Suivi et traçage du COVID-19 : Protéger la vie privée et les données lors de l'utilisation d'applications et de la biométrie

23 avril 2020

Messages clés

- Les technologies numériques, en particulier les applications mobiles et biométriques, font l'objet d'utilisations novatrices pour améliorer l'efficacité des réponses de première ligne des gouvernements face à la pandémie de COVID-19.
- Les informations et les tendances qui en résultent ont une valeur inestimable pour les gouvernements qui cherchent à suivre l'épidémie de COVID-19, à alerter les communautés vulnérables et à comprendre l'impact de mesures comme la distanciation physique et le confinement.
- La divulgation d'informations personnelles peut permettre au public de mieux localiser les cas potentiels d'infection au COVID-19 et de suivre la propagation du virus dans le temps. Toutefois, les solutions numériques utilisées actuellement pour la surveillance et le confinement ont des implications variables en termes de protection de la vie privée et des données.
- Des solutions de protection de la vie privée entièrement transparentes et responsables devraient être intégrées aux critères de conception afin de trouver un équilibre entre les avantages et les risques associés à la collecte, au traitement et au partage des données à caractère personnel. Les données ne devraient être conservées que pendant la durée nécessaire à la réalisation de la finalité spécifique pour laquelle elles ont été collectées.

Les gouvernements collaborent avec les fournisseurs de services de télécommunications pour accéder aux données de géolocalisation afin de suivre les mouvements de population

Alors que le COVID-19 continue à prendre des vies humaines et à secouer l'économie mondiale, les gouvernements recherchent en urgence de nouveaux outils innovants pour orienter l'élaboration des politiques et faire face à la crise. On voit apparaître des solutions numériques basées sur des données de géolocalisation visant à aider les autorités à surveiller et à contenir la propagation du virus. Certaines sont alimentées par les enregistrements des données d'appels mobiles (CDR), c'est-à-dire des données produites par les fournisseurs de services de télécommunications concernant les appels téléphoniques ou d'autres opérations de télécommunications, qui donnent des informations précieuses sur les mouvements de population. Comme les opérateurs de réseau desservent une grande partie de la population à travers des nations entières, les mouvements de millions de personnes à des échelles spatiales et temporelles fines peuvent être mesurés quasiment en temps réel. Les informations et les tendances qui en résultent ont une valeur inestimable pour les gouvernements qui cherchent à suivre l'épidémie de COVID-19, à alerter les communautés vulnérables et à comprendre l'impact de mesures comme la distanciation physique et le confinement.

Les opérateurs de télécommunications dans un certain nombre de pays de l'OCDE ont commencé à partager avec les pouvoirs publics des données de géolocalisation basées sur les CDR dans un format agrégé et anonymisé. Par exemple :

- La société de télécommunications allemande Deutsche Telekom fournit des données anonymisées sur les « flux de mouvements » de ses utilisateurs à l'Institut Robert-Koch, un institut de recherche et organisme gouvernemental chargé du contrôle et de la prévention des maladies.
- Le plan en cinq points du groupe Vodafone pour répondre à l'épidémie de COVID-19 prévoit de fournir aux gouvernements de grands ensembles de données anonymisées (comme une carte thermique agrégée et anonyme pour la région de Lombardie) pour aider les autorités à mieux comprendre les mouvements de population.
- La Commission européenne est actuellement en contact avec huit opérateurs de télécommunications européens pour obtenir des données de géolocalisation mobile anonymisées et agrégées, afin de coordonner les mesures de suivi de la propagation de l'épidémie de COVID-19. Afin de répondre aux préoccupations relatives à la protection de la vie privée, les données seront supprimées une fois la crise passée.

De nouvelles applications mobiles pour le « suivi » de l'épidémie de COVID-19 sont également lancées

Les applications mobiles délivrant des conseils santé constituent déjà une part significative de l'écosystème de la santé mobile et se sont avérées efficaces pour la prévention, le diagnostic précoce (par exemple, les vérificateurs de symptômes) et la mise en contact des utilisateurs avec les services de santé et les unités d'urgence au niveau local. Aujourd'hui, de nouvelles applications destinées aux consommateurs voient le jour dans le cadre du suivi de la pandémie. Ces applications suivent de plus en plus le modèle *open source* et sont le fruit de partenariats entre des entreprises technologiques, des universités, des cliniciens et les pouvoirs publics, responsables en dernier ressort de leur financement, de leur développement ultérieur et de leur mise en œuvre. Bien qu'elles ne permettent pas nécessairement d'appréhender l'ensemble de la population (par exemple, les personnes âgées qui peuvent ne pas avoir de smartphone ou ne pas le maîtriser), et ne sont pas exemptes d'erreurs (par exemple, lorsqu'elles ne peuvent pas faire la distinction entre les personnes d'un même ménage et celles des résidences voisines), ces applications fournissent aux pouvoirs publics un outil supplémentaire pour surveiller et contenir la propagation du virus. Les applications les plus citées sont notamment les suivantes :

- **TraceTogether** : Développée par l'Agence gouvernementale de technologie de Singapour (GovTech) en collaboration avec le ministère de la Santé, cette application utilise le Bluetooth pour suivre les personnes qui ont été exposées au virus. Ces informations sont utilisées pour identifier les contacts étroits en fonction de la proximité et de la durée d'une rencontre entre deux utilisateurs. Elle alerte ensuite ceux qui entrent en contact avec une personne testée positive ou qui présente un risque élevé d'être porteuse du coronavirus. Une fois qu'un individu est confirmé positif ou soupçonné d'être infecté, il peut choisir d'autoriser l'accès des hôpitaux, du ministère de la Santé et des tiers aux données de l'application afin d'aider à identifier les contacts étroits. Singapour prévoit de donner accès en *open source* au protocole d'échange de données sous-jacent, qui préserve la vie privée des utilisateurs.
- **Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)** : Plus de 130 scientifiques, technologues et experts de huit pays européens – dont la France, l'Allemagne et l'Italie – ont participé à une initiative à but non lucratif qui a conduit au développement d'une application libre permettant d'analyser les signaux Bluetooth entre les téléphones portables afin de détecter les utilisateurs qui ont été à proximité les uns des autres. L'application conserve de manière provisoire les données cryptées localement et, si, par la suite, les utilisateurs se révèlent positifs au test du COVID-19, elle peut alerter toute personne ayant été à proximité de la personne infectée au cours des jours précédents, tout en protégeant l'identité de l'ensemble des utilisateurs.
- **L'application de suivi de la Corée** : Financée par le gouvernement coréen, « Self-quarantine Safety App » est une application de suivi GPS et est utilisée par les autorités publiques pour fournir des informations sur l'épidémie de COVID-19, y compris les directives de quarantaine, et pour prévenir d'éventuelles violations des ordonnances d'auto-quarantaine. L'application peut également être utilisée pour l'auto-vérification et la déclaration volontaire auprès des autorités sanitaires. Les données collectées ne sont pas partagées avec des tiers.
- **C-19 COVID Symptom Tracker** *:* L'objectif de cette application développée au Royaume-Uni dans le cadre d'un partenariat entre des médecins et des scientifiques du King's College de Londres, une entreprise de science des données relatives à la santé (entreprise issue de King's College), et le Centre de l'Institut national de recherche sur la santé des hôpitaux Guy's & St Thomas', est de ralentir l'épidémie de COVID-19 en aidant les chercheurs à identifier : i) la vitesse de propagation du virus dans différentes zones ; ii) les zones à haut risque au Royaume-Uni ; et iii) les personnes les plus à risque, en améliorant la compréhension des symptômes liés à l'état pathologique sous-jacent. Selon les chercheurs, les données issues de l'étude peuvent révéler des informations essentielles sur les symptômes et l'évolution de l'infection chez différentes personnes. Elles peuvent également aider les chercheurs à comprendre pourquoi certaines personnes contaminées développent des symptômes plus graves, voire mortels, alors que d'autres ne présentent que des symptômes légers.
- En outre, **Apple et Google** vont également publier des interfaces de programmation d'application (API) qui permettent l'interopérabilité entre les appareils Android et iOS utilisant les applications des autorités de santé publique. Les utilisateurs pourront télécharger ces applications par le biais de leurs plateformes de téléchargement d'applications respectives. Les deux sociétés travailleront également de concert pour mettre en place une plateforme plus large de traçage des contacts basée sur le Bluetooth en intégrant cette fonctionnalité aux plateformes sous-jacentes. Cette solution permettrait à un plus grand nombre de personnes de participer, sur une base volontaire, et pourrait améliorer l'interaction avec un écosystème plus large d'applications et d'autorités sanitaires publiques.

Les applications de suivi peuvent intégrer différents niveaux de protection de la vie privée et des données

L'utilisation d'applications de collecte des données de géolocalisation peut permettre le partage de données, avec des protections formelles et intégrées de la vie privée et de la confidentialité, et permettre

aux utilisateurs de donner leur consentement explicite et éclairé à la collecte et au partage des données à caractère personnel les concernant (dans l'hypothèse où l'utilisation de l'application n'est pas obligatoire). Par exemple, l'application TraceTogether, à Singapour, comporte un certain nombre de garanties en matière de protection de la vie privée, notamment le fait qu'elle ne collecte ni n'utilise de données de géolocalisation et que les journaux de données sont conservés sous forme cryptée. Pour protéger la vie privée des utilisateurs, l'application de l'initiative européenne PEPP-PT crypte les données et anonymise les informations personnelles. En outre, dans la mesure où deux téléphones n'échangent jamais directement de données et où les pseudonymes des utilisateurs sont fréquemment modifiés, il est quasiment impossible de dévoiler leur identité.

Cependant, le spectre des données personnelles que ces applications collectent, traitent et partagent peut être très large et difficile à comprendre pour les utilisateurs. Dans de nombreux cas, les applications continuent à fonctionner en arrière-plan même lorsque l'appareil n'est pas utilisé. Certaines applications peuvent également échanger des informations avec d'autres applications par le biais d'interfaces de programmation d'application (API), générant ainsi des informations plus détaillées. Si l'Organisation mondiale de la santé (OMS) a salué les mesures de traçage étendues prises par la Corée, certaines utilisations, par les autorités locales, des données recueillies au moyen de l'application de suivi GPS sur les mouvements des cas confirmés ont soulevé des inquiétudes quant au respect de la vie privée. En réponse, le gouvernement coréen a récemment publié une directive limitant son utilisation à la divulgation des mouvements des cas confirmés conformément à la loi sur le contrôle et la prévention des maladies infectieuses adoptée en 2010, qui n'autorise la divulgation d'aucune information propre à la personne concernée.

L'exploitation des données biométriques s'accompagne à la fois d'avantages et de défis

La reconnaissance faciale a été l'une des données biométriques les plus fréquemment utilisées dans plusieurs pays pour surveiller la propagation de l'épidémie de COVID-19. La reconnaissance faciale permet aux autorités de réduire l'utilisation des technologies d'identification qui nécessitent un contact physique (comme la reconnaissance de l'iris et les empreintes digitales). Elle peut également être associée à d'autres technologies, notamment l'imagerie thermique améliorée par l'intelligence artificielle, afin de renforcer le suivi des citoyens susceptibles d'être testés positifs au COVID-19.

En Pologne, le gouvernement a lancé une application biométrique pour smartphone afin de confirmer que les personnes infectées par le COVID-19 restent en quarantaine. En République populaire de Chine (ci-après dénommée la « Chine »), la reconnaissance faciale a été utilisée pour empêcher les citoyens susceptibles d'être infectés par le COVID-19 de se déplacer. En outre, des entreprises chinoises ont mis au point une technologie qui pourrait permettre au gouvernement de réussir à identifier les personnes même lorsqu'elles portent un masque. En Fédération de Russie, des systèmes de reconnaissance faciale sont utilisés pour suivre les personnes qui ne respectent pas la quarantaine obligatoire.

Toutefois, le recours à la biométrie (y compris la reconnaissance faciale) en réponse à la pandémie de COVID-19 soulève un certain nombre de préoccupations en matière de protection de la vie privée et de sécurité, notamment lorsque ces technologies sont utilisées en l'absence d'orientations spécifiques ou de consentement explicite et pleinement éclairé. Les individus peuvent également rencontrer des difficultés dans l'exercice d'un large éventail de droits fondamentaux, notamment le droit d'accès aux données à caractère personnel qui les concernent, le droit à l'effacement et le droit d'être informés des finalités du traitement et des destinataires auxquels ces données sont communiquées. Les systèmes de reconnaissance faciale peuvent également présenter des biais technologiques inhérents, par exemple lorsqu'ils sont basés sur la race ou l'origine ethnique.

L'intégration de la protection de la vie privée aux critères de conception peut contribuer à réduire les risques

L'intégration de la protection de la vie privée aux critères de conception vise à assurer un niveau maximal de confidentialité en garantissant que des protections des données personnelles sont incluses par défaut dans le système. Cette solution peut, par exemple, impliquer l'utilisation de données agrégées, anonymisées ou pseudonymes afin d'offrir une protection supplémentaire de la vie privée, ou la suppression des données une fois leur objectif atteint.

Par exemple, l'application pour le COVID-19 développée par l'Institut norvégien de santé publique est conçue pour conserver des données de localisation pendant une période maximale de 30 jours. L'utilisation de solutions supplémentaires visant à renforcer la protection de la vie privée (comme le chiffrement homomorphe)[1] peut apporter une sécurité accrue, tout comme l'utilisation de bacs à sable de données, dans le cadre desquels l'accès à des données (personnelles) hautement sensibles n'est accordé que dans un environnement numérique et/ou physique restreint, à des utilisateurs de confiance. Un exemple de cette dernière solution est fourni par Flowminder, qui a collaboré avec des sociétés de télécommunications lors de l'épidémie d'Ebola de 2014-16 pour fournir aux épidémiologistes un accès sécurisé à des données de géolocalisation à faible résolution et dépersonnalisées. Flowminder utilise une stratégie similaire pour contribuer à la réponse à la crise du COVID-19.

Principales recommandations

Les technologies numériques offrent aux pouvoirs publics des outils puissants dans leurs efforts visant à contrôler la pandémie de COVID-19, mais il importe de reconnaître leurs implications en matière de protection de la vie privée et des données. Les applications de traçage des contacts doivent être mises en œuvre en toute transparence, en concertation avec les principales parties prenantes, avec l'intégration de solides protections de la vie privée aux critères de conception et dans le cadre de projets *open source* (le cas échéant). Les gouvernements devraient tenir compte des éléments suivants :

- Le fondement juridique de l'utilisation de ces technologies, qui varie selon le type de données collectées (par exemple, données personnelles, sensibles, pseudonymisées, anonymisées, agrégées, structurées ou non structurées).
- Le caractère proportionné de l'utilisation de ces technologies et de la collecte de données qui en découle, la manière dont les données sont conservées, traitées et partagées, et les destinataires de ces données (y compris les protocoles de sécurité et de protection par défaut de la vie privée mis en œuvre).
- La qualité des données collectées et leur adéquation à l'objectif visé.
- La qualité de l'information fournie au public, et le respect de principes de transparence et de responsabilité dans les approches adoptées.
- Le délai pendant lequel des technologies plus invasives qui collectent des données à caractère personnel peuvent être utilisées pour lutter contre la crise. Les données ne devraient être conservées que pendant la durée nécessaire à la réalisation de la finalité spécifique pour laquelle elles ont été collectées.

[1] Il permet de traiter des données cryptées sans révéler les informations qui y sont intégrées.

Pour aller plus loin

OCDE (2019a), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Éditions OCDE, Paris, https://doi.org/10.1787/276aaca8-en.

OCDE (2019b), *Recommandation du Conseil sur l'intelligence artificielle*, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449.

OCDE (2017), *Recommandation du Conseil sur la gouvernance des données de santé*, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0433.

OCDE (2015), « Mobile technology-based services for global health and wellness: Opportunities and challenges », page Web, OCDE, Paris, www.oecd.org/sti/ieconomy/mobile-technology-based-services-for-global-health.htm.

OCDE (2013), *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel,* OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188.

L'OCDE réunit des données, des informations, des analyses et des recommandations relatives aux défis sanitaires, économiques, financiers et sociétaux soulevés par les conséquences de la crise du COVID-19. Pour des informations complètes sur le coronavirus, rendez-vous sur notre page dédiée.