

**Décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le
ministère des solidarités et de la santé**

(N°MDM201047)

La Présidente de la Commission nationale de l'informatique et des libertés,

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

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 20 ;

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 ;

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

Vu l'arrêté du 30 mai 2020 définissant les critères de distance et de durée du contact au regard du risque de contamination par le virus du covid-19 pour le fonctionnement du traitement de données dénommé « StopCovid » ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

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

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

Vu la décision n° 2020-097C du 28 mai 2020 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le Secrétaire général de procéder ou de faire procéder à une mission de vérification de la conformité de tout traitement accessible à partir de l'application « StopCovid France », mis en œuvre par la direction générale de la santé du ministère des solidarités et de la santé, ou portant sur des données à caractère personnel collectées à partir de cette application, aux dispositions du règlement (UE) 2016/679 susvisé et de la loi n° 78-17 du 6 janvier 1978 modifiée ;

Vu les procès-verbaux de contrôle n° 2020-097/1 du 9 juin 2020, n° 2020-097/2 du 25 juin 2020 et n° 2020-097/3 du 26 juin 2020 ;

Vu les autres pièces du dossier ;

RÉPUBLIQUE FRANÇAISE

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

I. Le contexte

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, et plus particulièrement de la stratégie dite de « déconfinement » menée par le gouvernement, le ministère des solidarités et de la santé propose dans les magasins d'applications, depuis le 2 juin 2020, une application dénommée « StopCovid France », disponible sur ordiphones (« *smartphones* »). Le traitement de données personnelles dénommé « StopCovid », dont le responsable de traitement est le ministre chargé de la santé (direction générale de la santé), a été créé par le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid », complété par l'arrêté du ministre des solidarités et de la santé du 30 mai 2020, définissant les critères de distance et de durée du contact au regard du risque de contamination par le virus du covid-19 pour le fonctionnement du traitement de données dénommé « StopCovid ».

Avant le lancement de l'application, la Commission nationale de l'informatique et des libertés (ci-après la « CNIL » ou la « Commission ») a été saisie de deux demandes d'avis portant sur les modalités et conditions de mise en œuvre de l'application.

Dans un premier avis du 24 avril 2020, la Commission s'est prononcée sur la conformité générale aux règles de protection des données à caractère personnel du projet d'application mobile de « suivi de contacts » dénommée « StopCovid » tel qu'envisagé alors par le gouvernement. Dans un second avis du 25 mai 2020, la Commission s'est prononcée sur le projet de décret portant sur cette même application mobile.

L'application « StopCovid France » est une application de suivi de contacts (ou « *contact tracing* ») qui permet à chaque utilisateur d'enregistrer un historique de « contacts » avec d'autres utilisateurs, c'est-à-dire une information relative à la proximité entre deux terminaux mobiles. Elle permet à l'utilisateur de se déclarer diagnostiqué ou dépisté au virus SARS-CoV-2. Elle permet également aux utilisateurs d'être informés qu'ils ont été à proximité d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus SARS-CoV-2 et, le cas échéant, d'être invités à prendre attache avec un professionnel de santé pour être pris en charge le plus rapidement possible et, ainsi, d'être intégrés dans le système plus général de gestion du virus SARS-CoV-2 (systèmes d'information « SI-DEP » et « Contact Covid »).

L'application, dont le téléchargement et l'utilisation reposent sur une démarche volontaire de l'utilisateur, fonctionne grâce à la conservation de l'historique de proximité, constitué des pseudonymes émis par les ordiphones *via* la technologie Bluetooth à basse consommation (*Bluetooth Low Energy* — BLE).

En pratique, une fois installée et les fonctionnalités activées, l'application émet des messages Bluetooth spécifiques et en reçoit en provenance d'autres ordiphones sur lesquels l'application « StopCovid France » a été installée et activée.

Si un utilisateur de l'application est diagnostiqué ou dépisté positif au virus SARS-CoV-2, il peut le déclarer dans l'application grâce à un code fourni par le professionnel de santé (*via* un code de 6 caractères ou un QR Code). L'utilisation de ce code par l'utilisateur lui permet d'envoyer son historique de « contacts » au serveur central qui traite alors chacun des contacts présents dans l'historique, afin d'en estimer le risque de contamination au virus SARS-CoV-2. Le serveur maintient une base de données dont chaque enregistrement correspond à un utilisateur et contient le score de risque associé à cet utilisateur.

L'application contacte une fois par jour le serveur afin de vérifier le statut d'exposition de l'utilisateur. Les utilisateurs ayant été en contact (à moins d'un mètre pendant au moins 15 minutes) avec la personne diagnostiquée ou dépistée positive sont prévenus qu'ils ont été exposés à un risque de contamination au virus SARS-CoV-2. Ils sont alors invités à suivre des consignes spécifiques liées à la protection de leur santé et à la lutte contre la propagation du virus (surveillance des symptômes, confinement, mise en relation avec un professionnel de santé).

Une nouvelle version de l'application « StopCovid France » (version v1.1.*) a été déployée fin juin 2020, et constitue une version mise à jour de la version « StopCovid France » à sa date de lancement (version v1.0.*). Cette nouvelle version de l'application apporte deux changements majeurs. D'une part, la méthode d'authentification par « captcha » - qui permet de vérifier lors de l'activation initiale de l'application que cette dernière est utilisée par un être humain - qui reposait sur la technologie « reCaptcha » de la société GOOGLE, est désormais remplacée par la technologie « captcha » développée par la société ORANGE. D'autre part, une fonction de préfiltre de l'historique des contacts de l'utilisateur qui se déclare positif au virus SARS-CoV-2, fondée sur des critères de durée et de distance du contact, est activée pour agir au niveau du téléphone de l'utilisateur.

À ce jour, les deux versions de l'application coexistent. Les utilisateurs qui ont téléchargé l'application à compter du 25 juin 2020 ou qui ont procédé à la mise à jour de l'application depuis cette date disposent sur leurs ordiphones de la version v1.1.*. Les utilisateurs qui ont téléchargé l'application avant le 25 juin 2020 et n'ont pas procédé à sa mise à jour, disposent encore sur leurs ordiphones de la version antérieure v1.0.*.

Au jour des contrôles de la CNIL des 25 et 26 juin 2020, l'application « StopCovid France » dans sa version v1.0.* avait été téléchargée environ 1,9 million de fois et avait été activée environ 1,5 million de fois.

La version v1.1.* de l'application ayant été déployée au moment des contrôles réalisés par la CNIL, la délégation n'a pas pu constater durant ces missions le nombre d'installations et d'activations de la dernière version de l'application. Une demande d'information en ce sens a par conséquent été adressée ultérieurement au ministère des solidarités et de la santé. Le ministère a répondu le 10 juillet 2020 que le nombre d'applications « StopCovid France » installées et activées après la sortie de la v1.1.* s'élève à environ 147 000.

II. La procédure

En application de la décision n° 2020-097C du 28 mai 2020 de la Présidente de la Commission, une délégation de la CNIL a procédé à une mission de contrôle en ligne le 9 juin 2020 et a réalisé deux contrôles sur place les 25 et 26 juin 2020, aux fins de vérifier la conformité de tout traitement de données à caractère personnel réalisé à partir de l'application « StopCovid France » ou portant sur des données à caractère personnel collectées à partir de cette application, au regard des dispositions du règlement (UE) 2016/679 (ci-après « le règlement » ou le « RGPD ») et de la loi n° 78-17 du 6 janvier 1978 modifiée (ci-après la loi « Informatique et Libertés »).

Par la suite, le ministère des solidarités et de la santé a fourni à la délégation, par courriels des 19 juin, 4, 7, 8 et 10 juillet 2020, les documents complémentaires demandés lors des contrôles concernant, notamment, l'analyse d'impact relative au traitement des données personnelles issues de l'application, les contrats conclus entre le ministère des solidarités et de la santé et INRIA pour le développement et l'exploitation de l'application, le registre de traitement des données personnelles ainsi que la documentation technique relative au fonctionnement de l'application.

III. L'examen de la conformité du traitement

Dans le cadre de ces contrôles, la délégation a constaté que le fonctionnement de l'application « StopCovid France », notamment dans sa version v1.1.*, respecte pour l'essentiel les dispositions applicables relatives à la protection des données à caractère personnel.

La plupart des préconisations formulées par la Commission dans ses avis des 24 avril et 25 mai 2020 ont été prises en compte par le ministère des solidarités et de la santé.

La délégation a toutefois constaté certains manquements aux dispositions du RGPD et de la loi « Informatique et Libertés », objets de la présente mise en demeure.

1. Les manquements au regard des dispositions du RGPD

Un manquement à l'obligation de traiter des données personnelles selon les modalités prévues par le décret du 29 mai 2020, en application de l'article 5-1-a) du RGPD

L'article 5-1-a) du Règlement prévoit que : « *les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)* ».

La délégation a été informée que, dans la version de l'application « StopCovid France » disponible au jour du contrôle (version v1.0.* de l'application), lorsqu'un utilisateur se déclare avoir été diagnostiqué ou dépisté positif au virus SARS-CoV-2, l'ensemble de son historique de contacts est remonté au serveur central géré pour le compte du ministère des solidarités et de la santé, sans processus de pré-filtrage préalable des données, reposant sur des critères de distance et de durée du contact avec un autre utilisateur.

Or, le 5° du I de l'article 2 du décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid » prévoit que « *l'historique de proximité d'un utilisateur* » se limite aux données de contacts de l'utilisateur avec « *d'autres utilisateurs qui se trouvent, pendant une durée déterminée, à une distance de son téléphone mobile telle qu'il existe un risque suffisamment significatif qu'un utilisateur qui serait positif au virus covid-19 contamine l'autre* ».

Par ailleurs, le 6° du I de l'article 2 du décret précité précise que les données de « *l'historique de proximité des contacts à risque de contamination par le virus covid-19 (...) sont transmises par les utilisateurs diagnostiqués ou dépistés positifs au virus du covid-19 qui le souhaitent au serveur central* ».

Si les termes du décret et les éléments qui avaient été transmis à la Commission n'excluent pas qu'un filtrage complémentaire puisse être opéré au niveau du serveur central, il résulte toutefois de ces dispositions que le traitement autorisé par le décret du 29 mai 2020, conformément à ce qui avait été présenté à la Commission, doit procéder à un premier filtrage au niveau du téléphone.

Par conséquent, la version de l'application « StopCovid France » disponible au jour du contrôle (version v1.0.* de l'application) est contraire aux dispositions du décret du 29 mai 2020.

Les faits précités constituent un manquement aux obligations prévues à l'article 5-1-a) du RGPD.

Au demeurant, il est relevé que la conception de l'application décrite dans le décret, qui permet d'éviter la remontée de l'ensemble de l'historique de contacts de l'utilisateur au serveur central grâce au pré-filtrage des données de l'historique de proximité directement depuis l'ordinateur, constituait un choix particulièrement pertinent au regard de l'objectif de protection des données personnelles.

Il est également observé que la dernière version disponible de l'application (version v1.1.*) – dans laquelle la fonctionnalité de pré-filtrage des données de l'historique de contacts est active au niveau du téléphone de l'utilisateur – est conforme sur ce point au décret et davantage protectrice des données à caractère personnel.

La Présidente de la CNIL estime donc nécessaire, afin que le traitement respecte pleinement les dispositions du décret du 29 mai 2020, que le responsable de traitement cesse de faire remonter l'intégralité des données de l'historique de contacts de l'utilisateur au serveur central, par exemple en prenant toutes mesures appropriées permettant de généraliser l'usage de la nouvelle version de l'application.

Un manquement à l'obligation d'informer les personnes concernées

L'article 13 du Règlement exige du responsable de traitement qu'il fournisse, au moment où les données sont collectées, les informations relatives à son identité et ses coordonnées, celles du délégué à la protection des données, les finalités du traitement et sa base juridique, les destinataires ou catégories de destinataires des données à caractère personnel, le cas échéant les transferts de données personnelles hors de l'Union européenne, la durée de conservation des données personnelles, les droits dont bénéficient les personnes sur le traitement de leurs données ainsi que le droit d'introduire une réclamation auprès d'une autorité de contrôle.

La délégation a constaté que la politique de traitement des données à caractère personnel est fournie aux utilisateurs de l'application « StopCovid France » à partir d'une rubrique « confidentialité » - accessible lors du parcours d'activation de l'application - et depuis la page web <https://bonjour.stopcovid.gouv.fr/privacy.html> intitulée « Données personnelles » - également accessible depuis plusieurs liens du parcours d'activation de l'application. La rubrique « confidentialité » et la page « Données personnelles » informent les utilisateurs de l'application de l'identité et des coordonnées du responsable de traitement et du délégué à la protection des données, des finalités du traitement et de sa base juridique, de la durée de conservation des données, des droits des personnes concernées, notamment de leur droit à introduire une réclamation auprès de la CNIL.

La Présidente estime que l'information fournie est pour l'essentiel conforme au RGPD. Elle estime cependant que, sur un point, l'information fournie sur les catégories de destinataires des données est incomplète.

En effet, la rubrique « confidentialité » informe uniquement l'utilisateur que « *Les données sont partagées par [l'] application avec le serveur géré par le Ministère des Solidarités et de la Santé, seulement si vous êtes testé positif et avec votre accord* ». La section « destinataire des données » de la page « Données personnelles » ne contient par ailleurs qu'un seul paragraphe concernant les destinataires, rédigé en ces termes : « *Les utilisateurs identifiés par l'application comme contacts à risque d'avoir contracté le virus COVID-19 sont destinataires de l'information selon laquelle ils ont été à proximité d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus du COVID-19* ».

Or, la délégation a notamment été informée que INRIA, agissant en qualité d'assistant à la maîtrise d'œuvre du ministère des solidarités et de la santé, traite des données à caractère personnel issues de l'application « StopCovid France » pour le compte du ministère des solidarités et de la santé.

Par conséquent, les informations fournies aux utilisateurs de l'application « StopCovid France » relatives aux destinataires ou aux catégories de destinataires des données à caractère personnel devraient mentionner l'existence d'un sous-traitant et sont incomplètes sur ce point.

Ces faits constituent un manquement à l'article 13 du RGPD.

Un manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués par des sous-traitants pour le compte du responsable de traitement

L'article 28 du Règlement prévoit que lorsqu'un traitement est effectué par un sous-traitant, ce traitement est régi par un contrat ou un autre acte juridique qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées ainsi que les obligations et les droits du responsable de traitement. Ce contrat prévoit en outre les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement.

La délégation a constaté que INRIA est titulaire d'un marché d'assistance à la maîtrise d'œuvre pour le compte du ministère des solidarités et de la santé au titre, notamment, des missions de déploiement, d'infogérance, d'exploitation, d'hébergement et de maintenance évolutive de l'application « StopCovid ». Dans ce cadre, INRIA agit comme sous-traitant du traitement des données à caractère personnel pour le compte du ministère des solidarités et de la santé.

La délégation a constaté que le marché liant INRIA au ministère des solidarités et de la santé contient la plupart des mentions exigées par l'article 28 du RGPD. Il précise notamment l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel traitées ainsi que les catégories de personnes concernées.

La délégation a néanmoins constaté que les clauses des pièces contractuelles du marché d'assistance à la maîtrise d'œuvre qui lui ont été adressées à l'issue de ses missions de contrôle, et en réponse à la demande formulée dans ce cadre, sont incomplètes sur les obligations et les droits du responsable de traitement et sur les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement et, notamment, ne précisent pas que le sous-traitant aide le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits, que le sous-traitant aide le responsable de traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD et que le sous-traitant met à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 et permettre la réalisation d'audits.

Ces faits constituent un manquement à l'article 28 du RGPD.

Un manquement à l'obligation de réaliser une analyse d'impact complète

L'article 35-7-a) du Règlement impose que l'analyse d'impact relative à la protection des données contienne au moins « *une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable de traitement* ».

La délégation a constaté que le ministère des solidarités et de la santé a procédé, depuis le lancement de l'application « StopCovid France », à une mise à jour de son analyse d'impact relative à la protection des données personnelles issues de l'application. Le ministère des solidarités et de la santé a ainsi remis à la délégation une version de l'analyse d'impact mise à jour au 3 juillet 2020. Les études d'impact réalisées sont globalement conformes aux dispositions de l'article 35-7-a) et suivent, pour l'essentiel, les recommandations de la Commission.

La délégation a néanmoins constaté que la dernière version de l'AIPD ne précise pas que la solution anti DDOS (solution visant à prévenir les attaques par déni de service) proposée par la société ORANGE et implémentée dans l'application aux fins de sécurisation du système, entraîne la collecte des adresses IP (« *internet protocol* ») des utilisateurs de l'application.

Or, la délégation a constaté que lorsqu'un utilisateur se connecte à l'application « StopCovid France », l'adresse IP de l'ordiphone est collectée dans le cadre de la solution anti DDOS de la société ORANGE.

Il a par ailleurs été constaté que la collecte de cette donnée à caractère personnel n'a pas d'autre finalité, en l'espèce, que celle d'assurer la sécurité du dispositif.

La Présidente précise que la solution anti DDOS étant une solution de sécurité du dispositif, celle-ci n'avait pas à figurer dans le décret du 29 mai 2020. Dès lors, les données traitées par cette solution n'avaient pas non plus à figurer dans ce décret. La collecte des adresses IP dans ce cadre n'est donc pas irrégulière.

En revanche, dès lors que cette solution de sécurité entraîne une collecte de données à caractère personnel, la description de cette opération de traitement doit apparaître dans l'analyse d'impact réalisée par le responsable de traitement.

De même, la délégation a constaté que la collecte des données présentes sur l'équipement connecté de l'utilisateur dans le cadre de la technologie reCaptcha de la société GOOGLE déployée dans la version initiale de l'application (v1.0.* de l'application), n'est pas précisée dans l'analyse d'impact.

En ne décrivant pas la totalité des opérations de traitement des données à caractère personnel en lien avec l'application « StopCovid France » et les mesures pour limiter les risques, l'analyse d'impact établie par le ministère des solidarités et de la santé ne répond pas pleinement aux exigences de l'article 35 du RGPD.

Ces faits constituent un manquement à l'article 35 du RGPD.

2. Le manquement au regard des dispositions de la loi « Informatique et Libertés »

Un manquement à l'obligation d'informer l'utilisateur et d'obtenir son consentement avant d'inscrire et de lire des informations sur son équipement terminal de communication électronique

L'article 82 de la loi du 6 janvier 1978 modifiée dispose que :

« Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable de traitement ou son représentant :

1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;

2° Des moyens dont il dispose pour s'y opposer.

Ces accès inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

(...) »

La délégation a été informée que l'application « StopCovid France » contient dans ses deux versions une solution « captcha » destinée à évaluer si le comportement d'un utilisateur de l'application correspond ou non à celui d'un humain.

La délégation a été informée que la dernière version de l'application « StopCovid France » (version v.1.1.*) repose sur la technologie captcha développée par la société ORANGE, qui ne requiert aucune opération de lecture ou d'écriture sur l'ordiphone de l'utilisateur.

En revanche, la version initiale de l'application « StopCovid France » (version v1.0.*) contient la technologie reCaptcha, dans sa version « invisible », développée par la société GOOGLE.

La délégation a constaté que la société GOOGLE informe les développeurs de la technologie reCaptcha « *que le fonctionnement de l'API reCAPTCHA repose sur la collecte d'informations matérielles et logicielles (telles que les données sur les appareils et les applications) et que ces données sont transmises à Google pour analyse [...] Il vous incombe d'en informer les utilisateurs et de demander leur autorisation pour la collecte et le partage de ces données avec Google. Pour les utilisateurs en Union européenne, le ou les clients d'API, ainsi que vous-même, doivent se conformer aux Règles relatives au consentement de l'utilisateur dans l'UE* » (<https://www.google.com/recaptcha/admin/create?pli=1>).

Il résulte des informations fournies par la société GOOGLE aux développeurs que la collecte d'informations sur l'ordiphone de l'utilisateur n'a pas pour seule finalité la sécurisation de l'application mais permet également des opérations d'analyse de la part de cette société. La société informe elle-même les développeurs que le recours à cette solution est soumis aux exigences posées par l'article 82 de la loi « Informatique et Libertés », à savoir l'information et le recueil du consentement des personnes concernées pour ces opérations.

Or, la délégation a constaté que les utilisateurs de l'application « StopCovid France » dans sa version v1.0.* ne sont à aucun moment informés, notamment par une fenêtre de consentement au moment de l'activation de l'application, de la collecte d'informations stockées sur leurs équipements mobiles ni des moyens de refuser cette collecte.

Il en résulte également que le consentement de l'utilisateur portant sur l'accès aux informations stockées sur son équipement mobile ou sur l'inscription d'informations sur son équipement mobile n'est recueilli à aucun moment du parcours d'activation de l'application « StopCovid France ».

Ces faits constituent un manquement à l'article 82 de la loi Informatique et Libertés.

En outre, en l'état des informations dont elle dispose, la Présidente de la CNIL ne peut exclure que le reCaptcha Google puisse encore être utilisé par des personnes ayant téléchargé la version 1.0.* de l'application mais ne l'ayant pas encore activée.

IV. Observation complémentaire

La lutte contre l'épidémie de covid-19, qui relève de l'objectif à valeur constitutionnelle de protection de la santé, constitue un impératif majeur de nature à justifier, dans certaines conditions, des atteintes au droit à la protection de la vie privée et des données à caractère personnel.

Il est néanmoins rappelé que l'atteinte portée à la vie privée n'est admissible en l'espèce que si le gouvernement peut s'appuyer sur des éléments suffisants pour avoir l'assurance raisonnable que le dispositif de l'application « StopCovid France » est utile à la gestion de la crise. La Commission avait donc demandé, dans son avis du 25 mai 2020, que l'impact effectif du dispositif sur la stratégie sanitaire globale soit étudié et documenté par le gouvernement de manière régulière pendant toute sa période d'utilisation.

Il a été constaté, au jour des contrôles, que l'évaluation formelle de l'effectivité de l'application n'avait pas encore débuté et que le calendrier du travail d'évaluation n'avait pas encore été établi par le ministère.

La Présidente de la CNIL invite dès lors le ministère des solidarités et de la santé à engager dans les meilleurs délais cette démarche d'évaluation et à lui rendre compte de ses résultats.

Au vu des manquements précités, et compte tenu des informations dont elle a reçu communication de la part du ministère des solidarités et de la santé relatives au nombre d'applications encore installées dans la version v.1.0.* postérieurement à la sortie de la version v1.1.* de l'application, la Présidente de la CNIL met en demeure le ministère des solidarités et de la santé, sis 14 avenue Duquesne 75007, sous un délai d'un (1) mois à compter de la notification de la présente décision et sous réserve des mesures qu'il aurait déjà pu adopter, de :

- **cesser de faire remonter l'intégralité des données de l'historique de contacts de l'utilisateur au serveur central en méconnaissance du cadre légal défini par les dispositions du décret n° 2020-650 du 29 mai 2020, par exemple en forçant la mise à jour de l'application « StopCovid France » vers la nouvelle version v1.1.* par le blocage de l'application dans sa version v1.0.* ;**
- **compléter l'information fournie aux utilisateurs de l'application « StopCovid France » dans les conditions prévues à l'article 13 du Règlement, en fournissant aux utilisateurs une information complète sur les destinataires ou catégories de destinataires des données à caractère personnel issues de l'application ;**
- **veiller à ce que les contrats de sous-traitance conclus dans le cadre de l'exploitation de l'application « StopCovid France » contiennent les mentions prévues à l'article 28 du Règlement ;**
- **compléter l'analyse d'impact relative à la protection des données à caractère personnel issues de l'application « StopCovid France » conformément à l'article 35 du Règlement,**
 - en mentionnant la collecte de l'adresse IP de l'équipement mobile de l'utilisateur de l'application dans le cadre des mesures de sécurité du système reposant sur la solution anti DDOS de la société ORANGE,
 - en mentionnant la collecte des informations présentes sur l'équipement mobile de l'utilisateur dans le cadre de la technologie reCaptcha de la société GOOGLE déployée dans le cadre de la version v1.0.* de l'application, dans l'hypothèse où ces données seraient encore collectées ;

- **veiller, le cas échéant, à informer et recueillir le consentement des personnes concernées aux actions de lecture et d'écriture des informations présentes sur les terminaux de communication électronique par la société GOOGLE dans le cadre de la technologie reCaptcha (version v1.0.* de l'application), conformément aux dispositions de l'article 82 de la loi « Informatique et Libertés ».**
Cette injonction vise le cas des utilisateurs ayant téléchargé la version v1.0.* de l'application et ne l'ayant pas encore activée pour la première fois.
- **justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.**

À l'issue de ce délai, si le ministère des solidarités et de la santé s'est conformé à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, si le ministère des solidarités et de la santé ne s'est pas conformé à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l'une des mesures prévues par l'article 20 de la loi du 6 janvier 1978 modifiée.

La Présidente



Marie-Laure DENIS