Bird & Bird & Data Protection

Livre blanc sur les options possibles en protection des données personnelles pour le déploiement d'applications mobiles dans la lutte contre la pandémie de Covid-19.

Les pays européens ont réagi à la pandémie de covid-19 en adoptant des mesures sans précédent pour limiter les déplacements des personnes afin de contenir la propagation du virus. Alors que les gouvernements réfléchissent actuellement à la manière dont ils vont progressivement assouplir ces restrictions, il apparait clairement que les applications de suivi de contacts devraient faire partie de leur boîte à outils. Déjà déployées dans certains pays (par exemple à Singapour, en Chine, à Taïwan et en Corée du Sud), plusieurs pays de l'Union européenne («UE») ont commencé à développer de telles applications.

Lorsque les gouvernements de l'UE ont imposé le confinement en mars 2020, très peu de commentateurs se sont demandé dans quelle mesure cette décision portait atteinte au droit universel de libre circulation, tous étant surtout préoccupés par la nécessité de faire tout ce qui était nécessaire pour réduire le nombre de décès. Un mois plus tard, à l'heure où il est question de déterminer les mesures alternatives à mettre en œuvre après le confinement pour éviter une nouvelle vague épidémique, une mesure, le développement d'une application de suivi de contacts, suscite de nombreux débats quant à la possible atteinte qu'elle porterait à la vie privée. Dans ce débat, très peu de commentateurs ont mis en balance le droit au respect de la vie privée avec d'autres droits tels que le droit à la libre circulation et le droit à la protection de la santé, bien qu'ils soient également des droits fondamentaux.

L'objectif de ce livre blanc est d'expliquer la nécessité de mettre en balance ces droits fondamentaux, de trouver un moyen de développer des applications efficaces pour lutter contre la pandémie dans notre intérêt à tous, et de centrer le débat sur l'identification des garanties nécessaires aux droits et libertés des individus conformément aux principes de protection des données, au lieu de considérer comme acquis le fait que le consentement des personnes est la seule voie possible.

Ainsi, comme expliqué plus en détail dans ce livre blanc:

- la réflexion sur les applications de suivi de contacts menée par les gouvernements répond à un principe fondamental (**1**) ;
- lorsqu'ils développent une application de suivi de contacts, les gouvernements ont le devoir de trouver un équilibre entre le droit fondamental à la protection des données personnelles et d'autres droits et libertés fondamentaux tels que la liberté de circulation et le droit de travailler (**2**) ;
- les données de santé et les données de géolocalisation collectées par les applications de suivi de contacts sont soumises à des exigences strictes en vertu du droit de l'UE, avec des dispositions spécifiques en cas de menaces graves pesant sur la santé publique, sur lesquelles peuvent s'appuyer les gouvernements (**3**) ;
- conformément au droit de l'UE, les gouvernements ont le choix entre deux options : une utilisation volontaire de l'application (sur la base du consentement) ou l'adoption de mesures législatives pour l'utilisation de l'application par tous les citoyens (**4**) ;
- des garanties doivent être mises en place dans tous les cas et ce livre blanc fournit quelques suggestions de garanties (**5**).

1 La réflexion sur les applications de suivi de contacts menée par les gouvernements répond à un principe fondamental pour tous les pays européens

La réflexion menée par les gouvernements consistant à évaluer si les applications de suivi de contacts peuvent contribuer à la lutte contre la pandémie de covid-19 répond à un **principe fondamental pour tous les pays européens : la protection de la santé publique**.

À titre d'exemples : En **France**, ce principe est énoncé par le Préambule de la Constitution de 1946 selon lequel la Nation garantit à tous la protection de la santé. En **Allemagne**, l'article 2, paragraphe 2, de la Constitution allemande établit que toute personne a droit à la vie et à l'intégrité physique, ce qui implique pour le gouvernement allemand l'obligation de prendre des mesures pour éviter toute atteinte à la santé publique. En **Italie**, l'article 32 de la Constitution établit que la République italienne protège la santé comme un droit fondamental de l'individu et un intérêt de la communauté. Aux **Pays-Bas**, la Constitution stipule à l'article 22, paragraphe 1, que le gouvernement doit prendre des mesures pour promouvoir la santé publique. En **Espagne**, l'article 43 de la Constitution espagnole reconnaît le droit des individus à la protection de la santé et l'obligation des autorités de gérer et de diriger la santé publique.

S'ils n'envisagent pas le développement d'une application de suivi de contacts maintenant et que cet outil s'avère plus tard être crucial pour lutter contre la diffusion du COVID-19, les gouvernements auront manqué à leur obligation constitutionnelle de garantir la protection de la santé publique. **Par conséquent, si une application est nécessaire pour lutter contre la pandémie, les gouvernements ont le devoir de mettre en place une telle application, ou plus précisément de mettre en place la/les application(s)/technologie(s) qui combattent le mieux le virus d'une manière conforme au droit de l'UE et aux constitutions nationales.**

2. Les gouvernements ont le devoir de mettre en balance le droit fondamental à la protection des données personnelles avec les autres droits et libertés fondamentaux

Le droit fondamental à la protection des données personnelles n'interdit pas en soi le développement d'une application de suivi de contacts et les gouvernements doivent le mettre en balance avec les autres droits fondamentaux concernés.

Cela ne résulte pas d'une interprétation extensive de principes juridiques généraux : c'est ce que dit le RGPD[1]. Son considérant 4 le précise clairement :

> *"Le droit à la protection des données à caractère personnel n'est pas un droit absolu; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité.".*

Dans le processus de développement d'une application de suivi de contacts, **les gouvernements doivent donc trouver un point d'équilibre entre le droit à la protection des données personnelles reconnu par l'article 8 de la Charte des droits fondamentaux de l'Union européenne et d'autres libertés et droits fondamentaux, en particulier la liberté de circulation[2], la liberté professionnelle et le droit de travailler[3] qui subissent actuellement des restrictions sans précédent en raison du confinement.**

Tout d'abord, les gouvernements doivent évaluer si l'application a besoin de collecter des données personnelles pour atteindre son objectif de protection de la santé publique. **Si les données anonymes sont suffisantes, il n'est pas nécessaire de mettre en balance le droit à la protection des données personnelles avec d'autres droits car aucune donnée personnelle n'est traitée.**

Toutefois, **si une application de suivi de contacts a des effets limités lorsque les données sont rendues anonymes, le droit fondamental à la protection des données personnelles n'empêche pas l'utilisation de données personnelles.** Dans ce cas, les gouvernements doivent mettre en balance les droits et libertés fondamentaux prévus par les Constitutions nationales et la Charte des droits fondamentaux de l'UE. **Il en résulte d'une part que des données personnelles peuvent être**

[1] 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.
[2] Article 45 de la Charte des droits fondamentaux de l'Union européenne.
[3] Article 15 de la Charte des droits fondamentaux de l'Union européenne.

utilisées - à condition que des garanties solides soient mises en place, et d'autre part que le consentement n'est pas le seul moyen de garantir les droits et libertés des personnes (voir quelques suggestions de garanties dans la Section 6 ci-dessous).

Il est important de noter que l'affirmation souvent reprise selon laquelle "*les solutions technologiques les moins intrusives de la vie privée doivent être utilisées*" est - lorsqu'elle n'est accompagnée d'aucune réserve ou explication à l'appui - trompeuse. Cette affirmation est correcte s'il y a un choix possible entre deux moyens tout aussi efficaces. Toutefois, si une solution technologique est moins efficace qu'une autre ou pas encore disponible, une mise en balance doit être conduite.

3. Les données de santé et les données de géolocalisation collectées par les applications de suivi de contacts sont soumises à des exigences strictes en vertu du droit de l'UE, avec des dispositions spécifiques en cas de menaces graves pesant sur la santé publique.

Les développements suivants reposent sur le postulat que (i) le traitement de données anonymisées n'est pas suffisant pour aider le système de santé à assurer un déconfinement sécurisé et que (ii) le traitement de données de géolocalisation et de données de santé est nécessaire. La question de savoir si le traitement de données anonymisées est suffisant ou si la collecte de données personnelles (telles que des données de santé ou des données de géolocalisation) est nécessaire pour appuyer au mieux le combat contre le virus, sont factuelles/médicales et non de nature à être tranchées par des juristes.

D'un point de vue strictement juridique, les applications de suivi de contacts peuvent utiliser deux catégories de données hautement personnelles (les données de géolocalisation et les données de santé). Leur utilisation est toutefois soumise à des conditions strictes en vertu du droit de l'UE.

D'une part, les données de géolocalisation sont régies par l'article 9 de la directive européenne ePrivacy qui prévoit qu'elles ne peuvent être traitées pour d'autres fins que le routage des communications, sauf si les données sont rendues anonymes, ou si le consentement préalable des personnes a été recueilli, ou si une autre justification légale existe (c'est-à-dire une mesure législative prévue par le droit national applicable). D'autre part, les données de santé sont spécifiquement protégées par l'article 9 du RGPD, qui impose que le consentement des personnes soit recueilli ou qu'une autre des conditions alternatives énumérées dans ce même article soit remplie.

Dans les deux cas, le consentement préalable n'est pas le seul moyen et des dérogations existent, en cas de menaces graves pesant sur la santé publique (l'article 9, paragraphe 2, point i), du RGPD) ou pour la sauvegarde de la sécurité publique (article 15, paragraphe 1, de la directive ePrivacy), mais sous réserve de mesures législatives garantissant les droits et libertés des individus. De telles mesures peuvent déjà exister dans l'arsenal législatif préexistant de certains pays.

Dans l'application du principe de nécessité, il convient d'examiner si des solutions de suivi des contacts qui n'utilisent pas les données GPS (par exemple une solution Bluetooth basée sur une pseudonymisation aléatoire) sont disponibles, et permettent - sans collecte de données de géolocalisation - de lutter contre le virus de manière tout aussi efficace. Toutefois, il n'est pas requis d'attendre une solution qui n'est pas encore disponible ou d'utiliser une solution qui est moins adaptée. L'utilisation de données de géolocalisation peut donc être justifiée.

4. Utilisation sur la base du volontariat ou mesures législatives sauvegardant les droits et libertés : les gouvernements ont le choix !

Les gouvernements peuvent choisir entre deux options :

- **Option 1**: mettre en place une application basée sur le consentement des individus et qui peut être téléchargée/supprimée à tout moment (Utilisation volontaire).

- **Option 2**: adopter des mesures législatives pour garantir les droits et libertés pour l'utilisation d'une application par tous les citoyens (Mesures législatives).

Le choix entre ces deux options devrait être effectué à la lumière de leur efficacité dans la lutte contre le virus. Les applications de suivi de contacts ne seront réellement efficaces que si elles sont utilisées par la plus

grande partie possible de la population[4]. Le fait que le consentement ou l'adoption de mesures législatives constitue la meilleure manière d'atteindre cet objectif peut varier en fonction du pays et de sa culture. Mais il s'agit d'une question politique. D'un point de vue juridique, **les gouvernements ont le choix** !

Si l'option 1 (utilisation volontaire) est choisie, l'application doit en principe recueillir un consentement qui satisfait aux conditions de validité énoncées par le RGPD, en particulier l'exigence de **liberté de choix**. Selon le RGPD, le consentement n'est pas le seul moyen possible de collecter et de traiter des données personnelles, mais lorsque le consentement est utilisé, il doit être donné librement. Cela implique que le refus de consentir à l'utilisation de l'application ne devrait pas exposer la personne à des conséquences négatives. Cela signifie que chaque personne devrait pouvoir individuellement accepter ou refuser sans conséquence néfaste sur sa situation.

Dans ce contexte, l'intérêt pratique de cette approche questionne : si le fait de refuser d'utiliser l'application ne devait exposer à aucune conséquence de restriction de déplacement, cela signifie que celui qui refuserait d'utiliser l'application devrait pouvoir bénéficier quand même du déconfinement, au risque de propager le virus et mettre en danger la vie des autres. Il convient donc d'évaluer si cette approche aidera concrètement le travail des professionnels de santé pour mettre fin à la propagation du covid-19 et si la population trouvera un intérêt à utiliser l'application de suivi de contacts. Lorsque la santé et la sécurité publiques sont en jeu dans le contexte d'une crise sanitaire, et si une application est nécessaire pour lutter collectivement contre le virus, l'utilisation de cette application peut-elle dépendre d'un choix individuel ?

Si l'option 2 est choisie, des mesures législatives reflétant correctement les droits et libertés des individus devront être mises en place. De telles mesures législatives peuvent déjà exister en vertu des lois existantes d'un pays, c'est le cas par exemple de l'article 22, paragraphe 1, point c), de la loi fédérale allemande sur la protection des données. **Ce n'est pas le cas dans tous les pays européens. Par exemple, si la France choisit l'option 2 (utilisation d'une application par tous les citoyens), une nouvelle loi sera nécessaire parce que la loi française sur la protection des données (Loi Informatique et Libertés) ou d'autres lois (par exemple les lois en matière de surveillance ou la récente loi sur l'état d'urgence sanitaire) ne prévoient pas de mesures spécifiques à ce stade.** L'adoption d'une nouvelle loi dans un délai compatible avec l'urgence est possible[5].

Quelle que soit l'option choisie, son application devra comporter des garanties solides et respecter les principes du RGPD : proportionnalité, information claire fournie aux personnes, minimisation des données, finalités précises et légitimes, mesures techniques et organisationnelles, caractère provisoire du mécanisme de gestion de crise, etc. Nous donnons quelques exemples de garanties dans la section suivante.

5. Propositions de garanties

Les détails des applications développées par les gouvernements de l'UE ne sont pas encore officiellement arrêtés, notamment leurs finalités, leurs caractéristiques techniques ou encore la technologie sur laquelle elles vont reposer. Ce que nous avons présenté dans le tableau ci-dessous doit être considéré comme des suggestions à l'attention des gouvernements, sur la base des principes fondamentaux du RGPD. Elles devront être adaptées en fonction du projet spécifiquement envisagé par chaque gouvernement.

[4] Les épidémiologistes semblent s'accorder sur le fait qu'au moins 60% de la population doit utiliser une telle application pour que celle-ci soit utile.

[5] La récente loi sur l'état d'urgence sanitaire a été adoptée après seulement 4 jours de débats parlementaires. Cela prouve qu'une loi peut être adoptée rapidement. Une proposition de loi sur la création d'une application de suivi de contacts a déjà été soumise par un groupe de députés le 7 avril 2020. Le 28 avril 2020, le Parlement français débattra du déploiement d'une application de suivi de contacts.

Thème	Propositions de garanties
Limitation de la finalité	Les données personnelles doivent être collectées à des fins précises, explicites et légitimes. Dans le cadre de la lutte contre le covid-19, les applications et les traitements de données associés peuvent poursuivre différentes finalités légitimes. Chaque finalité doit être liée à la lutte contre le covid-19. Actuellement, les trois finalités suivantes sont principalement étudiées: • La **première finalité** est **l'observation des pratiques collectives** en suivant les mouvements de groupes de personnes pour identifier les zones à risque. Cette finalité ne nécessite généralement que l'utilisation de données anonymes. Les experts compétents ont déjà identifié ce domaine comme étant essentiel. • La **deuxième finalité** est le **suivi de contacts**. Il s'agit de retracer les déplacements des personnes testées positives, afin d'informer la population vivant dans les zones à haut risque et de pouvoir alerter les contacts récents qui ont croisé une personne malade. Un consensus s'est dégagé sur le fait que cette finalité nécessite la collecte et le traitement de données personnelles. Cette finalité ne semble pas pouvoir être atteinte uniquement à l'aide de données anonymes. • La **troisième finalité** est de **contrôler le confinement**, c'est-à-dire de surveiller le respect des quarantaines, comme en Corée et à Taïwan. C'est le plus intrusif en matière de vie privée. Contrairement à la première et à la deuxième finalité, il n'est pas évident que cette finalité soit justifiée. Il faut des preuves ou des indications solides que cela est réellement nécessaire et que le même résultat ou un résultat similaire ne peut être atteint avec des moyens moins intrusifs. Nous doutons que cela soit légitime dans un premier temps, mais nous pensons également que cela ne peut pas être absolument exclu à ce stade. En tout état de cause, cette finalité nécessiterait les garanties les plus élevées dans une démocratie. Les finalités de l'application devront être clairement identifiées et les personnes devront recevoir une information claire et complète à ce sujet.
Transparence	Les informations énumérées aux articles 13 et 14 du RGPD doivent être fournie aux utilisateurs de l'application, par exemple par le biais d'une note d'information sur la protection des données personnelles disponible au moment du téléchargement de l'application..
Minimisation des données / proportionnalité	Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire par rapport aux finalités de l'application. Parmi les différentes technologies qui peuvent être utilisées pour suivre les déplacements des personnes (bornage mobile, GPS, Bluetooth, cartes bancaires ou cartes de transport, vidéosurveillance...), le Bluetooth semble être plus respectueux de la vie privée au regard de la finalité de suivi des contacts. Par conséquent, si elle est disponible et suffisamment efficace, l'utilisation de cette technologie serait conforme à la législation sur la protection des données personnelles dans la mesure où elle est la plus en ligne avec le principe de minimisation des données. Toutefois, si la technologie Bluetooth n'est pas (encore) disponible ou s'il est nettement plus efficace d'utiliser par exemple une combinaison de Bluetooth et de géolocalisation, d'autres technologies peuvent être utilisées. Dans tous les cas, le gouvernement doit être en mesure de démontrer la nécessité et la proportionnalité des données personnelles collectées par rapport aux finalités poursuivies.

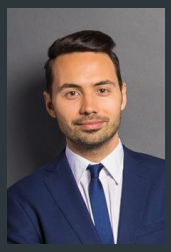
Exactitude	Une procédure aussi robuste que possible doit être mise en place : • pour certifier que lorsqu'une personne est déclarée porteur du Covid-19, cette information est exacte, c'est-à-dire basée sur un test (car elle déclenche des notifications aux autres personnes qui ont été exposées) ; • pour identifier les personnes qui ont été en contact avec la personne déclarée porteur du Covid-19. Les erreurs d'identification des personnes exposées au Covid-19 (faux positifs) devraient être limitées autant que possible par la solution. Il devrait être possible pour les utilisateurs de signaler de possibles erreurs. Le contenu de la notification envoyée aux personnes exposées (et en particulier les instructions données) doit être placé sous le contrôle des autorités sanitaires pour garantir leur pertinence. En effet, ces instructions (par exemple, quarantaine, obligation de porter un masque, obligation d'effectuer un test...) peuvent varier en fonction de la durée et de la proximité du contact avec la personne infectée. Un mécanisme devrait être mis en place pour que les personnes exposées puissent obtenir davantage d'informations auprès d'un professionnel de santé.
Durée de conservation limitée	Deux méthodes de stockage des données peuvent être mises en place : le stockage local des données dans les smartphones des particuliers, ou le stockage centralisé. Les deux peuvent être mises en place à condition que des mesures de sécurité techniques et organisationnelles adéquates soient mises en place. Le stockage local des données peut être considéré comme plus respectueux du principe de minimisation des données, mais un stockage centralisé peut être mis en place si nécessaire, sous réserve de la mise en place de mesures de sécurité appropriées.
Méthodes de stockage	Deux méthodes de stockage des données peuvent être mises en place : le stockage local des données dans les smartphones des particuliers, ou le stockage centralisé. Les deux peuvent être mises en place à condition que des mesures de sécurité techniques et organisationnelles adéquates soient mises en place. Le stockage local des données peut être considéré comme plus respectueux du principe de minimisation des données, mais un stockage centralisé peut être mis en place si nécessaire, sous réserve de la mise en place de mesures de sécurité appropriées.
Conception de l'application / Exigences techniques	Des garanties doivent être fournies concernant les algorithmes utilisés par l'application de suivi de contacts. Le fait que le code source de l'application soit ouvert (*open source*) est une garantie de transparence pour les personnes concernées qui peuvent auditer le code et s'assurer que l'application est utilisée uniquement aux fins pour lesquelles elle a été créée.
Sécurité	Des mesures techniques et organisationnelles robustes doivent être mises en place. Par exemple, si les données sont envoyées à un serveur central, elles doivent être transmises par un canal sécurisé. Des techniques de chiffrement peuvent être mises en œuvre pour sécuriser les communications de données entre l'application et le serveur et entre les applications, et pour protéger les informations stockées dans les applications et sur le serveur.
Mesures spécifiques pour les personnes vulnérables	Le gouvernement peut prendre des mesures spécifiques pour les mineurs, les personnes handicapées, les personnes moins qualifiées ou moins instruites, les personnes âgées. Par exemple, la notice d'information pourrait être adaptée pour ces personnes vulnérables.

Procédure de mise à l'arrêt de l'application et supervision	Une procédure peut être mise en place pour garantir que le mécanisme est arrêté et que les données sont supprimées une fois la crise terminée. Cette procédure peut fixer des critères pour déterminer "quand" l'application n'est plus nécessaire et "quelle" autorité (par exemple les autorités de santé publique) doit prendre cette décision. La procédure peut préciser par exemple comment arrêter la collecte de nouvelles données (instructions pour désinstaller l'application, désinstallation automatique, désactivation globale de l'application, etc.) et comment les données déjà collectées doivent être supprimées de toutes les bases de données. Certains membres qualifiés de l'autorité de protection des données locale (en France la CNIL) peuvent être désignés pour veiller à ce que les garanties soient dûment mises en œuvre et que la procédure de mise à l'arrêt de l'application soit effectivement activée lorsque les autorités publiques compétentes considèrent la crise terminée.

Key contacts

Willy Mikalef
Collaborateur Senior
Avocat au barreau de Paris

Tel: +33142686349
willy.mikalef@twobirds.com



Ariane Mole
Associée
Avocate au barreau de Paris

Tel: +33142686304
ariane.mole@twobirds.com

Ruth Boardman
Associée
Solicitor - Law Society of England & Wales

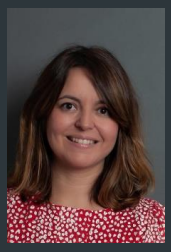
Tel: +442074156018
ruth.boardman@twobirds.com

Dr. Fabian Niemann
Associé
Avocat au barreau d'Allemagne

Tel: +4921120056000
fabian.niemann@twobirds.com

Lupe Sampedro
Associée
Avocate au barreau de Madrid

Tel: +442079826502
lupe.sampedro@twobirds.com



Frederique Dupuis-Toubol
Associée
Avocat au barreau de Paris

Tel: +442079826479
frederique.dupois-toubol@twobirds.com

Berend Van Der Eijk
Collaborateur Senior
Avocat au barreau des Pays-Bas

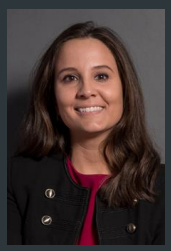
Tel: +31703538854
berend.vandereijk@twobirds.com

Debora Stella
Collaboratrice Senior
Avocate au barreau d'Italie

Tel: +390230356029
debora.stella@twobirds.com

Ester Vidal
Collaboratrice
Avocate au barreau de Madrid

Tel: +34917903232
ester.vidal@twobirds.com



twobirds.com

Abu Dhabi & Amsterdam & Beijing & Berlin & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw