Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19

Adoptées le 21 avril 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

adopté

Historique des versions

Version 1.1	5 mai 2020	Corrections mineures
Version 1.0	21 avril 2020	Adoption des lignes directrices

Table des matières

Le comité européen de la protection des données

vu l'article 70, paragraphe 1, point e), du 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 (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen, et en particulier son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES:

1 INTRODUCTION ET CONTEXTE

1 Les pouvoirs publics et les acteurs privés se tournent vers l'utilisation de solutions fondées sur l'exploitation de données dans le cadre de la réaction à la pandémie de COVID-19, ce qui suscite bon nombre de préoccupations en matière de respect de la vie privée.

2 L'EDPB souligne que le cadre juridique en matière de protection des données a été conçu de façon à être souple et que, dès lors, il peut constituer un outil de réaction efficace pour, à la fois, endiguer la pandémie et sauvegarder les droits de l'homme et les libertés fondamentales.

3 L'EDPB est fermement convaincu que, lorsque le traitement de données à caractère personnel est nécessaire pour gérer la pandémie de COVID-19, la protection des données est indispensable pour instaurer la confiance, créer les conditions d'acceptabilité sociale à l'égard de toute solution et garantir ainsi l'efficacité des mesures prises. Le virus ne connaissant pas de frontières, l'élaboration d'une approche européenne commune en réaction à la crise actuelle, ou à tout le moins la mise en place d'un cadre interopérable, semble préférable.

4 De manière générale, l'EDPB estime que les données et les technologies utilisées pour aider à lutter contre la COVID-19 devraient être employées pour outiller les personnes, plutôt que pour les contrôler, les stigmatiser ou les réprimer. En outre, si les données et les technologies peuvent être des outils importants, elles présentent des limites intrinsèques et peuvent seulement accroître l'efficacité d'autres mesures de santé publique. Les principes généraux d'efficacité, de nécessité et de proportionnalité doivent guider les mesures adoptées par les États membres ou les institutions de l'UE qui nécessitent le traitement de données à caractère personnel pour endiguer la pandémie de COVID-19.

5 Les présentes lignes directrices précisent les conditions et les principes applicables à l'utilisation proportionnée des données de localisation et des outils de recherche de contacts, à deux fins précises:

- l'utilisation de données de localisation pour soutenir la lutte contre la pandémie en modélisant la propagation du virus de façon à évaluer l'efficacité globale des mesures de confinement;

1 Les références aux «États membres» qui sont faites tout au long du présent document doivent être comprises comme des références aux «États membres de l'EEE».

- la recherche de contacts, qui vise à signaler aux personnes qu'elles se sont trouvées à proximité immédiate de quelqu'un dont il est ensuite confirmé qu'il est porteur du virus, afin de briser les chaînes de contamination le plus tôt possible.

6 L'efficacité de la contribution des applications de recherche de contacts à la gestion de la pandémie dépend de nombreux facteurs (tels que le pourcentage de personnes qui devraient installer ces applications ou la définition d'un «contact» en termes de proximité et de durée). En outre, de telles applications doivent s'inscrire dans le cadre d'une stratégie globale de santé publique visant à endiguer la pandémie, prévoyant, entre autres, un dépistage et une recherche manuelle de contacts ultérieure afin de lever tout doute. Le déploiement de ces applications devrait s'accompagner de mesures d'appui destinées à garantir que les informations communiquées aux utilisateurs sont replacées dans leur contexte, et que les alertes peuvent être utiles pour le système de santé publique. Sans cela, ces applications pourraient ne pas produire leur plein effet.

7 L'EDPB souligne que le RGPD et la directive 2002/58/CE (ci-après la «directive») contiennent tous deux des règles spécifiques qui permettent l'utilisation de données anonymes ou de données à caractère personnel pour aider les autorités publiques et d'autres acteurs au niveau national et au niveau de l'UE à surveiller et à contenir la propagation du virus SARS-CoV-2[2].

8 À cet égard, l'EDPB a déjà pris position sur le fait que l'utilisation d'applications de recherche de contacts devrait être volontaire et ne devrait pas s'appuyer sur le traçage des déplacements des personnes, mais plutôt sur des informations de proximité concernant les utilisateurs[3].

[2] Voir la précédente déclaration de l'EDPB relative à la pandémie de COVID-19.
[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 UTILISATION DES DONNÉES DE LOCALISATION

2.1 Sources de données de localisation

9 Il existe deux principaux types de données de localisation disponibles pour modéliser la propagation du virus et l'efficacité globale des mesures de confinement:

- les données de localisation collectées par les fournisseurs de services de communications électroniques (tels que les opérateurs de télécommunications mobiles) dans le cadre de leurs activités; et
- les données de localisation collectées par les applications des prestataires de services de la société de l'information dont les fonctionnalités exigent l'utilisation de ce type de données (par exemple, services de navigation, services de transport, etc.).

10 L'EDPB rappelle que les données de localisation[4] collectées auprès de fournisseurs de services de communications électroniques ne peuvent être traitées que dans le cadre des articles 6 et 9 de la directive. Cela signifie que ces données ne peuvent être communiquées aux autorités ou à d'autres tiers que si elles ont été anonymisées par le fournisseur ou, pour les données indiquant la position géographique de l'équipement terminal d'un utilisateur, qui ne constituent pas des données relatives au trafic, que si les utilisateurs ont donné leur consentement préalable[5].

11 En ce qui concerne les informations, y compris les données de localisation, collectées directement depuis l'équipement terminal, l'article 5, paragraphe 3, de la directive s'applique. Dès lors, le stockage d'informations dans l'appareil de l'utilisateur ou l'accès à des informations qui y sont déjà stockées n'est autorisé que si i) l'utilisateur a donné son consentement[6] ou ii) le stockage et/ou l'accès est strictement nécessaire pour le service de la société de l'information expressément demandé par l'utilisateur.

12 Des dérogations aux droits et obligations prévus dans la directive sont toutefois possibles en vertu de l'article 15, lorsque ces dérogations constituent une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour garantir certains objectifs[7].

13 En ce qui concerne la réutilisation de données de localisation collectées par un prestataire de services de la société de l'information à des fins de modélisation (par exemple, au moyen du système d'exploitation ou d'une application déjà installée), des conditions supplémentaires doivent être satisfaites. En effet, lorsque les données ont été collectées conformément à l'article 5, paragraphe 3, de la directive, elles ne peuvent être traitées ultérieurement que si la personne concernée donne une nouvelle fois son consentement ou si ce traitement ultérieur est fondé sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, du RGPD[8].

2.2 Gros plan sur l'utilisation de données de localisation anonymisées

14 En ce qui concerne l'utilisation des données de localisation, l'EDPB insiste sur le fait qu'il faudrait toujours privilégier le traitement de données anonymisées plutôt que de données à caractère personnel.

---

[4] Voir l'article 2, point c), de la directive.
[5] Voir les articles 6 et 9 de la directive.
[6] La notion de consentement dans la directive correspond toujours à la notion de consentement figurant dans le RGPD et doit satisfaire à l'ensemble des exigences relatives au consentement prévues à l'article 4, point 11), et à l'article 7 du RGPD.
[7] Aux fins de l'interprétation de l'article 15 de la directive, voir également l'arrêt de la CJUE du 29 janvier 2008 dans l'affaire C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU.
[8] Voir la section 1.5.3 des lignes directrices 1/2020 relatives au traitement des données à caractère personnel dans le contexte des véhicules connectés.

15 L'anonymisation fait référence à l'utilisation d'un ensemble de techniques visant à retirer la possibilité d'associer, moyennant un «effort raisonnable», les données à une personne physique identifiée ou identifiable. Ce «critère du caractère raisonnable» doit tenir compte aussi bien d'éléments objectifs (le temps, les moyens techniques) que d'éléments contextuels pouvant varier au cas par cas (rareté d'un phénomène, compte tenu de facteurs tels que la densité de la population concernée ou encore la nature et le volume des données). Si les données ne satisfont pas à ce critère, cela signifie qu'elles n'ont pas été anonymisées et donc qu'elles relèvent toujours du RGPD.

16 L'évaluation de la fiabilité de l'anonymisation repose sur trois critères: i) la possibilité d'isoler un individu au sein d'un groupe plus grand sur la base des données; ii) la possibilité de relier deux enregistrements concernant la même personne; et iii) la possibilité d'inférer, avec une forte probabilité, des informations inconnues concernant une personne.

17 La notion d'anonymisation est susceptible d'être mal comprise et est souvent confondue avec la pseudonymisation. Si les données anonymisées peuvent être utilisées sans aucune restriction, les données pseudonymisées, quant à elles, relèvent toujours du RGPD.

18 Il existe de nombreux moyens d'anonymiser efficacement des données[9], avec toutefois une réserve. Il est impossible d'anonymiser une seule donnée, ce qui signifie que seuls des ensembles de données peuvent ou non être rendus anonymes. À cet égard, toute intervention sur un schéma de données unique (au moyen du chiffrement ou de toute autre transformation mathématique) peut au mieux être considérée comme une pseudonymisation.

19 Les processus d'anonymisation et les tentatives de ré-identification constituent des domaines de recherche actifs. Il est essentiel que les responsables du traitement qui utilisent des solutions d'anonymisation suivent les évolutions récentes dans ce domaine, en particulier en ce qui concerne les données de localisation (provenant des opérateurs de télécommunications et/ou des services de la société de l'information) qui sont réputées difficiles à anonymiser.

20 En effet, de nombreuses recherches ont démontré[10] qu'il était possible que *des données de localisation que l'on pensait anonymisées* ne le soient pas vraiment. Les traces des déplacements des personnes sont, de manière intrinsèque, fortement corrélées et uniques et sont, par conséquent, vulnérables aux tentatives de ré-identification dans certaines circonstances.

21 Un schéma de données unique localisant une personne sur un laps de temps significatif ne peut être complètement anonymisé. Cela peut toujours être le cas si la précision des coordonnées géographiques enregistrées n'est pas suffisamment réduite, si les détails de la trace sont supprimés, et même si seule la localisation des endroits où la personne concernée reste longtemps est conservée. C'est également le cas pour les données de localisation mal agrégées.

22 Pour que l'anonymisation soit possible, les données de localisation doivent être traitées avec soin afin de satisfaire au critère du caractère raisonnable. Il s'agit de prendre en compte des ensembles de données de localisation, ainsi que de traiter des données provenant d'un groupe raisonnablement large de personnes en utilisant les techniques d'anonymisation fiables disponibles, pour autant qu'elles soient correctement et efficacement mises en œuvre.

23 Enfin, compte tenu de la complexité des processus d'anonymisation, la transparence est fortement conseillée quant à la méthode d'anonymisation.

---

[9] (de Montjoye et al., 2018) «On the privacy-conscientious use of mobile phone data»
[10] (de Montjoye et al., 2013) «Unique in the Crowd: The privacy bounds of human mobility» et (Pyrgelis et al., 2017) «Knock Knock, Who's There? Membership Inference on Aggregate Location Data»

3 APPLICATIONS DE RECHERCHE DE CONTACTS

3.1 Analyse juridique générale

24 Le suivi systématique et à grande échelle de la localisation des personnes physiques et/ou des contacts entre ces personnes constitue une grave intrusion dans leur vie privée. Ce suivi ne peut être légitimé que si les utilisateurs l'acceptent de manière volontaire pour chacune des finalités respectives. Cela signifie, notamment, que les personnes qui décident de ne pas utiliser ces applications ou qui ne peuvent pas les utiliser ne devraient en aucune manière être désavantagées.

25 Pour garantir l'obligation de rendre des comptes, il convient de définir clairement le responsable du traitement pour toute application de recherche de contacts. L'EDPB estime que les autorités sanitaires nationales pourraient être les responsables du traitement[11] pour ces applications; d'autres responsables du traitement peuvent également être envisagés. En tout état de cause, si différents acteurs interviennent dans le déploiement d'applications de recherche de contacts, leurs rôles et responsabilités doivent être clairement établis dès le départ et expliqués aux utilisateurs.

26 En outre, en ce qui concerne le principe de limitation des finalités, les objectifs doivent être suffisamment spécifiques pour exclure tout traitement ultérieur à des fins étrangères à la gestion de la crise sanitaire de la COVID-19 (par exemple, des fins commerciales ou répressives). Une fois l'objectif clairement défini, il sera nécessaire de veiller à ce que l'utilisation des données à caractère personnel soit adéquate, nécessaire et proportionnée.

27 Dans le contexte d'une application de recherche de contacts, il convient d'accorder une attention particulière au principe de minimisation des données ainsi qu'aux principes de protection des données dès la conception et de protection des données par défaut:

- les applications de recherche de contacts ne nécessitent pas le traçage de la localisation des différents utilisateurs. Il convient plutôt d'utiliser des données de proximité;
- les applications de recherche de contacts pouvant fonctionner sans identification directe des personnes, il convient de mettre en place des mesures appropriées pour empêcher la ré-identification;
- les informations collectées devraient être stockées dans l'équipement terminal de l'utilisateur et seules les informations utiles devraient être collectées en cas d'absolue nécessité.

28 En ce qui concerne la licéité du traitement, l'EDPB observe que les applications de recherche de contacts nécessitent le stockage d'informations dans l'équipement terminal et/ou l'accès à des informations qui y sont déjà stockées, lesquels relèvent de l'article 5, paragraphe 3, de la directive. Si ces opérations sont strictement nécessaires pour permettre au fournisseur de l'application de fournir le service expressément demandé par l'utilisateur, le traitement ne nécessite pas le consentement de ce dernier. Pour les opérations qui ne sont pas strictement nécessaires, le fournisseur doit demander le consentement de l'utilisateur.

29 L'EDPB relève en outre que le simple fait que l'utilisation d'applications de recherche de contacts se fasse sur une base volontaire ne signifie pas pour autant que le traitement des données à caractère personnel reposera nécessairement sur le consentement. Lorsque les autorités publiques fournissent un service fondé sur un mandat qui leur est conféré par la loi et qui est conforme aux exigences établies par celle-ci, il apparaît que la base juridique la plus pertinente pour le traitement réside dans le fait que celui-ci est nécessaire à l'exécution d'une mission d'intérêt public [article 6, paragraphe 1, point e), du RGPD].

[11] Voir également la communication de la Commission européenne «Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données», Bruxelles, le 16 avril 2020, C(2020) 2523 final.

30 Il est précisé à l'article 6, paragraphe 3, du RGPD que le fondement du traitement visé à l'article 6, paragraphe 1, point e), est défini par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis. Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement[12].

31 La base juridique ou la mesure législative qui fournit la base juridique de l'utilisation d'applications de recherche de contacts devrait toutefois prévoir des garanties significatives, notamment une référence à la nature volontaire de l'application. Elle devrait préciser clairement la finalité et les limitations explicites concernant l'utilisation ultérieure des données à caractère personnel et identifier clairement le ou les responsables du traitement concernés. Elle devrait également indiquer les catégories de données concernées, ainsi que les entités auxquelles les données à caractère personnel peuvent être communiquées (et les finalités pour lesquelles elles peuvent l'être). Selon le degré d'ingérence, elle devrait prévoir des garanties supplémentaires, compte tenu de la nature, de la portée et des finalités du traitement. Enfin, l'EDPB recommande également d'y inclure, dès que possible, les critères permettant de déterminer quand l'application sera supprimée ainsi que de désigner l'entité qui sera chargée de déterminer ce moment et sera tenue de rendre des comptes à ce sujet.

32 Toutefois, si le traitement des données repose sur une autre base juridique, telle que le consentement [article 6, paragraphe 1, point a)][13] par exemple, le responsable du traitement devra veiller au respect des conditions strictes qui doivent être observées pour que cette base juridique soit valable.

33 En outre, le recours à une application pour lutter contre la pandémie de COVID-19 pourrait conduire à la collecte de données relatives à la santé (par exemple, le statut d'une personne infectée). Le traitement de ces données est autorisé lorsqu'il est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique et satisfait aux conditions énoncées à l'article 9, paragraphe 2, point i), du RGPD[14], ou pour des finalités en rapport avec les soins de santé, tel que décrites à l'article 9, paragraphe 2, point h), du RGPD[15]. En fonction de la base juridique, le traitement de ces données pourrait également reposer sur le consentement explicite [article 9, paragraphe 2, point a), du RGPD].

34 Conformément à la finalité initiale, l'article 9, paragraphe 2, point j), du RGPD autorise également le traitement de données relatives à la santé lorsqu'il est nécessaire à des fins de recherche scientifique ou à des fins statistiques.

35 La crise sanitaire actuelle ne devrait pas servir de prétexte pour fixer des règles disproportionnées en matière de conservation des données. La limitation de stockage devrait tenir compte des besoins réels et de la pertinence d'un point de vue médical (ce qui peut inclure des considérations épidémiologiques telles que la période d'incubation, etc.), et les données à caractère personnel ne devraient être conservées que pendant la durée de la crise de la COVID-19. Passée cette crise, l'ensemble des données à caractère personnel devraient, de manière générale, être supprimées ou anonymisées.

36 L'EDPB est d'avis que de telles applications ne peuvent pas remplacer, mais seulement soutenir la recherche manuelle de contacts effectuée par du personnel de santé publique qualifié, à même de déterminer si des contacts étroits sont susceptibles ou pas d'entraîner une transmission du virus [par exemple en cas d'interaction avec une personne protégée par des

---

[12] Voir le considérant 41.

[13] Les responsables du traitement (en particulier les autorités publiques) doivent accorder une attention particulière au fait que le consentement ne devrait pas être considéré comme ayant été donné librement si la personne ne dispose pas d'une véritable liberté de choix de refuser ou de retirer son consentement sans subir de préjudice.

[14] Le traitement doit reposer sur le droit de l'Union ou le droit d'un État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel.

[15] Voir l'article 9, paragraphe 2, point h), du RGPD.

équipements adaptés (un caissier, etc.) ou non]. L'EDPB souligne que les procédures et les processus, y compris les algorithmes utilisés par les applications de recherche de contacts, devraient être étroitement supervisés par du personnel qualifié afin de limiter le risque de faux positifs et de faux négatifs. En particulier, les conseils concernant les prochaines mesures ne devraient pas reposer exclusivement sur un traitement automatisé.

37 Afin de garantir l'équité, l'obligation de rendre des comptes et, de façon plus générale, le respect du droit dans le cadre de leur utilisation, les algorithmes doivent pouvoir être vérifiés et devraient être réexaminés régulièrement par des experts indépendants. Le code source de l'application devrait être rendu public pour permettre un contrôle aussi large que possible.

38 Il y aura toujours un certain nombre de faux positifs. Étant donné que l'établissement d'un risque d'infection peut avoir des conséquences importantes pour les personnes, telles qu'un maintien en auto-isolement jusqu'à ce qu'elles soient testées négatives, il faut pouvoir corriger les données et/ou les résultats d'analyses ultérieures. Bien entendu, cela ne devrait s'appliquer qu'aux scénarios et aux mises en œuvre dans lesquels les données sont traitées et/ou stockées d'une manière telle que ce type de correction soit techniquement faisable et dans lesquels les effets négatifs susmentionnés soient susceptibles de se produire.

39 Enfin, l'EDPB considère qu'une analyse d'impact relative à la protection des données doit être effectuée avant la mise en œuvre de tels outils, le traitement étant considéré comme très risqué (données relatives à la santé, adoption à grande échelle anticipée, suivi systématique, utilisation d'une nouvelle solution technologique)[16]. L'EDPB recommande vivement la publication d'analyses d'impact relatives à la protection des données.

3.2 Recommandations et exigences fonctionnelles

40 Selon le principe de minimisation des données, entre autres mesures de protection des données dès la conception et par défaut[17], les données traitées devraient être limitées au strict minimum. L'application ne devrait pas collecter d'informations non pertinentes ou non nécessaires, telles que l'état civil, les identifiants de communication, des éléments du répertoire des appareils, des messages, des journaux d'appels, des données de localisation, les identifiants d'appareils, etc.

41 Les données diffusées par les applications ne doivent inclure que certains identifiants uniques et pseudonymes générés par l'application et spécifiques à celle-ci. Ces identifiants doivent être renouvelés régulièrement, à une fréquence compatible avec la finalité consistant à contenir la propagation du virus et suffisante pour limiter le risque d'identification et de traçage physique des personnes.

42 Les mises en œuvre de la recherche de contacts peuvent suivre une approche centralisée ou décentralisée[18]. Ces deux approches devraient être considérées comme des options viables, pour autant que des mesures de sécurité adéquates soient en place, chacune ayant ses avantages et ses inconvénients. Dès lors, la phase conceptuelle de développement d'une application devrait toujours prévoir un examen approfondi de ces deux concepts mettant en balance leurs effets respectifs sur la protection des données/la vie privée et leurs éventuelles répercussions sur les droits des personnes.

43 Les serveurs associés au système de recherche de contacts ne peuvent collecter que l'historique de contacts ou les identifiants pseudonymes d'un utilisateur diagnostiqué comme infecté par le virus, après une évaluation appropriée par les autorités sanitaires et une action volontaire

---

[16] Voir les lignes directrices du groupe de travail «article 29» (adoptées par l'EDPB) concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679.

[17] Voir les lignes directrices 4/2019 de l'EDPB relatives à l'article 25 du RGPD – Protection des données dès la conception et protection des données par défaut

[18] En général, la solution décentralisée répond mieux au principe de minimisation.

de l'utilisateur. En outre, le serveur ne peut conserver la liste des identifiants pseudonymes des utilisateurs infectés ou leur historique de contacts que le temps nécessaire pour informer les utilisateurs potentiellement infectés de leur exposition, et il ne devrait pas essayer d'identifier des utilisateurs potentiellement infectés.

44 Il se peut que la mise en place d'une méthode globale de recherche de contacts incluant à la fois des applications et une recherche manuelle de contacts nécessite le traitement d'informations supplémentaires dans certains cas. Dans ce contexte, ces informations supplémentaires devraient rester stockées dans le terminal de l'utilisateur et n'être traitées qu'en cas de stricte nécessité et avec le consentement préalable et spécifique de l'utilisateur.

45 Des techniques cryptographiques de pointe doivent être mises en œuvre pour sécuriser les données stockées sur les serveurs et dans les applications, ainsi que les échanges entre les applications et le serveur distant. Une authentification mutuelle entre l'application et le serveur doit également être exécutée.

46 Le signalement d'utilisateurs comme étant infectés par le SARS-CoV-2 dans l'application doit faire l'objet d'une autorisation en bonne et due forme, par exemple au moyen d'un code à usage unique lié à une identité pseudonyme de la personne infectée et à une station de test ou à un professionnel de la santé. S'il n'est pas possible d'obtenir la confirmation de manière sécurisée, aucun traitement de données supposant la validité du statut de l'utilisateur ne devrait avoir lieu.

47 Le responsable du traitement, en collaboration avec les autorités publiques, doit communiquer de manière claire et explicite le lien permettant de télécharger l'application nationale officielle de recherche de contacts afin de réduire le risque d'utilisation d'une application tierce.

4 CONCLUSION

48 Le monde est confronté à une importante crise de santé publique exigeant des réactions fortes, qui auront des conséquences au-delà de cette situation d'urgence. Le traitement automatisé de données et les technologies numériques peuvent jouer un rôle essentiel dans la lutte contre la COVID-19. Il faut toutefois se méfier de l'«effet de cliquet». Il est de notre responsabilité de veiller à ce que chaque mesure prise dans ces circonstances extraordinaires soit nécessaire, limitée dans le temps et d'une portée minimale et à ce qu'elle fasse l'objet d'un véritable réexamen périodique et d'une évaluation scientifique.

49 L'EDPB souligne que l'on ne devrait pas avoir à choisir entre une réaction efficace à la crise actuelle et la protection de nos droits fondamentaux: les deux sont possibles. En outre, les principes de la protection des données peuvent jouer un rôle très important dans la lutte contre le virus. La législation européenne en matière de protection des données autorise l'utilisation responsable de données à caractère personnel à des fins de gestion de la santé, tout en garantissant que les droits et libertés individuels ne s'en trouvent pas affectés.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

ANNEXE - APPLICATIONS DE RECHERCHE DE CONTACTS GUIDE D'ANALYSE

0. Avertissement

Les orientations ci-après ne sont ni prescriptives ni exhaustives, et le seul but de ce guide est de fournir des orientations générales aux concepteurs d'applications de recherche de contacts et aux personnes chargées de leur mise en œuvre. D'autres solutions que celles décrites ici peuvent également être utilisées et être licites pour autant qu'elles soient conformes au cadre juridique applicable (à savoir le RGPD et la directive).

Il convient également de noter que le présent guide est de nature générale. Par conséquent, les recommandations et les obligations contenues dans le présent document ne peuvent pas être considérées comme exhaustives. Toute évaluation doit se faire au cas par cas et il se peut que certaines applications nécessitent des mesures supplémentaires ne figurant pas dans le présent guide.

1. Résumé

De nombreux États membres envisagent l'utilisation d'applications de *recherche de contacts** pour aider les personnes à savoir si elles ont été en contact avec une personne infectée par le SARS-CoV-2.

Les conditions auxquelles ces applications doivent satisfaire pour contribuer efficacement à la gestion de la pandémie ne sont pas encore définies. Elles devront l'être avant toute mise en œuvre de ce type d'applications. Néanmoins, il est utile de fournir aux équipes de développement en amont des lignes directrices contenant des informations pertinentes afin que la protection des données à caractère personnel puisse être garantie dès le stade de la conception.

Il convient de noter que le présent guide est de nature générale. Par conséquent, les recommandations et les obligations contenues dans le présent document ne peuvent pas être considérées comme exhaustives. Toute évaluation doit se faire au cas par cas et il se peut que certaines applications nécessitent des mesures supplémentaires ne figurant pas dans le présent guide. Ce dernier vise à fournir des orientations générales aux concepteurs d'applications de recherche de contacts et aux personnes chargées de leur mise en œuvre.

Il se peut que certains critères aillent au-delà des exigences strictes découlant du cadre de protection des données. Ces critères visent à garantir le plus haut niveau de transparence, de manière à favoriser l'acceptation sociale des applications de recherche de contacts.

À cette fin, les éditeurs d'applications de recherche de contacts devraient tenir compte des critères suivants:

- L'utilisation d'une telle application doit être strictement volontaire. Elle ne peut pas conditionner l'accès à des droits garantis par la loi. Les personnes doivent avoir le contrôle total de leurs données à tout moment et devraient être en mesure de choisir librement d'utiliser une telle application.
- Les applications de recherche de contacts sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et de nécessiter la réalisation d'une analyse d'impact relative à la protection des données avant leur déploiement.

- Il est possible d'obtenir des informations sur la proximité entre les utilisateurs de l'application sans les localiser. Ce type d'application ne nécessite pas et, dès lors, ne devrait pas impliquer l'utilisation de données de localisation.

- Lorsqu'un utilisateur est diagnostiqué infecté par le SARS-CoV-2, seules les personnes avec lesquelles il a été en contact étroit pendant la durée de conservation des données pertinente sur le plan épidémiologique pour la recherche des contacts devraient être informées.

- Il se peut que le fonctionnement de ce type d'application nécessite, en fonction de l'architecture choisie, l'utilisation d'un serveur centralisé. Dans ce cas et conformément aux principes de minimisation des données et de protection des données dès la conception, les données traitées par le serveur centralisé devraient être limitées au strict minimum:

    - lorsqu'un utilisateur est diagnostiqué infecté, les informations concernant ses contacts étroits antérieurs ou les identifiants diffusés par son application peuvent être collectés, mais uniquement avec son accord. Il convient de mettre en place une méthode de vérification permettant d'affirmer que la personne est effectivement infectée sans identifier l'utilisateur. Techniquement, ce serait possible en avertissant les contacts uniquement après l'intervention d'un professionnel de la santé, par exemple au moyen d'un code spécial à usage unique;

    - les informations stockées sur le serveur central ne devraient ni permettre au responsable du traitement d'identifier les utilisateurs qui ont été diagnostiqués infectés ou qui ont été en contact avec ceux-ci, ni permettre l'inférence de schémas de contacts qui ne sont pas nécessaires pour déterminer les contacts pertinents.

- Le fonctionnement de ce type d'application nécessite la diffusion de données qui sont lues par les appareils d'autres utilisateurs, ainsi que la réception et l'enregistrement des données diffusées:

    - il est suffisant d'échanger des identifiants pseudonymes entre les appareils mobiles des utilisateurs (ordinateurs, tablettes, montres connectées, etc.), par exemple en les diffusant [notamment via la technologie Bluetooth à basse consommation (*Bluetooth Low Energy* - BLE)];

    - les identifiants doivent être générés à l'aide de processus cryptographiques de pointe;

    - les identifiants doivent être renouvelés régulièrement pour réduire le risque de traçage physique et les tentatives de mise en relation.

- Ce type d'application doit être sécurisé pour garantir la sécurité des processus techniques. En particulier:

    - l'application ne devrait pas communiquer aux utilisateurs des informations leur permettant d'inférer l'identité ou le diagnostic d'autres utilisateurs. Le serveur central ne doit ni identifier les utilisateurs ni inférer des informations les concernant.

Avertissement: les principes ci-dessus sont liés à la finalité déclarée des applications de *recherche de contacts*, et uniquement à celle-ci, à savoir uniquement informer de manière automatique les personnes potentiellement exposées au virus (sans devoir les identifier). Les exploitants de l'application et son infrastructure peuvent être contrôlés par l'autorité de contrôle compétente. Suivre l'ensemble ou une partie des présentes lignes directrices ne suffit pas nécessairement à garantir le plein respect du cadre de protection des données.

2. Définitions

Contact	Dans le cadre d'une application de recherche de contacts, un contact est un utilisateur impliqué dans une interaction avec un utilisateur confirmé porteur du virus; cette interaction, par sa durée et la distance entre les personnes, entraînant un risque d'exposition significative à l'infection par le virus. Les paramètres relatifs à la durée d'exposition et à la distance entre les personnes doivent être évalués par les autorités sanitaires et peuvent être définis dans l'application.
Données de localisation	On entend par «données de localisation» toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques qui indiquent la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public (au sens de la directive), ainsi que les données provenant d'autres sources potentielles, ayant trait à: • la latitude, la longitude ou l'altitude du lieu où se trouve l'équipement terminal; • la direction du mouvement de l'utilisateur; ou • le moment auquel l'information sur la localisation a été enregistrée.
Interaction	Dans le contexte de l'application de recherche de contacts, une interaction est définie comme l'échange d'informations entre deux appareils situés à proximité immédiate l'un de l'autre (dans l'espace et dans le temps), dans les limites de la portée de la technologie de communication utilisée (par exemple le Bluetooth). Cette définition exclut la localisation des deux utilisateurs concernés par l'interaction.
Porteur du virus	Dans le présent document, nous considérons que les porteurs du virus sont les utilisateurs qui ont été testés positifs au virus et qui ont reçu un diagnostic officiel de la part de médecins ou de centres de santé.
Recherche de contacts	Les personnes qui ont été en contact étroit (selon des critères définis par des épidémiologistes) avec une personne infectée par le virus courent un risque élevé d'être également infectées et d'infecter d'autres personnes à leur tour. La recherche de contacts est une méthode de contrôle de la maladie qui permet de recenser toutes les personnes ayant été à proximité immédiate d'un porteur du virus de manière à vérifier si elles présentent un risque d'infection et à prendre les mesures sanitaires appropriées à leur égard.

3. Généralités

GEN-1	L'application est un outil qui doit venir en complément des techniques de recherche de contacts classiques (notamment les entretiens avec les personnes infectées), à savoir que son utilisation doit s'inscrire dans un programme de santé publique plus vaste. Elle peut uniquement être utilisée jusqu'à ce que les techniques de recherche manuelle de contacts permettent à elles seules de gérer le nombre de nouvelles infections.
GEN-2	Au plus tard lorsque le «retour à la normale» sera décidé par les autorités publiques compétentes, une procédure devra être mise en place pour mettre fin à la collecte d'identifiants (désactivation globale de l'application, instructions de désinstallation de l'application, désinstallation automatique, etc.) et activer la suppression de toutes les données collectées dans l'ensemble des bases de données (applications mobiles et serveurs).
GEN-3	Le code source de l'application et de son logiciel serveur doit être ouvert, et les spécifications techniques doivent être rendues publiques, de sorte que toute partie concernée puisse vérifier le code et, le cas échéant, contribuer à l'améliorer, corriger les éventuels défauts et garantir la transparence en ce qui concerne le traitement des données à caractère personnel.
GEN-4	Les étapes du déploiement de l'application doivent permettre de valider progressivement son efficacité du point de vue de la santé publique. Un protocole d'évaluation, précisant les indicateurs permettant de mesurer l'efficacité de l'application, doit être défini en amont à cette fin.

4. Finalités

PUR-1	L'application doit avoir pour seule finalité la recherche de contacts de sorte que les personnes potentiellement exposées au SARS-CoV-2 puissent être averties et prises en charge. Elle ne peut pas être utilisée à une autre fin.
PUR-2	L'application ne peut pas être détournée de son utilisation principale aux fins du contrôle du respect des mesures de quarantaine ou de confinement et/ou de la distanciation sociale.
PUR-3	L'application ne peut pas être utilisée pour tirer des conclusions sur la localisation des utilisateurs sur la base de leur interaction et/ou de tout autre moyen.

5. Considérations fonctionnelles

FUNC-1	L'application doit offrir une fonctionnalité permettant aux utilisateurs d'être informés qu'ils ont été potentiellement exposés au virus, cette information reposant sur la proximité avec un utilisateur infecté au cours d'une fenêtre de X jours avant le test de dépistage positif (la valeur X étant définie par les autorités sanitaires).

FUNC-2	L'application devrait fournir des recommandations aux utilisateurs identifiés comme ayant été potentiellement exposés au virus. Elle devrait transmettre des instructions concernant les mesures à suivre par l'utilisateur et devrait permettre à ce dernier de demander des conseils. Dans ce cas, une intervention humaine serait obligatoire.
FUNC-3	L'algorithme qui mesure le risque d'infection en tenant compte des facteurs de distance et de temps, et qui détermine donc si un contact doit être enregistré dans la liste de contacts, doit pouvoir être adapté en toute sécurité afin de tenir compte des connaissances les plus récentes sur la propagation du virus.
FUNC-4	**Les utilisateurs doivent être avertis s'ils ont été exposés au virus**, ou doivent recevoir régulièrement des informations leur permettant de savoir s'ils ont ou non été exposés au virus, pendant la période d'incubation de celui-ci.
FUNC-5	L'application devrait être interopérable avec d'autres applications développées dans les États membres, de sorte que les utilisateurs voyageant dans différents États membres puissent être effectivement avertis.

6. Données

DATA-1	L'application doit pouvoir diffuser et recevoir des données au moyen de technologies de communication de proximité telles que le Bluetooth à basse consommation (*Bluetooth Low Energy* - BLE) afin de permettre la recherche de contacts.
DATA-2	Les données diffusées doivent inclure des identifiants pseudo-aléatoires cryptographiquement forts, générés par l'application et spécifiques à celle-ci.
DATA-3	Le risque de collision entre identifiants pseudo-aléatoires devrait être suffisamment faible.
DATA-4	Les identifiants pseudo-aléatoires doivent être renouvelés régulièrement, à une fréquence suffisante pour limiter le risque de ré-identification, de traçage physique ou de mise en relation des personnes par quiconque, y compris par des opérateurs de serveur central, d'autres utilisateurs de l'application ou des tiers malveillants. Ces identifiants doivent être générés par l'application de l'utilisateur, éventuellement sur la base d'un noyau fourni par le serveur central.
DATA-5	Selon le principe de minimisation des données, l'application ne peut pas collecter de données autres que celles qui sont strictement nécessaires aux fins de la recherche de contacts.
DATA-6	L'application ne peut pas collecter de données de localisation pour la recherche de contacts. Les données de localisation peuvent être traitées dans le seul but de permettre à l'application d'interagir avec des applications similaires dans d'autres pays, et leur précision devrait être limitée à ce qui est strictement nécessaire à cette seule fin.

DATA-7	L'application ne devrait pas collecter de données relatives à la santé autres que celles qui sont strictement nécessaires aux finalités de l'application, sauf à titre facultatif et dans le seul but de faciliter le processus décisionnel en matière d'information de l'utilisateur.
DATA-8	Les utilisateurs doivent être informés de toutes les données à caractère personnel qui seront collectées. Ces données ne devraient être collectées qu'avec l'autorisation de l'utilisateur.

7. Propriétés techniques

TECH-1	L'application devrait utiliser les technologies disponibles telles que les technologies de communication de proximité [par exemple le Bluetooth à basse consommation (*Bluetooth Low Energy* - BLE)] pour détecter les utilisateurs à proximité de l'appareil sur lequel l'application est installée.
TECH-2	L'application devrait conserver un historique des contacts de l'utilisateur dans l'appareil, pour une durée limitée et prédéfinie.
TECH-3	L'application peut s'appuyer sur un serveur central pour mettre en œuvre certaines de ses fonctionnalités.
TECH-4	L'application doit reposer sur une architecture s'appuyant le plus possible sur les appareils des utilisateurs.
TECH-5	À l'initiative des utilisateurs signalés comme étant infectés par le virus et après la confirmation de leur statut par un professionnel de la santé dûment qualifié, leur historique de contacts ou leurs propres identifiants devraient être communiqués au serveur central.

8. Sécurité

SEC-1	Un mécanisme doit permettre de vérifier le statut des utilisateurs signalés comme étant positifs au SARS-CoV-2 dans l'application, par exemple en fournissant un code à usage unique lié à une station de test ou à un professionnel de la santé. S'il n'est pas possible d'obtenir la confirmation de manière sécurisée, les données ne peuvent pas être traitées.
SEC-2	Les données envoyées au serveur central doivent être transmises par un canal sécurisé. Le recours aux services de notification proposés par les fournisseurs de plateformes de systèmes d'exploitation devrait faire l'objet d'une évaluation approfondie et ne devrait pas entraîner la divulgation de données à des tiers.
SEC-3	Les demandes ne peuvent pas être vulnérables à la manipulation par un utilisateur malveillant.
SEC-4	Des techniques cryptographiques de pointe doivent être mises en œuvre pour sécuriser les échanges entre l'application et le serveur ainsi qu'entre les applications, et, de manière générale, pour protéger les informations stockées dans les applications et sur le serveur. Parmi les techniques pouvant être utilisées

	figurent par exemple: le chiffrement symétrique et asymétrique, les fonctions de hachage, le test dit du «private membership», l'intersection d'ensemble privée, la récupération d'informations privées, le chiffrement homomorphique, etc.
SEC-5	Le serveur central ne peut pas conserver les identifiants de connexion réseau (par exemple les adresses IP) des utilisateurs, y compris de ceux qui ont été diagnostiqués positifs et ont communiqué leur historique de contacts ou leurs propres identifiants.
SEC-6	Afin d'éviter les usurpations d'identité ou la création de faux utilisateurs, le serveur doit authentifier l'application.
SEC-7	L'application doit authentifier le serveur central.
SEC-8	Les fonctionnalités du serveur devraient être protégées contre les attaques par relecture.
SEC-9	Les informations transmises par le serveur central doivent être signées afin de pouvoir authentifier leur origine et leur intégrité.
SEC-10	L'accès à la totalité des données stockées sur le serveur central et non accessibles au public doit être réservé à des personnes autorisées.
SEC-11	Le gestionnaire des autorisations de l'appareil au niveau du système d'exploitation peut uniquement demander les autorisations requises pour accéder aux modules de communication et les utiliser lorsque nécessaire, pour stocker les données dans le terminal et pour échanger des informations avec le serveur central.

9. Protection des données à caractère personnel et de la vie privée des personnes physiques

Rappel: les lignes directrices suivantes concernent une application dont la seule finalité est la recherche de contacts.

PRIV-1	Les échanges de données doivent respecter la vie privée des utilisateurs (et notamment le principe de minimisation des données).
PRIV-2	L'application ne peut pas permettre l'identification directe des utilisateurs lorsqu'ils l'utilisent.
PRIV-3	L'application ne peut pas permettre le traçage des déplacements des utilisateurs.
PRIV-4	L'utilisation de l'application ne devrait pas permettre aux utilisateurs d'apprendre quoi que ce soit sur d'autres utilisateurs (et notamment s'ils sont ou non porteurs du virus).
PRIV-5	La confiance dans le serveur central doit être limitée. La gestion du serveur central doit suivre des règles de gouvernance clairement définies et inclure toutes les mesures nécessaires pour garantir la sécurité dudit serveur. La localisation du serveur central devrait permettre un contrôle effectif par l'autorité de contrôle compétente.
PRIV-6	Une analyse d'impact relative à la protection des données doit être réalisée et devrait être rendue publique.
PRIV-7	L'application devrait seulement révéler à l'utilisateur s'il a été exposé au virus, sans fournir, si possible, d'informations sur d'autres utilisateurs, le nombre d'expositions et les dates d'exposition.
PRIV-8	Les informations transmises par l'application ne peuvent pas permettre aux utilisateurs d'identifier les utilisateurs porteurs du virus ni les déplacements de ces derniers.
PRIV-9	Les informations transmises par l'application ne peuvent pas permettre aux autorités sanitaires d'identifier les utilisateurs potentiellement exposés sans leur accord.
PRIV-10	Les demandes envoyées par l'application au serveur central ne peuvent révéler aucune information sur le porteur du virus.
PRIV-11	Les demandes envoyées par l'application au serveur central ne peuvent révéler aucune information superflue concernant l'utilisateur, à l'exception, éventuellement, et uniquement si nécessaire, de ses identifiants pseudonymes et de sa liste de contacts.
PRIV-12	Les tentatives de mise en relation ne peuvent pas être possibles.
PRIV-13	Les utilisateurs doivent pouvoir exercer leurs droits au moyen de l'application.
PRIV-14	La suppression de l'application doit entraîner la suppression de l'ensemble des données collectées localement.
PRIV-15	L'application ne devrait collecter que les données transmises par des instances de l'application ou par des applications équivalentes interopérables. Aucune donnée

	liée à d'autres applications et/ou d'autres dispositifs de communication de proximité ne devrait être collectée.
PRIV-16	Afin d'éviter la ré-identification par le serveur central, des serveurs proxy devraient être installés. L'utilisation de ces serveurs transparents a pour but de mélanger les identifiants de plusieurs utilisateurs (tant ceux des porteurs du virus que ceux envoyés par les demandeurs) avant de les partager avec le serveur central, de manière à ce que ce dernier ne puisse pas connaître les identifiants (tels que les adresses IP) des utilisateurs.
PRIV-17	L'application et le serveur doivent être développés et configurés avec soin afin de ne pas collecter de données superflues (par exemple, aucun identifiant ne devrait figurer dans les journaux de serveurs, etc.) et d'éviter l'utilisation de tout kit de développement logiciel (SDK) tiers collectant des données à d'autres fins.

La plupart des applications de recherche de contacts en cours d'examen suivent deux grandes approches lorsqu'un utilisateur est déclaré infecté: elles peuvent, soit envoyer à un serveur l'historique de contacts de proximité qu'elles ont obtenu en analysant les contacts, soit envoyer la liste de leurs propres identifiants qui ont été diffusés. Les principes suivants sont déclinés selon ces deux approches. Le fait que ces deux approches soient abordées ici ne signifie pas que d'autres ne sont pas possibles ou même préférables, par exemple des approches qui mettent en œuvre une certaine forme de chiffrement E2E ou qui appliquent d'autres technologies renforçant la sécurité ou le respect de la vie privée.

9.1. Principes s'appliquant uniquement **lorsque l'application envoie une liste de contacts au serveur**:

CON-1	Le serveur central doit collecter l'historique de contacts des utilisateurs signalés comme étant positifs au SARS-CoV-2, à la suite d'une action volontaire de leur part.
CON-2	Le serveur central ne peut pas conserver ni diffuser la liste des identifiants pseudonymes des utilisateurs porteurs du virus.
CON-3	L'historique de contacts stocké sur le serveur central doit être supprimé une fois les utilisateurs avertis de leur proximité avec une personne diagnostiquée positive.
CON-4	Sauf lorsque l'utilisateur détecté positif partage son historique de contacts avec le serveur central ou lorsque l'utilisateur adresse une demande au serveur pour connaître son exposition potentielle au virus, aucune donnée ne doit sortir de l'appareil de l'utilisateur.
CON-5	Tout identifiant figurant dans l'historique local doit être supprimé après X jours à compter du moment où il a été collecté (la valeur X étant définie par les autorités sanitaires).
CON-6	Les historiques de contacts communiqués par différents utilisateurs ne devraient pas faire l'objet d'un traitement ultérieur, par exemple ils ne devraient pas être mis en corrélation croisée en vue d'une cartographie globale de la proximité.

CON-7	Les données stockées dans les journaux des serveurs doivent être limitées au strict nécessaire et doivent respecter les exigences en matière de protection des données.

9.2. Principes s'appliquant uniquement lorsque l'application envoie une liste de ses propres identifiants au serveur:

ID-1	Le serveur central doit collecter les identifiants, diffusés par l'application, des utilisateurs signalés comme étant positifs au SARS-CoV-2, à la suite d'une action volontaire de leur part.
ID-2	Le serveur central ne peut pas conserver ni diffuser l'historique de contacts des utilisateurs porteurs du virus.
ID-3	Les identifiants stockés sur le serveur central doivent être supprimés après avoir été envoyés aux autres applications.
ID-4	Sauf lorsque l'utilisateur détecté positif partage ses identifiants avec le serveur central ou lorsque l'utilisateur adresse une demande au serveur pour connaître son exposition potentielle au virus, aucune donnée ne doit sortir de l'appareil de l'utilisateur.
ID-5	Les données stockées dans les journaux des serveurs doivent être limitées au strict nécessaire et doivent respecter les exigences en matière de protection des données.