CORONAVIRUS ET PROTECTION DES DONNEES PERSONNELLES

Conseils pratiques publié le **15/09/2021**, vu **1174 fois**, Auteur : Murielle Cahen

Si les technologies de l'information et de la communication peuvent contribuer à lutter contre la pandémie de Covid-19, il faut faire attention à la protection des données personelles

En plus des données permettant de localiser les individus, une seconde catégorie de données personnelles est mobilisée par les technologies de l'information pour lutter contre la pandémie : il s'agit bien entendu des données à caractère médical, qui ont vocation à permettre de surveiller des symptômes pour décider ou orienter une prise en charge ou à préciser l'étiologie de l'infection.

Alors que le confinement sera progressivement levé à partir du 11 mai prochain, comme l'a annoncé le Président de la République lors de son allocution du 13 avril, le Gouvernement a annoncé son intention de recourir après cette date, à l'instar d'autres pays comme Singapour, à une application de suivi des interactions sociales des personnes (« contact tracing » ou « proximity tracing »), nommée STOPCOVID. La CNCDH s'inquiète du fait que la gestion de la crise sanitaire puisse donner lieu à l'expérimentation par les pouvoirs publics de nouvelles technologies dont l'impact sur les droits et libertés fondamentaux serait considérable.

La compréhension des principes de la réglementation relative à la protection des données à caractère personnel part d'un constat : celui de la généralisation de l'outil informatique dans le quotidien. L'utilisation des nouvelles technologies est autant une source de progrès que de risques d'immixtion dans la vie privée.

En effet, les informations et les données qui nous concernent font l'objet chaque jour de multiples opérations de collecte, de transfert et, plus généralement, de traitement que ce soit au travail au cours d'un simple appel téléphonique ou de l'envoi d'un SMS et, encore plus, sur Interne.

Forte d'une réflexion engagée dans le passé à l'égard des enjeux attachés au développement de ces outils numériques, aux questions relatives aux données personnelles, et bien que les détails de l'application STOPCOVID ne soient pas encore totalement connus, la CNCDH a décidé de s'autosaisir de la question de l'utilisation d'outils numériques de suivi des personnes en raison des risques d'atteintes aux libertés individuelles et collectives, notamment le respect de la vie privée et la protection des données personnelles, et de discriminations.

De ce qui précède, il faudrait ajouter que loi Informatique et libertés pose une interdiction de principe des traitements de données à caractère personnel relatives à la santé du fait qu'elles sont considérées comme des données sensibles. Certains traitements de données de santé s'avérant indispensables au bon fonctionnement de notre société ou utiles aux personnes concernées par la collecte, de nombreuses exceptions sont prévues. Reste une question inévitable : quelle sécurité pour nos données personnelles et nos vies privées ?

I) La protection de la vie-privée : un droit fondamental

A) Coronavirus - StopCovid : le Gouvernement obtient un « oui » circonstancié de la CNIL

Dans son discours mardi à l'Assemblée, Édouard Philippe a insisté sur la nécessité de casser les chaînes de transmission, en identifiant au plus vite les personnes ayant été au contact des personnes infectées. Des brigades sanitaires, d'environ 20 000 à 30 000 personnes, seront chargées de remonter la liste des cas contacts, pour les inviter à se faire tester.

Pour cela, l'article 6 va créer une base de données pour ces enquêtes épidémiologiques. Ce fichier pourra contenir des données de santé et d'identification sur les personnes infectées et celles ayant été en contact avec elles, le cas échéant sans leur consentement. Il pourra également être nourri des données de Santé publique France, de l'assurance maladie et des agences régionales de santé. Les services de santé et les laboratoires autorisés à réaliser les tests pourront avoir accès aux données.

Les mesures d'application seront précisées par un décret en Conseil d'État, pris après avis de la CNIL, et par ordonnances. L'application de tracking « StopCovid » pourra être mise en place par ces ordonnances, mais le premier ministre a promis un débat et un vote spécifique, quand sa mise en œuvre aura avancé.

Point d'attention sur la notion de volontariat. - Le volontariat ne doit pas uniquement se traduire par le choix, pour l'utilisateur, de télécharger puis de mettre en œuvre l'application ou la faculté de la désinstaller. Il signifie également qu'aucune conséquence négative n'est attachée à l'absence de téléchargement ou d'utilisation de l'application. Ainsi le téléchargement ou l'utilisation de cette application ne doit conditionner ni l'accès aux tests et aux soins ; ni la possibilité de se déplacer, dans le cadre de la levée du confinement ; ni l'accès à certains services (comme les transports en commun) ; ni certains droits ou accès par les institutions publiques ou les employeurs. Les utilisateurs ne doivent pas non plus être contraints de sortir en possession de leur équipement mobile.

Durée nécessairement limitée de la conservation des données. - La collecte et le traitement de données opérées par l'application doivent être temporaires, d'une durée limitée à celle de l'utilité du dispositif. Les données devront être supprimées dès le moment où l'utilité de l'application ne sera plus avérée. La CNIL recommande donc que l'impact du dispositif sur la situation sanitaire soit étudié et documenté de manière régulière, pour aider les pouvoirs publics à décider ou non de son maintien. 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 ».

Recommandations sur l'architecture et la sécurisation de l'application. - Dans le cas où le recours à ce dispositif serait adopté à l'issue d'un débat au Parlement, la CNIL émet des recommandations qui portent sur : la responsabilité du traitement ; la nécessité de réaliser une analyse d'impact sur la protection des données ; l'exactitude des données ; la sécurité des données ; le respect des droits des personnes sur leurs données à caractère personnel. Elle souligne que l'ensemble de ces précautions et garanties est de nature à favoriser la confiance du public dans ce dispositif, qui constitue un facteur déterminant de sa réussite et de son utilité.

La nécessité d'un fondement juridique. - La Commission estime opportun que le recours à un dispositif volontaire de suivi de contact pour gérer la crise sanitaire actuelle dispose d'un fondement juridique explicite dans le droit national. Elle demande au Gouvernement de la saisir à nouveau du projet d'application et du projet de norme l'encadrant lorsque la décision aura été prise et le projet précisé. Dans un communiqué, le Gouvernement indique qu'il réalisera et publiera une analyse d'impact sur la protection des données et soumettra de nouveau le projet finalisé, le cas échéant accompagné des projets de dispositions réglementaires envisagées. Il précise que, comme le demande la CNIL, le code source de l'application, du serveur central et leur paramétrage seront ouverts.

B) Risque quant à l’atteinte disproportionnée aux libertés fondamentales

Interrogée par le gouvernement sur son projet d’application "StopCovid", la Commission lui a rappelé les nombreuses conditions à respecter pour assurer la conformité au RGPD et à la loi Informatique et libertés d’une telle application estimée fortement attentatoire à la vie privée. Une atteinte disproportionnée aux libertés fondamentales.

Afin de limiter le caractère intrusif des fonctionnalités des applications, les orientations de la Commission européenne mettent l'accent sur la nécessité de respecter les principes de protection des données personnelles :

· Les autorités sanitaires nationales seront responsables du traitement des données

C'est ce que préconise la Commission européenne compte tenu du caractère sensible des données qui pourront être obtenues. Elle estime que cela permettra également de renforcer la confiance des utilisateurs et l'acceptation des applications.

· Les utilisateurs doivent conserver le contrôle sur leurs données

?Pour la Commission, la confiance dans les applications passe aussi par la maîtrise de ses données personnelles. Pour cela, il est impératif de remplir plusieurs conditions telles que

l'installation de l'application sur une base volontaire, la séparation des fonctionnalités de manière à obtenir un consentement pour chacune d'entre elles, le stockage local sur le terminal de l'utilisateur, la fourniture d'informations aux personnes, la possibilité d'exercer leurs droits, etc.

· Le traitement doit disposer d'une base juridique

La Commission européenne estime que le consentement est la base juridique la plus appropriée pour le stockage d'informations sur l'appareil de la personne concernée ou l'accès à des informations déjà stockées.

Quant au choix de la base légale pour le traitement des données par les autorités sanitaires, la Commission estime que "compte tenu de la nature des données à caractère personnel concernées (en particulier relatives à la santé) ainsi que des circonstances de l'actuelle pandémie de COVID- 19, le fait de prendre la législation comme base juridique contribuerait à la sécurité juridique, car cette législation :

- prescrirait en détail le traitement de données spécifiques relatives à la santé et préciserait clairement les finalités du traitement ;

- indiquerait clairement qui est le responsable du traitement, et qui peut accéder aux données en question ;

- exclurait la possibilité de traiter les données en question pour des finalités différentes de celles énumérées dans la législation ;

- et prévoirait des garanties spécifiques".

Bien entendu, la Commission précise que le choix de l'obligation légale comme base juridique "ne change rien au fait que les personnes restent libres d'installer l'application ou non et de partager leurs données avec ces autorités".

· Le principe de minimisation des données doit s'appliquer

?La Commission rappelle que seules les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard de leur finalité peuvent être traitées. Elle prend pour exemple l'analyse des symptômes ou la télémédecine, finalités pour lesquelles l'accès à la liste des contacts de la personne concernée n'est évidemment pas nécessaire.

· Les finalités de l'application doivent être déterminées avec précision

?Plusieurs finalités peuvent être poursuivies par le traitement de données : fourniture d'informations du point de vue des autorités sanitaires, analyse des symptômes et télémédecine, recherche de contacts et avertissement (dans ce dernier cas, la Commission recommande d'indiquer une finalité très précise, par exemple "conservation des coordonnées des personnes utilisant l'application et susceptibles d'avoir été exposées à l'infection par le COVID-19, afin d'avertir les personnes pouvant avoir été infectées").

· Fixer des limites strictes pour la conservation des données

?La Commission recommande de fixer des délais de conservation selon la pertinence d'un point de vue médical ainsi qu'en fonction de la durée réaliste pour prendre les mesures administratives nécessaires. Ainsi, pour la fonctionnalité de recherche de contacts, les données doivent être effacées dès lors qu'elles ne sont plus nécessaires pour prévenir les personnes concernées. En tout état de cause, la Commission préconise un délai maximum d'un mois. Elle précise en revanche que ces données peuvent être conservées plus longtemps à des fins de recherches ou d'établissement d'un rapport de surveillance, à condition qu'elles le soient sous forme anonymisée.

· Garantir la sécurité des données

Il apparaît enfin essentiel à la Commission que les données soient stockées sur le terminal de l'utilisateur sous forme cryptée, en utilisant des techniques cryptographiques de pointe, et dans un format pseudonymisé.

Elle prône la création et le stockage d'identifiants d'utilisateurs temporaires qui changent régulièrement, au cours de la collecte de données de proximité par Bluetooth, plutôt que le stockage du véritable identifiant du dispositif. Cela afin d'offrir une protection supplémentaire contre les écoutes et le pistage par des pirates informatiques qui pourraient identifier des personnes.

II) Le recours au numérique : l'élément central d'une stratégie de protection de la santé publique d'une stratégie de déconfinement

A) Covid-19 : les outils numériques au cœur de la stratégie de déconfinement

Parce qu'omniprésents dans la vie des citoyens de l'Union, les outils numériques ont toutes les chances de devenir une arme précieuse dans la lutte contre le coronavirus. Une possibilité que la Commission invite aujourd'hui à explorer, grâce à des recommandations précises destinées aux États membres et l'idée d'une boîte à outils commune.

« L'Europe est plus forte lorsqu'elle agit comme un seul homme » : voilà comment Thierry Breton, commissaire au marché intérieur, résume l'état d'esprit qui règne aujourd'hui au sein des institutions européennes. La crise sanitaire actuelle place les États membres et l'UE face à des défis sans précédent pour les systèmes de santé et la stabilité économique de l'Union, comme pour les habitudes de vie et les valeurs européennes communes. Des bouleversements que les États membres ne pourront pas combattre en agissant seuls : pour la Commission, une crise d'une telle magnitude requiert une action commune de tous les membres et institutions de l'UE, dans un esprit de solidarité essentiel. Et aujourd'hui, parmi les différents travaux communs de réflexion qui occupent l'Union, le rôle des outils numériques dans la levée progressive du confinement intéresse tout particulièrement.

A la Commission, l'heure est à la réflexion : comment développer une approche commune de l'UE à propos de l'utilisation des applications et données mobiles dans la lutte contre la pandémie de Covid-19 et la préparation du déconfinement ? Et surtout, comment garantir la sécurité des données utilisées dans l'Union européenne, berceau du RGPD et modèle absolu de protection des données personnelles ?

La pièce maîtresse des recommandations de la Commission est l'idée d'une boîte à outils à double utilité, qui permettrait à la fois de mieux accompagner les citoyens et d'étoffer le travail des chercheurs. En bref, cette boîte à outils viendrait à la fois :

- faciliter l'organisation des citoyens face au virus, avec une approche coordonnée paneuropéenne de l'utilisation d'applications mobiles permettant aux citoyens d'adopter des mesures efficaces, notamment pour la distanciation sociale, et pour faciliter l'alerte, la prévention et le traçage des contacts ;

- et faciliter la modélisation de l'évolution du virus, via une approche commune qui permettrait de modéliser et de prévoir l'évolution du virus grâce aux données de localisation mobile, bien entendu anonymisées et agrégées.

Pour le développement de la boîte à outils, les États membres devront se réunir et rencontrer les représentants des institutions européennes, dès à présent et fréquemment par la suite. L'idée, ici, est de leur permettre de partager leurs constatations et suggestions quant à la meilleure façon d'utiliser les données sans négliger la sécurité des données personnelles et de la vie privée.

B) Différents types de suivi numérique

Le Comité national pilote d'éthique du numérique distingue deux types de suivis numériques : le suivi collectif et le suivi individuel. Le suivi collectif concerne des groupes de population identifiés selon des critères variés, par exemple géographiques ou des critères de santé, de vulnérabilité, etc. Le suivi individuel, quant à lui, concerne les personnes elles-mêmes.

Celles-ci pourraient inclure l'ensemble de la population, les personnes testées positivement, les personnes qui présentent des symptômes compatibles avec ceux de la maladie, celles ayant été en contact ou à proximité physique de personnes testées positivement, ou les contacts enregistrés dans le carnet d'adresses d'une personne.

Les moyens de suivi individuel pourraient, selon le Comité, être mis en œuvre de manière obligatoire ou sur une base volontaire.

Dans le cas du suivi obligatoire, seraient invoqués l'urgence des mesures, les impératifs de santé publique ainsi que le besoin de toucher une plus grande partie de la population.

Dans le cas du suivi volontaire, l'adhésion libre serait encouragée par une information au public sur l'utilité du suivi et par un appel au sens civique, une incitation sociale, par exemple par envoi de SMS et de messages publics.

Le Comité alerte, par ailleurs, sur la nécessité de définir la fin de l'urgence sanitaire et la sortie de crise pour fixer légalement la durée des mesures de suivi afin qu'elle soit la plus limitée possible. Le risque étant que ces mesures d'exception s'installent dans la durée.

Afin d'éviter toutes dérives, le Comité recommande :

En cas de mesures volontaires de suivi numérique, de garantir le consentement libre et éclairé des personnes concernées ;

De définir et d’annoncer une durée légale strictement limitée et de garantir les conditions de sa réversibilité ;

De ne pas recourir à la prolongation automatique des autorisations de suivi ;

De prévoir la désactivation automatique des mesures de suivi individuel après l'expiration du délai légal ainsi que les moyens d’en rendre compte publiquement ;

D’évaluer la nécessité et proportionnalité des mesures à des intervalles réguliers ;

De définir les critères d’efficience des mesures et de les évaluer de manière régulière ;

De mettre en œuvre les moyens spécifiques et adaptés pour garantir leur sécurité et prévenir tout mésusage ;

De permettre aux personnes de signaler une erreur, de recevoir une réponse à leur requête et d’initier un recours en cas de préjudice subi ;

En cas d’adhésion volontaire, de permettre aux personnes de revenir sur leur engagement et de permettre l’effacement des données collectées ;

D’imposer une certification des applications spécifiques de suivi par les autorités publiques.

Auditionnée par la commission des lois de l’Assemblée nationale, le 8 avril, la Présidente de la CNIL a affirmé que si un suivi individualisé des personnes était mis en œuvre, il faudrait qu’il soit basé sur le volontariat, avec un consentement réellement libre et éclairé. Elle a par ailleurs ajouté que le fait de refuser l’application n’aurait aucune conséquence préjudiciable. En revanche, alerte la CNIL, si un dispositif de suivi des personnes était mis en place de manière obligatoire, une disposition législative serait nécessaire.

SOURCES :

· https://www.cnil.fr/fr/crise-sanitaire-audition-de-marie-laure-denis-presidente-de-la-cnil-devant-la-commission-des-lois

. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041842574&categorieLien=id

· https://www.bfmtv.com/tech/l-application-stopcovid-sera-testee-a-partir-du-11-mai-1907394.html

· https://www.lemonde.fr