Avis n° 43/2020 du 26 mai 2020

Objet: Demande d'avis concernant une proposition de loi relative à l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population (CO-A-2020-049)

L'Autorité de protection des données (ci-après « l'Autorité »);

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis du Président de la Chambre des Représentants, Monsieur Patrick DEWAEL, reçue le 15mai 2020;

Vu le rapport de Madame Alexandra Jaspar, Directrice du Centre de Connaissances de l'Autorité de protection des données ;

Émet, le 26 mai 2020, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Président de la Chambre des Représentants a sollicité l'avis de l'Autorité concernant une proposition de loi relative à l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population (ci-après « la proposition de loi »).

2. Cette proposition de loi fait suite à un projet d'arrêté royal ayant le même objet et sur lequel l'Autorité s'est prononcée par voie d'avis 34/2020 en date du 28 avril dernier et auquel l'Autorité renvoie pour les aspects non couverts dans le présent avis.

3. Il est précisé dans l'exposé des motifs que « *les applications numériques de traçage de contact permettent aux citoyens de constater eux-mêmes qu'ils ont été en contact avec une personne contaminée sans savoir qui est la personne contaminée et sans que les localisations où ces personnes se sont rendues soient sauvegardées ni dans l'application de traçage de contacts, ni dans une banque de données centrale* ».

4. Le but premier de la proposition de loi consiste à déterminer les conditions auxquelles doivent satisfaire les applications de traçage de contact utilisées pour la gestion de la pandémie sur le territoire belge,[1] afin que les traitements de données qu'elles génèrent soit minimalisés et que les garanties essentielles pour se prémunir contre le risque de ré-identification des utilisateurs de ces applications et pour la préservation de leurs droits et libertés soient en place.

5. Selon la proposition de loi, Sciensano enregistrera dans un fichier log les clefs sécurisées des utilisateurs de l'application contaminés et mettra ce fichier à disposition des autres utilisateurs de ces applications (sur base de ces clefs, les autres utilisateurs pourront déduire à l'aide de leur application la présence d'un éventuel numéro de série temporaire lié, ce qui générera alors un avertissement qu'ils ont eu un contact à risque avec une personne contaminée). Ainsi, selon l'exposé des motifs, la technique utilisée (DP3T) permet d'assurer l'échange de l'information selon laquelle les utilisateurs ont eu un contact à risque sans que les utilisateurs ne soient identifiés ni par le gestionnaire du serveur de l'application ni par les autres utilisateurs.

6. L'Autorité souligne que son avis a été émis en extrême urgence et est donc limité aux points essentiels.

7. Elle accueille favorablement certaines améliorations apportées au texte par rapport au projet d'Arrêté royal qui lui a été soumis: justification de la proportionnalité des traitements de données effectués au

[1] Le titre de la proposition de loi mériterait d'être adapté en ce sens.

moyen des applications, justification de la raison d'être du délai de conservation des données de 3 semaines, ajout qu'un non utilisateur ne peut pas être désavantagé, obligation pour Sciensano d'empêcher tout croisement de données (sur la formulation de cette obligation, voir ci-après et la note de bas de page y relative), utilisation de données anonymisées pour la recherche épidémiologique, utilisation du système DP3T basé sur la technologie Bluetooth et la cryptographie.

8. L'Autorité rappelle que les autorités de protection des données des Etats de l'Union européenne ont émis ensemble, au travers du Comité européen de la protection des données (ci-après « CEPD »), des lignes directrices[i] sur les applications de traçage. L'Autorité insiste sur la nécessité de veiller à leur respect.

II. EXAMEN

a. Introduction

9. Le but premier de la proposition de loi consiste à déterminer les conditions auxquelles doivent satisfaire les applications de traçage de contact utilisées dans le cadre de la gestion de la pandémie sur le territoire belge et à confier à Sciensano la gestion de ce système de traçage. Par souci de clarté, le titre de la proposition de loi mérite d'être reformulé en ce sens.

b. Remarque préalable sur le caractère nécessaire de l'utilisation des applications de traçage et des traitements de données auxquels elles donnent lieu

10. En tant qu'ingérence importante dans la vie privée de la population, le protocole choisi étant bon mais présentant néanmoins des risques, et au vu du risque d'accoutumance que l'utilisation généralisée des technologies de traçage implique, le choix de proposer l'utilisation de ce type d'applications à la population ne peut se faire que s'il constitue une mesure non seulement proportionnée mais également nécessaire.

11. Si le caractère proportionné des applications de traçage peut et doit être encadré par voie législative pour que les citoyens puissent lui conférer la confiance requise à son fonctionnement[2], leur caractère nécessaire est dépendant de facteurs externes qui doivent être présents et justifiés lors de leur mise à disposition par la ou les autorités compétentes (cela requiert que soient au préalable posées certaines questions, en ce compris : les personnes ayant eu un contact à risque pourront-elles se faire tester ou seront-elle mises en quarantaine ?, le taux de personnes asymptomatiques mais contagieuses ne met-

[2] L'efficacité de l'utilisation de ces applications de traçage dépend du nombre de personnes qui les installent et les activent.

il pas à mal l'efficacité de ce type d'application ? et pour le surplus cf. le point A de l'avis précité 34/2020). Sur base des réponses à ces questions, l'autorité publique compétente devra être en mesure d'attester que son choix est nécessaire et pertinent dans la gestion du déconfinement de la population. Ce choix devra être documenté adéquatement avant la mise à disposition des applications au public et à intervalles de temps adéquats réguliers. Cette analyse devra être intégrée dans l'analyse d'impact préalable à la protection des données qui devra être réalisée en exécution de l'article 35 du RGPD avant la diffusion de l' (ou des) application(s) et du dispositif qui l'/les accompagne.

12. Seules les autorités publiques qui ont reçu du législateur une mission de service public qui le nécessite peuvent mettre en place ce type de dispositifs (art. 6.1.e RGPD). Les traitements de données encadrés en l'espèce concernent des catégories particulières de données, au sens de l'article 9.1 du RGPD (à savoir, des données concernant la santé). Par conséquent, le niveau d'exigence requis quant à la qualité de la loi encadrant ces applications et le dispositif qui les encadre se doit d'être élevé et cette législation doit prévoir des garanties pour les personnes concernées au vu du risque élevé d'atteinte à leurs droits et libertés. L'article 9.2, i) du RGPD prévoit en effet que le traitement de ce type de données peut être réalisé s'il est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique mais seulement à la condition qu'un tel traitement soit encadré par une norme législative (ou réglementaire) prévoyant des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés des personnes concernées.

c. Garanties liées à l'impossibilité de ré-identification - Responsable de traitement - vérification du respect des conditions – soumission obligatoire de l'analyse d'impact préalable à la protection des données à l'Autorité et publication de cette analyse et de l'avis de l'Autorité

13. Le protocole DP3T prévoit une série de garanties, en ce compris la minimisation des données collectées (seul les clefs des personnes infectées sont partagées, pas de partage direct du graphe social), une génération des clefs sur le téléphone de l'utilisateur, ainsi que des protections contre les risques de recoupements de données et la ré-identification des personnes concernées. Bien que le protocole soit bon, il n'élimine pas tous les risques par exemple le risque pour une personne de pouvoir déterminer qui l'a infecté ou de déterminer la localisation de personnes infectées. Sur ces aspects, il est renvoyé à l'article de Serge Vaudenay professeur et directeur du Laboratoire de sécurité et de cryptographie (LASEC) à l'Ecole polytechnique fédérale de Lausanne (EPFL) qui met en avant les différentes attaques possibles et la façon de les gérer au mieux[3]Il est indispensable que, d'une part, la subsistance d'une part de risques soit reflétée dans la proposition de loi afin notamment que le Parlement et les personnes

[3] Serge Vaudenay, Analysis of DP3T – Between Scylla and Charybdis, 8 avril 2020, EPFL, Lausanne, disponible en ligne à l'adresse suivante https://eprint.iacr.org/2020/399.pdf

concernées ne se voient pas privés de cette information et, d'autre part, (2) l'analyse de proportionnalité puisse être faite en connaissance de cause. Or la proposition de loi est muette quant au contenu de ce protocole, quant aux garanties qu'il apporte, quant aux risques subsistant et quant aux stratégies de mitigation des risques qui doivent être implémentées au niveau de l'application.

14. La description du fonctionnement des applications (faite dans l'exposé des motifs, et non pas dans le dispositif de la proposition de loi, ce que l'Autorité invite le demandeur à corriger) et des spécifications auxquelles doivent répondre les applications (article 4§2 de la proposition de loi) ne permet pas de garantir que des stratégies de mitigation suffisantes sont imposées au niveau de l/des application(s) de traçage qui sera/ont choisi(e)s.

15. La description du protocole ne contient pas le numéro de version ou « type » du protocole qui est proposé. Plusieurs designs ont été proposés par le consortium DP3T.

16. Les fréquences de rafraîchissement des clefs ainsi que des numéros de séries temporaires sont des éléments essentiels pour l'anonymité du système et pour éviter les risques de traçage. La proposition de loi ne contient pas d'information sur la fréquence de rafraîchissement des clefs et des identifiants « aléatoires » (en réalité temporaires)

17. La lecture de cette disposition semble même indiquer que les spécifications prévues pour les applications ré-introduisent des risques de ré-identification en principe annihilés par le protocole DP3T. En effet, il semble à la lecture de la proposition de loi que la vérification du statut positif d'une personne se fasse à travers l'entrée dans l'application de son numéro de téléphone et de la date du test. L'application envoie ensuite au serveur la/les clefs de la personne permettant son traçage sur plusieurs semaines. Pour pouvoir prétendre à la mise en place d'un système fonctionnant à l'aide de données anonymes et excluant toute possibilité de ré-identification :

    a. il y a lieu que le code d'autorisation fourni à l'utilisateur l'autorisant à envoyer sa/ses clefs dans la base de données lui soit fourni par un opérateur différent que l'opérateur en charge de la gestion de la base de données des clefs. Une fois que les clefs ont été vérifiées, les données liant un code d'autorisation au numéro de téléphone et à la date du test doivent être effacées;
    b. le système doit fonctionner avec plusieurs (et non pas une) clés, sans possibilité de savoir, y compris pour Sciensano, qu'elles sont liées à la même personne, elles doivent être fréquemment rafraichies et il doit être possible pour l'utilisateur de vérifier que la clé a changé (voire idéalement de supprimer à postériori toute génération de clés pendant une période donnée).

Or le système semble générer l'information selon laquelle une personne infectée (non-identifiée directement) a eu un contact prolongé avec une autre personne infectée (également non-identifiée directement) et/ou à des intervalles X, ce qui n'est pas en général concevable dans le cas d'un système anonyme ou les clés d'une même personne ne sont pas liées entre elles.
La description du système ne permet pas de s'assurer que Sciensano ne prendra pas contact par téléphone avec les personnes concernées (ce qui supposerait une conservation de leur numéro de téléphone et ferait en sorte que le système ne fonctionnerait en réalité pas sur une base anonymisée).

18. Pour servir tant la sécurité juridique que la lisibilité de la proposition de loi, l'Autorité considère que la notion d'application de traçage doit faire l'objet d'une définition en son article 3. Cette définition précisera que ces applications présentent des garanties contre le risque de ré-identification de leurs utilisateurs tel qu'explicité dans l'exposé des motifs[4] (application basée sur le système de cryptographie DP3T qui permet l'information de l'utilisateur qu'il a eu un contact à risque avec une personne contaminée sans savoir qui est la personne contaminée et sans que les localisations de ces personnes ne soient collectées ni dans l'application de traçage de contacts, ni dans une banque de données centrale). De plus, cette définition précisera utilement que, en aucun cas, une application de traçage ne peut permettre la transmission en temps réel de l'information d'un contact à risque avec une personne contaminée.

19. La proposition de loi désigne Sciensano comme responsable du traitement à l'article 6 de la proposition de loi.

20. L'Autorité détecte un risque important lié au fait que, en sus de ce qui est repris au point 15 ci-dessus et bien que la proposition de loi impose l'adoption par Sciensano de mesures pour garantir que les données collectées par cet organisme en exécution de la proposition de loi ne soient pas recoupées avec d'autres données provenant d'autres bases de données[5], cet organisme se voit déjà allouer, par le biais d'un autre projet normatif en voie d'adoption[6] (voir l'avis y relatif de l'Autorité publié le 25 mai 2020), la gestion d'une base de donnée massive concernant des personnes contaminées par le coronavirus COVID 19. . L'Autorité rappelle qu'une des composantes essentielles des applications de

[4] Il est précisé dans l'exposé des motifs que « *les applications numériques de traçages de contact permettent aux citoyens de constater eux-mêmes qu'ils ont été en contact avec une personne contaminée sans savoir qui est la personne contaminée et sans que les localisations où ces personnes se sont rendues soient sauvegardées ni dans l'application de traçage de contacts, ni dans une banque de données centrale* ».

[5] La formulation de l'article 11, §2 laisse d'ailleurs à désirer étant donné qu'il est précisé que « *les informations conservées dans la liste log et la banque de données visées à l'article 8, §§1 et 2 ne sont aucunement interconnectées* ». Or, la liste log est visée à l'article 8,§1er et c'est la banque de données de recherche de Sciensano qui est visée à l'article 8,§2 de la proposition de loi. Il convient en lieu et place de préciser que toute interconnexion de données collectée par le biais de l'application de traçage avec n'importe quelles autres données à caractère personnel est interdite au même titre que toute tentative de ré-identification des utilisateurs d'une application de traçage.

[6] Proposition de loi portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19, Chambre des représentants, doc 55, 1249/1.

traçage, non seulement en terme de protection de la vie privée mais également en terme de confiance qu'elle doit générer dans le chef de la population, consiste à assurer l'échange d'information entre les personnes infectées et leur contact à risque tout en les préservant contre le risque qu'elles soient ré-identifiées.

21. De plus, il convient de préciser à propos de quels traitements de données cette désignation est faite. A défaut, cette désignation n'apporte ni la prévisibilité ni la clarté requise. De ce que l'Autorité peut comprendre, il s'agit de désigner le responsable du traitement qui optera pour la ou les applications présentant les caractéristiques légalement requises et qui assurera la gestion du serveur lié à son/leur utilisation (fichier log conservant et mettant à disposition de tous les utilisateurs les clefs sécurisées des utilisateurs contaminés en vue de la génération de l'alerte de l'existence d'un contact à risque auprès des utilisateurs concernés). L'auteur de la proposition de loi doit compléter la désignation du responsable de traitement en précisant à propos de quels traitements de données à caractère personnel cette désignation est faite. En outre, si, comme l'Autorité peut le comprendre, c'est Sciensano qui va décider quelles applications de traçage seront utilisées et mises à disposition du public en Belgique, il convient de le préciser également.

22. L'Autorité rappelle également que l'utilisation d'une seule et unique application diminuerait le risque de voir apparaitre des applications ne répondant pas aux conditions techniques et légales requises et présentant des risques importants pour le respect de la confidentialité des données des citoyens. Dès lors, l'Autorité recommande qu'un article soit ajouté à la proposition de loi pour préciser que Sciensano endossera la responsabilité de vérifier et de garantir que les applications qui seront proposées au public seront conformes à toutes les spécifications légales requises ainsi qu'à celles du CEPD. Une garantie complémentaire pour les personnes concernées qui parait indiquée à mettre en place serait de prévoir dans la proposition de loi qu'avant toute mise à disposition au public d'une application de traçage, Sciensano est tenu de soumettre son AIPD relative à ladite application à l'avis préalable de l'Autorité avec obligation de publier cette AIPD ainsi que l'avis de l'Autorité sur cette AIPD.

23. Comme requis par le CEPD, l'entièreté du code source de chaque/l'application devra également être publié et l'Autorité insiste pour que cette publication ait lieu suffisamment avant la date de mise à disposition de l'/chaque application afin de permettre son analyse par des spécialistes. Elle recommande que tous ses « builds » soient vérifiables.

d. <u>Finalités des traitements de données réalisés au moyen des applications numérique de traçage de contacts et principe de minimisation.</u>

24. L'article 4 de la proposition de loi tente de déterminer les finalités des traitements de données à caractère personnel qui seront réalisés à l'aide des applications de traçage.

25. Tout d'abord, il est erronément précisé que les applications réalisent un traitement de données. Ce n'est pas une application qui réalise un traitement de données mais une personne physique ou morale. Cela doit être corrigé. De plus, en plus de préciser les fonctionnalités générales auxquelles les applications de traçage devront répondre, il convient de préciser clairement quels sont les traitements de données réalisés par Sciensano pour assurer le fonctionnement du système de traçage.

26. De plus, la formulation de la 1ère et 2nde finalité pose question et mérite d'être améliorée. Selon notre compréhension du système, les applications de traçage doivent être mises à disposition des utilisateurs pour permettre l'échange entre eux de l'information selon laquelle ils ont eu un contact à risque avec un utilisateur contaminé sans que les utilisateurs ne soient identifiés ni par le gestionnaire du serveur de l'application ni pas les utilisateurs. La communication de l'information qu'un utilisateur est contaminé n'apparait donc pas comme une finalité première de l'application mais uniquement comme un prérequis.

27. Par ailleurs, le principe de minimisation du RGPD implique de ne traiter que des données strictement nécessaires et pertinentes pour la finalité poursuivie. Dès lors, au vu de la définition des contacts à haut risque déterminée par le SPF Santé publique et le Centre de crise (contact de moins de 1,5 mètres avec une personne contaminée pendant plus de 15 minutes), l'Autorité considère que seuls ces contacts (le cas échéant avec une marge d'erreur acceptable du type « contact de moins de 4 mètres de distance pendant plus de 10 minutes ») doivent être captés (d'autant plus que la technologie Bluetooth permet de capter les contacts jusqu'à 100 mètres, ce qui est manifestement disproportionné pour la finalité poursuivie). La rédaction de la finalité devra être revue sur cette base et une définition de la notion de « contact à risque » conforme aux recommandations officielles sera utilement intégrée à l'article 3 de la proposition de loi par souci de sécurité juridique.

28. En ce qui concerne la 3ème finalité visée à l'article 4 de la proposition de loi (recherche épidémiologique), l'Autorité considère que cette finalité ne nécessite pas d'être spécifiquement encadrée dans la proposition de loi dans la mesure où le respect des dispositions pertinentes du RGPD et de la LTD en matière de recherche suffit. Ceci, d'autant plus que l'article 10 de la proposition de loi prévoit une interdiction de traitement ultérieur des données collectées dans le cadre de la gestion de ce système de traçage, à l'exception des traitements ultérieurs à des fins de recherche scientifique et statistique réalisés conformément à l'article 89 du RGPD et au titre 4 de la loi cadre[7].

[7] Et ce, même si l'Autorité comprend que, au-delà de la collecte de données supplémentaires effectuée à des fins de recherche et qui n'est pas nécessaire pour les opérations de traçage, le serveur ne collecte aucune information supplémentaire qui ne soit pas déjà publique.

29. Ceci dit, si l'objectif est de collecter des données supplémentaires exclusivement à cette fin de recherche (ce que semble indiquer la manière dont une partie du système est conçu), l'Autorité voit un problème fondamental dans cette collecte et cet objectif complémentaires qui induisent un risque de ré-identification et d'établissement du graphe social des personnes, et ce alors que l'objectif de la proposition de loi est de modaliser les applications de traçage pour minimiser le risque de ré-identification. Sans compter que ni la proposition de loi ni l'exposé des motifs ne justifient le caractère proportionné de cette collecte pour la finalité visée.

30. L'ajout de cette finalité de recherche épidémiologique nuit à la compréhension du projet et risque d'entrainer de la confusion dans le chef des utilisateurs de l'application. L'Autorité recommande donc la suppression des dispositions de la proposition de loi relatives à l'encadrement de la recherche, d'autant plus que certaines sont contradictoires avec la garantie de la réalisation de ces recherches au moyen de données anonymes.

e. Paramètres requis pour les applications de traçage – principe de minimisation du RGPD

31. Même si, à juste titre, la proposition de loi prévoit que l'installation et l'utilisation d'une application de traçage ne se fera que sur base volontaire, il importe que les paramètres de ces applications soient conformes au RGPD. C'est l'objet de l'article 4, §2 qui détermine les fonctionnalités requises des applications de traçage.

32. D'un point de vue général, l'Autorité considère que, pour assurer une meilleure lisibilité et prévisibilité ainsi qu'une sécurité juridique quant à ces fonctionnalités techniques requises pour se prémunir contre le risque de ré-identification (irréversibilité du hashing, fréquence de changement des numéros de série temporaires non personnalisés,…), les concepts suivants utilisés doivent être définis à l'article 3 de la proposition de loi :
    a. Clé sécurisée (dans la définition, il sera utilement prévu que seuls des algorithmes cryptographiques conformes à l'état actuel de l'art peuvent être utilisés afin d'assurer l'intégrité et la confidentialité des échanges) ;
    b. Utilisateur d'une application numérique de traçage ;
    c. Numéro de série temporaire non personnalisé (et non « aléatoire »).

33. Concernant l'article 4, §2, 6ème tiret, qui détermine les limites en termes de collecte et de sauvegarde de données par et dans les appareils terminaux des utilisateurs via la technologie Bluetooth, l'Autorité renvoie à ses propos repris au point précédent concernant le principe de minimisation des données. Cette disposition sera adaptée en conséquence pour être conforme au RGPD.

34. En outre, une interdiction de collecter tout identifiant lié au terminal de l'utilisateur (adresse mac du terminal,….) doit être ajoutée à titre de garantie pour les personnes concernées contre leur ré-identification. La précision de l'utilisation de la technologie Bluetooth mérite également d'être reprise dans le dispositif même de la proposition de loi étant donné qu'elle constitue une caractéristique spécifique du système. L'Autorité insiste par ailleurs pour que la liste des spécifications inclue que les applications doivent empêcher toute possibilité de géo-localiser les utilisateurs.

35. De plus, l'article 4, §2, dernier tiret précisera utilement l'identification de l'autorité compétente qui sera chargée de désactiver les applications numériques de traçage une fois qu'elles ne seront plus nécessaires pour la gestion du déconfinement.

36. L'article 4,§3 de la proposition de loi prévoit que « *des spécifications techniques auxquelles les applications numériques de traçages de contacts doivent satisfaire sont prévues sur le site web du responsable du traitement* ». L'autorité considère que c'est au Roi qu'il appartient de déterminer ces modalités techniques et ce, en tenant compte des lignes directrices émises par le CEPD et que c'est à Sciensano de s'assurer que les applications répondent à ces modalités techniques. De plus, il convient de préciser dans le dispositif de loi que ces modalités techniques doivent assurer que les fonctionnalités visées aux paragraphes deux du même article sont respectées et qu'elles assurent que les utilisateurs de l'application de traçage sont protégés contre le risque de ré-identification par tout tiers.

37. A ce sujet, d'un de point de vue général, il importe qu'à tout le moins, que tous les flux de données liés au fonctionnement du système de traçage soient adéquatement sécurisés pour éviter toute attaque et tout détournement du système à des fins malicieuses. Il s'agit de sécuriser les flux suivants : serveur vers les applications, applications vers l'autorité en charge de recevoir les notifications de personnes infectées et des flux entre les applications mêmes (entre les équipements terminaux de utilisateurs de l'application). Il importe que ces mesures techniques prévoient de telles mesures de sécurisation. L'usage d'une plate-forme de tiers de confiance semble à cet effet indispensable.

f. <u>Caractère volontaire de l'utilisation de l'application de traçage</u>

38. Il est fondamental que la proposition de loi prévoie que l'installation, l'utilisation et la désinstallation d'une application de traçage soit effectuée dès que et uniquement si un utilisateur en a émis le souhait. Bien que ce soit clairement la volonté de l'auteur de la proposition de loi, il convient de le préciser.

39. L'auteur de la proposition de loi n'a pas suivi la suggestion de l'Autorité faite dans son avis 34/2020 de prévoir des sanctions civiles et/ou administratives et/ou pénales pour toute personne qui lierait l'accès à un bien ou à un service à l'utilisation d'une application de traçage. Ceci est motivé dans l'exposé des motifs par le fait que des campagnes de promotion de l'utilisation d'une application de traçage seront

envisagées. L'Autorité considère que des campagnes de promotion pourront être mises en œuvre sans pour autant devoir lier l'utilisation de ces applications à l'accès à un bien ou un service. Si un tel conditionnement était réalisé en pratique, cela mettrait à néant le caractère volontaire de l'utilisation de l'application. Afin de pouvoir disposer de la confiance du public, il importe que le caractère volontaire de ce système soit garanti par des sanctions. L'Autorité recommande également que la proposition de loi reprenne de manière explicite une disposition visant à confirmer que l'utilisation d'applications de traçage est et restera, en toute hypothèse, strictement volontaire, qu'aucune pression quelconque ne sera exercée sur les citoyens à cet égard et que ce volontariat se matérialise dans toutes les composantes du dispositif : installation de l'application, activation de la communication par Bluetooth, prise de contact avec un professionnel de santé, notification du caractère positif de son diagnostic ou résultat positif à un examen de dépistage à la COVID-19 dans l'application, réalisation du dépistage suite à la réception d'une notification, désinstallation de l'application.

g. Transparence des traitements de données générés par l'utilisation de l'application

40. L'article 6 § 2 fait référence à l'obligation d'information de Sciensano en exécution de l'article 13 du RGPD. Concernant les modalités de communication de ces informations, il est renvoyé au considérant 24 de l'avis précité 34/2020 de l'Autorité. Une attention particulière devra y être portée. La confiance des utilisateurs potentiels ne peut être de mise que s'ils sont, clairement et de manière appropriée, dûment informés de la façon dont fonctionnera le système d'applications de contact et de l'entièreté des collectes et échanges de données qu'il engendra ainsi que de ses finalités concrètes et opérationnelles.

h. Conservation des données localement dans les appareils terminaux des utilisateurs et dans le fichier log centralisé

41. L'article 7 de la proposition de loi porte sur la conservation des données utilisées ou générées dans le cadre de l'utilisation des applications de traçage.

42. Tout d'abord, il convient de lever le flou qui entoure cette disposition quant aux catégories de personnes qui assure la conservation des données prévues (clefs sécurisées, numéros de série temporaires non personnalisés générés par les applications, fuseaux horaires comprenant une date et une partie de la journée de 6 heures dans lesquels un contact entre utilisateurs a eu lieu ainsi que la distance et la durée du contact). Selon notre compréhension du système, il s'agit de données qui sont conservées localement dans les équipements terminaux des utilisateurs. Cela doit être précisé.

43. De plus, conformément au principe de minimisation des données explicité ci avant, ces données doivent être réduites au strict nécessaire au regard de la notion de contact à risque telle que déterminée par le SPF Santé publique et le centre de crise (cf. supra). Cet article sera adapté en conséquence.

i. Collecte du numéro de téléphone et de l'information selon laquelle l'utilisateur de l'application de traçage est contaminé

44. L'article 7, §2 prévoit que « *l'utilisateur peut insérer volontairement les informations suivantes dans l'application numérique de traçage de contacts :*
    a. *la contamination de COVID-19 constatée*[8] *;*
    b. *le numéro de téléphone de l'utilisateur*. »

45. La collecte du numéro de téléphone de l'utilisateur constitue incontestablement le maillon faible du système prévu par l'auteur de la proposition de loi. En effet, ce numéro de téléphone rompt la garantie de non identification de l'utilisateur.

46. Ceci étant, l'Autorité comprend, au vu de l'exposé des motifs, que ce numéro de téléphone est nécessaire pour que Sciensano puisse envoyer un sms de vérification à l'utilisateur après vérification et constatation de l'authenticité de l'application de traçage utilisée. Une fois ce code sms introduit dans l'application, Sciensano donnera l'autorisation à l'application de l'utilisateur d'uploader la clef sécurisée et la date présumée de contamination vers le fichier log central contenant les clefs sécurisées de tous les utilisateurs contaminés.

47. Comme indiqué plus haut, lAutorité recommande fortement l'utilisation de codes à usage unique pour la validation de l'envoi des clés vers le serveur, sans entrée du numéro de téléphone dans l'application. Si l'entrée du numéro d téléphone était néanmoins indispensable, l'Autorité considère qu'il est impératif, non seulement, de préciser, à l'article 7 §2 de la proposition de loi, cette seule et unique finalité d'utilisation du numéro de téléphone de l'utilisateur[9] (avec interdiction de traitement ultérieur) mais également, de prévoir explicitement dans le dispositif de la proposition de loi, d'une part, que le code d'autorisation (définition à insérer à l'article 3 de la proposition de loi) est un code généré aléatoirement et non lié à aucune donnée d'identification de l'utilisateur ou de son terminal et d'autre part, que le numéro de téléphone de l'utilisateur est effacé par Sciensano directement après son envoi du sms à l'utilisateur contaminé. Sur ce dernier point, si l'intention de l'auteur de la proposition de loi est de prévoir l'effacement immédiat par Sciensano du numéro de téléphone et de l'information selon laquelle le titulaire de ce numéro de téléphone est contaminé à l'article 9, §1, al. 3, il convient

[8] Selon notre compréhension, il semble plus adéquat de viser l'information selon laquelle l'utilisateur disposant de telle clef privée est contaminé par le COVID-19

[9] Sous réserve de ce qui est écrit plus haut quant à la requête de l'Autorité de s'assurer

d'améliorer la clarté de la rédaction de cette dernière disposition (et de prévoir les garanties additionnelles recommandées ci-avant).

48. L'article 7,§ 3 de la proposition de loi détermine le moment auquel il est demandé à l'utilisateur d'insérer son numéro de téléphone dans l'application de traçage à savoir, le moment où il se trouve chez le prestataire de soins de santé pour le prélèvement en vue du test PCR effectué pour vérifier s'il est contaminé ou non. A ce sujet, l'Autorité s'interroge sur le choix de ce moment qui lui semble prématuré étant donné que, vu la finalité d'utilisation de ce numéro de téléphone, il apparait indiqué de proposer cela à l'utilisateur uniquement au moment où on lui apprend le résultat positif de son test. A défaut de justification, l'auteur de la proposition de loi modifiera la détermination de ce moment en ce sens.

j. Centralisation de données par Sciensano

49. L'article 8 de la proposition de loi détermine la liste des données qui seront conservées de matière centralisée par Sciensano, à la fois pour la finalité de gestion du système des applications numériques de traçage et à la fois pour la finalité de recherche.

50. L'Autorité n'a pas de remarque à faire sur la liste des données centralisées pour la 1ère finalité mis à part que cette liste doit être limitative. Il convient donc de préciser que seules ces informations sont centralisées.

51. Quant à la liste des données visées à l'article 8, §2, l'Autorité renvoie à sa remarque ci-dessus concernant la finalité de recherche. L'objet principal de la proposition de loi étant d'encadrer un système faisant appel à des applications de traçage de manière telle qu'elles répondent, entre autres choses, au principe de minimisation des données, il n'apparait pas pertinent de prévoir une collecte de données supplémentaires pour la réalisation de la finalité de recherche, qui ne sont pas nécessaires pour la finalité de traçage (nombre de rencontres que l'utilisateur a eu avec une personne infectée et pour chacune des rencontres le nombre de jours depuis la date de la contamination COVID). De plus, l'Autorité ne peut apprécier le caractère proportionné de ces données en l'absence d'explication dans l'exposé des motifs et de justification quant au caractère nécessaire de ces données pour mener les recherches envisagées, de même que la nécessité de les collecter de cette manière par rapport aux autres méthodes de collecte actuellement en place pour la réalisation de la recherche épidémiologique qui a déjà lieu.

k. Durée de conservation des données dans les équipements terminaux et dans le fichier log centralisé et désactivation des applications numériques de traçage

52. L'article 9 de la proposition de loi fixe la durée de conservation des données collectées[10] tant au niveau des terminaux des utilisateurs qu'au niveau du fichier centralisé de Sciensano à un maximum de 3 semaines ce qui, au vu des explications reprises dans l'exposé des motifs, apparait pertinent et nécessaire pour la réalisation de la finalité poursuivie.

53. L'article 9 §3 détermine que les applications de traçage seront **désactivées** dès qu'un arrêté royal proclamant la fin de l'état d'épidémie du coronavirus COVID-19 aura été publié au Moniteur belge. Etant donné qu'il est possible que les applications de traçage ne s'avèrent plus nécessaires avant ce moment, l'Autorité considère qu'il convient de préciser dans la proposition de loi que la désactivation du système devrait être prévue à un terme fixe (à reprendre dans la proposition de loi), avec la possibilité pour le ministre compétent de le prolonger moyennant justification.

l. Traitement ultérieur à finalité de recherche

54. L'article 10 de la proposition de loi prévoit, à titre de garantie pour les droits et libertés des utilisateurs, une interdiction de traitement ultérieur des données collectées à l'exception des traitements pour finalités de recherche et de réalisation de statistiques.

55. L'autorité relève que l'alinéa 2 de l'article 10 doit se référer à l'entièreté de l'article 89 et non seulement à ses paragraphes 2 et 3 étant donné que le paragraphe 1er impose le respect du principe de minimisation des données dans le cadre de la réalisation de la recherche et l'utilisation de données ne permettant pas ou plus l'identification des personnes concernées dès que cela suffit pour la finalité de recherche. D'ailleurs, au vu de l'article 4 de la proposition de loi, il semble indiqué de simplement préciser que ces traitements ultérieurs seront réalisés sur base de données anonymisées.

m. Gestion des accès et des utilisateurs

56. L'article 11 de la proposition de loi prévoit un système de gestion des accès et utilisateurs à la liste log et à la banque de données qu'il est envisagé de constituer pour la finalité de recherche épidémiologique.

57. L'autorité s'interroge sur l'utilité de cet article étant donné que d'une part, selon l'article 4, la recherche épidémiologique sera réalisée sur base de données anonymisées et d'autre part, la gestion du fichier log sera, selon la compréhension de l'Autorité, centralisée auprès de Sciensano et nécessitera

[10] Concernant la liste des données visées, il est renvoyé aux remarques précédentes de l'Autorité sur le principe de minimisation des données. Cette disposition sera adaptée en conséquence sur ce point.

uniquement des accès par les utilisateurs de l'application qui par nature, ne peuvent pas être ré-identifiés.

58. Si l'intention de l'auteur de la proposition de loi est de conférer à d'autres personnes que les utilisateurs des applications de traçage des accès à ces bases de données, il est impératif de déterminer dans le dispositif de la loi ces destinataires ainsi que les circonstances et raisons pour lesquelles il doivent y avoir accès en justifiant le caractère légitime et proportionné de ces accès. Sans précision à ce sujet dans l'exposé des motifs, l'Autorité ne peut apprécier le caractère légitime et proportionné de tels accès et s'interroge fortement à ce sujet étant donné que sur base de l'exposé des motifs de tels accès n'apparaissent ni légitimes ni nécessaires pour la réalisation de la finalité du système des applications de traçage.

59. Par ailleurs, il n'est pas précisé dans la proposition de loi que les utilisateurs des applications auront accès au fichier log afin que leur application puisse prendre connaissance de la clef privée des utilisateurs contaminés afin d'en générer le numéro de série temporaire et de vérifier si ce numéro figure dans leurs propres contacts se trouvant sur leur appareil terminal (ce qui générera un message d'avertissement à leur attention du fait qu'il ont eu un contact à risque avec une personne infectée). Par souci de prévisibilité et de clarté, cela doit être précisé dans la proposition de loi.

n. <u>Choix du message qui sera envoyé par le gouvernement dans le message d'alerte aux utilisateurs ayant eu un contact à risque avec une personne infectée</u>

60. L'objet de la proposition de loi ne consiste pas à déterminer le type de message qui sera communiqué aux utilisateurs qui auront eu un contact à risque avec une personne contaminée. Ceci étant, il est renvoyé à ce sujet au considérant 30 de l'avis 34/2020. Il importe que le libre arbitre des utilisateurs des applications de traçage puisse être préservé.

PAR CES MOTIFS,

L'Autorité estime, que si la nécessité de la mise à disposition d'applications de traçage pour la gestion du déconfinement est démontrée, les conditions pour assurer le caractère conforme au RGPD de leur utilisation doivent encore être mises en place et l'Autorité estime à cet effet que la proposition de loi doit être adaptée conformément aux remarques soulevées dans le présent avis, à savoir :

1. Explication des composantes essentielles du protocole DP3T, des garanties qu'il offre, des risques subsistant et des raisons pour lesquelles il faut conclure au caractère néanmoins proportionné des traitements de données qui seraient effectués;
2. Explication du fonctionnement du système de traçage afin notamment de garantir que les risques mitigés par le protocole DP3T ne sont pas ré-introduits par des applications et/ou un système permettant une ré-identification ;
3. Précision à l'article 6 des catégories de traitements de données à propos desquels la désignation du responsable du traitement est faite et attribution d'une mission de vérification du caractère conforme aux spécifications légales des applications mises à disposition du public;
4. Mise en place d'une obligation de soumission de la ou des AIPD qui devront être réalisées à l'Autorité et adoption de mesures de publicité de ces AIPD et des avis de l'APD sur ces AIPD;
5. Mise en place de mesures de publicité pour l'entièreté du code source de la ou des applications choisies, et ce, suffisamment à l'avance ;
6. Reformulation de la finalité pour laquelle le système d'application de traçage est mis en place;
7. Suppression de la finalité de recherche comme finalité du système de traçage et adaptation en conséquence de la proposition de loi;
8. Amélioration de la lisibilité de la proposition de loi et de la prévisibilité des traitements qui découleront de l'utilisation des applications de traçage en y ajoutant les définitions des concepts importants tels que celui d'application de traçage, d'utilisateur, de contact à risque, de code d'autorisation, de clef sécurisée, de numéro de série temporaire non personnalisés, de ministre compétent,…;
9. Respect du principe de minimisation des données dans la détermination des données qui seront collectées et traitées dans le cadre du système de traçage mis en place et ce au niveau de plusieurs articles de la proposition
10. Ajout, parmi les fonctionnalités techniques imposées aux applications de traçage, que la désactivation puisse être réalisée par le ministre compétent et attribution au Roi la tâche de déterminer les spécifications techniques auxquelles les applications devront satisfaire;
11. Imposition de sanctions pour toute personne qui lierait l'utilisation des applications de traçage à l'accès à un bien ou un service (cons. 31);

12. Clarification que la conservation des données visée à l'article 7 concerne la conservation des données dans l'équipement terminal de l'utilisateur (cons. 34) ;
13. Adoption des garanties spécifiques pour limiter le risque de ré-identification sur base du numéro de téléphone de l'utilisateur infecté (cons. 39) ;
14. Détermination du moment auquel il est demandé à l'utilisateur de communiquer son numéro de téléphone conformément au principe de proportionnalité (cons. 40) ;
15. Précision que la liste des données centralisées par Sciensano pour la finalité de gestion du système de traçage est une liste limitative (cons. 42) ;
16. Ajout à l'article 9, §3 que les applications de traçage seront désactivées dès que le ministre compétent aura constaté leur caractère non nécessaire pour la gestion du déconfinement (cons. 45) ;
17. Précision à l'article 10 que les traitements ultérieurs à des fins de recherche des données collectées par Sciensano dans le cadre de la gestion des applications de traçage se feront sur base de données anonymisées (cons. 47) ;
18. Rectification de l'article 11 traitant de la gestion des accès et utilisateur conformément aux considérants 48 à 50 et suppression de toute disposition de laquelle on peut déduire un échange de données non nécessaire pour la gestion des applications de traçage ;
19. Précision des accès auxquels les utilisateurs des applications de traçage disposeront (cons. 51)

L'Autorité recommande également

1. Que l'analyse de nécessité de la décision d'utiliser ce type d'application soit dûment documentée et intégrée dans l'AIPD qui devra être faite ;
2. Qu'une attention particulière soit accordée à la façon dont l'information des personnes concernées sera réalisée quant au fonctionnement des applications de traçage et aux échange de données qu'elles génèreront ;
3. Que le libre arbitre des utilisateurs des applications de traçage soit préservé (cons. 52).

(sé) Alexandra Jaspar

Directrice du Centre de Connaissances

[i] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020.