Conseil des barreaux européens
La voix des avocats européens
Rue Joseph II, 40/8 - B-1000 Bruxelles
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

Déclaration du CCBE sur les applications de suivi des contacts spéciales Covid-19

15/05/2020

Le Conseil des barreaux européens (CCBE) représente les barreaux de 45 pays, soit plus d'un million d'avocats européens. Le CCBE répond régulièrement au nom de ses membres aux consultations sur les politiques qui concernent les citoyens et les avocats européens.

Dans cette déclaration, le CCBE souhaite exprimer ses préoccupations et énoncer un certain nombre de principes qui doivent être respectés lorsque les gouvernements et les acteurs privés se tournent vers l'utilisation d'applications de suivi des contacts comme composante d'un programme plus large de limitation de l'infection et de contrôle de la pandémie de Covid-19.

La déclaration suivante repose sur les conclusions exposées dans les considérations du CCBE sur l'utilisation des applications de suivi des contacts spéciales Covid-19, qui se trouvent en annexe ci-dessous.

Le CCBE reconnaît qu'il est impératif pour les gouvernements nationaux de protéger la santé de leurs citoyens et de limiter d'urgence la propagation de l'infection. Il note que les gouvernements nationaux de toute l'Europe introduisent ou proposent d'introduire des applications de suivi des contacts comme moyen d'y parvenir, tout en faisant remarquer que l'utilisation de ces applications est susceptible de constituer une violation des droits fondamentaux, y compris le droit à la vie privée et le droit à la limitation du traitement des données personnelles. De telles violations ne peuvent être acceptables que si elles sont justifiées selon le principe de la proportionnalité.

Le CCBE affirme donc les ***principes*** suivants :

1. Aucun système de suivi des contacts ne doit être déployée autrement que conformément à l'**état de droit** ;
2. Aucun système de suivi des contacts ne doit *reposer sur* la collecte par les autorités publiques de données relatives au trafic mobile ou d'autres formes de données de géolocalisation, et aucune application de suivi des contacts ne doit *recueillir* ces données autrement que de manière pleinement justifiée par des motifs de santé publique, et qui soit ouverte, transparente et avec le consentement explicite de l'utilisateur ;
3. Le fonctionnement de toute application de suivi des contacts doit **respecter les droits fondamentaux** et être **proportionné**. Celle-ci doit notamment être à la fois conforme à la loi et manifestement nécessaire dans une société démocratique pour assurer la protection de la santé publique ;
4. Le fonctionnement d'une telle application de suivi des contacts doit respecter les dispositions du **règlement général sur la protection des données** (RGPD) et fonctionner en particulier conformément aux principes de traitement des données précisées à l'article 5 du RGPD ;
5. La base de fonctionnement d'une telle application et la manière dont elle collecte et conserve les données doivent être ouvertes et **transparentes** ;

6. Il ne doit **pas y avoir d'obligation** pour les citoyens d'installer ou d'utiliser une telle application, ni d'incitations susceptibles de désavantager ceux qui ont choisi de ne pas installer et utiliser l'application ;
7. Le fonctionnement de l'application doit avoir lieu sous le **contrôle de l'utilisateur** et pouvoir être temporairement **interrompu**, ou l'application doit pouvoir **désinstallée** à tout moment par l'utilisateur ;
8. Des mesures appropriées doivent être prises pour permettre à l'utilisateur d'exclure la collecte de données à caractère personnel lorsque ces données concernent le fait et les circonstances d'une réunion entre un citoyen et un avocat et lorsque cette réunion relève ou peut relever du **secret professionnel/*legal professional privilege*** ;
9. Les données collectées ne doivent être **traitées que par les autorités sanitaires compétentes** et ne doivent être accessibles à aucun autre organisme ni agence ;
10. L'exercice de la liberté de traverser une frontière nationale ou toute autre frontière ne doit être subordonnée ni au téléchargement, ni à la possession ni au fonctionnement d'une application de suivi des contacts ;
11. Des dispositions appropriées doivent être prises afin de garantir que le fonctionnement de l'application ainsi que la conservation et le traitement des données personnelles soient **interrompus** et que toutes les bases de données contenant des données personnelles (y compris les données personnelles pseudonymes) soient **détruites** lorsque l'urgence prend fin ;
12. Dans la mesure où l'utilisation ou le fonctionnement de l'application peut être régi ou facilité par des pouvoirs d'urgence, la législation autorisant les pouvoirs en cas d'urgence doit contenir une **clause de temporisation** adéquate.

En application de ces principes, l'application doit être conforme aux ***exigences minimales*** suivantes :

- Le système de suivi des contacts dans son ensemble doit respecter le principe de **minimisation des données,** et la collecte et le traitement des données à caractère personnel doivent être manifestement justifiables à des fins de santé publique ;
- En particulier, la **finalité** pour laquelle les données sont collectées et traitées doit porter exclusivement sur le suivi des contacts aux fins de la lutte contre l'infection dans le cadre de la pandémie de Covid-19 et toute mutation du virus ;
- L'application ne doit pas entraîner la collecte ni le traitement de données qui ne sont pas nécessaires aux fins du suivi des contacts ;
- Avant son lancement, l'application doit faire l'objet d'une **évaluation** complète **d'impact sur la protection des données** ;
- Le code source du programme doit être mis à disposition pour une **vérification indépendante** de son efficacité et de sa sécurité, que ce soit par un organisme indépendant ou par la publication du code source ;
- L'application doit être **évaluée en permanence** en ce qui concerne son efficacité et sa conformité aux droits fondamentaux et aux obligations concernées en matière de protection des données et mise à jour si nécessaire ;
- L'application doit pouvoir être **désinstallée** à tout moment sans laisser de trace ;
- L'application doit être conçue de manière à permettre aux utilisateurs de choisir de transmettre ou non des données concernant leur propre infection ;

- À cette fin, l'**accès aux données** ne doit pas être accessible à d'autres personnes que les autorités de santé publique compétentes. Des contrôles techniques et juridiques doivent garantir cette limitation de finalité et d'accès ;
- Les données personnelles (y compris les données personnelles liées à des pseudonymes) doivent être **conservées pendant une durée n'excédant pas celle nécessaire** à la réalisation de l'objectif pour lequel elles ont été collectées, ces données étant supprimées (de préférence automatiquement) dès qu'elles ne sont plus nécessaires à la lutte contre le coronavirus provoquant la maladie Covid-19 ;
- Il est ***recommandé*** que les autorités nationales visent autant que possible, au moment du développement des applications de suivi des contacts, à s'assurer de l'interopérabilité des applications avec celles utilisées dans les autres États, en particulier les États voisins.
- Il est ***recommandé*** que l'autorité nationale de protection des données compétente ait la possibilité d'examiner le logiciel et les procédures administratives et autres procédures associées à l'application afin d'en vérifier la proportionnalité et le respect des principes de minimisation des données avant que l'application ne soit mise à la disposition du public.

ANNEXE: Considérations du CCBE sur les applications de suivi des contacts spéciales Covid-19

ANNEXE : Considérations du CCBE sur les applications de suivi des contacts spéciales Covid-19

1. Introduction

Alors que le monde entier prend conscience que la Covid-19 ne sera probablement pas éliminée de sitôt, et que les dégâts économiques dus à la cessation quasi-totale de l'activité économique sont de plus en plus manifestes, les gouvernements cherchent des moyens de reprendre un semblant de vie normale, même s'ils parlent plutôt de « nouvelle normalité ».

Du point de vue de la santé publique, il existe plusieurs conditions préalables à la suppression des mesures de confinement strictes, la plus importante dans la discussion actuelle étant 1) premièrement, que le taux de transmission ait considérablement diminué et 2) deuxièmement, étant donné la contagiosité élevée de la maladie, qu'un système solide de suivi des contacts permette de retrouver et de mettre en quarantaine les personnes qui ont été en contact avec une personne infectée. Pour que cette dernière condition soit remplie, il est nécessaire d'avoir à disposition un système de dépistage complet (afin de savoir qui peut être infecté) et un moyen de suivre les contacts.

En ce qui concerne le système de dépistage, il est peu probable que le dépistage universel d'une population entière puisse jamais être mis en œuvre, notamment parce que les tests ne donnent qu'une image de la situation au moment où ils sont réalisés. Le processus de suivi des contacts n'est pas nouveau. Il est utilisé dans le cadre d'épidémies de maladies infectieuses depuis plus d'un siècle et la plupart des États, dans le cadre de la mise en œuvre de leur politique de santé publique, sont en mesure de mettre en place des processus manuels de suivi des contacts. Ces processus peuvent être efficaces, mais ils sont loin d'être parfaits. Prenez l'exemple d'une personne infectée qui se déplace en transports en commun dans une grande ville : non seulement cette personne ne pourra pas se souvenir de toutes les personnes avec lesquelles elle a été en contact, mais elle ne saura même pas qui elles étaient. C'est pourquoi les gouvernements envisagent d'utiliser des applications de suivi des contacts afin d'automatiser cette tâche, soit en remplacement, soit en conjonction avec les moyens manuels traditionnels de suivi des contacts.

Si un État cherchait à rendre obligatoire l'utilisation d'applications de suivi des contacts (il est possible de le soutenir) afin de garantir que le suivi des contacts soit aussi répandu et efficace que possible, cela représenterait un problème immédiat et immense pour le droit fondamental à la vie privée et aurait du mal à être accepté par le public. L'un des problèmes, et non des moindres, serait de savoir comment imposer l'utilisation de l'application par une personne qui n'a pas (et ne souhaite peut-être pas avoir) de téléphone portable. D'un autre côté, un système à participation volontaire serait susceptible d'entraîner un taux d'utilisation plus faible et de limiter dès lors l'utilité de l'application. Néanmoins, le recours à une incitation « de manière douce » pour promouvoir l'utilisation de l'application, tel que le fait d'exiger de l'activer avant d'entrer dans certains lieux ou d'emprunter les transports en commun, a des conséquences énormes sur les libertés civiles.

Le débat sur l'utilisation des applications devrait néanmoins reconnaître que les applications de suivi des contacts ne peuvent jamais être totalement couronnées de succès, premièrement en raison des faiblesses inhérentes à tout système de suivi des contacts (tel qu'expliqué plus haut) et deuxièmement parce que celles-ci ne pourront jamais être universelles : tout le monde ne dispose pas d'un téléphone portable ou n'a pas un téléphone portable équipé de la technologie Bluetooth sur soi, allumé et avec de la batterie.

Ces observations sont faites d'emblée étant donné que le débat sur l'utilisation des applications est souvent clairement mené en se fondant sur l'hypothèse facile mais fausse que les applications de suivi de contacts constituent la panacée. Il est largement reconnu dans les milieux de la santé publique que les applications de suivi des contacts, si elles sont utilisées, doivent venir en renfort aux méthodes manuelles traditionnelles de suivi des contacts et être utilisées parallèlement à celles-ci.

Cela dit, le mieux ne doit pas être l'ennemi du bien, et l'expérience pratique en Asie montre que les applications peuvent contribuer de manière significative au contrôle des infections. La question est plutôt de savoir si payer le prix des libertés civiles et des droits fondamentaux pour l'acquisition de cette contribution est, en réalité, un pacte faustien.

2. Les droits fondamentaux : le contexte juridique

La collecte de données par une application soulève des préoccupations tant en ce qui concerne la législation sur la protection des données que, de manière plus large, les droits au respect de la vie privée et familiale en vertu de l'article 8 de la Convention européenne des droits de l'homme (CEDH) et de l'article 7 de la Charte des droits fondamentaux de l'Union européenne, ainsi que les droits à la protection des données personnelles en vertu de l'article 8 de la Charte de l'Union européenne.

En ce qui concerne l'article 8 de la CEDH, le droit n'est pas absolu :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Dans les circonstances actuelles, l'utilisation d'une application et, en théorie, l'utilisation obligatoire d'une application pourraient être justifiées par la protection de la santé et, en théorie, par l'intérêt du bien-être économique (permettant la réintroduction progressive de l'activité économique), donc la question devient une question de proportionnalité. Il convient de ne pas oublier le double critère non seulement « nécessaire » mais « nécessaire dans une société démocratique ». Il peut alors être difficile de justifier des mesures excessivement invasives comme celles qui ont été adoptées en Chine mais, comme toujours, le problème est de savoir où poser la limite.

De manière moins évidente, l'article 6 de la CEDH pourrait être engagé dans certains cas. Le fait qu'une personne donnée ait consulté un avocat donné à un moment donné et en un lieu donné est, en soi, susceptible de relever du secret professionnel/*legal professional privilege*. Dans la mesure où une application pourrait enregistrer des données relatives à un tel fait, cela pourrait constituer une violation des droits de l'article 6. Toutefois, les mêmes questions de proportionnalité ne pourraient pas être utilisées pour justifier une telle surveillance en vertu des droits de l'article 8, puisque l'article 6 n'est pas engageable. Le secret professionnel/*legal professional privilege* l'emporte sur la santé publique.

En vertu du règlement général sur la protection des données (RGPD), les données personnelles recueillies seraient des données personnelles de catégorie spéciale au sens de l'article 9 et qui, en vertu du paragraphe 2 de l'article 9 bénéficient d'une protection renforcée et ne peuvent être traitées que si (extraits) :

« a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ;

[…]

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde

des droits fondamentaux et des intérêts de la personne concernée ;

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 ;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents. »

Lorsque le traitement de données à caractère personnel de catégorie spéciale est autorisé en vertu de l'article 9, paragraphe 2, le traitement doit également remplir les obligations prévues à l'article 6 du RGPD et être conforme aux principes généraux du traitement des données à caractère personnel énoncés à l'article 5 du RGPD.

En particulier, l'article 5, paragraphe 1, point c), dispose que les données à caractère personnel doivent être :

« c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ; »

En outre, l'article 25 exige la mise en œuvre de la protection des données dès la conception et par défaut. Cela implique que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement doivent être traitées. Cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité.

3. Trouver l'équilibre

Comme indiqué ci-dessus, un équilibre doit être trouvé entre, d'une part, l'effet positif sur la santé publique découlant de l'utilisation des applications de suivi des contacts et, d'autre part, le degré d'intrusion dans les droits fondamentaux découlant de l'utilisation de ces applications.

a) La santé publique

Lors des discussions liées à ce document, une délégation a évoqué les problèmes liés à l'utilisation d'une application lorsque (selon le consensus) l'utilisation d'une telle application est volontaire, comme indiqué ci-dessus. Cette délégation a mis l'accent sur le risque réel qu'une application inefficace ou, en tout cas, dont l'efficacité n'est pas optimale, puisse même être contreproductive en créant un faux sentiment de sécurité et en encourageant les personnes à prendre des risques injustifiés. La délégation a posé la question : « Est-il vraiment nécessaire de créer une application qui a peu de chance de fonctionner pour permettre au gouvernement de montrer qu'il fait quelque chose ? »

La réponse à cette question telle qu'elle est formulée est évidente, mais l'hypothèse selon laquelle une application a peu de chances de fonctionner peut sembler trop pessimiste étant donné que les preuves existantes tendent à soutenir l'idée que, bien qu'elles ne constituent pas une solution complète, les applications de suivi des contacts ont un rôle important à jouer dans le cadre d'un régime plus large de suivi des contacts et de contrôle des infections.

b) La centralisation de la base de données ?

Une question connexe se pose : les applications de suivi de contacts doivent-elles stocker les données à caractère personnel localement sur les appareils sur lesquels l'application est chargée (un modèle distribué) ou sur une base de données centrale ?

Certains commentateurs et au moins une des délégations ayant contribué à ce document ont exprimé leur inquiétude quant à l'utilisation d'une base de données centralisée, notamment du fait qu'une application distribuée tient mieux compte du respect de la vie privée dès la conception qu'une application centralisée. Les gouvernements européens optent pour la plupart pour le modèle de données distribuées, la France et le Royaume-Uni privilégiant actuellement une base de données centralisée en Angleterre (bien que les gouvernements décentralisés d'Écosse, du pays de Galles et d'Irlande du Nord continuent chacun à envisager leurs propres solutions). L'Allemagne, qui avait également développé un modèle de base de données centralisée, est passée à un stade relativement tardif à un modèle distribué. À l'évaluation de l'équilibre entre la santé publique et les droits fondamentaux, si tous les modèles centralisés et tous les modèles distribués produisaient sensiblement le même résultat en matière de santé publique, il est défendable que l'utilisation d'un modèle distribué serait plus proportionnée.

Cependant, la réalité est qu'il existe potentiellement une grande diversité d'applications, certaines étant décentralisées et d'autres utilisant une base de données centralisée, mais chacune programmée de manière différente, chacune avec un éventail de fonctionnalités, chacune étant déployée de manière différente et chacune soumise à des régimes administratifs différents. En conséquence, l'utilisation des applications de suivi des contacts a des effets divers sur la santé publique et il devient difficile, de manière générale, d'affirmer que l'adoption d'un type d'application permettra nécessairement d'atteindre un meilleur équilibre entre la protection de la santé publique et l'intrusion dans la vie privée que l'adoption d'un autre type d'application.

En effet, dans ses *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*[1] (adoptées le 21 avril 2020), le Comité européen de la protection des données a déclaré (au paragraphe 42) :

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

Dans ces circonstances, bien qu'il faille peut-être examiner de manière soucieuse la conformité d'une application spécifique en matière de respect de la vie privée et de protection des données, il n'est pas vraiment possible de se prononcer, de manière générale, sur la question de savoir si une base de données centralisée ou un modèle décentralisé est préférable, au-delà de l'observation évidente que, dans le cas d'un modèle centralisé, il est d'autant plus important de garantir la sécurité de la base de données centrale, non seulement parce que le piratage de la base de données constituerait en soi une intrusion flagrante dans le droit à la vie privée, mais aussi parce que, à moins que le public ne puisse

[1] Voir https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_fr.pdf

être convaincu que des mesures de sécurité rigoureuses sont en place, le simple risque de piratage pourrait saper la confiance du public et entraîner une moindre utilisation de l'application. En tout état de cause, étant donné que certains gouvernements adoptent en fait des modèles centralisés, la considération essentielle est de formuler une approche qui fixe des normes minimales pour garantir la proportionnalité, quel que soit le modèle d'application adopté.

Tel que le montrent les dispositions juridiques exposées ci-dessus, il est possible, dans des circonstances appropriées, de justifier l'utilisation d'une application de suivi des contacts (qu'elle soit centralisée ou distribuée) conformément à l'article 8 de la CEDH, à condition que son utilisation respecte l'exigence de proportionnalité. Cela serait possible en délimitant strictement les objectifs pour lesquels les données sont recueillies, en interdisant toute autre utilisation et, sur le plan organisationnel, en veillant à ce que les données soient stockées spécifiquement au sein du système de santé publique. Un tel système pourrait éventuellement être conforme au RGPD.

(c) Le danger d'une dérive de mission

La création d'un appareil de surveillance étendu et sans précédent afin d'atteindre un objectif de santé publique nécessaire est une tentation séduisante pour un État de s'engager dans une dérive de mission dans la sphère de la santé publique, en étendant l'application pour suivre la grippe ou les foyers d'intoxication alimentaire, ou pour rendre les données disponibles au-delà de la sphère de la santé publique, afin de permettre la surveillance par les services de renseignement ou les organes chargés de l'application de la loi voire, dans certains États, d'utiliser les données pour s'engager dans une ingérence globale dans les droits fondamentaux tels que le droit à la liberté d'expression.

Ces préoccupations ne sont pas illusoires. L'exemple de l'utilisation des données de surveillance (avec un système de signaux verts et rouges) en Chine est bien connu, mais un autre exemple plus proche de nous est le mécanisme de surveillance introduit en Israël[2]. La surveillance y est utilisée pour suivre et tracer les infections virales, ce qui serait jusqu'ici acceptable s'il n'existait pas deux aspects extrêmement préoccupants : le premier réside dans le fait que, au lieu d'une application, l'État utilise d'autres mécanismes de surveillance plus insidieux, en particulier la collecte de données de localisation des téléphones portables auprès des opérateurs de téléphonie mobile et, deuxièmement, bien que la collecte serve effectivement à suivre l'épidémie de Covid-19, la surveillance est assurée par le Shin Bet, l'agence de renseignement israélienne.

Il est essentiel pour la création de moyens électroniques de suivi des contacts qui soient proportionnés que leur utilisation soit volontaire et que les applications ne nécessitent pas, pour leur fonctionnement, un accès non consensuel aux données de localisation obtenues à partir des données relatives au trafic des communications mobiles. Cela ne signifie pas qu'une application ne devrait jamais pouvoir transférer de données de localisation mais, pour qu'elle puisse le faire, il faut qu'elle le fasse de manière ouverte, transparente et avec le consentement de l'utilisateur, qui doit avoir la possibilité d'empêcher le transfert de ces données. Le déploiement de moyens détournés plus habituellement utilisés par les services de renseignement n'est jamais acceptable.

Il n'y a qu'un pas entre la collecte de données de localisation (même si elles sont recueillies de manière proportionnée) et l'utilisation des données de localisation relatives à une adresse IP donnée pour permettre l'identification des personnes qui ont apparemment enfreint les réglementations en matière de quarantaine. Et s'il y a infraction aux règles en matière de quarantaine, pourquoi n'y aurait-il pas d'autres formes d'activités illégales ?

Cette tentation de dérive de mission existe et a eu lieu au sein de l'Union européenne, par exemple en Allemagne, dans l'État de Bade-Wurtemberg : la police a déjà eu accès aux données sanitaires détenues par les autorités de santé publique afin de contribuer au contrôle de toute violation des restrictions de contacts et de faciliter les poursuites ultérieures[3].

[2] Voir https://www.bbc.co.uk/news/world-middle-east-52579475

[3] Voir https://www.swr.de/swraktuell/baden-wuerttemberg/polizei-zugriff-corona-daten-100.html

Ce type d'ingérence potentiellement disproportionnée dans les droits énoncés à l'article 8 de la CEDH est inquiétante non seulement en soi mais également en ce qui concerne ce à quoi elle pourrait conduire, mais elle est également contreproductive en ce sens qu'elle est susceptible de saper la confiance du public qui est plus que jamais nécessaire pour permettre à tout système de suivi des contacts de réussir ses objectifs en matière de santé publique.

(d) L'interopérabilité et les déplacements transfrontaliers

Le modèle actuel de développement des applications nationales est que les différents gouvernements adaptent différentes solutions en fonction des différentes situations nationales. Il en résulte un risque de manque d'interopérabilité entre les applications et, par conséquent, des problèmes dans les déplacements transfrontaliers des utilisateurs d'applications.

Si une personne franchit une frontière avec une application qui n'est pas compatible avec celle qui est utilisée dans le pays où elle voyage, elle devra charger l'application fournie par le pays dans lequel elle voyage afin de continuer à bénéficier des avantages d'un système de notification automatique. C'est une chose que l'utilisateur pourrait effectuer sans problème, surtout pour une visite de courte durée, ce qui créerait une lacune dans la couverture. Ce constat est regrettable et, lors du développement de leurs applications, les gouvernements nationaux peuvent juger utile de chercher, dans la mesure du possible, à en assurer l'interopérabilité. Cependant, il n'est pas toujours possible de parvenir à l'interopérabilité, en particulier lorsque les données pertinentes résident dans une base de données centrale. Si, pour y remédier, les gouvernements nationaux cherchent à convenir que les données doivent pouvoir être partagées, il est dès lors primordial, pour assurer la proportionnalité, que cela soit justifiable pour des raisons de santé publique et que cela se fasse de manière transparente et avec le consentement de l'utilisateur.

En outre, il serait clairement inacceptable, en raison de l'atteinte qui serait portée au caractère volontaire et consensuel nécessaire pour garantir la proportionnalité que, lors du franchissement d'une frontière, il devienne obligatoire qu'une personne ait ou soit obligée de télécharger une application qui fonctionne dans le pays dans lequel elle souhaite passer.

e) Une préoccupation ciblée

Dans ce contexte, il ressort qu'il existe deux domaines de préoccupation spécifiques et ciblés :

(a) Est-ce que le régime juridique prévoit les garanties nécessaires pour garantir que l'utilisation d'une application de suivi des contacts est proportionnée et respecte les principes du traitement des données ?

b) Quelles sont les exigences juridiques et organisationnelles requises pour garantir la confiance dans le respect des droits à la vie privée et à la protection des données de manière proportionnée ?

4. Garanties minimales

En examinant la question des exigences minimales régissant l'utilisation d'une application de suivi des contacts d'une manière qui assure une protection adéquate des droits fondamentaux et des réglementations en matière de protection des données, le CCBE suit une voie bien tracée. Il a déjà été fait référence aux lignes directrices du Comité européen de la protection des données et il convient également d'attirer l'attention sur les commentaires de l'Institut des droits humains de l'IBA (IBAHRI) à ce sujet dans le numéro 3 de son *Bulletin sur la liberté d'expression* (du 5 mai 2020)[4].

L'IBAHRI approuve spécifiquement une liste compilée par Amnesty International :

1) Les mesures de surveillance doivent être « légales, nécessaires et proportionnées ».

[4] https://www.ibanet.org/Human_Rights_Institute/Freedom-of-Expression.aspx

2) Les extensions du suivi et de la surveillance doivent être assorties de clauses de caducité.

3) L'utilisation des données doit être limitée aux fins liées à la Covid-19.

4) La sécurité et l'anonymat des données doivent être protégés et leur protection doit être démontrée à partir d'éléments probants.

5) La surveillance numérique doit éviter d'exacerber la discrimination et la marginalisation.

6) Tout partage de données avec des tiers doit être défini par la loi.

7) Il doit y avoir des garanties contre les abus et des procédures doivent être mises en place pour protéger les droits des citoyens à réagir aux abus.

8) Une « participation significative » de toutes les parties prenantes serait nécessaire, en particulier des experts de la santé publique et des groupes de population les plus marginalisés.

Bien que cette liste constitue un point de départ utile, toute réponse apportée par le CCBE doit être plus précise et tenir compte du contexte européen.

Dans ce contexte, il serait sûrement plus judicieux d'approfondir la réflexion en abordant une série de questions qui découlent directement de la discussion précédente.

4.1 Les applications de suivi des contacts sont-elles en principe acceptables en termes de libertés civiles et de protection des données ?

Il ne fait aucun doute que l'endiguement de la propagation du coronavirus est un objectif commun d'une importance exceptionnelle et qu'il est, dans une très large mesure, dans l'intérêt du public, à la fois pour garantir la santé publique et pour permettre, dans les meilleurs délais compatibles avec la protection de la santé publique, de renverser les restrictions imposées aux droits fondamentaux des citoyens. Dans ce contexte, l'utilisation de moyens techniques ou l'intégration de processus reposant sur des technologies peuvent offrir des possibilités qui constituent un élément essentiel d'une stratégie plus large de suivi et de contrôle.

Il est néanmoins primordial que les droits fondamentaux et l'état de droit soient respectés. Chaque solution technique proposée doit être évaluée avec soin, tant en ce qui concerne sa conception que sa mise en œuvre, afin de garantir qu'elle respecte le principe de proportionnalité. Elle doit être à la fois conforme au droit et manifestement nécessaire dans une société démocratique pour assurer la protection de la santé publique.

4.2 L'utilisation de l'application doit-elle être obligatoire ?

Il serait tout à fait disproportionné de rendre obligatoire l'utilisation d'une application. Non seulement il s'agirait d'une dérogation flagrante aux droits fondamentaux, mais ce serait également irréalisable étant donné que tous les citoyens ne possèdent pas ou n'ont pas à leur disposition un téléphone portable. Par conséquent, il ne devrait y avoir aucune obligation d'utiliser les applications de suivi. Il est peu probable qu'il soit possible de faire respecter une telle obligation et d'en contrôler le respect sans limiter massivement le droit à l'autodétermination informationnelle et les droits fondamentaux garantissant la confidentialité et l'intégrité des systèmes informatiques et des données à caractère personnel. L'utilisation de ces applications ne devrait être possible que de manière volontaire. Même en temps de crise, les restrictions aux droits fondamentaux ne doivent pas aller jusqu'à abolir *de facto* ces droits.

4.3 Quelles sont les exigences minimales à recommander pour assurer une protection adéquate des droits fondamentaux ?

- La finalité pour laquelle les données sont collectées et traitées doit porter exclusivement sur le suivi des contacts aux fins de la lutte contre l'infection dans le cadre de la pandémie de Covid-19 et toute mutation du virus.

- Il est nécessaire de s'assurer que l'application n'entraîne ni la collecte ni le traitement de données qui ne sont pas nécessaires aux fins du suivi des contacts.
- Il est essentiel, afin d'assurer la confiance du public, à la fois pour obtenir une adoption aussi vaste que possible de l'application et rassurer quant au respect de la vie privée lors de la conception et quant à l'efficacité médicale de l'application, que le code source du programme soit mis à disposition pour une vérification indépendante de son efficacité et de sa sécurité, que ce soit par un organisme indépendant ou par la publication du code source.
- Avant son lancement, l'application doit faire l'objet d'une évaluation complète d'impact sur la protection des données.
- L'application doit être évaluée en permanence en ce qui concerne son efficacité et sa conformité aux droits fondamentaux et aux obligations concernées en matière de protection des données et mise à jour si nécessaire.
- Étant donné que l'installation de l'application relève du libre choix de l'utilisateur, ce dernier doit pouvoir décider librement, à tout moment, d'envoyer une notification concernant sa propre infection. Cette décision peut être prise par défaut, mais avec la possibilité pour l'utilisateur de passer outre le réglage par défaut.
- Le principe de minimisation des données doit être respecté. En particulier, les données conservées et envoyées concernant l'infection d'un utilisateur, ou l'exposition d'autres personnes susceptibles d'avoir été infectées, doivent être justifiées de manière démontrable à des fins de santé publique. La manière précise dont la minimisation des données peut être obtenue dépend en partie de l'architecture de l'application, et notamment du fait que l'application repose sur des données distribuées ou sur une base de données centralisée.
- Les données créées et traitées lors de l'utilisation de l'application et, dans le cas d'un modèle centralisé, conservées et traitées dans la base de données doivent être traitées uniquement pour la finalité pour laquelle elles ont été recueillies, à savoir le suivi des contacts aux fins de la lutte contre la Covid-19.
- À cette fin, l'accès aux données ne doit pas être accessible à d'autres personnes que les autorités de santé publique compétentes. Des contrôles techniques et juridiques doivent garantir cette limitation de finalité et d'accès.
- Les données personnelles (y compris les données personnelles liées à des pseudonymes) doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation de l'objectif pour lequel elles ont été collectées. Il convient notamment de veiller à ce que ces données soient supprimées (de préférence automatiquement) dès qu'elles ne sont plus nécessaires (par exemple, à la fin de la période d'incubation avec éventuellement une courte marge de sécurité temporelle).
- Il faudrait envisager de permettre à l'autorité nationale de protection des données compétente d'examiner le logiciel et les procédures administratives et autres procédures associées à l'application afin d'en vérifier la proportionnalité et le respect des principes de minimisation des données avant que l'application ne soit mise à la disposition du public. Une telle procédure permettra à la fois de vérifier la proportionnalité de manière indépendante et, tout en renforçant la confiance du public, d'encourager l'adoption de l'application.

4.4 Existe-t-il des considérations particulières en matière de secret professionnel ?

N'oublions pas qu'une rencontre entre une personne et son avocat à un endroit et à un moment donnés est en soi susceptible de relever du secret professionnel, de sorte que tout mécanisme de suivi des contacts qui conserve ou permet de récupérer cette information est susceptible de porter atteinte au secret professionnel/*legal professional privilege*. Une telle intrusion peut être justifiée par un test

de proportionnalité au titre de l'article 8 de la CEDH (bien que cela semble improbable étant donné la protection accrue accordée par la Cour européenne des droits de l'homme à la communication avocat-client), mais si la rencontre est liée à une poursuite pénale ou à un litige, alors une telle intrusion constituera toujours une violation de l'article 6 qui est de toute évidence un droit absolu.

Les problèmes liés à une application obligatoire ou à un système de collecte de données de localisation, comme celui employé en Israël, sont évidents, mais d'aucuns pourraient penser qu'ils ne se posent pas dans le cas d'une application volontaire : ni l'avocat ni son client ne sont obligés d'utiliser l'application et, s'ils l'ont installée, ceux-ci peuvent toujours la désactiver avant de se rencontrer. Toutefois, il existe toujours un risque de violation du secret professionnel/*legal professional privilege* si l'application est installée mais qu'elle ne peut pas être temporairement désactivée ou si l'avocat ou son client oublie tout simplement de la désactiver. Même une application décentralisée présente un risque potentiel pour le secret professionnel/*legal professional privilege* si la réidentification et la désanonymisation des données permettent d'établir un lien entre un client et son avocat.

Dans ces circonstances, et pour assurer la protection en matière de secret professionnel/*legal professional privilege*, au minimum :

- toute application doit être conçue de manière à pouvoir être temporairement désactivée, et
- les avocats et leurs clients doivent être vigilants et s'assurer que l'application est désactivée avant de se rencontrer.

4.5 Quels sont les mécanismes juridiques et réglementaires nécessaires ?

Il est essentiel que l'utilisation des applications de suivi des contacts soit conforme aux exigences de l'état de droit. Celles-ci ne doivent pas être introduites et utilisées en dehors de toute légalité. Toutefois, la nécessité de mettre en place des mécanismes juridiques ou réglementaires spéciaux pour garantir le respect des exigences minimales énoncées ci-dessus peut dépendre en partie de la manière dont la technologie de suivi des contacts est introduite dans chaque pays.

Tous les pays européens (à l'exception du Bélarus) sont signataires de la Convention européenne des droits de l'homme, et il existe déjà dans les pays européens un ensemble de lois primaires, de règlements et de jurisprudence régissant la protection de la vie privée ainsi que la collecte et le traitement des données, notamment le GDPR (dans l'EEE, en Suisse et au Royaume-Uni). Il est tout à fait possible de créer une application de suivi des contacts respectant les principes minimaux ci-dessus sans qu'il soit nécessaire de recourir à une législation ou une réglementation spéciale.

Néanmoins, certains pays peuvent avoir choisi de faciliter la création d'applications de suivi des contacts en vertu de pouvoirs d'urgence spéciaux et, même dans les pays où il n'existe pas d'obligation légale stricte de promulguer une législation spéciale, des pressions ont été exercées par certains milieux pour que les applications de suivi des contacts soient pourtant soumises à une législation spéciale.

À cet égard, toute législation spéciale de ce type, qu'elle concerne, au sens strict, les applications de suivi des contacts ou, au sens large, les pouvoirs d'urgence, doit être reconnue comme étant exceptionnelle et n'exister que pour répondre à l'urgence actuelle et doit contenir une clause de temporisation appropriée, un point souligné avec force par l'Organisation pour la sécurité et la coopération en Europe[5].

Lorsque l'utilisation d'une application de suivi des contacts n'est pas soumise à une législation spéciale, il est plus difficile de garantir que les principes de traitement des données ne soient pas enfreints en faisant en sorte que l'application poursuive son activité et que les données personnelles soient conservées au-delà de la fin de l'urgence, même si l'ordre juridique ne permet pas une telle continuation. Dans ces circonstances, si une application est introduite autrement qu'au moyen d'une

[5] Voir https://www.osce.org/odihr/449311

législation ou d'une réglementation spéciale, une clause de temporisation doit être explicitement prévue dans les dispositions administratives en vertu desquelles elle est créée et, en tout état de cause, les autorités compétentes en matière de protection des données et la société civile en général doivent veiller à ce que l'application ne soit pas maintenue en service au-delà du moment où son utilisation cesse de constituer une ingérence proportionnée dans les droits fondamentaux.

5. Conclusion

La discussion qui précède est résumée dans la Déclaration du CCBE sur les applications de suivi des contacts spéciales Covid-19.