pour ces établissements, de mettre à disposition un code-QR, ou encore sur l'obligation faite aux personnes concernées d'enregistrer leurs visites afin que celles-ci puissent être alertées en cas de risque de contamination. La Commission n'est donc pas pleinement en mesure d'apprécier la proportionnalité de la collecte envisagée.

Elle prend néanmoins acte des précisions du ministère selon lesquelles, dans l'hypothèse où l'enregistrement des visites constituerait une obligation pour les personnes concernées (clients, visiteurs, employés, etc.), deux dispositifs, l'un numérique (codes-QR), l'autre non numérique (un cahier de rappel par exemple), seraient mis à leur disposition par les responsables des établissements visés. Elle rappelle qu'il s'agit d'une garantie essentielle, dans la mesure où l'utilisation d'une application sur la base du volontariat ne saurait par nature conditionner l'accès à certains lieux, notamment s'agissant d'établissements pouvant recevoir du public (transports en commun, salles de sport, restaurants, bars, etc.). Par ailleurs, elle appelle l'attention du ministère sur la nécessité de s'assurer que tout dispositif alternatif non numérique respecte les normes d'accessibilité, afin de permettre aux personnes en situation de handicap qui n'utiliseraient pas l'application d'accéder aux lieux concernés.

Elle prend également acte de ce que le périmètre précis du dispositif fera prochainement l'objet d'arbitrages par les autorités sanitaires compétentes. Afin de minimiser l'atteinte portée au droit à la protection des données à caractère

personnel, la Commission recommande que le caractère obligatoire du dispositif soit, le cas échéant, limité aux seuls ERP présentant un risque élevé. Elle appelle en outre à la plus grande vigilance s'agissant des lieux dont la fréquentation est susceptible de révéler des données faisant l'objet d'une protection particulière, tels les lieux de culte ou les lieux de réunion syndicale ou politique. Elle recommande que le dispositif ne soit pas rendu obligatoire dans ces lieux et que des mesures sanitaires appropriées, complémentaires au dispositif des enquêtes sanitaires de droit commun, soient prévues afin de limiter suffisamment le risque de contamination.

La Commission invite enfin le ministère à prévoir de nouvelles garanties de nature à minimiser davantage les risques de traçage des utilisateurs, telles qu'une limitation de la durée de validité des codes-QR voire l'utilisation de codes à usage unique.

Sur les dispositions du projet de décret

L'intégration du dispositif précité de codes-QR dans l'application TousAntiCovid implique la modification du décret n° 2020-650 du 29 mai 2020 susvisé sur plusieurs points et appelle les observations suivantes de la Commission.

A titre liminaire, la Commission invite le ministère à modifier le second alinéa de l'article 1-I du décret n° 2020-650 précité afin de préciser que le dispositif repose sur deux serveurs centraux distincts.

En premier lieu, il est prévu d'ajouter, au projet d'article 1-II-7° dudit décret, une finalité rendant compte du dispositif de code-QR tel que présenté ci-dessus. La Commission relève que la rédaction projetée est très proche de la finalité d'alerte des cas contacts préexistante du traitement TousAntiCovid prévue au 1° des mêmes dispositions, qu'il n'apparaît pas impérativement nécessaire de modifier sur ce point. Elle relève en outre que les spécifications du protocole TAC-W indiquent que l'objectif spécifique de la solution consiste également à permettre l'identification des clusters potentiels dans les lieux clos rassemblant du public. Elle demande dès lors la modification du projet de décret sur ces deux points.

En deuxième lieu, le projet d'article 2-I-12° du décret n° 2020-650 du 29 mai 2020 entend permettre la collecte des *informations relatives à la fréquentation d'un lieu clos permettant le rassemblement ou la réunion de plusieurs personnes obtenues par un QR-code mis à disposition à l'intérieur ou devant ce lieu* et précise que ces informations *sont stockées sur le serveur central en vue d'informer l'utilisateur qu'il a été en contact avec une personne diagnostiquée ou dépistée positive au virus du covid-19 et ayant fréquenté le même lieu durant la même plage horaire* .

A cet égard, la Commission considère que le projet de décret définit trop largement les données collectées dans ce cadre et ne comporte dès lors pas les garanties juridiques de nature à assurer le respect du principe de minimisation des données traitées établi par l'article 5.1.c du RGPD alors même que, conformément aux éléments transmis par le ministère, ces données apparaissent effectivement limitées à ce qui est nécessaire au regard de la finalité. Elle invite ainsi le ministère à modifier le projet de décret afin de préciser les catégories de données collectées au titre de cette nouvelle finalité et prend acte, à cet égard, de l'absence de traitement de l'identifiant de l'application spécifique à chaque utilisateur.

En outre, la rédaction actuelle du projet de décret laisse ouverte la possibilité d'une conservation générale et indifférenciée, au sein du serveur central, des informations relatives à tous les lieux fréquentés par l'ensemble des utilisateurs de l'application. La Commission considère que le projet de décret devrait être modifié afin de préciser, conformément aux éléments transmis par le ministère, que seules les informations relatives aux lieux fréquentés par les utilisateurs qui se sont déclarés positifs dans l'application font l'objet d'un stockage au sein du serveur central. Cet élément constitue en effet, à ses yeux, une garantie substantielle.

En troisième lieu, le projet de décret précise que les données sont conservées sur le serveur central pendant quinze jours à compter de leur enregistrement par l'application de l'équipement mobile de la personne concernée.

Si cette durée n'appelle pas d'observation de la part de la Commission, elle invite le ministère à préciser également dans le projet de décret la durée de conservation des données stockées localement, ainsi que la possibilité offerte à l'utilisateur de l'application de supprimer, à tout moment, un lieu visité de son historique, directement depuis son terminal.

Sur l'information des personnes concernant le dispositif relatif aux codes-QR

Il est prévu que les personnes concernées soient informées du dispositif sur place, *via* un affichage sur les lieux concernés, ainsi qu'en ligne au sein de l'application TousAntiCovid et sur le site web dédié à l'application.

Elle précise qu'une information, compréhensible par le plus grand nombre, devra être placée à l'endroit du code-QR afin que les personnes soient en mesure de comprendre ce à quoi elle se rattache. Enfin, la Commission recommande, afin d'assurer l'homogénéité et la conformité de ces mesures d'information aux articles 12 et 13 du RGPD, que des modèles d'affichage standardisés et adaptés aux différents cas d'usage soient mis à la disposition des établissements concernés au sein de la plateforme permettant de générer les codes-QR.

Sur les mesures de sécurité

A titre liminaire, la Commission souligne la prise en compte effective des principes de protection des données et de sécurité dès la conception du dispositif, qui apparaissent comme des préoccupations constantes des concepteurs de l'application. Toutefois, compte tenu des délais très contraints dans lesquels elle a été amenée à se prononcer, son analyse a particulièrement porté sur le dispositif envisagé à court terme, même si l'évolution de TAC-W vers un protocole qualifié de dynamique offrira de meilleures garanties en termes de protection des données et de sécurité, sous réserve de ses conditions de mise en œuvre effectives.

A cet égard, la Commission rappelle que la publication de la documentation technique et du code informatique des nouvelles fonctionnalités du dispositif ainsi que la prise en compte des commentaires de la communauté scientifique permettront l'amélioration continue du dispositif et la correction d'éventuelles vulnérabilités, visant à garantir la sécurité

des données. Elle invite donc le ministère à poursuivre et amplifier la démarche d'ouverture encadrant la mise en œuvre initiale de StopCovid.

La Commission considère qu'un tel dispositif doit, en particulier, prévenir tout détournement de la finalité épidémiologique et tout abus de l'infrastructure envisagée. Ainsi, compte tenu du rôle clé joué par les serveurs centraux pour le suivi de contacts et la gestion des lieux contacts, elle estime nécessaire que des mesures de sécurité organisationnelles et techniques adaptées soient mises en place afin notamment de prévenir tout acte malveillant sur cet environnement.

La Commission prend acte que les deux protocoles ROBERT et TAC-W fonctionnent indépendamment, avec notamment une séparation logique des flux et des serveurs respectifs, afin que les données de chacun des protocoles ne puissent pas être reliées, et d'éviter tout risque d'inférence d'information.

Elle relève que le protocole envisagé ne prévoit pas que le serveur central connaisse précisément les lieux fréquentés par les personnes déclarées positives. Toutefois, le serveur collecte les identifiants uniques et aléatoires contenus dans les codes QR remontés lorsqu'un utilisateur se déclare positif dans l'application. Bien que la table de correspondance entre cet identifiant aléatoire et le nom ou la localisation de l'établissement ne semble pas être connue par le serveur, cette information existe par ailleurs et pourrait donc être reliée aux données stockées sur le serveur, ce qui serait susceptible d'affaiblir le niveau de sécurité global du traitement.

A cet égard, la Commission relève que lors de la remontée des historiques de lieux fréquentés d'un utilisateur qui se déclare positif, le serveur applique une fonction de hachage à l'identifiant du lieu contact, en utilisant l'algorithme SHA256 et en l'associant à différentes valeurs d'un paramètre, de façon semblable à un sel, sans que cette mise en œuvre corresponde à l'état de l'art en la matière pour éviter les rapprochements. Si la Commission comprend de cette pratique qu'elle vise à limiter les possibilités pour des tiers de réidentifier les lieux fréquentés par les utilisateurs, elle invite le ministère à mettre en place, sans tarder, des mesures encore plus efficaces, telles que le recours à des codes-QR dynamiques, dont l'usage est d'ores et déjà prévu par le ministère et qui pourrait améliorer substantiellement la sécurité des données traitées.

Par ailleurs, elle rappelle que tout échange de données entre application et serveur doit être sécurisé, par exemple en mettant en œuvre des algorithmes cryptographiques à l'état de l'art, et qu'il doit s'effectuer de manière robuste de telle sorte que la simple observation de la communication ne permet pas d'inférer des informations sur les utilisateurs de l'application. La Commission recommande également que les données stockées sur le serveur et celles stockées sur le terminal de l'utilisateur soient chiffrées à l'aide d'un algorithme cryptographique à l'état de l'art. Elle rappelle à cet égard que les clés de chiffrement devront avoir une taille suffisante et devront être gérées dans des conditions permettant d'en assurer la confidentialité.

Enfin, afin de prévenir l'accès à l'historique des lieux enregistrés localement, par des personnes autres que l'utilisateur de l'application, la Commission recommande la mise en œuvre dans l'application mobile de mécanismes de restriction d'accès adéquats.

Sur les autres modifications apportées au décret n° 2020-650 du 29 mai 2020

S'agissant de la priorisation des cas contacts dans l'accès aux examens ou aux tests de dépistage

Le projet d'article 1-II-4° du décret n° 2020-650 du 29 mai 2020 entend permettre aux utilisateurs de l'application ayant le statut de *contacts à risque de contamination* de bénéficier d'un examen ou d'un test de dépistage dans des conditions de réalisation prioritaire.

A cet égard**,** la Commission rappelle que le fait de télécharger et d'utiliser l'application TousAntiCovid n'emporte pas, *de facto*, la possibilité de bénéficier d'un accès prioritaire à ces examens, seuls les utilisateurs notifiés comme contacts à risques étant concernés par ce caractère prioritaire. Elle relève en outre que la modification projetée du décret s'inscrit dans le cadre de la doctrine de priorisation mise en place par le ministère au cours de ces derniers mois, pour faire face à l'accroissement du nombre de personnes se présentant dans les laboratoires de biologie médicale pour se faire dépister, en priorisant le dépistage des cas-contacts .

Dès lors que cet accès prioritaire ne sera pas réservé aux utilisateurs de l'application, mais ouvert à tous les cas-contacts , la Commission estime que ce dispositif ne saurait remettre en cause le caractère volontaire de l'utilisation de l'application. Il est néanmoins nécessaire que l'information fournie, notamment dans l'application elle-même, soit sans ambiguïté sur le fait que la priorité est attachée à la qualité de cas-contact et non à l'utilisation de l'application par elle-même.

S'agissant de l'élargissement des fonctionnalités proposées par l'application

Les projets d'article 1-II-6° et 1-II-8° du décret n° 2020-650 du 29 mai 2020 permettent d'élargir les finalités du traitement de données afin d'y intégrer les nouvelles fonctionnalités de l'application TousAntiCovid successivement mises en œuvre depuis le déploiement de la version 2.0. Ils prévoient ainsi que le traitement de données a notamment pour finalités :

- d'informer les utilisateurs sur la circulation du virus au niveau national et local (lorsque l'utilisateur renseigne un code postal dans ce dernier cas), sur les mesures ou actions de promotion, de prévention et d'éducation pour la santé ainsi que sur les données d'utilisation de l'application et de les orienter vers d'autres outils numériques mis en œuvre pour la gestion de l'épidémie ;
- de permettre aux personnes utilisatrices de l'application de stocker des données à caractère personnel sur leur ordiphone en vue de générer des justificatifs requis par les autorités publiques. Pour ce faire, des données telles que le nom, le prénom et l'adresse sont enregistrées sur le terminal pour ne pas avoir à être renseignées à chaque génération d'un nouveau justificatif.

La Commission s'interroge sur la nécessité d'encadrer de tels traitements par décret. D'une part, l'administration les a déjà mis en œuvre dans le cadre de l'application TousAntiCovid et certains sites internet d'administration 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 personnelles étant stockées et traitées uniquement localement, à la discrétion et pour le compte du seul utilisateur, 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. En ce sens, il convient de relever que les dispositions du décret relatives à ces traitements ne sont pas conformes aux exigences de la Commission (durée de conservation, liste des destinataires, etc.) mais qu'il n'apparaît pas opportun de réglementer ces aspects qui, dans le cadre du fonctionnement du logiciel en cause, doivent rester à la discrétion du particulier qui utilise l'application.

La Commission prend acte du fait que le Gouvernement souhaite faire de la mise à disposition de ces outils au public une obligation pour l'administration, édictée par le projet de décret. Elle relève les garanties prévues par le ministère s'agissant de ces finalités, dans une logique de minimisation des données et de protection des données dès la conception et par défaut. Ainsi, les données susceptibles d'être collectées tant pour l'obtention d'informations sanitaires relatives à un lieu d'intérêt (identifié par le code postal) que pour la génération des attestations de déplacement dérogatoires seront stockées sur l'ordiphone de l'utilisateur et ne feront l'objet d'aucun traitement sur le serveur central. En outre, conformément au principe de limitation de la conservation des données, le code postal renseigné pour obtenir des informations locales sur la situation sanitaire ne sera pas conservé et le code-QR permettant de disposer d'une attestation dérogatoire de déplacement ne peut être conservé plus de vingt-quatre heures à compter de sa date de validité. Les données renseignées par l'utilisateur sur les sites et applications référencées au sein de TousAntiCovid ne font l'objet d'aucun traitement de données dans le cadre de l'application.

Sur la réalisation d'analyses statistiques

Le projet d'article 1-II-5° du décret n° 2020-650 du 29 mai 2020 a pour objet de préciser la finalité statistique attribuée au traitement en mentionnant la réalisation d' *analyses statistiques à partir des données anonymes issues de l'application afin adapter les mesures de gestion nécessaires pour faire face à l'épidémie* .

D'après les éléments transmis par le ministère, ces analyses statistiques ne constituent ni des traitements à des fins de recherche, d'études et d'évaluation dans le domaine de la santé, ni des traitements visant à adapter les mesures de gestion nécessaires à la lutte contre l'épidémie. Dans la mesure où elles ont pour seule vocation l'amélioration des performances de l'application, la Commission demande que le projet de décret soit précisé sur ce point et sur les données effectivement traitées à cette fin.

Dans l'hypothèse où l'élaboration de telles statistiques nécessiteraient la mise en œuvre d'opérations de lecture ou d'écriture sur le terminal de l'utilisateur, la Commission rappelle que celles-ci pourront être exemptées de consentement sous la réserve que ces opérations soient conformes à l'article 5 des lignes directrices de la Commission relatives aux *cookies et autres traceurs* . A défaut, le consentement devra être recueilli, conformément à l'article 82 de la loi du 6 janvier 1978 modifiée.

Par ailleurs, le projet d'article 2-I-6° bis du décret n° 2020-650 du 29 mai 2020 prévoit que pourront être collectées *la date de la remontée de l'historique de proximité des contacts à risque de contamination par le virus du covid-19, la date de la dernière notification du statut contact à risque de contamination et, le cas échéant, la date d'apparition du premier symptôme et la date du prélèvement positif* .

Tout d'abord, la Commission prend acte des précisions apportées par le ministère selon lesquelles de telles données ne seront utilisées que dans le cadre de la réalisation des analyses statistiques précédemment évoquées. A cet égard, elle recommande au ministère que le projet de décret soit explicité sur ce point.

La Commission relève que ces données, transmises au serveur central au moment de la remontée de l'historique de proximité des contacts à risque de contamination, ne sont pas liées aux identifiants des personnes effectivement contaminées, ce qui apparait une mesure de minimisation protectrice de la vie privée des personnes concernées.

Sur la collecte de nouvelles données pour la fonctionnalité de suivi des contacts via la technologie Bluetooth

Le projet de décret entend permettre la collecte de nouvelles données dans le cadre de la fonctionnalité de suivi des contacts *via* la technologie Bluetooth . Le projet d'article 2-I-7° du décret n° 2020-650 du 29 mai 2020 autorise le traitement de la date de dernier contact des utilisateurs à l'une des personnes diagnostiquées ou dépistées positives à la COVID-19 ou une approximation de cette dernière à plus ou moins un jour.

Selon le ministère, le traitement de cette donnée, inférée à partir des contacts remontés par l'application, à vocation à améliorer la précision des recommandations formulées à l'utilisateur notifié s'agissant, d'une part, de la période à respecter pour se faire dépister suite au dernier contact et, d'autre part, de la période durant laquelle ce dernier doit rester isolé. En effet, à ce jour, la date préconisée est celle de la notification qui reste dépendante du délai pris par le cas index pour se faire tester et se déclarer positif dans l'application. Dès lors, la Commission estime cette donnée pertinente au regard de la finalité du traitement.

Sur l'introduction d'un système de notifications push

La Commission relève que l'AIPD transmise mentionne que les dispositifs fonctionnant sous le système d'exploitation iOS ont désormais recours à un système de notifications push . En effet, le ministère indique que le bon fonctionnement de l'application sur ces appareils nécessite, en raison des limitations techniques imposées par Apple, qu'elle soit réactivée périodiquement, faute de quoi les interrogations régulières du serveur central pour vérifier le statut d'exposition au virus de l'utilisateur ne pourraient intervenir. Techniquement, ce système se traduit par l'envoi d'une notification qui implique l'envoi de données supplémentaires au serveur central ainsi qu'au serveur de notification d'Apple, et notamment un

identifiant unique spécifique au terminal et à l'application. Dès lors, elle invite le ministère à compléter le projet de décret afin de mentionner, au titre des données traitées, les données techniques nécessaires à ces notifications *push* .

Par ailleurs, la Commission reconnaît l'intérêt de recourir à cette fonctionnalité, par ailleurs commune à la plupart des applications développées sur iOS (notamment pour avertir l'utilisateur d'une mise à jour), dans le cadre de la crise sanitaire, dès lors qu'elle permet de réveiller l'application aux fins d'interroger le serveur central. Elle attire néanmoins l'attention du ministère sur le fait que cette fonctionnalité pourrait entraîner des transferts de données vers les Etats-Unis nécessaires au bon fonctionnement technique de l'application. Elle invite le ministère à se rapprocher de la société Apple pour avoir confirmation que cette fonctionnalité n'implique pas de transfert ou pour essayer, le cas échéant et dans la mesure du possible, de les éviter. En tout état de cause, l'information des utilisateurs de l'application devra être clarifiée en conséquence.

Sur la durée de mise en œuvre de l'application

La Commission relève que la durée de mise en œuvre est cohérente avec 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.

Sur l'analyse d'impact sur la protection des données

La Commission appelle l'attention du ministère sur la nécessité de mettre régulièrement à jour l'analyse d'impact sur la protection des données (AIPD) avant de mettre en œuvre les évolutions successives de l'application.

Si la Commission prend acte de ce que le ministère a initié une démarche de gestion des risques incluant un volet vie privée, elle regrette que l'AIPD dédiée au dispositif relatif aux codes-QR codes mis à disposition dans certains lieux, en cours de réalisation, ne lui ai pas été transmise en appui de la saisine. La Commission demande que celle-ci lui soit transmise et rappelle en tout état de cause que les risques résiduels devront être ramenés à un niveau acceptable. Elle réitère enfin son appel à la transparence sur ce point et recommande que cette AIPD soit rendue publique.

La Présidente

Marie-Laure DENIS