e-legal

Revue de droit et de criminologie
de l'Université libre de Bruxelles

La vie privée à l'épreuve de la pandémie de Covid-19 : comparaison des approches d'Etats européens dans la mise en place d'applications numériques

Par Clément Legrand

e-legal, Spécial COVID19

Pour citer l'article :
Clément Legrand, « La vie privée à l'épreuve de la pandémie de Covid-19 : comparaison des approches d'Etats européens dans la mise en place d'applications numériques », *in e-legal, Revue de droit et de criminologie de l'ULB*, Spécial COVID19, octobre 2020.

Adresse de l'article :
http://e-legal.ulb.be/special-covid19/dossier-special-covid19/la-vie-privee-a-l-epreuve-de-la-pandemie-de-covid-19-comparaison-des-approches-d-etats-europeens-dans-la-mise-en-place-d-applications-numeriques

§1. Lorsque l'épidémie du virus SRAS-COV-2 (« Covid-19 ») s'est étendue au territoire de l'Union européenne, les différents Etats membres ont été contraints d'établir des mesures de prévention pour ralentir et limiter au maximum la propagation du virus dans la population. Parmi ces mesures, certaines impliquent des restrictions importantes aux droits et libertés fondamentales de la population, telles que la liberté de circulation ou la protection de la vie privée. Au cours de cette crise, la collecte et le traitement d'informations relatives, notamment, aux individus qui ont été contaminés par le virus[1] ainsi qu'aux personnes ayant été en contact avec une personne contaminée ont été présentés comme des outils indispensables dans la lutte contre la propagation du virus et la recherche scientifique[2].

§2. Afin d'assurer que ces traitements respectent le cadre juridique établi par l'Union européenne en matière de protection des données à caractère personnel (et plus particulièrement le Règlement Générale sur la Protection des Données (« RGPD »)[3]), les autorités de protection des données des Etats membres de l'Union européenne ont rapidement été confrontées à la nécessité de publier des avis, des lignes directrices et des recommandations visant à permettre une lutte efficace contre le virus dans le respect de la vie privée des individus. Ces avis portaient, dans un premier temps, principalement sur les mesures que pouvaient prendre les employeurs pour limiter la propagation du virus sur le lieu de travail.

§3. Les autorités de protection des données ont également été consultées, parfois en extrême urgence, dans le cadre de la mise en œuvre de différentes solutions de traçage, que ce traçage soit manuel ou intervienne via une application de « suivi de contact » à installer sur smartphone. A l'heure où l'Europe se prépare à faire face à une « deuxième vague » d'infections au coronavirus, la mise en place de ce type d'outil attire l'attention de la presse et la question de la protection de la vie privée occupe une place majeure dans le débat public.

§4. Un véritable dialogue s'est instauré entre les autorités des protections des données et les gouvernements en charge de gérer la crise. En témoignent les nombreux avis rendus par l'autorité de protection des données belge (« APD ») et les délibérations rendues par l'autorité de protection française (la Commission Nationale de l'Informatique et des Libertés, aussi appelée la « CNIL ») ainsi que les premiers contrôles que cette dernière a effectués à propos de l'application déployée en France[4].

§5. Dans cet article, nous procéderons à la présentation des modes de raisonnement des autorités de protection des données dans leur analyse des différents protocoles intégrés dans les applications de traçage de contacts au sein de l'Union européenne. Nous verrons ensuite quels sont les points d'attention

soulevés par le Comité Européen de la Protection des Données (« CEPD ») concernant les applications de traçage, et verrons les analyses des autorités de protection de données concernant un projet d'application de traçage « centralisé » (analyse par la CNIL de l'application française) et un projet d'application de traçage « décentralisé » (analyse par l'APD de l'application belge). Enfin, nous nous attarderons sur le rôle de la Cour de Justice de l'Union européenne dans la protection de la vie privée, et sur la question de savoir comment cette dernière pourrait appliquer sa jurisprudence récente à ce type d'applications.

Les autorités de protection des données et le traçage de contacts

L'approche des autorités de protection des données

§6. Pour quiconque n'est pas habitué à la méthode d'analyse établie par le RGPD, il est important de rappeler que le RGPD est un règlement dont une partie des dispositions repose sur une évaluation du risque (« *risk-based* »)[5]. Cela signifie que, pour ces dispositions, les obligations applicables à un traitement de données personnelles varieront en fonction du risque posé par le traitement en question[6]. Ces risques dépendront des circonstances spécifiques de chaque traitement et, notamment, des catégories de données collectées, des finalités envisagées, de l'éventuelle position de faiblesse des personnes concernées (tels que des mineurs), des destinataires de ces données ou de la manière dont le traitement est envisagé. Dès lors, deux traitements de données personnelles basés sur des données similaires et avec des finalités similaires (voire identiques) peuvent poser des risques différents et entraîner des obligations différentes pour les responsables du traitement, ces obligations ayant pour objet de limiter les risques identifiés[7].

§7. Il n'est dès lors pas étonnant que les avis des autorités de protection des données n'indiquent pas nécessairement si une solution est, dans l'absolu, conforme ou non au RGPD mais qu'elles indiquent, au regard de toutes les circonstances pertinentes d'un traitement de données, quels sont les risques identifiés et les mesures requises pour les limiter ainsi que les aspects du traitement de données qui peuvent être justifiés au regard, par exemple, des données collectées et des finalités poursuivies.

§8. Par ailleurs, comme les autorités l'ont elles-mêmes rappelé[8], il faut chasser l'idée selon laquelle le RGPD constitue un obstacle à la mise en place d'une solution technologique. Comme indiqué dans son quinzième considérant, le RGDP est neutre sur le plan technologique : il ne vise pas à s'appliquer à (ou à interdire) un type de technologie en particulier. Le CEPD l'indique : « Le cadre juridique en matière de protection des données a été conçu de façon à être souple et, 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 »[9]. Selon les autorités de protection des données, le RGPD peut d'ailleurs renforcer la confiance des personnes concernées dans ce type de solutions et accroître l'adhésion de la population[10].

§9. Toutefois, les autorités préviennent que les applications de traçage ne peuvent être l'unique outil dans la lutte contre le virus. Comme le rappel, entre autres, le CEPD, « 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 » et précise que « sans cela, ces applications pourraient ne pas produire leur plein effet »[11]. Lors de son audition devant le parlement français[12], la présidente de la CNIL appelait à la vigilance contre la tentation du « solutionnisme technologique ». Si ces déclarations peuvent, à première vue, sembler sortir du cadre de la mission de protection de la vie privée, nous verrons ci-dessous que le RGPD requiert que tout traitement de données personnelles soit approprié (et, par extension, efficace) au vu des finalités pour lesquelles les données ont été collectées. Dès lors, une application de traçage de contacts pourrait fonctionner parfaitement et pourtant être dénuée d'efficacité si, par exemple, il n'est pas possible que les individus identifiés comme ayant été en contact avec une personne contaminée par les applications de traçage puissent eux-mêmes être dépistés.

(Dé)centralisation : les différents protocoles intégrés dans les applications de traçage

§10. Au début du mois d'avril 2020, les institutions européennes se sont prononcées en faveur de la mise en place d'une approche commune dans le développement de solutions technologiques et d'applications mobiles afin de lutter contre la propagation du virus[13]. La Commission européenne a notamment insisté sur la nécessité pour les Etats membres d'assurer l'interopérabilité de ces applications et ce, afin de rompre les chaînes de transmission transfrontalières[14]. Dans sa recommandation, la Commission européenne envisage tant l'usage d'applications d'alerte et de traçage de contacts que l'usage d'applications qui pourraient être considérées comme des dispositifs médicaux (dont la finalité serait le diagnostic, la prévention, le contrôle, la prédiction, le pronostic, le traitement ou l'atténuation d'une maladie). C'est pourtant principalement vers le développement de solutions de traçage que la réflexion des Etats membres s'est portée[15].

§11. La plupart des applications qui sont en cours de développement ou qui sont déjà disponibles dans certains Etats membres peuvent être distinguées en deux grandes catégories, qu'en tant que juristes, nous pourrions être tentés de qualifier de *summa divisio*, à savoir, les applications intégrant un protocole « centralisé », d'une part, et les applications intégrant un protocole « décentralisé », de l'autre. Le CEPD a indiqué que ces deux approches sont « des options viables » même s'il estime que l'approche décentralisée répond en général mieux au principe de minimisation (que nous analyserons plus bas)[16]. Pour la bonne compréhension de la présente contribution il est utile d'en décrire brièvement leurs fonctionnements (simplifiés).

§12. Le protocole décentralisé le plus utilisé en Europe est le *Decentralized Privacy-*

Preserving Proximity Tracing (aussi appelé « DP-3T »)[17]. Une application intégrant ce protocole open source utilisera la technologie Bluetooth du smartphone de l'utilisateur pour détecter les smartphones des autres utilisateurs dans un rayon défini. Lorsqu'un smartphone détectera qu'un autre smartphone utilisant la même application entre dans ce rayon défini, les deux téléphones communiqueront entre eux des informations sur l'intensité et la durée de la rencontre présumée entre leurs deux propriétaires, ainsi qu'un ou plusieurs code(s) d'identification temporaire(s) généré(s) par l'application et stocké(s) directement sur les smartphones. Ainsi, l'application génère régulièrement des codes d'identification temporaires pour ses propriétaires, mais elle retient également, pendant une certaine durée, les codes d'identification temporaires générés par les autres applications avec lesquelles l'application a communiqué (pouvant dès lors indiquer un contact entre les deux propriétaires des smartphones sur lesquels ces applications sont installées). Si un utilisateur de ce type d'application est diagnostiqué positif au coronavirus Covid-19, cet utilisateur recevra un code unique lui permettant d'indiquer son diagnostic dans son application. L'application communiquera alors tous les codes d'identification temporaires se rapportant à la personne contaminée au serveur central. Le serveur central identifiera ces codes temporaires comme se rapportant à une personne contaminée par le virus (sans connaître l'identité de la personne, puisque les identifiants temporaires sont générés de manière décentralisée par l'application), afin que les applications de tous les autres utilisateurs puissent vérifier si elles ont également stocké un de ces identifiants dans la mémoire de leur smartphone, ce qui indiquerait qu'ils ont eu un contact avec une personne dont le diagnostic a été confirmé. L'utilisateur non-affecté est ainsi prévenu qu'il a probablement été en contact avec une personne contaminée, afin qu'il puisse prendre les mesures adéquates. L'Etat belge a opté pour ce type de protocole pour son application « Coronalert », de même que l'Allemagne, l'Autriche et l'Estonie. C'est également une approche similaire qui a été développée par Google et Apple pour faire face au coronavirus Covid-19[18].

§13. En ce qui concerne l'approche centralisée, les principales alternatives (également open source) au protocole DP3T sont le *Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT/PEPP)*[19] et le *ROBust and privacy-presERving proximity Tracing* (*ROBERT*)[20], ce dernier étant utilisé pour l'application « StopCovid » en France. L'application « Tous Anti-Covid » (qui remplace l'application StopCovid sans en changer le protocole) fonctionne également par le biais de la technologie Bluetooth des smartphones, afin de détecter les autres smartphones utilisant l'application dans un certain rayon. Cette fois, au lieu de générer des identifiants de manière décentralisée, c'est le serveur central qui attribue un identifiant aléatoire permanent, permettant ensuite de créer plusieurs identifiants aléatoires temporaires pour chaque application. Si un utilisateur confirme qu'il a été diagnostiqué positif au virus, il l'indiquera dans l'application par le biais d'un code unique. Son application importera l'ensemble des identifiants (stockés sur le smartphone) avec lesquelles l'utilisateur est

présumé avoir eu des contacts vers le serveur central. L'application enverra alors tous les « contacts » de la personne contaminée, mais pas l'identifiant de la personne contaminée elle-même. Outre la France, la Hongrie et l'Islande ont également développé une application ayant un protocole centralisé[21] (pour cette dernière, l'application utilise un mécanisme différent, basé sur les données de géolocalisation).

Analyse des applications de traçage de contacts par les autorités

§14. Quel que soit le type de protocole choisi pour les applications de traçage de contacts, le responsable du traitement[22] doit se conformer aux grands principes du RGPD[23], résumés en son article 5. Dès lors, la plupart des analyses de traitement de données à caractère personnel au regard du RGPD suivent en principe une structure similaire et posent les mêmes grandes questions (qui sont par la suite plus ou moins précisées, en fonction des dispositions applicables).

Ces principes sont les suivants :

1. le principe de licéité, loyauté, transparence, qui requiert que les données personnelles soient traitées de manière licite, loyale et transparente au regard de la personne concernée ;

2. le principe de limitation des finalités, qui requiert que les données soient collectées pour des finalités déterminées, explicites et légitimes ;

3. le principe de minimisation des données qui requiert que les données personnelles soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;

4. le principe d'exactitude qui requiert que les données personnelles soient exactes et, si nécessaire, tenues à jour ;

5. le principe de limitation de la conservation qui requiert que les données personnelles soient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; et

6. le principe d'intégrité et de confidentialité, qui requiert que les données personnelles soient traitées de façon à garantir leur sécurité appropriée, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Enfin, le dernier principe est le « principe de responsabilité », qui impose la responsabilité du respect des principes précités au responsable du traitement, ainsi que l'obligation d'être capable de démontrer ce respect.

Par souci de cohérence, nous allons analyser les positions des autorités de protection des données belge (APD) et française (CNIL), ainsi que celle du CEPD,

en suivant ce même ordre.

Le principe de licéité, de loyauté et de transparence

§15. Afin qu'un traitement de données personnelles (tel que la mise en place d'une application de traçage de contacts) soit considéré comme licite, il doit pouvoir être justifié par l'une des cinq « bases légales » prévues de manière exhaustive à l'article 6 du RGPD[24]. Ces bases légales définissent les circonstances dans lesquelles un responsable du traitement peut justifier le traitement de données à caractère personnel et ont une influence importante sur les droits des personnes concernées[25]. Par exemple, un traitement peut être justifié par le consentement de la personne concernée, mais également par la nécessité pour l'exécution d'un contrat auquel la personne concernée est partie ou pour le respect d'une obligation légale à laquelle le responsable du traitement est soumis. Par ailleurs, le RGPD considère les données relatives à la santé comme des « catégories particulières de données » dont le traitement est en principe interdit, à moins de remplir une des conditions de son article 9.2.

Cela signifie qu'en plus de répondre aux conditions de l'article 6 du RGPD, le responsable du traitement doit s'assurer que le traitement répondra également aux conditions de l'article 9.2 du RGPD, qui prévoit des exigences additionnelles quant aux circonstances permettant de justifier un traitement de données relatives à la santé.

§16. En combinant les exigences de l'article 6 et de l'article 9 du RGPD, il apparaît que les Etats membres qui souhaitent mettre en place des applications de traçage disposent de deux solutions : soit obtenir le consentement explicite des personnes concernées[26] ; soit adopter une loi permettant le traitement de données pour des motifs d'intérêt public dans le domaine de la santé publique, pour autant que cette loi prévoie des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés des personnes concernées[27].

§17. Selon le CEPD, la base juridique la plus pertinente pour le traitement envisagé dans le cadre d'applications de traçage est la nécessité à l'exécution d'une mission d'intérêt public[28].

§18. Par ailleurs, comme le rappelle l'APD dans ses avis[29], l'exécution de ce type de traitement, bien que rentrant dans le cadre d'une mission d'intérêt public, constitue un ingérence au droit à la vie privée et ne peut être admise, conformément à l'article 6.3 du RGDP et à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, que si elle est « nécessaire et proportionnée à l'objectif (ou aux objectifs) qu'elle poursuit et qu'elle est encadrée par une norme suffisamment claire et précise dont

l'application est prévisible pour les personnes concernées ». L'évaluation de la nécessité du traitement impose à la fois de démontrer, sur la base d'éléments factuels et objectifs, (i) l'efficacité du traitement de données ainsi que (ii) le fait que le traitement constitue la mesure la moins intrusive au regard de l'objectif poursuivi.

§19. Partant de ce constat, le CEPD, la CNIL et l'APD s'accordent sur une série de mesures qu'ils recommandent d'intégrer dans la norme permettant d'assurer la proportionnalité des traitements effectués par les applications de traçage de contacts.

- La première mesure est de prévoir que l'utilisation de l'application doit se faire sur une base strictement volontaire[30]. Ce volontariat doit être établi à chaque étape de l'utilisation de l'application : l'installation, l'activation du Bluetooth, la notification des résultats d'un examen de dépistage au coronavirus Covid-19 ou la désinstallation de l'application. Les Etats ne peuvent rendre l'installation de l'application obligatoire pour accéder à des droits et services (tels que les transports en commun ou une sortie du confinement)[31], l'utilisation de l'application ne peut être sujette à aucune sanction pénale ou civile ni à aucun acte discriminatoire. L'APD suggère même de prévoir la possibilité d'imposer des sanctions pénales ou administratives à toute personne qui lierait l'accès à un bien ou à un service à l'utilisation d'une application de traçage[32]. Il convient de noter que la base volontaire de l'utilisation de l'application n'implique pas que le traitement de données qui en résulte soit basé sur le consentement de la personne concernée[33]. Cela peut s'expliquer par les conditions strictes qui entourent l'obtention d'un consentement valide au regard du RGPD[34]. Un des exemples les plus parlants de cette distinction entre un consentement valide au sens du RGPD et un consentement au sens général du terme est le traitement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie. En effet, bien que d'un point de vue contractuel, la personne concernée a donné son consentement au contrat et aux traitements de données personnelles qui en résultent, ces traitements seront justifiés au regard du RGPD par la nécessité contractuelle (article 6.1b du RGPD) et non par le consentement (article 6.1a du RGPD), car le consentement ne serait pas considéré comme entièrement libre, étant obligatoire pour obtenir une contrepartie contractuelle[35].

- Ensuite, comme nous l'avons déjà mentionné plus haut, les applications ne peuvent pas purement remplacer la recherche manuelle de contacts effectuée par du personnel de santé publique qualifié[36]. Elles doivent s'inscrire dans une approche globale afin d'en assurer l'efficacité[37].

- En ce qui concerne l'efficacité des applications de traçage mêmes, les autorités prennent note des justifications avancées par les Etats[38], mais elles encouragent les Etats à régulièrement réévaluer la mise en place de ces applications pour

vérifier, sur la base d'éléments suffisants, que l'application est utile à la gestion de la crise et que l'ingérence reste nécessaire au regard des circonstances[39]. La CNIL insiste notamment sur la nécessité d'efficacité des applications, même si une partie de la population pourrait ne pas disposer de téléphones adaptés à l'installation de l'application, en particulier les personnes les plus vulnérables ainsi que les plus jeunes (qui pourraient jouer un rôle sensible dans la propagation du virus). De plus, une partie des personnes contaminées par le virus sont asymptomatiques et pourraient ne pas communiquer leurs contaminations à l'application[40].

- Toujours dans un souci d'efficacité, les autorités recommandent l'utilisation d'une seule application et d'éviter la concurrence entre plusieurs applications[41]. La CNIL insiste sur le fait que cette application devrait être disponible pour le public le plus large possible, ce qui implique qu'elle soit largement compatible avec les différents types d'appareils et offerte sur les différentes plateformes de distribution des applications. Le CEPD recommande d'identifier clairement l'application nationale officielle de traçage de contacts pour réduire le risque d'utilisation d'une application tierce[42].

§20. En ce qui concerne la question de la transparence du traitement des données, tant le CEPD que l'APD et la CNIL plaident pour la publication du code source de l'application, afin de permettre aux experts indépendants d'en vérifier les algorithmes (ainsi que le code du serveur central et leurs paramétrages)[43].

§21. De plus, l'APD et la CNIL rappellent que le principe de transparence requiert qu'une information conforme aux articles 13 et 14 du RGPD soit fournie de manière claire et accessible. La publication de cette information sur un site internet n'est pas suffisante, les personnes concernées devant également recevoir une information (« simple et courte ») à propos de leurs droits et des éléments principaux du traitement lors de l'installation de l'application[44]. Enfin, la CNIL insiste pour que les modalités de mise à disposition de cette information permettent aux personnes en situation de handicap d'en prendre connaissance aisément et que l'information puisse être compréhensible par les mineurs d'âge.

§22. Si les mesures précitées sont partagées par la CNIL et l'APD concernant la mise en place des applications, certaines mesures sont spécifiquement requises par la CNIL pour couvrir les risques liées au protocole « centralisé » ROBERT et par l'APD, pour couvrir les risques liés au protocole « décentralisé » DP3T.

§23. Dans le cas d'une application de traçage de contacts intégrant un modèle centralisé, le CEPD avait déjà précisé que les données stockées sur le serveur central devraient être limitées au strict minimum, et que la communication des pseudonymes des personnes avec qui la personne contaminée avait été en contact

ne pouvait s'accompagner de la communication du pseudonyme de la personne contaminée elle-même[45]. Pour la CNIL, la centralisation des pseudonymes des personnes ayant été en contact avec une personne contaminée, sans préciser le lien entre la personne contaminée et ses contacts, s'avère être un choix protecteur de la vie privée[46]. Il nous semble que, si ce choix permet en effet de ne pas centraliser des informations relatives à la santé des personnes contaminées, la ré-identification de la personne concernée pourrait permettre d'inférer bien plus d'informations la concernant (outre le fait qu'elle est contaminée) que dans le modèle décentralisé où l'information stockée sur le serveur central se limite aux pseudonymes temporaires des personnes contaminées. Le CEPD prévient d'ailleurs qu'un modèle centralisé ne peut permettre « l'inférence de schémas de contacts qui ne sont pas nécessaires pour déterminer les contacts pertinents »[47].

§24. La CNIL estime également que le chiffrement de la base centrale et la répartition de fragments des clefs de chiffrement entre plusieurs entités (de préférence de natures différentes et présentant un haut niveau d'indépendance) devrait limiter le risque de ré-identification et de détournement de la base de données centrale[48].

§25. Dans le cas d'une application de traçage de contacts intégrant un modèle décentralisé, l'APD note quant à elle que le protocole DP3T permet de minimiser les données collectées et de ne pas partager le graphe social. Toutefois, elle signale une réintroduction « des risques de ré-identification en principe annihilés par le protocole DP3T »[49]. En effet, pour qu'un utilisateur puisse confirmer sa contamination dans l'application, il devait communiquer son numéro de téléphone et la date du test qu'il a passé. L'utilisateur reçoit ensuite un code d'autorisation à indiquer dans l'application pour communiquer ses pseudonymes temporaires au serveur central. Au vu du risque de ré-identification, l'APD recommande dès lors que l'opérateur en charge de communiquer le code d'autorisation soit un opérateur différent de celui qui gère le serveur central contenant les pseudonymes des personnes contaminées et que les données soient effacées dès que le code d'autorisation aura été vérifié. L'APD recommande également que le code d'autorisation soit généré aléatoirement et qu'il ne soit pas lié à un élément d'identification de la personne concernée[50]. Dans ce contexte, elle recommande enfin que le système fonctionne avec plusieurs pseudonymes temporaires et une période de rafraîchissement telle que l'opérateur du serveur central ne pourrait déterminer que les pseudonymes appartiennent à la même personne contaminée[51]. Dans son Avis du 7 Septembre 2020, l'APD[52] note que la création d'une base de données spécifique qui stockerait « très temporairement » le résultat du test et le numéro que l'application de l'utilisateur a attribué à ce test (et qui a été communiqué au responsable du traitement en charge du suivi), à la place du mécanisme utilisant le numéro de téléphone, vise à limiter ce risque de ré-identification. Ce risque est en effet désormais limité dans le temps et est également limité par le fait que cette information est stockée dans une base de

données séparée de la base de données principale, qui comprend beaucoup plus de données personnelles. L'APD invite toutefois le responsable du traitement à justifier de la nécessité de recourir à ce mécanisme dans le cadre d'une analyse d'impact relative à la protection des données[53].

Le principe de limitation des finalités

§26. En ce qui concerne le principe de limitation des finalités, il n'est pas étonnant de constater que le CEPD, l'APD et la CNIL se rejoignent parfaitement sur le principe selon lequel les finalités de traitement des applications de traçage doivent être décrits de manière claire et précise et avec suffisamment de précision pour interdire tout traitement des données qui ne s'inscrirait pas dans la gestion de la crise de la Covid-19[54]. Il doit par exemple être clair que la finalité d'une application de traçage ne peut être de surveiller le respect des mesures de confinement ou de prendre des mesures répressives. La CNIL note également que les applications n'ont pas pour objet d'organiser une prise de contact avec les personnes alertées, ni d'établir le nombre de personnes infectées ou leur localisation[55]. L'APD recommande, quant à elle, de ne pas inclure une finalité de « recherche épidémiologique » par rapport à l'application de traçage, pour éviter la confusion dans le chef des utilisateurs de l'application (cette finalité étant prévue par ailleurs dans le cadre des dispositions sur le traçage « manuel »)[56].

Le principe de minimisation des données

§27. Conformément au principe de minimisation, le responsable du traitement ne peut collecter plus d'informations que ce qui est nécessaire aux finalités du traitement.

Les applications ne peuvent dès lors pas collecter des informations qui ne sont pas pertinentes (par exemple, l'état civil, les identifiants de communication, les messages, l'historique des appels, etc.)[57]. Il est également crucial que les applications ne collectent pas d'information permettant de relier un pseudonyme à l'appareil sur lequel l'application est utilisée (telle que l'adresse MAC du téléphone)[58].

§28. Dans ce cadre, le CEPD, la CNIL et l'APD[59] s'accordent sur le fait que le traçage de contacts ne nécessite pas la collecte des données de localisation (qui sont d'ailleurs également soumises aux règles de la Directive 2002/58). Les applications pouvant fonctionner avec des données pseudonymisées, il convient de mettre en place les mesures adéquates pour empêcher une ré-identification des personnes concernées et s'assurer que les données sont bien stockées uniquement sur l'appareil de l'utilisateur, sauf en cas « d'absolue nécessité »[60].

§29. La CNIL et l'APD soulignent également le fait que les applications devraient être conçues de manière à pouvoir évaluer la distance entre les individus pour que seuls les contacts à haut risque d'engendrer une contamination donnent lieu à une alerte[61].

§30. La CNIL suggère également de permettre à l'utilisateur de définir des périodes de temps pendant lesquelles l'application ne devrait pas considérer les contacts comme étant à risque. Cela permettrait, selon la CNIL, de limiter le nombre de fausses alertes (et dès lors, le traitement des données par le serveur central) en prenant en compte le contexte des rencontres[62]. La CNIL donne l'exemple d'un professionnel de la santé qui recevrait indubitablement des patients atteints par la Covid-19 mais qui serait protégé par le matériel médical adéquat.

§31. La CNIL indique enfin que l'approche centralisée de l'application StopCovid et le fait que seuls les pseudonymes générés par les applications associées aux personnes avec lesquelles un individu infecté a été en contact soient communiqués au serveur central s'inscrivent dans le plein respect des principes de protection des données personnelles[63].

Le principe d'exactitude

§32. Le CEPD note qu'il existe un risque de faux positif dans le cadre du dépistage du virus. A ce titre, et considérant les conséquences d'une « fausse alerte » pour les personnes alertées, le CEPD insiste sur la nécessité de prévoir la possibilité de corriger les données communiquées dans la mesure où ce serait techniquement possible[64].

Le principe de limitation de la conservation

§33. Sur le point de la limitation de conservation des données collectées, le CEPD, l'APD et la CNIL[65] sont d'accord sur le principe que les données ne peuvent être conservées que pour la durée nécessaire à la réalisation de la finalité du traitement, en tenant compte des besoins réels et de la pertinence de ces données d'un point de vue médical. En tout état de cause, les données à caractère personnel ne peuvent être conservées que pour la durée de la crise de la Covid-19. Après cela, les données devront être supprimées ou anonymisées[66]. L'APD note en outre qu'il convient de pouvoir justifier la durée de conservation des données (il s'agissait en l'occurrence de choisir entre une conservation de 14 jours ou de 3 semaines) et cite l'exemple de la durée de contagiosité des individus affectés[67].

Le principe d'intégrité et de confidentialité

§34. Outre les mesures de pseudonymisation et les mesures prises pour protéger

les clefs de chiffrement décrites ci-dessus, le CEPD, la CNIL et l'APD requièrent la mise en place de « techniques cryptographiques de pointe » afin d'apporter une sécurité suffisante aux données stockées sur le serveur central, ainsi que sur les appareils des personnes concernées. Cette cryptographie devra également protéger les échanges entre les applications et le serveur central[68]. Une authentification mutuelle entre l'application et le serveur doit également être exécutée[69].

La Cour de Justice de l'Union européenne

§35. Les sections précédentes ont mis en lumière les dialogues qui se sont établis entre la Commission européenne, le Parlement européen, les Etats membres et les autorités de protection des données. Les solutions et la législation développées dans le cadre de la gestion de la crise de la Covid-19 devront également prendre en compte le rôle important qu'exerce la Cour de Justice de l'Union européenne dans la définition de la protection de la vie privée et des données personnelles.

§36. En effet, dans sa jurisprudence récente, la Cour de Justice n'a pas hésité à prendre des décisions quelque peu spectaculaires et ayant un impact considérable sur la protection de la vie privée. Dans un arrêt récent[70], la Cour de Justice a ainsi invalidé un mécanisme permettant aux sociétés établies en Europe de communiquer des données personnelles vers les sociétés établies aux États-Unis participant à ce mécanisme (appelé le « bouclier de protection des données UE-États-Unis »). Ce mécanisme en remplaçait un autre, déjà invalidé par la Cour en 2015[71]. Pour les sociétés qui justifiaient leur traitement sur la base de ce mécanisme, cela signifie en pratique qu'elles auraient dû cesser tout transfert de données personnelles vers les Etats-Unis jusqu'à mettre en œuvre un mécanisme de transfert différent (comme ceux prévus aux articles 46 et suivants du RGPD).

§37. En 2014, la Cour a rendu le célèbre arrêt *Digital Rights Ireland*[72] qui a invalidé la Directive 2006/24[73]. Cette directive imposait une rétention, pour une durée de six mois à deux ans, de certaines données concernant les communications électroniques ou téléphoniques (par exemple leur dates, heures, durée, mais à l'exclusion du contenu de ces communications). La directive justifiait ces règles par la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme. La Cour a considéré que l'obligation générale de rétention de ces informations sans différenciation, limitation ou exception, portait une atteinte disproportionnée au droit à la vie privée et à la protection des données, prévus par les articles 7 et 8 de la Charte des droit fondamentaux de l'Union européenne.

§38. Bien que la mise en place d'application de traçage s'inscrive dans un contexte différent, l'arrêt *Digital Rights Ireland* peut servir d'avertissement aux Etats qui souhaiteraient s'affranchir du cadre légal de la protection de la vie privée et des données personnelles ou qui n'instaureraient pas les garanties appropriées, telles que celles détaillées dans les sections précédentes.

Conclusion

§39. Nous conclurons sur la question que se pose tout citoyen désirant installer une application de traçage de contacts (qu'elle soit basée sur un protocole centralisé ou décentralisé) : est-ce que cette application respecte la vie privée de ses utilisateurs ? Il nous semble que la réponse nécessite une certaine nuance.

Tout d'abord, on peut considérer que les Etats membres disposent désormais d'un cadre juridique clair et précis concernant la mise en œuvre d'applications de traçage de contacts, eu égard aux nombreux avis émis par les autorités de protection des données (dont nous avons analysé une partie dans cette étude). Par ailleurs, il semble que ces avis, en Belgique et en France ont effectivement été suivis sur certains éléments importants. A cet égard, l'accord de coopération belge[74] et son accord de coopération d'exécution[75] instituant le traçage numérique prévoient explicitement entre autres que l'utilisation de l'application doit être volontaire, que le code source de l'application et l'analyse d'impact relative à la protection des données doivent être publiés, que les données doivent être pseudonymisées et définir clairement les finalités du traitement. En ce qui concerne la France, la CNIL a indiqué avoir déjà effectué des contrôles concernant l'application de traçage et a constaté que le fonctionnement de celle-ci respectait pour l'essentiel la règlementation relative à la vie privée, mais a relevé quelques manquements liés à la première version de l'application, ces manquements ayant disparu dans une mise à jour ultérieure[76]. Les deux protocoles (centralisé et décentralisé) semblent *a priori* apporter un haut niveau de garantie vis-à-vis de la protection des données au regard des obligations contenues dans le RGPD. Il nous semble néanmoins, comme le soutient le CEPD, que le protocole décentralisé (notamment le DP3T) apporte des garanties plus importantes au regard du RGPD. L'application belge se limite en effet à rapporter les clefs relatives à un utilisateur testé positif, là où l'application française partage les clefs relatives à l'ensemble des contacts, ce qui risquerait de permettre d'inférer des informations plus détaillées sur l'individu en question (notamment en cas de ré-identification accidentelle).

Toutefois, il nous semble qu'il y a un élément inconnu à ce jour et qui aura une importance significative dans la détermination de la proportionnalité de l'ingérence que constitue l'utilisation de ce type d'application dans la vie privée de ses utilisateurs : nous ne connaissons pas la réelle efficacité de ce type d'applications de traçage. Comme nous l'avons vu, le risque que les applications de traçage créent pour les droits et libertés fondamentales des personnes concernées, même s'il est accompagné de toutes les mesures et garanties recommandées par les autorités, ne sera admissible dans une société démocratique que s'il est proportionné et, partant, efficace, au regard de l'objectif poursuivi. La première étape pour que ce type d'applications fonctionne est d'emporter l'adhésion la plus large possible de la population. Or, les chiffres disponibles par rapport à

l'utilisation de l'application « StopCovid » en France montrent que l'application n'a pas eu de réel succès[77] (l'application a d'ailleurs été récemment remplacée par une nouvelle version intitulée « Tous Anti-Covid », mais cette application reste basée sur le protocole ROBERT). De plus, on peut se demander quelle sera l'efficacité réelle de ce type d'application dans le cadre de la gestion plus globale de la crise. Certaines mesures, comme la limitation plus ou moins stricte des contacts sociaux ou l'absence de possibilité de tester les personnes asymptomatiques sont des éléments qui limitent l'utilité pratique de l'application. Il est malaisé de déterminer si les applications seront toujours considérées comme un outil efficace dans la gestion de la crise, en combinaison avec ces autres mesures plus restrictives[78]. Ce type d'ingérence dans la vie privée de la population pourrait dès lors ne plus être proportionnée au regard de ses objectifs et être vouée à disparaître à plus ou moins court terme.

§40. Enfin, outre les aspects relatifs à la protection de la vie privée et à la lutte contre la pandémie du coronavirus Covid-19, il nous semble opportun de conclure cette contribution en regardant vers l'avenir. Nous sommes d'avis que ce type de question juridique deviendra de plus en plus fréquent. Le développement technologique permet de résoudre de plus en plus de problèmes qui autrefois restaient sans réponse. Pour s'adapter à cette évolution, les juristes devront probablement être capables de développer de nouvelles compétences, telles que la capacité de réfléchir à l'intégration de normes dans des logiciels et à définir des algorithmes, voire à apprendre le codage informatique.

1. Qu'il s'agisse du suivi des personnes contaminées par les méthodes traditionnelles ou par le biais d'applications mobiles. ↩

2. N. Ni Loideain, Regulating health research and respecting data protection: a global dialogue, IDPL, 2020, Vol. 10, No.2, p.115. ↩

3. 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, OJ L 119, 4.5.2016, p. 1–88 (aussi connu sous son acronyme anglais « GDPR »). ↩

4. https://www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles, *20 juillet 2020, consulté le 13 août 2020*. ↩

5. R. Gellert, *We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Right-Based and the Risk Based Approaches to Data Protection*, EDPLR, Avril 2016, p.483. ↩

6. Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 30 Mai 2014, WP 218, p.3. Notons toutefois qu'une partie des dispositions du RGPD ne repose pas sur une évaluation du risque (par exemple, les droits des personnes concernées d'être informées ou de pouvoir demander l'accès à leurs données personnelles). ↩

7. Ibidem, p. 4. ↩

8. Voyez notamment CEPD, *Lignes directrices4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19*, 21 avril 2020, disponible sur https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_fr.pdf (ci-après, « CEPD 4/2020 »), p.8, n°29. ↩

9. CEPD, p.4 n°2. ↩

10. CEPD, p.4 n°3. ↩

11. Comité Européen de la Protection des Données, 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, 21 avril 2020, disponible sur : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_fr.pdf, p.5, n°6 ; Délibération de la CNIL n° 2020–046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » (demande d'avis n° 20006919) (ci-après, « Délibération n° 2020–046 »), p.8. ↩

12. Audition CNIL, Parlement français, Audition de la Commission des lois à l'Assemblée nationale, propos liminaires de Madame Marie-Laure Denis, Présidente de la CNIL, mercredi 8 avril 2020, disponibles sur https://www.cnil.fr/sites/default/files/atoms/files/propos_liminaire-audition_commission_des_lois-assemblee_nationale-8–04–2020.pdf, p.5. ↩

13. Recommandation (UE) n° 2020/518 de la Commission du 8 avril 2020 concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées, JO L114, 14 avril 2020 ; European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)), n°52 ; eHealth Network, *Interoperability guidelines for approved contact tracing mobile applications in the EU*, disponible sur https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf. ↩

14. Recommandation (UE) n° 2020/518 de la Commission du 8 avril 2020, *op. cit.*, p. 114/10, n°15. ↩

15. Voyez le recensement des applications de traçage effectué par la Vrije Universiteit Brussel, disponible sur le site suivant : https://lsts.research.vub.be/en/contact-tracing-apps. ↩

16. EDPB, p.10, n°42. ↩

17. Ce protocole est décrit sur le site https://github.com/DP-3T/documents. ↩

18. Voyez la description sur le site suivant https://www.apple.com/covid19/contacttracing. ↩

19. Ce protocole est décrit sur le site https://github.com/pepp-pt/pepp-pt-documentation. ↩

20. Ce protocole est décrit sur le site https://github.com/ROBERT-proximity-tracing/documents. ↩

21. Pour la Hongrie, voyez https://virusradar.hu/privacy-policy. Pour l'Islande, voyez https://github.com/aranja/rakning-c19-app et https://www.covid.is/app/privacystatement. ↩

22. Défini par l'article 4.7 du RGPD comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement […] ». ↩

23. Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données, 2018,* p.130. ↩

24. Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, Idem, 2018, p.158. ↩

25. Par exemple, le droit à la portabilité des données ne s'applique que lorsque le traitement est justifié par le consentement de la personne concernée ou la nécessité d'une exécution contractuelle (voyez l'article 20 du RGPD). ↩

26. Articles 6.1 a) et 9.2 a) du RGPD. ↩

27. Articles 6.1 e) et 9.2 i) du RGPD. ↩

28. CEPD, p.8, n°29. ↩

29. Notamment dans son Avis n° 64/2020 du 20 juillet 2020 en réponse à la Demande d'avis concernant un projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano (CO-A2020–076) (ci-après, « Avis n°64/2020 »), p.5, n°11 et 12. ↩

30. CEPD 4/2020, p.13, n°1. ↩

31. Délibération n° 2020–046, p.5 ; 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) (ci-après « Avis n° 43/2020 »), p. 11, n°39. ↩

32. Avis n° 64/2020, p.26, n°80. ↩

33. CEPD 4/2020, p.8, n°29. ↩

34. Voyez les articles 7 et 8 du RGPD en la matière. ↩

35. EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, p.10 n°26. ↩

36. CEPD 4/2020, p.10, n°36. ↩

37. Voyez notes infrapaginales n°11 et 12. ↩

38. Délibération n° 2020–056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (demande d'avis n° 20008032) (ci-après « Délibération n° 2020–056 »), p.3. ↩

39. Avis n° 64/2020, n°77, p.24 ; Délibération n° 2020–046, p.6. ↩

40. Délibération n° 2020–046, p.8. ↩

41. Avis n° 43/2020, p.7, n°22 ; Délibération n° 2020–046, p.7. ↩

42. 42 CEPD 4/2020, p.11, n°47. ↩

43. CEPD 4/2020, p.10 n°37 ; Délibération n° 2020–046, p.11 ; Avis n° 43/2020, p.7, n°23. ↩

44. Délibération n° 2020–056, p.9 ; Avis n° 34/2020 du 28 avril 2020 en réponse à la demande d'avis concernant un avant-projet d'arrêté royal n° XXX portant exécution de l'article 5, § 1, 1°, de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus COVID-19 (II), dans le cadre de 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-2020–041) (ci-après « Avis n° 34/2020 »), p.8, n°24. ↩

45. CEPD 4/2020, p.14, n°1. ↩

46. Délibération n° 2020–056, p.6. ↩

47. CEPD 4/2020, p.14, n°1. ↩

48. Délibération n° 2020–056, p.12. ↩

49. Avis n° 43/2020, p.5, n°17. ↩

50. Avis 43/2020, p.12, n°47. ↩

51. Ibidem. ↩

52. Avis n° 79/2020 du 7 septembre 2020 relatif à un projet d'arrêté royal portant exécution de l'arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano et d'un projet d'accord de coopération d'exécution conclu entre l'Etat fédéral,

la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1er, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980 (CO-A-2020–099), p.6, n°13. ↩

53. Cette analyse d'impact a été publiée et est disponible sur le site suivant : https://coronalert.be/wp-content/uploads/2020/09/20200915-DPIA_contactopsporingsapplicatie-Belgie-V.5_final_FR.pdf, consulté le 28 octobre 2020. ↩

54. CEPD 4/2020, p.8, n°26 ; Avis 43/2020, p.7, n°24 et s. ; Délibération n° 2020–046, p.4. ↩

55. Délibération n° 2020–046, p.5. ↩

56. Avis 43/2020, p.9, n°30. ↩

57. CEPD 4/2020, p.10, n°40. ↩

58. Délibération n° 2020–046, p.10 ; Avis 43/2020, p.10, n°34. ↩

59. CEPD 4/2020, p.8, n°27 ; Avis 43/2020, p.10, n°34 ; Délibération n° 2020–056, p.4. ↩

60. CEPD 4/2020, p.8, n°27. ↩

61. Délibération n° 2020–046, p.9 ; Avis 43/2020, p.8, n°27. ↩

62. Délibération n° 2020–056, p.7, n°38 et 39. ↩

63. Délibération n° 2020–046, p.4. ↩

64. CEPD 4/2020, p.10, n°38. ↩

65. CEPD 4/2020, p.9, n°35 ; Avis 43/2020, p.14, n°52 et 53 ; Délibération n° 2020–056, p.9. ↩

66. CEPD 4/2020, p.9, n°35. ↩

67. Avis n° 34/2020, p.12, n° 34. ↩

68. Avis 43/2020, p.10, n°37.

    37 ; Délibération n° 2020–056, p.12. ↩

69. CEPD 4/2020, p.10, n°45. ↩

70. CJUE, 16 juillet 2020, *Schrems II*, C-311/18. ↩

71. CJUE, 6 octobre 2015, *Schrems*, C-362/14. ↩

72. CJUE, 8 avril 2014, *Digital Rights Ireland*, C-293/12 et C-594/12, récemment confirmé par les arrêts du 6 octobre 2020 C623/17, C511/18, C512/18 et C520/18. ↩

73. Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105 du 13.4.2006, p. 54–63. ↩

74. Accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspections d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID–19 se fondant sur une base de données auprès de Sciensano, qui a été approuvé par les différents parlements. ↩

75. Accord de coopération d'exécution du 13 octobre 2020 entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1er, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980. ↩

76. Délibération n° 2020–087 du 10 septembre 2020 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 (mai à août 2020), p.14, n°66 et s. ↩

77. Voy. https://www.lemonde.fr/pixels/article/2020/07/31/coronavirus-les-autorites-francaises-appellent-a-nouveau-a-installer-l-application-stopcovid_6047823_4408996.html, consulté le 14 août 2020. ↩

78. Il ne s'agit pas de remettre en doute l'efficacité ou le bien-fondé de ces mesures plus restrictives, mais plutôt de souligner qu'organiser un système de traçage numérique pourrait ne plus être efficace dans certains contextes. ↩