II

(Communications)

COMMUNICATIONS PROVENANT DES INSTITUTIONS, ORGANES ET ORGANISMES DE L'UNION EUROPÉENNE

COMMISSION EUROPÉENNE

COMMUNICATION DE LA COMMISSION

Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données

(2020/C 124 I/01)

1 CONTEXTE

La pandémie de COVI-19 a fait naître un défi sans précédent pour l'Union et les États membres, leurs systèmes de soins de santé, leur mode de vie, leur stabilité économique et leurs valeurs. Les technologies et données numériques ont un rôle précieux à jouer dans la lutte contre la crise de la COVID-19. Les applications mobiles généralement installées sur les smartphones (les «applications») peuvent aider les autorités de santé publique, tant au niveau national qu'au niveau de l'UE, à surveiller et à maîtriser la pandémie de COVID-19 et sont particulièrement utiles dans la phase de levée des mesures de confinement. Elles peuvent fournir des orientations directes aux citoyens et soutenir les efforts de recherche de contacts. Dans plusieurs pays, aussi bien dans l'Union européenne qu'au niveau mondial, les autorités nationales ou régionales ainsi que les développeurs ont annoncé le lancement d'applications dotées de différentes fonctionnalités destinées à contribuer à la lutte contre le virus.

Le 8 avril 2020, la Commission a adopté une recommandation concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées (ci-après la «recommandation») ([1]). La recommandation vise notamment à développer une approche européenne commune (la «boîte à outils»), coordonnée au niveau de l'Union, de l'utilisation d'applications mobiles permettant aux citoyens de prendre des mesures efficaces de distanciation sociale, et servant à l'alerte, à la prévention et à la recherche de contacts, afin de limiter la propagation de la COVID-19. La recommandation énonce les principes généraux qui devraient accompagner l'élaboration d'une telle boîte à outils et elle fait savoir que la Commission publiera d'autres orientations, notamment sur les conséquences de l'utilisation des applications dans ce domaine sur la protection des données à caractère personnel et le respect de la vie privée.

Avec la feuille de route européenne commune pour la levée des mesures de confinement liées à la COVID-19, la Commission, en coopération avec le président du Conseil européen, a énoncé un certain nombre de principes destinés à accompagner la suppression progressive des mesures de confinement liées à la pandémie de COVI-19. Les applications mobiles, dont les fonctionnalités de recherche de contacts, peuvent jouer un rôle important dans ce contexte. Selon les caractéristiques des applications et leur degré d'utilisation au sein de la population, elles peuvent avoir une incidence importante sur le diagnostic de la maladie, son traitement et sur la gestion de la COVID-19 au sein et en dehors du milieu hospitalier. Elles sont particulièrement utiles lorsque les mesures de confinement sont levées et que le risque d'infection augmente étant donné que de plus en plus de personnes sont en contact les unes avec les autres. Ces applications peuvent aider à interrompre la chaîne de transmission de l'infection de manière plus rapide et plus efficace que les mesures générales de confinement et elles peuvent réduire le risque de propagation importante du virus. Elles devraient donc constituer un élément important de la stratégie de sortie, en complément d'autres mesures telles que des capacités de dépistage accrues ([2]). L'une des conditions préalables importantes pour le développement, l'acceptation et l'adoption de ces applications par les particuliers est la confiance. Les citoyens doivent être certains que leurs droits fondamentaux sont respectés et que les applications ne seront utilisées qu'aux fins spécifiquement définies, qu'elles ne seront pas utilisées pour la surveillance de masse et que les citoyens resteront maîtres de leurs données. Il s'agit là des principes de base pour permettre à ces applications de maîtriser la propagation du virus avec précision et efficacité. Il est dès lors essentiel de

([1]) Recommandation C(2020) 2296 final du 8 avril 2020 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.
([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

recenser les solutions les moins intrusives et respectant totalement les exigences en matière de protection des données à caractère personnel et de respect de la vie privée énoncées dans le droit de l'Union. En outre, les applications devront être désactivées au plus tard lorsque la pandémie sera déclarée sous contrôle. Les applications devront également inclure les dispositifs les plus performants de protection des informations.

Les présentes orientations tiennent compte de la contribution du comité européen de la protection des données ([3]) et des discussions au sein du réseau «santé en ligne». Le comité européen de la protection des données prévoit de publier des lignes directrices au cours des jours prochains sur la géolocalisation et d'autres outils de traçage dans le cadre de la pandémie de COVID-19.

Champ d'application des orientations

Afin de garantir une approche cohérente dans l'ensemble de l'UE et de fournir des orientations aux États membres et aux développeurs d'applications, le présent document énonce des caractéristiques et des exigences auxquelles les applications doivent satisfaire pour garantir le respect de la législation de l'UE en matière de protection des données à caractère personnel et de respect de la vie privée, en particulier le règlement général sur la protection des données ([4]) (RGPD) et la directive «vie privée et communications électroniques» ([5]). Les présentes orientations n'abordent aucune autre condition, notamment les restrictions que les États membres auraient pu inclure dans leur législation nationale en ce qui concerne le traitement des données relatives à la santé.

Les orientations ne sont pas juridiquement contraignantes. Elles sont sans préjudice du rôle de la Cour de justice de l'UE, qui est la seule institution pouvant donner une interprétation du droit de l'Union faisant autorité.

Les présentes orientations concernent uniquement les applications d'utilisation volontaire qui aident à combattre la pandémie de COVID-19 (les applications téléchargées, installées et utilisées sur une base volontaire par les personnes) et présentant une ou plusieurs des fonctionnalités suivantes:

— fournir des informations exactes aux personnes sur la pandémie de COVID-19;

— fournir des questionnaires d'auto-évaluation et des conseils aux personnes (fonctionnalité d'analyse des symptômes) ([6]);

— avertir les personnes qui se sont trouvées à proximité d'une personne infectée pendant un certain temps afin de fournir des informations sur un autoconfinement éventuel et sur les centres de dépistage (fonctionnalité de recherche de contact et d'avertissement);

— prévoir un espace de communication entre les patients soumis à l'auto-isolement et les médecins ou permettant un diagnostic plus poussé et des conseils de traitement (recours accru à la télémédecine).

En vertu de la directive «vie privée et communications électroniques», imposer l'utilisation d'une application faisant intervenir les droits relatifs à la confidentialité des communications énoncés à l'article 5 n'est possible que par une loi qui est nécessaire, appropriée et proportionnée pour protéger certains objectifs spécifiques. Étant donné le degré élevé d'intrusion de cette approche et les défis y afférents, notamment en termes de mise en place de garanties appropriées, la Commission est d'avis qu'une analyse approfondie est nécessaire avant de recourir à cette option. C'est pourquoi la Commission recommande le recours à des applications d'utilisation volontaire.

Les présentes orientations ne couvrent pas les applications visant à faire appliquer les exigences en matière de quarantaine (y compris celles qui sont obligatoires).

2 CONTRIBUTION DES APPLICATIONS À LA LUTTE CONTRE LA COVID-19

La fonctionnalité d'analyse des symptômes est un outil permettant aux autorités de santé publique de guider les citoyens en matière de dépistage de la COVID-19 et de fournir des informations sur l'auto-isolement, la manière d'éviter la transmission à d'autres et le moment où il convient de solliciter des soins. Elle peut également compléter la surveillance dans le cadre des soins de santé primaires et fournir des informations plus précises sur les taux de transmission de la COVID-19 dans la population.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) 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 (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([5]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») (JO L 201 du 31.7.2002, p. 37).

([6]) Si les applications fournissent des informations relatives au diagnostic, à la prévention, au contrôle, à la prédiction ou au pronostic, il convient d'évaluer si elles ne peuvent pas être considérées comme des dispositifs médicaux conformément au cadre réglementaire relatif aux dispositifs médicaux. En ce qui concerne ledit cadre, voir la directive 93/42/CEE du Conseil du 14 juin 1993 relative aux dispositifs médicaux (JO L 169 du 12.7.1993, p. 1) et le règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux (JO L 117 du 5.5.2017, p. 1).

Les fonctionnalités de recherche de contacts et d'avertissement sont des outils permettant d'identifier les personnes qui ont été en contact avec une personne infectée par la COVID-19 et de les informer sur les mesures adéquates à prendre, telles que l'autoconfinement, le dépistage ou la fourniture de conseils sur la marche à suivre en cas de symptômes. Ces fonctionnalités sont donc utiles tant aux personnes qu'aux autorités de santé publique. Elles peuvent également jouer un rôle important dans la gestion des mesures de confinement dans les scénarios de relâchement de ces mesures. Son efficacité peut être renforcée par une stratégie visant à élargir les tests aux personnes présentant des symptômes bénins.

Ces deux fonctionnalités peuvent également constituer une source de données utile pour les autorités de santé publique et faciliter la transmission de ces données aux autorités épidémiologiques nationales et au Centre européen de prévention et de contrôle des maladies (ECDC). Cela permettrait de comprendre les modes de transmission et d'estimer, en combinaison avec les résultats des tests, la valeur prédictive positive des symptômes respiratoires dans une communauté donnée et de fournir des informations sur le niveau de circulation du virus.

Le degré de fiabilité des estimations est directement lié au nombre et à la fiabilité des données transmises.

Par conséquent, en combinaison avec des stratégies adéquates de dépistage, les fonctionnalités d'analyse des symptômes et de recherche des contacts permettent de fournir des informations sur le niveau de circulation du virus et d'évaluer l'incidence des mesures de distanciation physique et de confinement. Comme indiqué dans la recommandation, pour permettre la collaboration transfrontière et garantir la détection des contacts entre les utilisateurs de diverses applications différentes (ce qui est particulièrement important dans les déplacements transfrontières de citoyens), il convient de garantir l'interopérabilité entre les solutions informatiques des différents États membres. Lorsqu'une personne infectée est en contact avec un utilisateur d'une application d'un autre État membre, la transmission transfrontière de données à caractère personnel de cet utilisateur aux autorités sanitaires de son État membre devrait être possible dans la mesure strictement nécessaire. Les travaux sur cette question s'inscriront dans le cadre de la boîte à outils annoncée par la recommandation. L'interopérabilité doit être assurée à la fois par les exigences techniques et par l'amélioration de la communication et de la coopération entre les autorités sanitaires nationales. Un modèle de coopération particulière ([7]) pourrait également servir de modèle de gouvernance pour les applications de recherche des contacts au cours de la pandémie de COVID-19.

3 Éléments en vue d'une utilisation fiable et responsable des applications

Les fonctionnalités incluses dans les applications peuvent avoir différentes répercussions pour un large éventail de droits consacrés par la Charte des droits fondamentaux de l'UE, tels que la dignité humaine, le respect de la vie privée et familiale, la protection des données à caractère personnel, la libre circulation, la non-discrimination, la liberté d'entreprendre et la liberté de réunion et d'association. L'atteinte à la vie privée et au droit à la protection des données à caractère personnel peut être particulièrement forte car certaines fonctionnalités reposent sur un modèle faisant un usage intensif des données.

Les éléments présentés ci-après visent à fournir des orientations sur la manière de limiter le caractère intrusif des fonctionnalités des applications afin de garantir le respect de la législation de l'UE en matière de protection des données à caractère personnel et de vie privée.

3.1 Les autorités sanitaires nationales (ou les entités exécutant des missions d'intérêt public dans le domaine de la santé) en tant que responsables du traitement des données

Il est essentiel d'établir à qui incombe la définition des moyens et des finalités du traitement (le responsable du traitement) pour déterminer l'autorité chargée de faire respecter les règles de l'UE en matière de protection des données à caractère personnel, et notamment qui informe les personnes téléchargeant l'application du traitement réservé à leurs données à caractère personnel (existantes ou générées par l'appareil, comme un smartphone, sur lequel l'application est installée), de leurs droits, ainsi que de l'identité du responsable en cas de violation des données, etc.

Compte tenu du caractère sensible des données à caractère personnel qui pourront être obtenues et de la finalité de leur traitement décrit plus loin, la Commission considère que les applications devraient être conçues de manière à confier la responsabilité du traitement aux autorités sanitaires nationales (ou aux entités exécutant des missions d'intérêt public dans le domaine de la santé) ([8]). Les responsables du traitement sont chargés de veiller au respect du RGPD (principe de responsabilité). L'étendue de cet accès devrait être limitée sur la base des principes énoncés à la section 3.5 ci-dessous.

([7]) Cette coopération existe déjà en ce qui concerne le projet MyHealth@EU pour l'échange de dossiers de patients et les prescriptions électroniques. Voir également l'article 5, paragraphe 5, et le considérant 17 de la décision d'exécution 2019/1765 de la Commission.

([8]) Voir le considérant 45 du RGPD.

Cela contribuera aussi à renforcer la confiance de la population et, partant, l'acceptation des applications (et des systèmes d'information sur les chaînes de transmission de l'infection qui les sous-tendent) et à faire en sorte qu'elles atteignent l'objectif poursuivi en matière de protection de la santé publique. Les politiques, exigences et contrôles sous-jacents devraient être alignés et mis en œuvre de manière coordonnée par les autorités sanitaires nationales compétentes.

3.2 **Garantir que les utilisateurs conservent le contrôle**

Un élément déterminant pour permettre aux personnes de faire confiance aux applications consiste à leur apporter la preuve qu'elles gardent la maîtrise de leurs données à caractère personnel. À cette fin, la Commission considère que les conditions suivantes, en particulier, devraient être remplies:

— l'installation de l'application sur leur appareil devrait se faire sur une base volontaire, sans que cela ne nuise aux personnes qui décideront de ne pas télécharger/utiliser cette application;

— il convient de ne pas grouper différentes fonctionnalités (comme, par exemple, la fonctionnalité «information», la fonctionnalité d'analyse des symptômes, la recherche des contacts et l'envoi d'avertissements), de façon à permettre à la personne de donner son consentement pour chacune d'entre elles. Cela ne devrait pas empêcher l'utilisateur de combiner différentes fonctionnalités si le fournisseur lui en donne la possibilité;

— en cas d'utilisation de données de proximité [données générées par l'échange de signaux Bluetooth à basse consommation (BLE) entre appareils sur une distance et pendant une durée pertinentes sur le plan épidémiologique], ces données devraient être stockées sur l'appareil de la personne concernée. Si ces données doivent être partagées avec les autorités sanitaires, ce partage ne peut avoir lieu qu'après confirmation de la contamination de la personne concernée par la COVID-19 et à condition que cette dernière choisisse de les partager;

— les autorités sanitaires devraient fournir aux personnes toutes les informations nécessaires concernant le traitement de leurs données à caractère personnel (conformément aux articles 12 et 13 du RGPD et à l'article 5 de la directive «vie privée et communications électroniques»);

— la personne devrait être en mesure d'exercer ses droits en vertu du RGPG (en ce qui concerne, en particulier, l'accès, la rectification et l'effacement). Toute limitation éventuelle des droits conférés par le RGPD et la directive «vie privée et communications électroniques» devrait être conforme à ces actes et être nécessaire, proportionnée et prévue par la législation;

— les applications devraient être désactivées au plus tard lorsque la pandémie sera déclarée maîtrisée; la désactivation ne devrait pas dépendre de la désinstallation par l'utilisateur.

3.3 **Base juridique du traitement**

Installation des applications et stockage d'informations sur l'appareil de l'utilisateur

Comme indiqué ci-dessus, conformément à la directive vie privée et communications électroniques (article 5), le stockage d'informations sur l'appareil de l'utilisateur ou l'accès aux informations déjà stockées n'est autorisé que si i) l'utilisateur a donné son consentement ou ii) le stockage et/ou l'accès sont strictement nécessaires au service de la société de l'information (par exemple, à l'application) expressément demandé (c'est-à-dire installée et activée) par l'utilisateur.

Le stockage d'informations sur l'appareil de la personne et l'accès aux informations déjà stockées sur cet appareil sont normalement nécessaires pour que les applications fonctionnent. En outre, la fonctionnalité de recherche des contacts et d'avertissement nécessite que d'autres informations (telles que les pseudonymes d'identification éphémères, modifiés périodiquement, des utilisateurs de cette fonctionnalité se trouvant à proximité) soient stockées sur l'appareil de l'utilisateur. Par ailleurs, cette fonctionnalité peut exiger des utilisateurs (infectés ou probablement infectés) qu'ils chargent des données de proximité. Ce chargement n'est pas nécessaire au fonctionnement de l'application en tant que telle. Par conséquent, les exigences de l'option ii) mentionnées à l'alinéa précédent ne sont pas remplies. Le consentement [l'option i) ci-dessus] constitue donc la base la plus appropriée des activités concernées. Ce consentement devrait être «donné librement», «spécifique», «explicite» et «éclairé» au sens du RGPD. Il devrait être exprimé par un acte positif clair de l'intéressé, ce qui exclut les formes de consentement tacites (par exemple le silence, l'inactivité) ([9]).

([9]) Voir les lignes directrices du comité européen de la protection des données sur le consentement: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Base juridique du traitement par les autorités sanitaires nationales – législation de l'Union ou des États membres

En général, les autorités sanitaires nationales traitent des données à caractère personnel lorsqu'une obligation légale inscrite dans la législation de l'UE ou de l'État membre concerné le prévoit et remplit les conditions énoncées à l'article 6, paragraphe 1, point c), et à l'article 9, paragraphe 2, point i), du RGPD, ou lorsque ce traitement est nécessaire à l'exécution d'une mission d'intérêt public reconnue par la législation de l'UE ou de l'État membre concerné ([10]).

Toute législation nationale doit prévoir des mesures spécifiques et appropriées pour protéger les droits et libertés des personnes concernées. En règle générale, plus l'incidence sur les libertés individuelles est importante, plus les garanties correspondantes prévues dans la législation applicable devraient être solides.

Les législations de l'UE et des États membres qui existaient avant la flambée de COVID-19 et celles que les États membres adoptent spécifiquement pour lutter contre la propagation d'épidémies peuvent, en principe, servir de base juridique pour le traitement des données des personnes si elles prévoient des mesures permettant de surveiller les épidémies et si elles satisfont aux autres exigences énoncées à l'article 6, paragraphe 3, du RGPD.

Compte tenu de la nature des données à caractère personnel concernées (en particulier les données relatives à la santé en tant que catégorie spéciale de données à caractère personnel) 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 i) prescrirait en détail le traitement de données spécifiques relatives à la santé et préciserait clairement les finalités du traitement, ii) indiquerait clairement qui est le responsable du traitement, à savoir l'entité traitant les données, et qui, outre le responsable du traitement, peut accéder aux données en question, iii) exclurait la possibilité de traiter les données en question pour des finalités différentes de celles énumérées dans la législation et iv) prévoirait des garanties spécifiques. Afin de ne pas compromettre l'utilité et l'acceptation publiques des applications, le législateur national devrait veiller tout particulièrement à ce que la solution choisie soit aussi inclusive que possible vis-à-vis des citoyens.

Le traitement par les autorités sanitaires sur la base de la législation ne change rien au fait que les personnes restent libres d'installer l'application ou non et de partager leurs données avec ces autorités. La désinstallation de l'application ne devrait donc pas avoir de conséquences négatives pour les utilisateurs.

Les applications de recherche des contacts et d'avertissement permettent d'avertir les personnes. Lorsque cet avertissement est fourni directement par l'application, la Commission attire l'attention sur l'interdiction de soumettre les personnes à une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques les concernant ou les affectant de manière significative de façon similaire (article 22 du RGPD).

3.4 **Minimisation des données**

Les données produites par des appareils et déjà stockées antérieurement dans ces appareils sont protégées comme suit:

— en tant que «données à caractère personnel», à savoir toute information se rapportant à une personne physique identifiée ou identifiable (article 4, paragraphe 1, du RGPD), elles sont protégées au titre du RGPD. Les données relatives à la santé bénéficient d'une protection supplémentaire (article 9 du RGPD);

— en tant que «données de localisation», à savoir les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques, indiquant la position géographique de l'équipement terminal de l'utilisateur, elles sont protégées au titre de la directive «vie privée et communications électroniques» (article 5, paragraphe 1, articles 6 et 9) ([11]);

— toute information stockée dans un équipement terminal de l'utilisateur ou à laquelle il est accédé à partir d'un équipement terminal de l'utilisateur est protégée en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques».

Les données à caractère non personnel (comme les données irréversiblement anonymisées) ne sont pas protégées au titre du RGPD.

La Commission rappelle que le principe de la minimisation des données exige que seules les données à caractère personnel qui sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard de leur finalité ([12]) peuvent être traitées. Il convient d'évaluer la nécessité de traiter les données à caractère personnel et leur pertinence au regard de la finalité ou des finalités poursuivies.

La Commission note, par exemple, que si la finalité de la fonctionnalité est l'analyse des symptômes ou la télémédecine, elle ne requiert pas l'accès à la liste de contacts de la personne qui possède l'appareil.

([10]) Article 6, paragraphe 1, point e), du RGPD.

([11]) Le code des communications électroniques dispose que les services équivalents sur le plan fonctionnel aux services de communications électroniques sont couverts.

([12]) Principe de la minimisation des données.

La production et le traitement de données moins nombreuses limitent les risques en matière de sécurité. En conséquence, le respect des mesures de minimisation des données fournit également des garanties en matière de sécurité.

— Fonctionnalité d'information

Une application dotée de cette seule fonctionnalité ne devra traiter aucune donnée relative à la santé des personnes. Elle se limitera à leur fournir des informations. À cette fin, aucune information stockée dans un équipement terminal et à laquelle il est accédé à partir d'un équipement terminal ne peut être traitée dans une mesure qui n'est pas nécessaire à la fourniture de l'information.

— Fonctionnalités d'analyse des symptômes et de télémédecine

Si l'application comprend une ou deux de ces fonctionnalités, elle traitera des données relatives à la santé des personnes. En conséquence, une liste des données pouvant être traitées devrait figurer dans la législation sous-jacente applicable aux autorités sanitaires.

En outre, les autorités sanitaires pourraient avoir besoin des numéros de téléphone des personnes qui ont utilisé la fonction d'analyse des symptômes et téléchargé les résultats. Les informations stockées dans un équipement terminal et auxquelles il est accédé à partir d'un équipement terminal ne peuvent être traitées que dans la mesure où ce traitement est nécessaire pour permettre à l'application d'atteindre sa finalité et de fonctionner.

— Fonctionnalité de recherche des contacts et d'avertissement

La majorité des contaminations au COVID-19 se produisent par des gouttelettes qui ne circulent que sur une distance limitée. L'identification, dès que possible, des personnes qui se sont trouvées à proximité d'une personne infectée est un facteur essentiel pour rompre la chaîne de transmission de l'infection. La détermination de la proximité est fonction de la distance et de la durée d'un contact et devrait se faire d'un point de vue épidémiologique. La rupture de la chaîne de transmission de l'infection est particulièrement pertinente pour éviter la résurgence des infections lors de la phase de sortie de crise.

Les données de proximité pourraient être nécessaires à cet égard. Pour la mesure de la proximité et de l'étroitesse des contacts, les communications par Bluetooth à basse consommation (*Bluetooth Low Energy* - BLE) entre appareils semblent plus précises, et donc plus appropriées, que l'utilisation des données de géolocalisation (GNSS/GPS ou données de localisation cellulaire). Le BLE empêche la possibilité de pistage (contrairement aux données de géolocalisation). La Commission recommande dès lors l'utilisation des données de communications par BLE (ou générées par une technologie équivalente) pour déterminer la proximité.

Les données de localisation ne sont pas nécessaires à la finalité des fonctionnalités de recherche de contacts, l'objectif de ces dernières n'étant pas de suivre les mouvements des individus ni de faire appliquer des prescriptions. En outre, le traitement des données de localisation dans le contexte de la recherche de contacts serait difficile à justifier au regard du principe de la minimisation des données et pourrait poser des problèmes en matière de sécurité et de respect de la vie privée. Pour cette raison, la Commission conseille de ne pas utiliser les données de localisation dans ce contexte.

Quels que soient les moyens techniques utilisés pour déterminer la proximité, il n'apparaît pas nécessaire de stocker l'heure exacte du contact ni le lieu (si ces données sont disponibles). Toutefois, il pourrait être utile de stocker la date du contact, afin de savoir s'il a eu lieu alors que la personne présentait des symptômes (ou 48 heures avant ([13])) et de donner des orientations sur le message de suivi, notamment pour fournir des conseils sur la durée de l'autoconfinement.

Les données de proximité ne devraient être générées et traitées que s'il existe un risque réel d'infection (qui dépend de l'étroitesse et de la durée du contact).

Il convient de noter que la nécessité et la proportionnalité de la collecte de données dépendront donc de facteurs comme la disponibilité des installations de dépistage, notamment lorsque des mesures telles que le confinement ont déjà été prises. L'avertissement des personnes qui ont été en contact étroit avec une personne infectée peut prendre deux formes:

Première méthode: une alerte est automatiquement envoyée via l'application aux personnes qui ont été en contact étroit lorsqu'un utilisateur notifie à l'application - avec l'accord ou la confirmation de l'autorité sanitaire, par exemple au moyen d'un code QR ou TAN - qu'il a été testé positif (traitement décentralisé). Le contenu du message d'alerte devrait de préférence être déterminé par l'autorité sanitaire. Deuxième méthode: les identifiants temporaires arbitraires sont stockés sur un serveur dorsal détenu par l'autorité sanitaire (solution de serveur dorsal). Les utilisateurs ne peuvent pas être directement identifiés au moyen de ces données. Grâce à ces identifiants, les utilisateurs qui ont été en contact étroit avec un utilisateur testé positif reçoivent une alerte sur leur appareil. Si les autorités sanitaires souhaitent contacter les utilisateurs qui ont été en contact étroit avec une personne infectée également par téléphone ou par SMS, elles ont besoin du consentement de ces utilisateurs pour la fourniture de leurs numéros de téléphone.

([13]) La personne infectée est contagieuse 48 h avant l'apparition des symptômes.

3.5 **Limiter la divulgation/l'accessibilité des données**

— Fonctionnalité d'information:

Aucune information qui est stockée dans l'équipement terminal et à laquelle un accès a eu lieu depuis celui-ci ne peut être partagée avec les autorités sanitaires, si ce n'est celles nécessaires à la fonctionnalité d'information. Cette fonctionnalité étant limitée à la fourniture du moyen de communication, les autorités sanitaires n'auront accès à aucune autre donnée.

— Fonctionnalités d'analyse des symptômes et de télémédecine:

La fonctionnalité d'analyse des symptômes peut être utile aux États membres pour orienter les citoyens au sujet de l'opportunité de se faire dépister et pour fournir des informations sur l'isolement et quant à savoir quand et comment accéder à des soins de santé, en particulier pour ce qui est des groupes à risque. Cette fonctionnalité peut également compléter la surveillance dans le cadre des soins de santé primaires et contribuer à comprendre quels sont les taux d'infection à la COVID-19 parmi la population. Par conséquent, il peut être décidé que les autorités sanitaires compétentes et les autorités épidémiologiques nationales devraient avoir accès aux informations fournies par le patient. L'ECDC pourrait recevoir des données agrégées des autorités nationales à des fins de surveillance épidémiologique.

Si l'option retenue est celle d'une prise de contact effectuée par des agents sanitaires plutôt que par l'intermédiaire de l'application elle-même, le numéro de téléphone des utilisateurs de l'application devra également être divulgué aux autorités sanitaires nationales.

— Fonctionnalité de recherche des contacts et d'avertissement:

— Données de la personne infectée

Les applications attribuent des identifiants éphémères, générés de manière pseudo-aléatoire et modifiés périodiquement, aux téléphones qui sont en contact avec l'utilisateur. Une première option (dite «traitement décentralisé») consiste à stocker ces identifiants sur l'appareil de l'utilisateur. Une autre option (dite «solution à serveur dorsal») permet de prévoir que ces identifiants arbitraires soient stockés sur le serveur auquel ont accès les autorités sanitaires. La solution décentralisée répond mieux au principe de minimisation. Les autorités sanitaires ne devraient avoir accès qu'aux données de proximité provenant de l'appareil d'une personne infectée afin de pouvoir prendre contact avec les personnes risquant d'avoir été infectées.

Ces données ne seront mises à la disposition des autorités sanitaires que lorsque la personne infectée (une fois dépistée) les aura partagées avec les autorités sanitaires de manière proactive.

Il convient de ne pas informer la personne infectée de l'identité des personnes avec lesquelles elle a eu des contacts potentiellement pertinents d'un point de vue épidémiologique et qui seront alertées.

— Données des personnes ayant été en contact (épidémiologique) avec la personne infectée

Il convient de ne pas divulguer l'identité de la personne infectée aux personnes avec lesquelles il/elle a été en contact épidémiologique. Il suffit d'indiquer à ces dernières qu'elles ont été en contact épidémiologique avec une personne infectée au cours de 16 derniers jours. Comme signalé plus haut, les données concernant la date et le lieu de ces contacts ne devraient pas être stockées. Il n'est donc ni nécessaire, ni possible de communiquer ces données.

Pour la recherche des contacts épidémiologiques d'un utilisateur d'application électronique dont l'infection est avérée, seul devrait être communiqué aux autorités sanitaires nationales l'identifiant des personnes avec lesquelles la personne infectée a été en contact épidémiologique dans les 48 heures ayant précédé l'apparition des symptômes et au cours des 14 jours suivant celle-ci, la proximité et la durée des contacts étant déterminantes à cet égard.

L'ECDC pourrait recevoir des données de recherche des contacts sous forme agrégée de la part des autorités nationales aux fins d'une surveillance épidémiologique portant sur des indicateurs à définir en collaboration avec les États membres.

3.6 **Prévoir des finalités de traitement précises**

La base juridique (droit de l'Union ou de tel ou tel État membre) devrait prévoir la finalité du traitement. Cette finalité devrait être spécifique, de sorte qu'il n'y ait aucun doute quant au type de donnée à caractère personnel devant faire l'objet d'un traitement afin d'atteindre l'objectif désiré, et explicite. .

La/les finalité(s) précise(s) sera/seront fonction des fonctionnalités des applications. Il peut y avoir plusieurs finalités pour chaque fonctionnalité d'une application. Pour donner aux personnes le plein contrôle de leurs données, la Commission recommande de ne pas grouper des fonctionnalités différentes. En tout état de cause, la personne devrait avoir la possibilité de choisir entre différentes fonctionnalités ayant chacune une finalité distincte.

La Commission déconseille d'utiliser des données collectées dans les conditions susmentionnées à d'autres fins que la lutte contre la COVID-19. S'il s'avérait nécessaire de poursuivre des finalités telles que la recherche scientifique ou les statistiques, celles-ci devraient alors figurer dans la liste d'origine des finalités et être communiquées clairement aux utilisateurs.

— Fonctionnalité d'information:

cette fonctionnalité a pour objet la fourniture d'informations pertinentes du point de vue des autorités sanitaires dans le contexte de la crise.

— Fonctionnalités d'analyse des symptômes et de télémédecine:

La fonctionnalité d'analyse des symptômes peut donner une indication de la proportion des personnes signalant des symptômes compatibles avec la COVID-19 qui sont véritablement infectées (par ex. en effectuant des prélèvements ou des tests sur tout ou partie des personnes présentant de tels symptômes, si faire se peut). Cette identification de la finalité devrait préciser clairement que les données médicales à caractère personnel seront traitées de manière à donner à la personne la possibilité i) de déterminer par elle-même, sur la base d'une série de questions posées, si elle a développé des symptômes de la COVID-19, ou ii) d'obtenir des conseils médicaux en pareil cas.

— Fonctionnalité de recherche des contacts et d'avertissement:

La simple indication d'une finalité telle que «prévention de nouvelles infections par la COVID-19» n'est pas suffisamment spécifique. Dans ce cas, la Commission recommande de préciser davantage la/les finalité(s) avec une formule du type: «conservation des coordonnées des personnes utilisant l'application et susceptibles d'avoir été exposées à l'infection par la COVID-19, afin d'avertir les personnes pouvant avoir été infectées».

3.7 **Fixer des limites strictes pour la conservation des données**

Le principe de limitation de la conservation impose de ne pas conserver les données à caractère personnel plus longtemps que nécessaire. Les délais devraient être fixés selon la pertinence d'un point de vue médical (en fonction de la finalité de l'application: la période d'incubation, etc.) de même qu'en fonction de la durée réaliste pour prendre les mesures administratives pouvant être nécessaires.

— Fonctionnalité d'information:

si une donnée est collectée lors de l'installation de cette fonctionnalité, il convient de l'effacer sur-le-champ. Rien ne justifie la conservation de telles données.

— Fonctionnalités d'analyse des symptômes et de télémédecine:

De telles données devraient être effacées par les autorités sanitaires après un délai maximum d'un mois (période d'incubation assortie d'une marge) ou après que la personne a été testée négative. Les autorités sanitaires peuvent conserver les données plus longtemps à des fins de recherches ou d'établissement d'un rapport de surveillance, pourvu que ce soit sous une forme anonymisée.

— Fonctionnalité de recherche des contacts et d'avertissement:

Il y a lieu d'effacer les données de proximité dès qu'elles ne sont plus nécessaires pour prévenir les personnes concernées. Cela devrait être le cas après un délai maximum d'un mois (période d'incubation assortie d'une marge) ou après que la personne a été testée négative. Les autorités sanitaires peuvent conserver les données de proximité plus longtemps à des fins de recherches ou d'établissement d'un rapport de surveillance, pourvu que ce soit sous une forme anonymisée.

Les données devraient être stockées sur l'appareil de l'utilisateur et seules celles communiquées par les utilisateurs et étant nécessaires pour atteindre la finalité de leur collecte devraient être chargées sur le serveur mis à la disposition des autorités sanitaires lorsque cette option a été choisie (à savoir, ne charger sur le serveur que les données des «contacts proches» d'une personne testée positive à l'infection par la COVID-19).

3.8 **Garantir la sécurité des données**

La Commission recommande que les données soient stockées sur le terminal de la personne sous forme cryptée en utilisant des techniques cryptographiques de pointe. Au cas où les données sont stockées sur un serveur central, l'accès, y compris administratif, devrait être consigné.

Les données de proximité devraient uniquement être générées et stockées sur le terminal de la personne sous forme cryptée et dans un format pseudonymisé. Afin de veiller à ce que tout pistage par des tiers soit impossible, le Bluetooth devrait pouvoir être activé sans devoir activer d'autres services de localisation.

Au cours de la collecte de données de proximité par Bluetooth à basse consommation (Bluetooth Low Energy), il est préférable de créer et de stocker des identifiants d'utilisateurs temporaires qui changent régulièrement plutôt que de stocker le véritable identifiant du dispositif. Cette mesure offre une protection supplémentaire contre les écoutes et le pistage par des pirates informatiques et rend donc plus difficile l'identification des personnes.

La Commission recommande que le code source de l'application soit rendu public et disponible pour examen.

Des mesures supplémentaires visant à sécuriser les données traitées peuvent être envisagées, notamment avec la suppression automatique ou l'anonymisation des données une fois dépassé un certain délai. De manière générale, le niveau de sécurité devrait être adapté au volume et au caractère sensible des données à caractère personnel traitées.

Toutes les transmissions du dispositif personnel vers les autorités sanitaires nationales devraient être chiffrées.

Lorsque la législation nationale prévoit que les données à caractère personnel collectées peuvent également être traitées à des fins de recherche scientifique, la pseudonymisation devrait, en principe, être utilisée.

3.9 **Garantir l'exactitude des données**

Garantir l'exactitude des données à caractère personnel traitées est non seulement une condition préalable à l'efficacité de l'application, mais également une exigence au titre de la législation en matière de protection des données à caractère personnel.

Dans ce contexte, il est essentiel de veiller à l'exactitude des informations sur la question de savoir si un contact avec une personne infectée (distance et durée épidémiologiques) a eu lieu, afin de minimiser le risque d'avoir des faux positifs. Les scénarios dans lesquels deux utilisateurs de l'application sont en contact dans la rue, dans les transports publics ou dans un bâtiment devraient être pris en considération. Il est peu probable que l'utilisation de données de localisation basées sur des réseaux de téléphonie mobile soit suffisamment précise pour l'objectif recherché.

Il est donc recommandé de s'appuyer sur des technologies permettant une évaluation plus précise du contact (comme le Bluetooth).

3.10 **Associer les autorités de protection des données**

Les autorités de protection des données devraient être pleinement associées et consultées dans le cadre du développement de l'application et devraient suivre de près son déploiement. Étant donné que le traitement des données dans le cadre de l'application sera considéré comme un traitement à grande échelle de catégories particulières de données (données relatives à la santé), la Commission attire l'attention sur l'article 35 du RGPD concernant l'analyse d'impact relative à la protection des données.