Traçage des données mobiles dans la lutte contre le Covid-19

Analyse des potentiels et des limites

Référencement des méthodes
et des exemples étrangers

NOTE PARLEMENTAIRE

Version 1.0 du lundi 6 avril 2020

Ce document a vocation à s'enrichir au fur et à mesure des retours et participations de ses lecteurs. Pour toute proposition, écrivez à : mounir.mahjoubi@assemblee-nationale.fr

Mounir MAHJOUBI, député de Paris

RestezChezVous

LE NUMÉRIQUE AU SERVICE DE LA SANTÉ ET DES LIBERTÉS

Le monde compte désormais plus de 3,4 milliards de personnes confinées. Bien que coupées physiquement de leur famille, de leurs proches et de leurs collègues, elles n'en demeurent pas moins connectées à leurs communautés. Les liens sociaux et le sentiment d'appartenance survivent grâce à Internet et à la téléphonie. En cette période d'isolement, ces technologies n'ont jamais été aussi précieuses pour l'Humanité. Et elles peuvent le devenir plus encore par l'utilisation du traçage des données mobiles afin de contrarier la propagation du SARS-CoV-2. La gravité de la situation appelle à se saisir de tous les moyens à disposition, sans toutefois compromettre nos valeurs et nos libertés. Il en va de la confiance en nos institutions.

De nombreux pays y réfléchissent. La Chine, Taïwan et la Corée du Sud exploitent de nombreux leviers technologiques, parfois avec succès, mais en questionnant les libertés. Des pays leur ont emboîté le pas, à l'image d'Israël et de la Pologne. D'autres, tels que la France, l'Allemagne et les Etats-Unis, y songent avec précaution. De nombreux chercheurs sont mobilisés dans une réflexion qui mêle santé publique, informatique et droits fondamentaux.

Le débat éthique est ouvert et des avis parfois tranchés s'expriment à travers le monde : pour certains, on doit pouvoir utiliser toute technologie disponible si c'est au service des vies sauvées et de l'intégrité de l'Etat ; pour d'autres, il faudrait au contraire se priver de tout usage de ces technologies au nom de la protection des libertés individuelles. Entre ces deux voies extrêmes, la plupart des Etats trace un chemin d'équilibre qui correspond à leur histoire et à leurs valeurs.

Le 27 mars, la revue scientifique Nature Medicine pose ainsi les termes du débat : l'éthique ne doit pas nécessairement fermer la porte à la géolocalisation des personnes mais doit encadrer ses usages. La CNIL rappelle que tous les usages ne se valent pas : les modalités d'application sont aussi nombreuses que variées. L'éthique impose de les sélectionner suivant des principes de proportionnalité, de transparence, de temporalité réduite et de contrôle par le Parlement, par des autorités indépendantes et par la société civile. Aussi, le débat ne doit pas porter sur l'usage du traçage mobile de manière générale. Il doit amener à s'interroger sur chacune des modalités envisageables. Si le diable réside souvent dans les détails, les solutions s'y trouvent également.

Certaines méthodes de *tracking* et de *backtracking*, qui s'appuient sur des données anonymes ou nominatives, proposent un équilibre entre la préservation des libertés individuelles et la protection sanitaire des citoyens. Sous certaines conditions, leur rapport bénéfice/risque peut être supérieur à celui du non-recours.

Ce document d'analyse a pour vocation d'alimenter utilement le débat public sur l'utilisation des données mobiles des citoyens en situation d'épidémie exceptionnelle et grave. Fondé sur une revue de presse française et internationale, il expose la diversité des solutions et leurs implications technologiques et éthiques. Cette note n'exprime pas mon avis personnel. Elle est un outil à la main du Parlement, des autorités en charge et de tous les citoyens pour les aider à mieux appréhender le sujet dans sa complexité. Il s'agit de penser et de construire ensemble les meilleures solutions pour la France.

Mounir MAHJOUBI

Traçage des données mobiles dans la lutte contre le Covid-19

Analyse des potentiels et des limites

Synthèse

L'usage du traçage des données mobiles dans la lutte contre la pandémie de Covid-19 répond à trois finalités :

1. L'observation des pratiques collectives de mobilité et de confinement *(i.e. cartographie des déplacements de population)*.
2. L'identification des sujets *"contact" (i.e. backtracking ou contact tracking)*.
3. Le contrôle des confinements individuels *(i.e. tracking ou bracelet électronique virtuel)*.

Plusieurs technologies supportent ces usages à travers le monde :

- le bornage téléphonique,
- des applications GPS,
- des applications Bluetooth,
- les systèmes de cartes bancaires et de transport,
- la vidéosurveillance, dotée ou non d'intelligence artificielle.

Chaque couple de technologie et usage témoigne d'un potentiel et de limites propres. Et chacun d'eux amène à une réflexion éthique particulière. Aussi, seule une analyse détaillée des méthodes permet d'apprécier les possibilités d'un juste équilibre entre les objectifs de santé publique et la préservation des libertés individuelles.

Les cartographies de mobilités collectives (1er usage) sont utiles aux stades 1 et 2 de l'épidémie. Elles suscitent peu de contestation éthique. Des opportunités existent pour les exploiter davantage à des niveaux géographiques plus fins. Pour cela, de nombreux opérateurs mobiles et fournisseurs d'application se disent disposés à travailler avec les autorités sanitaires.

L'identification des sujets *"contact"* (2ème usage) est très utile aux stades 1 et 2, ainsi que pour éviter un rebond après un stade 3. Elle alimente cependant des inquiétudes justifiées quant à la protection de la vie privée. Ces inquiétudes doivent amener à délimiter les recours aux possibilités techniques, mais non à les exclure complètement. La question du consentement de l'utilisateur est débattue dans de nombreux pays. En la matière, les applications Bluetooth de *contact tracing* semblent créer un

consensus du fait de leur aspect plus protecteur des libertés individuelles. Pour autant, elles n'ont pas encore fait la preuve de leur efficacité sanitaire. Des applications GPS sans remontée automatique offrent également d'intéressantes opportunités protectrices des données personnelles. Dans certains pays, des dispositifs étatiques de collecte et traitement massif de données sans consentement des utilisateurs ont été mis en place dans le cadre de mesures exceptionnelles. L'efficacité réelle de ces dispositifs reste à ce jour mal évaluée.

Enfin, le contrôle du confinement à domicile (3ème usage) est utilisé à tous les stades de l'épidémie ; aux stades 1 et 2 pour les quarantaines des personnes malades et au stade 3 pour le confinement plus général de la population. Il pose un défi pleinement éthique mais moins technologique. Il pose la question de la coercition par les autorités des règles de confinement au niveau individuel. Quel contrôle et quelles sanctions ? Plus éloignés des cultures de nombreux pays d'Europe, dont la France, ces dispositifs sont pleinement utilisés en Asie.

Les opportunités offertes par les nouvelles technologies ont pour clé de voûte l'acceptation populaire. Celle-ci repose sur plusieurs exigences, dont une proportionnalité des méthodes aux objectifs, une pleine transparence des pratiques, et notamment des codes informatiques, et une véritable gouvernance indépendante de contrôle, en capacité d'évaluer efficacement et à tout moment les pratiques et leurs performances sanitaires.

Pour un débat utile et éclairé sur le sujet, l'analyse doit être nourrie. Ce document a pour vocation d'y contribuer. Pour chacun des trois usages annoncés, il détaille les technologies et les modalités à considérer. Il présente les avantages et les limites techniques. Il aborde les implications éthiques et les modulations envisageables. Enfin, il procure des exemples d'implémentations à l'étranger.

Ce document a été réalisé avec mon équipe parlementaire dans les conditions actuelles de confinement, sa pertinence et son exhaustivité seront renforcées par les retours et participations de ses lecteurs. Des versions augmentées seront régulièrement proposées. Pour toute proposition, écrivez à : mounir.mahjoubi@assemblee-nationale.fr.

Sommaire

1er usage

Observer les pratiques collectives de mobilité et de confinement

(i.e. cartographie des déplacements de population)

Finalités : → *Obtenir une vision nationale et régionale*
→ *Obtenir une vision affinée à l'échelle d'un quartier*

Techniques : *1) Traitement des données issues du bornage des opérateurs télécoms*
2) Traitement de données GPS issues d'applications mobiles
3) Système de cartes bancaires

L'observation des mouvements de population à travers le territoire est l'usage le plus respectueux des libertés individuelles et de la vie privée. Il est ainsi particulièrement répandu dans le monde, et notamment en Europe. La France y a elle-même recours, comme en témoigne le récent partenariat entre Orange et l'Inserm.

La méthode repose sur des données collectives et anonymisées transmises par les opérateurs téléphoniques qui permettent la construction d'une vue d'ensemble. L'identification d'une personne en particulier est impossible.

Pour l'Etat, l'enjeu de données fiables et détaillées sur les mouvements de population est double :

- A l'échelle nationale et régionale : Adapter par anticipation les capacités médicales, sociales et sécuritaires en fonction du nombre réel de personnes présentes à un endroit donné.
- A l'échelle d'un quartier : Détecter les espaces publics anormalement fréquentés en temps de confinement pour permettre d'adapter localement les réponses sociales, sanitaires et sécuritaires.

1er usage : Observer les pratiques collectives de mobilité et de confinement

Technique 1 : TRAITEMENT DES DONNÉES ISSUES DU BORNAGE DES OPÉRATEURS TÉLÉCOMS

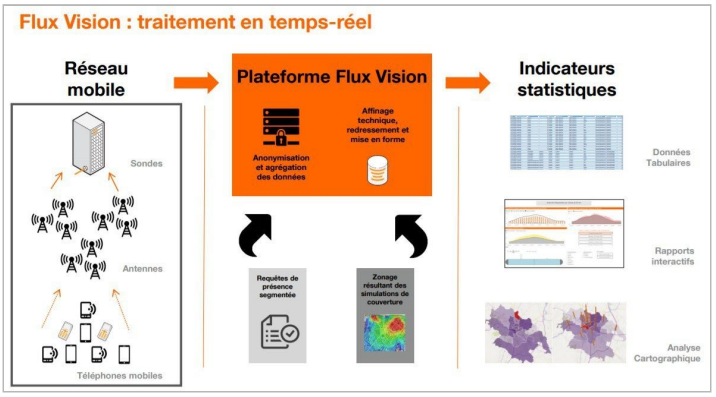
Comment ça marche ?

Pour transmettre ou recevoir de l'information, qu'il s'agisse d'un appel, d'un SMS ou d'un accès à Internet, les téléphones mobiles se connectent à l'antenne relais la plus puissante étant à leur proximité. Lors des transferts de données, les opérateurs enregistrent des informations de connexion et les conservent en mémoire durant une année. Il leur est alors possible d'attester de la présence d'un téléphone autour d'une borne, dans un périmètre donné, avec un historique de 12 mois. Orange, Free, SFR et Bouygues Télécom se partagent en France 40 000 pylônes relais.[1]

Antenne relais [2]

Les opérateurs font usuellement commerce de ces données, notamment auprès de collectivités locales qui souhaitent mieux observer et comprendre leurs flux touristiques ou de mobilité. Dans la présentation de son offre Flux Vision, Orange déclare transformer 140 millions de données européennes par minute.[3]

[1] *LeFigaro.fr. Caroline Piquet. Bornage : comment les enquêteurs font parler les téléphones des suspects. 11 janvier 2018.*
[2] *Photo Jacques Demarthon. AFP. Présente ici dans un article de Libération datant de 2011.*
[3] *Site Orange Business. Valeur correspondant à l'année 2019.*



Flux Vision [4]

Les données de bornage s'avèrent précieuses pour mieux informer les modèles épidémiologiques. L'enjeu est de prévoir au mieux la propagation territoriale du virus pour adapter localement et par anticipation les capacités médicales.

Une autre application des données de bornage serait de constater de façon anonyme le respect collectif des règles de confinement à l'échelle d'un quartier, d'une rue ou d'une place. Elles pourraient en effet renseigner sur les espaces publics anormalement fréquentés. L'Etat pourrait alors adapter localement ses interventions sociales, sanitaires et sécuritaires.

Cette application, trop peu utilisée, pourrait constituer une nouvelle opportunité pour les autorités. Elle nécessiterait de demander aux opérateur de s'engager contre le Covid-19, comme d'autres l'ont fait à l'étranger.

Quels sont les avantages ?

Les données de bornage sont générées automatiquement et conservées un an dès lors qu'une personne utilise son téléphone portable.

Contrairement au traçage par GPS, aucune activation n'est requise côté utilisateurs.

Les données sont agrégées et anonymisées par les opérateurs avant leur partage aux autorités. En ce sens, la méthode respecte le RGPD.

Quelles sont les limites technologiques ?

L'utilisation de ces informations offre une vue de haut volontairement floue. C'est à la fois son avantage en termes de protection des libertés individuelles et son principal défaut en termes opérationnels.

[4] *https://www.cerema.fr/system/files/documents/2018/04/5_Pimont-Strambi_0.pdf*

Quels enjeux éthiques ?

A l'échelle régionale ou urbaine, les données de bornage, une fois agrégées et anonymisées permettent un usage strictement respectueux du RGPD. Les méthodes sont éprouvées techniquement et légalement par plusieurs années d'usages commerciaux.

La question est plus sensible s'agissant d'agrégations réduites à un quartier, une rue ou une place. Certes plus utiles, ces informations deviennent aussi plus sensibles. Convenablement exploitées, elles permettraient un meilleur respect du confinement. Rendues publiques, sans explications et mal interprétées, elles pourraient mener à stigmatiser injustement des groupes d'habitants.

Pour les données à l'échelle réduite, les considérations éthiques pourraient ainsi mener à se poser la question :

- d'un usage par les autorités sans diffusion publique des données ;
- de la mise en place d'une gouvernance indépendante de contrôle de ces usages.

Quels sont les exemples d'utilisation ?

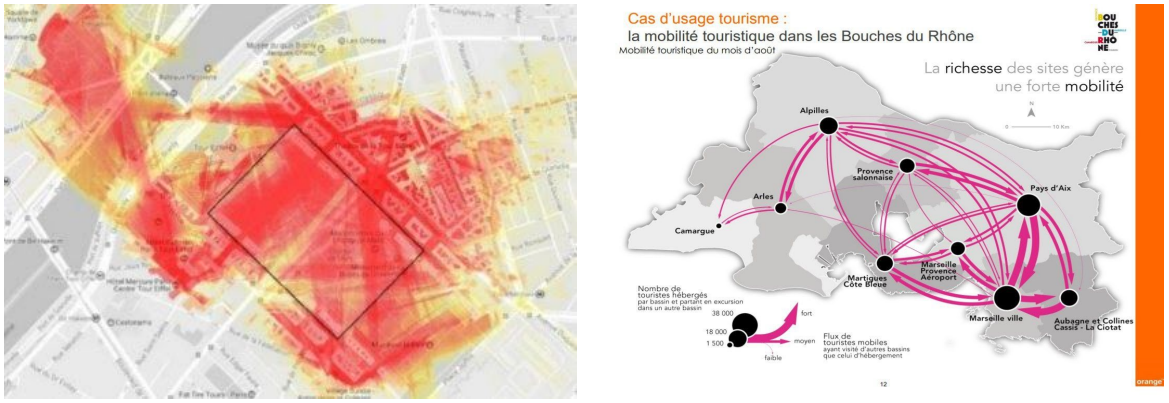
FRANCE

Partenariat Orange Inserm : Observer les pratiques collectives de mobilité [5]

À l'annonce du confinement ou par anticipation, de nombreux ménages français ont migré vers leur résidence secondaire ou dans leur famille. À partir de ses données de bornage, Orange estime que 1,2 million de Franciliens ont quitté le Grand Paris entre le 13 et le 20 mars. Inversement, l'Île de Ré a vu sa population bondir de 30%.

L'ampleur des mobilités pré-confinement a rendu caduque les données injectées dans les modèles épidémiologiques. Pour y remédier, Orange transmet à l'Inserm des jeux de valeurs agrégées et anonymisées pour informer au mieux ses modèles.

D'autres opérateurs se sont dit prêts à participer à l'effort national.



Images tirés d'une présentation Orange Flux Vision [6]

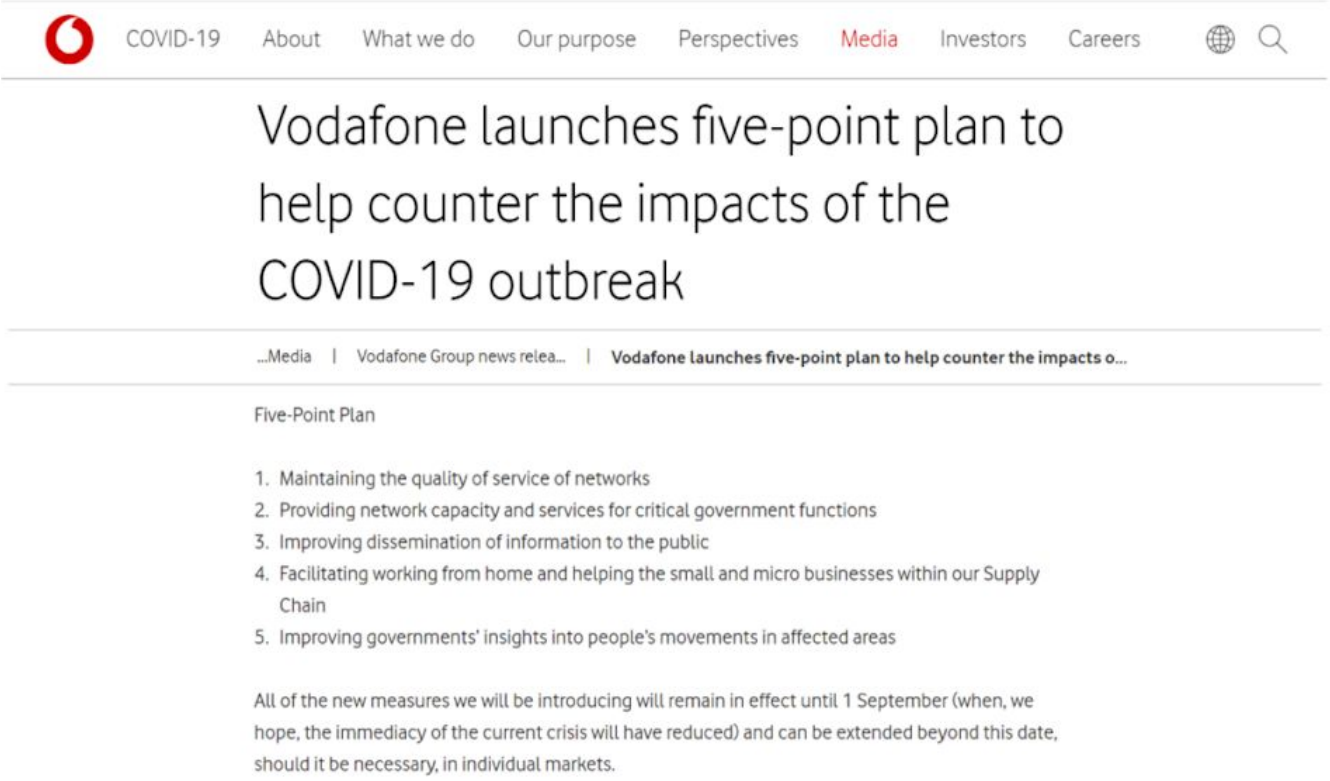
[5] *LeParisien.fr. Damien Licata Caruso. Plus d'un million de Franciliens ont quitté la région parisienne avant le confinement : comment Orange le sait. 26 mars 2020.*
[6] *https://www.cerema.fr/system/files/documents/2018/04/5_Pimont-Strambi_0.pdf*

ITALIE

Observer les pratiques collectives de confinement à l'échelle d'une ville

En l'absence de contrôle adéquat, certaines personnes ne respectent pas scrupuleusement le confinement. Grâce aux données transmises par les opérateurs de téléphonie, les autorités italiennes ont observé mi-mars que 40% des Milanais confinés effectuaient encore des déplacements de plus de 300 mètres. Les autorités ont donc renforcé la coercition. Le taux de verbalisation a atteint 3% de la population. Celui des déplacements a lui été réduit à 14% début avril.[7]

Vodafone déclare livrer régulièrement à l'Etat italien des cartes de densité et de déplacement de mobiles anonymisés.[8]



Le plan de l'opérateur Vodafone pour lutter contre le coronavirus en 5 étapes

[7] *Reportage France 2. Journal de 20 heures du 5 avril 2020. Journaliste : Alban Mikoczy.*
[8] *Site de Vodafone. Vodafone launches five-point plan to help counter the impacts of the COVID-19 outbreak. 18 mars 2020.*

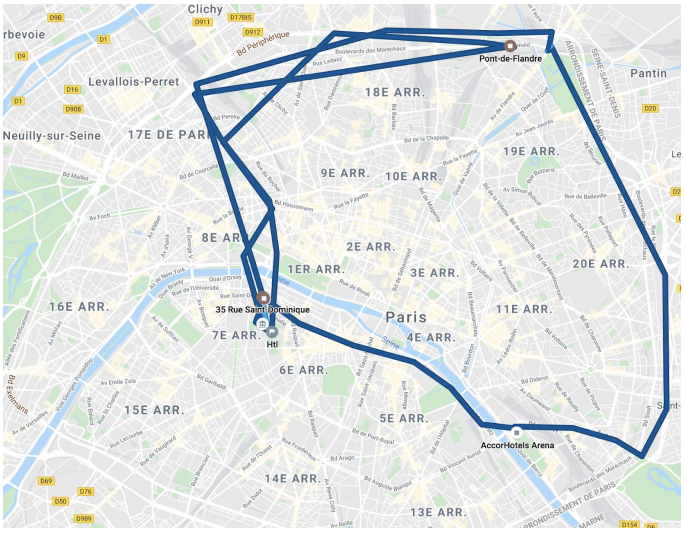
Technique 2 : TRAITEMENT DE DONNÉES GPS ISSUES D'APPLICATIONS MOBILES

Comment ça marche ?

La technologie GPS repose sur une constellation de satellites pour effectuer une géolocalisation précise où que l'on soit dans le monde.

Pour fonctionner, de nombreuses applications mobiles récupèrent et stockent les coordonnées GPS de leurs utilisateurs. Il en va ainsi d'applications populaires, telles que Google Maps, Waze, Facebook, Instagram, Whatsapp ou encore Lime.

Les historiques ainsi constitués par les applications les plus utilisées peuvent ainsi être agrégés et anonymisés pour témoigner de mouvements de population à l'échelle d'un continent, d'un pays, d'une ville ou d'un quartier.



Exemple d'historique de données GPS Google Maps d'un utilisateur parisien.

Quels sont les avantages ?

Près de 8 Français sur 10 possèdent un *smartphone*. Une large majorité utilise déjà régulièrement une application populaire qui collecte leurs coordonnées GPS, à l'image de Google Maps (Android) ou d'Apple Plans (IOS).

Quelles sont les limites technologiques ?

Le fonctionnement de la puce GPS suppose une activation côté utilisateurs et l'activation d'une application.

De nombreuses applications installées sur les téléphones collectent déjà des données de géolocalisation pouvant être valorisées dans la lutte contre l'épidémie de Covid-19. L'un des enjeux

est d'identifier ces fournisseurs de services pour ensuite envisager comment leurs informations pourraient être employées dans le respect des libertés individuelles et de la vie privée. Voir les exemples ci-dessous, dont Covimoov par Geo4Cast.

Quels enjeux éthiques ?

D'abord de nature individuelle, les historiques de localisation GPS sont agrégés et anonymisés par les éditeurs avant toute diffusion.

Les agrégats à l'échelle d'une ville ou d'un quartier amènent à s'interroger sur les usages qui peuvent être envisagés et sur le risque de stigmatisation de ceux qui y habitent.

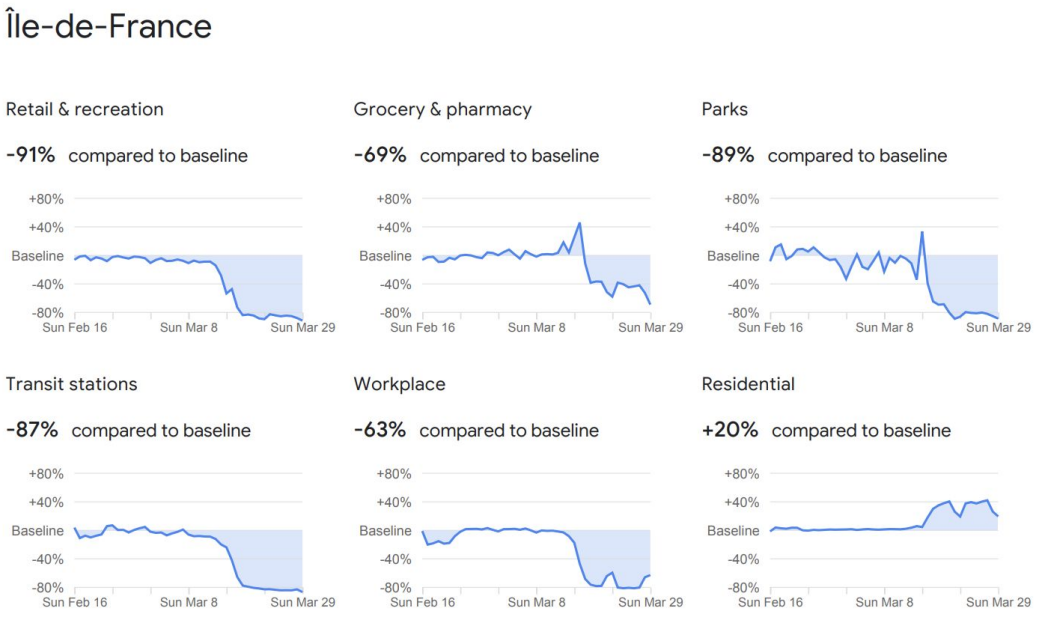
Quels sont les exemples d'utilisation ?

GOOGLE

Community Mobility Reports : Observer les pratiques collectives de fréquentation

Google propose à ses utilisateurs d'enregistrer en continu leurs déplacements et de maintenir l'historique à leur disposition. Compte tenu d'une colossale base d'utilisateurs, Google dispose d'un volume critique de données. Depuis le 3 avril, la société produit des rapports nationaux portant sur la fréquentation des espaces de vie (logements, bureaux, boutiques, parcs et transports). Pour la France, un détail régional est disponible.

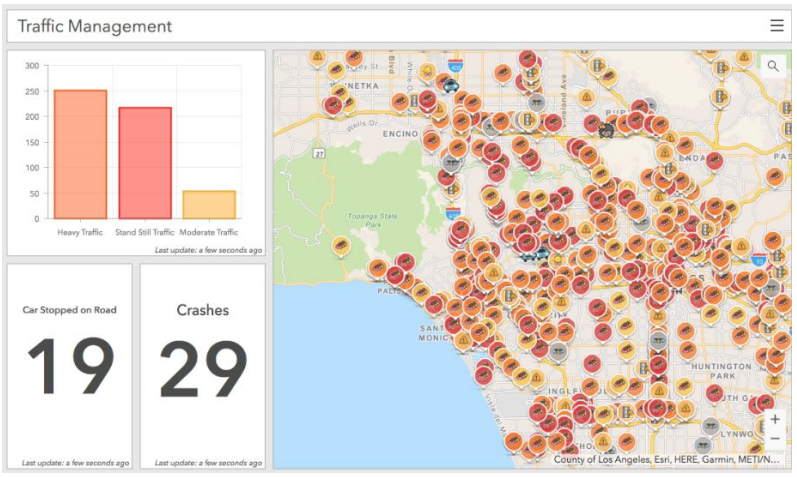
Dans le contexte actuel d'effort sanitaire, ces publications présentent en l'état peu d'intérêt. Google explique agir dans la limite des conditions d'utilisation acceptées par les utilisateurs.



Les changements de mobilité des Français en raison de la Covid-19

WAZE

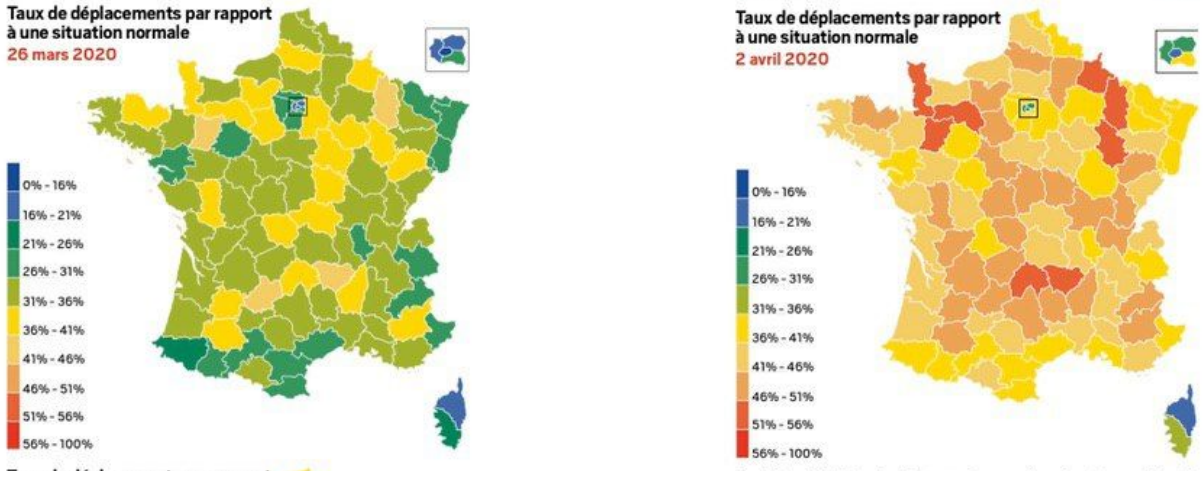
A l'instar des opérateurs téléphoniques, Waze valorise ses données de déplacements au profit des villes. Son service *Waze for Cities Data* permet de percevoir les trajets routiers de millions d'utilisateurs. Cette fonctionnalité accompagne des villes dans leurs plans de transports et d'infrastructures. Elle pourrait également profiter aux autorités sanitaires lors d'épidémies.



Exemple de tableau de bord Waze sur l'état du trafic

GEO4CAST [9] [10]

Plusieurs applications intègrent déjà les services de Geo4Cast. Ceci leur permet de récolter de grandes quantités d'informations géographiques sur leurs utilisateurs. A partir de ces informations anonymisées, la société a produit un indicateur de déplacements. Cet indicateur sert à observer l'évolution des déplacements dans les territoires. Il est également à la base de l'application Covimoov, récemment développée.



Les taux de déplacements des Français par rapport à une situation normale les 26 mars 2020 et 2 avril 2020

[9] *Le JDD. Respect du confinement : les Français se relâchent. 5 avril 2020*
[10] *20 minutes. Y-a-t-il un relâchement des Français face au confinement ? 5 avril 2020*

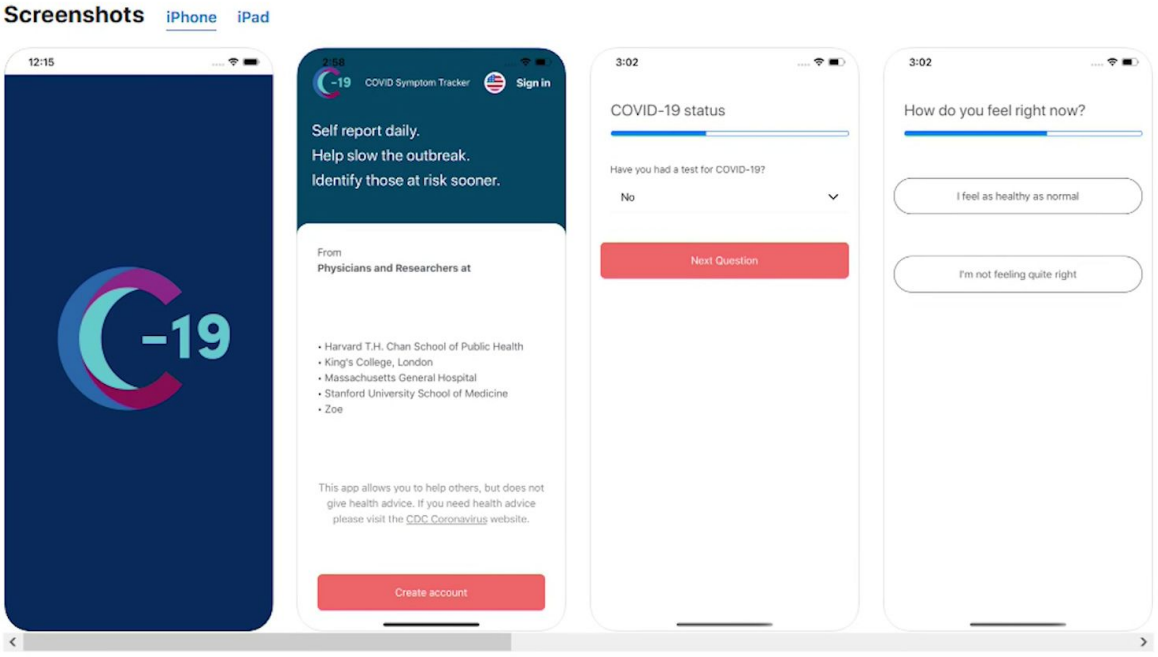
ROYAUME-UNI [11] [12] [13] [14]

C-19 Covid Symptom Tracker : Informer sur la propagation géographique de la maladie

En collaboration avec la *start-up* Zoe, des chercheurs du King's College ont récemment développé l'application C-19 Covid Symptom Tracker. Lors de la création d'un compte, des informations personnelles, telles que le code postal ou l'âge, sont demandées aux utilisateurs. Une fois l'application installée, il faut renseigner son état de santé quotidiennement. Les scientifiques et le NHS (National Health Service) peuvent ainsi observer en temps réel la propagation de la maladie sur le territoire.

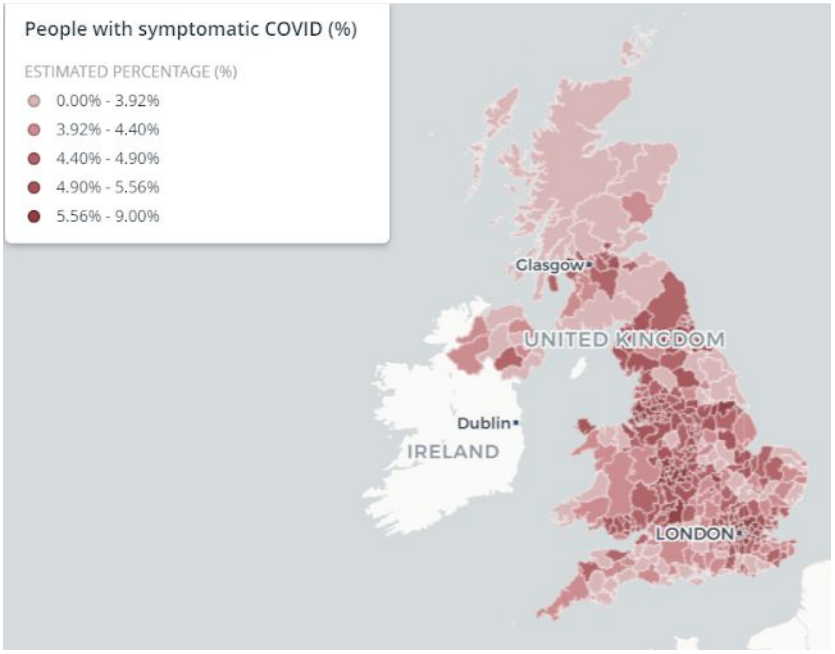
Bien que l'application ne soit pas un outil de diagnostic et ne serve pas à informer les utilisateurs de la propagation géographique de la maladie, elle permet néanmoins de réaliser des cartographies rendues publiques. Cet outil de recherche fournit des informations utiles aux professionnels de santé. Le NHS s'en sert pour étudier l'évolution du virus et pour allouer ses ressources de manière optimale.

Lancée le 24 mars au Royaume-Uni, l'application a connu un vif succès, avec plus de 750 000 téléchargements en 24 heures.



Captures d'écran de l'application C-19 Covid Symptom Tracker

[11] *2M.Une application lancée au Royaume-Uni pour limiter la propagation du nouveau coronavirus. 27 mars 2020*
[12] *Le Petit Journal. Une application pour découvrir où est le Covid-19 à Londres exactement. 26 mars 2020*
[13] *Site officiel de l'application : https://covid.joinzoe.com/*
[14] *Techcrunch. Self-reporting app tracking COVID-19 symptoms in UK sees 750K downloads in 24 hours. 25 mars 2020*



Exemple de carte publique produite grâce à l'application C-19 Covid Symptom Tracker

Technique 3 : SYSTÈME DE CARTES BANCAIRES

Comment ça marche ?

À chaque paiement ou retrait par carte bancaire, une autorisation est transmise à la banque. Le lieu de transaction est alors enregistré. Suivant cette information, une banque peut retracer les déplacements d'un client. En agrégeant les données, elle peut observer les mouvements de population et les taux d'activité à travers le territoire.

Peu usité, les banques et les réseaux de traitement de cartes bancaires disposent de données permettant de créer des informations utiles mais très inférieures aux données des opérateurs mobiles ou d'application GPS.

Quels sont les avantages ?

En France, plus de 50% des paiements sont réalisés par carte bancaire.

Quelles sont les limites technologiques ?

L'usage d'une carte de paiement ne renseigne pas le nombre de personnes qui accompagnent le propriétaire de la carte (conjoint, enfants, amis…).

Quels enjeux éthiques ?

Ils sont de même nature que ceux posés par l'usage des données agglomérées des opérateurs télécoms étudiées précédemment.

Quels sont les exemples d'utilisation ?

Pas d'exemple identifié.

2ème usage

Identifier les personnes *"contact"*

(i.e. backtracking ou contact tracking)

Finalités :
- *→ Retracer le parcours récent des personnes testées positives*
- *→ Informer la population des zones à risque*
- *→ Relever directement les contacts récents entre les individus testés positifs et des personnes tierces*

Techniques :
1) *Traitement des données issues du bornage des opérateurs télécoms*
2) *Traitement des données GPS issues d'applications mobiles*
3) *Traitement de connexions Bluetooth issues d'applications mobiles*
4) *Traitement des données issues des cartes bancaires et de transport*
5) *Traitement des données issues de la vidéosurveillance*

Pour endiguer l'épidémie de Covid-19, notamment aux stades 1 et 2, et pour éviter un rebond post-confinement, les experts recommandent d'identifier les personnes ayant récemment été au contact d'un sujet infecté. L'enjeu est de leur proposer un test de dépistage et d'opérer leur mise en quarantaine. Pour cela, il est nécessaire de retracer le parcours récent des patients testés positifs.

En France, les professionnels de santé recourent pour cela à des questionnaires individuels et des enquêtes de terrain. Or cela demande du temps et les discours, étant basés sur la mémoire des personnes, manquent souvent de précisions. En définitive, l'efficacité de la méthode est insuffisante. Aussi, plusieurs pays recourent au traçage de données mobiles pour compléter ces informations.

A partir des itinéraires des personnes testées positives, les autorités cherchent à définir deux types d'information :

- Identifier les lieux et zones qui ont présenté un ou plusieurs cas positifs. A l'échelle d'un quartier, d'un pâté de maison ou d'un lieu spécifique (magasin, bureaux, établissement scolaire, etc.) afin d'informer publiquement et/ou personnellement toutes les personnes qui ont pu y passer un certain temps.
- Faire la liste nominative des personnes ayant eu une interaction ou un contact rapproché et durable avec la personne infectée afin d'informer personnellement les personnes concernées.

S'il y a consensus sur le besoin d'identifier les personnes ayant eu une interaction rapprochée, les stratégies divergent toutefois. Selon les pays et les experts, l'utilité de rendre public les zones à risque et celle de contacter l'intégralité de personnes y ayant été détectées sont appréciées différemment.

Les applications mobiles basées sur le Bluetooth et sur les données GPS concentrent aujourd'hui toute l'attention. Cependant, un usage des données issues des opérateurs mobiles semble pouvoir offrir des perspectives, notamment pour identifier des zones ou des lieux.

2ème usage : L'identification des sujets "contact"

Technique 1 : TRAITEMENT DES DONNÉES ISSUES DU BORNAGE DES OPÉRATEURS TÉLÉCOMS

Comment ça marche ?

Pour transmettre ou recevoir de l'information, les téléphones mobiles se connectent à l'antenne relais la plus puissante étant à leur proximité. Lors des transferts de données, les opérateurs enregistrent des informations de connexion. Il leur est alors possible d'attester de la présence d'un téléphone autour d'une borne, dans un périmètre donné, avec un historique de 12 mois. En recourant aux données de bornage des abonnés testés positifs, les opérateurs sont en mesure de retracer leurs déplacements.

Dans certains pays, ces données peuvent être récupérées directement sans le consentement de la personne malade. Dans d'autres, on demande à la personne d'accepter que ses données opérateurs soient transmises à l'autorité.

Quels sont les avantages ?

Les données existent déjà. Il n'y a pas d'activation nécessaire coté utilisateurs.

Quelles sont les limites technologiques ?

La précision est médiocre : des précisions de plusieurs centaines de mètres sont courantes, au mieux de 10 mètres dans les grandes villes. En zone rurale, elle tombe à plusieurs kilomètres.

Dès lors, il peut être complexe d'identifier de façon certaine une personne ayant effectivement été au contact (< 1 mètre).

Néanmoins, ces données peuvent être utiles pour identifier des zones *cluster*. En réunissant l'historique des données de bornage de plusieurs centaines de personnes testées positives dans la même ville, on pourrait identifier de nouveaux noeuds de passage/quartier que l'enquête n'aurait pas décelé.

Quels enjeux éthiques ?

Consentement

Il s'agit là d'une utilisation de données personnelles nominatives particulièrement intrusives. Les différents pays qui recourent à cette méthode le font avec ou sans le consentement des personnes testées positives.

On parle de deux types de consentements :

- Celui de la personne testée positive à qui l'on peut proposer de refuser ou d'accepter ce *"backtracking"*.
- Celui des sujets identifiés comme *"contact"*. Afin de les identifier, il faut réunir un nombre important d'informations de toutes les personnes ayant été détectées près d'une borne. Se pose

alors la question de QUI y accède : soit l'opérateur, ainsi chargé d'informer lui-même l'utilisateur en l'invitant à se rapprocher des autorités, soit l'Etat à qui l'opérateur remettrait toutes les données. Les enjeux éthiques sont bien plus importants dans le second choix.

Stockage et utilisation des données

Avec ou sans consentement, se pose la question du risque provenant de la création d'une base de données entre les mains de l'Etat de tous les historiques de déplacement d'un nombre important de citoyens. Il s'agit d'un débat traditionnel en Europe sur la protection des données personnelles.

Cette question peut se résoudre en proposant plusieurs limitations :

- Durée de vie des données enregistrées et leur suppression progressive pour chaque utilisateur.
- Date limite d'utilisation du processus global limitée à la crise sanitaire.
- Utilisation stricte des données dans un seul but.
- Création d'une gouvernance indépendante de contrôle .

Les autorités nationales et européennes de protection des données personnelles ont toutes émis des recommandations afin de créer des cadres respectueux du RGPD.

Publicité des données

Les considérations éthiques mènent à poser la question des informations qui pourraient être rendues publiques. A la fois dans un but de transparence mais aussi de politique innovante d'Open Data, plusieurs pays ont fait le choix de rendre publiques de nombreuses informations de traçage mobile des personnes testées positives.

Si tous les pays ont fait le choix d'anonymiser les noms, les pratiques ont été diverses quant aux autres informations rendues publiques : adresse exacte de la personne, trajets et parcours individuels exhaustifs sur 14 jours, etc. D'autres pays se sont contentés de rendre uniquement publics les zones et lieux sans possibilité de retracer le parcours d'une personne donnée.

Quels sont les exemples d'utilisation ?

TAIWAN

Un itinéraire rendu public

Lorsqu'une personne est testée positive au SARS-CoV-2, les autorités taïwanaises obtiennent de son fournisseur téléphonique son itinéraire récent. Les lieux et les moments à risque sont identifiés et publiquement dévoilés. Pour chaque cas confirmé, le sexe, l'âge, l'itinéraire récent et les symptômes sont rendus publics. Le croisement de différentes sources d'information permet parfois de découvrir l'identité des personnes.

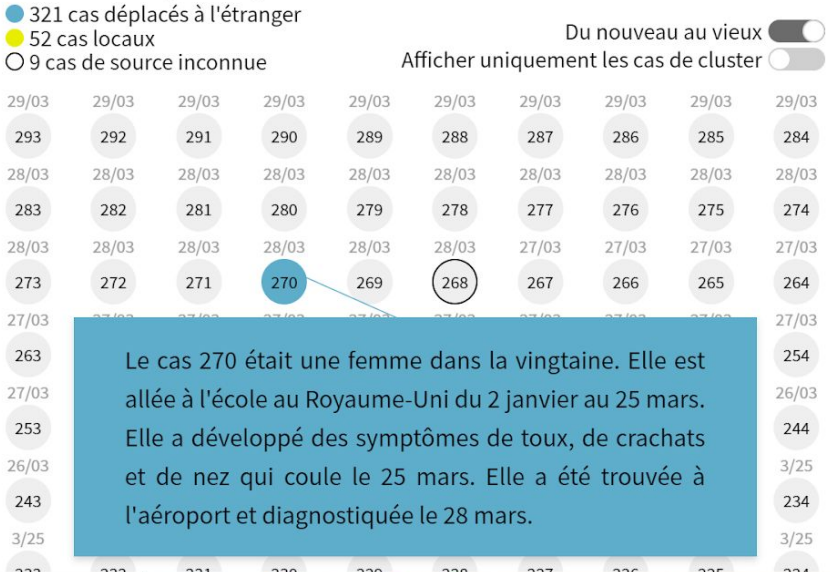


Image tirée du site internet du journal taïwanais United Daily News

ISRAËL [15] [16] [17]

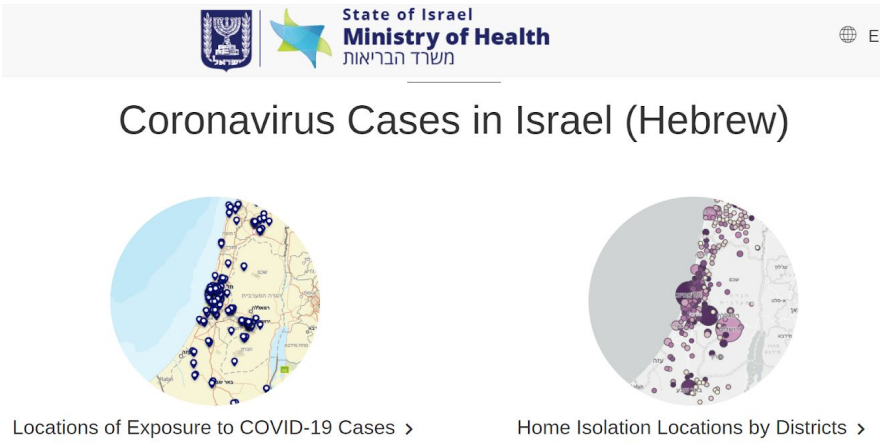
Un recours aux données de bornage par les services secrets

Le 16 mars, l'Etat israélien a étendu pour 30 jours les prérogatives du service de renseignement intérieur, le Shin Bet, à l'identification des sujets *"contact"*. Officiellement, le Shin Bet ne peut conserver les données recueillies plus de 14 jours.

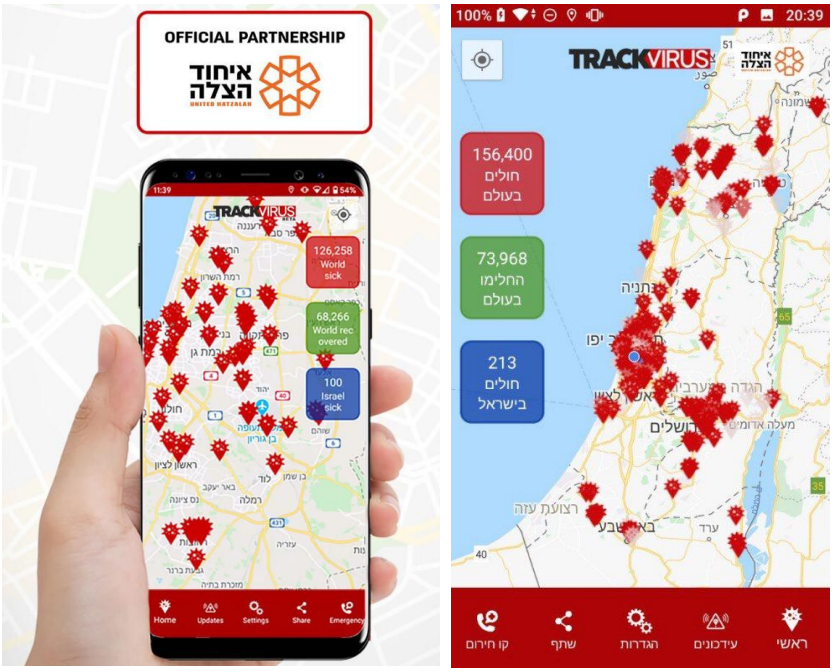
C'est la méthode du bornage téléphonique qui semble être utilisée, bien qu'aucune communication officielle n'en fasse état. Les identités relevées sont transmises au ministère de la santé. Celui-ci informe les personnes de leur mise en quarantaine par SMS.

[15] *Site du Ministère de la Santé israélien. Rubrique News.*
[16] *Site du Ministère de la Santé israélien. Rubrique coronavirus*
[17] *LeMonde.fr. Louis Imbert. Coronavirus : Israël approuve des méthodes de surveillance électronique de masse. 17 mars 2020.*

Les parcours des malades sont rendus publics sur le site du ministère de la santé. Ce site permet d'ailleurs d'alerter les autorités d'un non respect de l'isolation. Il met à jour la liste des patients positifs et spécifie les endroits par lesquels ils sont passés. Enfin, il renseigne les endroits où les individus sont en quarantaine.



Des éditeurs de logiciel tirent partie de ces données publiques. En témoigne l'application TrackVirus, développée en partenariat avec United Hatzalah, une organisation israélienne de secouristes et d'urgentistes.



Capture d'écran de l'application israélienne TrackVirus

CORÉE DU SUD

La Corée du Sud rend publics les déplacements récents des personnes testées positives au Covid-19. Au début de l'épidémie, bien que l'identité des patients était maintenue secrète, l'Etat publiait certaines informations personnelles, comme l'âge, le sexe ou encore le quartier de résidence. Il s'est avéré que ces informations, recoupées avec d'autres, pouvaient permettre d'identifier les patients. La Corée du Sud a donc réduit les informations dévoilées pour éviter les reconnaissances. Les lieux de passage demeurent publics. Ils sont à l'origine de nombreuses applications qui informent leurs utilisateurs.

2ème usage : L'identification des sujets "contact"

Technique 2 : TRAITEMENT DES DONNÉES GPS ISSUES D'APPLICATIONS MOBILES

Comment ça marche ?

Trois usages des données GPS permettent d'identifier les sujets *"contact"* :

1. **Retracer le parcours récent des personnes testées positives**

   Comme pour l'historique de bornage, une application se charge d'enregistrer le parcours réalisé par une personne. Si, *in fine*, celle-ci est testée positive, ces informations peuvent être partagées avec les autorités avec ou sans le consentement de la personne.

2. **Informer la population des zones à risque**

   Pour s'informer de leur passage dans les zones à risque, ou pour les éviter, les utilisateurs installent une application mobile qui enregistre leurs déplacements et les compare à une carte publique et actualisée des zones à risque. Ainsi informés, les utilisateurs peuvent eux-mêmes, le cas échéant, solliciter un dépistage et pratiquer une distanciation sociale plus rigoureuse. Cet usage ne nécessite pas de partager ses informations personnelles avec les autorités.

3. **Relever directement les contacts récents entre les individus testés positifs et des personnes tierces**

   Les utilisateurs installent une application mobile qui enregistre les contiguïtés avec les autres utilisateurs. Lorsqu'un utilisateur est testé positif, il se déclare afin que tous les utilisateurs qu'il a rencontré puissent être informés d'une situation à risque.

Quels sont les avantages ?

Près de 8 Français sur 10 possèdent un *smartphone* et emportent donc avec eux une puce GPS. Dans leur majorité, ils sont habitués aux applications qui exploitent leurs coordonnées GPS en contrepartie d'un service.

En extérieur, la précision des GPS est relativement bonne : de 5 mètres à seulement 30 centimètres.

Quelles sont les limites technologiques ?

La localisation GPS peut ne pas fonctionner, ou manquer de précision, dans certains espaces confinés (supermarchés, métro).

L'installation d'une application et l'activation de la puce GPS sont nécessaires pour que la position soit transmise à un acteur tiers (éditeur de logiciels, autorité publique).

Pour identifier efficacement les sujets *"contact"*, une application doit être utilisée par un nombre important d'utilisateurs dans la population (de 25 à 60 % selon différentes sources). Le seuil étant difficile à atteindre, le succès repose sur d'importants efforts de communication : promotion dans les

médias, appui du gouvernement, recommandations des professionnels de santé… Une solution alternative serait de rendre l'installation obligatoire, au détriment toutefois des libertés individuelles.

Quels enjeux éthiques ?

Informations montantes et descendantes

Les enjeux éthiques sont différents selon qu'il s'agit d'une application montante, qui envoie les données de l'utilisateur vers un serveur, ou s'il s'agit d'une application descendante, qui reçoit les données de risque et les compare dans le téléphone sans aucune transmission de données personnelles à l'extérieur.

En cas d'information montante, on se retrouve dans la même réflexion éthique que pour la technique 1 du bornage. Dans le cas des informations descendantes, les libertés des utilisateurs sont bien mieux protégées.

Concernant les historiques des proximités, ils peuvent être enregistrés de manière cryptée sur la mémoire interne des téléphones et sans inclure l'identité de la personne (on utilise un code de référence lié à son téléphone). Des modèles de gestion associative, ou décentralisée, peuvent aussi être établis.

Une transparence complète sur le code informatique peut être envisagée, ainsi qu'un audit indépendant sur le caractère éthique et la sécurité du code.

Consentement à l'installation de l'application

L'efficacité des applications qui recueillent la proximité entre utilisateurs repose sur une masse critique. Suivant le journal Les Echos, une telle application est efficace si 60% de la population l'utilise et qu'une campagne de dépistage y soit associée.[18] Il s'agit là d'un seuil élevé et les autorités pourraient ainsi être tentées de recourir à des mesures coercitives pour motiver les installations, telles qu'une obligation d'usage. Cette obligation pourrait être rendue possible par l'intermédiaire des opérateurs mobiles ou des fournisseurs de système d'exploitation des téléphones.

Quels sont les exemples d'utilisation ?

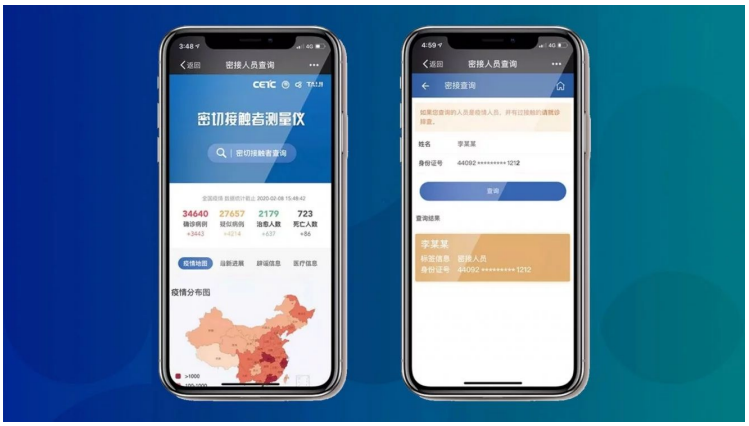
CHINE [19] [20]

Close Contact Detector : une app' en libre téléchargement, opaque et reliée aux bases de données gouvernementales

Depuis le 8 février, le ministère de la Santé propose en libre téléchargement l'application Close Contact Detector, qui informe ses utilisateurs lorsqu'ils ont été en contact étroit avec une personne infectée ou susceptible de l'être. L'application accède à l'historique des déplacements et le compare aux bases de données personnelles constituées par plusieurs agences gouvernementales, dont celles des autorités de santé et des transports. L'application conseille à ceux qui ont été en contact étroit de rester

[18] *LesEchos. Benoît Georges. Quelles données, pour quel suivi ?1 avril 2020.*
[19] *Le Figaro.fr. Coronavirus: la Chine accroît la surveillance de la population. 15 février 2020.*
[20] LCI.fr. "Close Contact Detector" : la Chine lance une appli qui localise les personnes infectées par le coronavirus. 13 février 2020

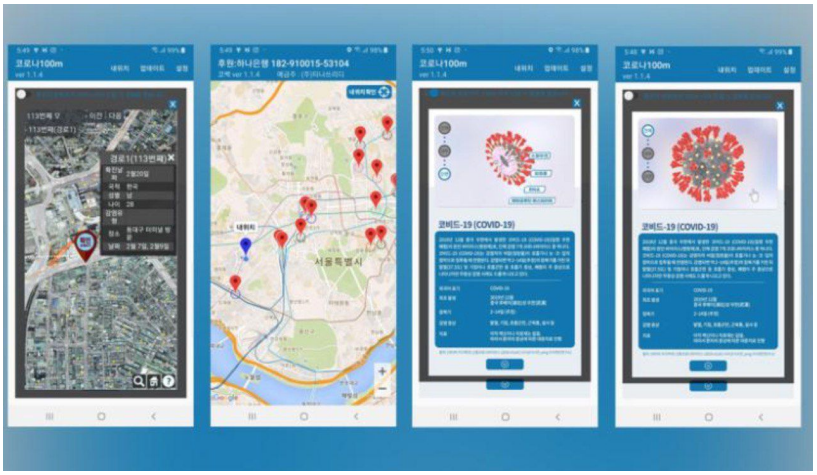
chez eux et de contacter les autorités sanitaires locales. Bien que non obligatoire, et reposant donc sur le consentement, l'application comptait déjà 221 millions d'utilisateurs début mars.



CORÉE DU SUD

Les éditeurs d'application s'emparent des données publiées par les autorités pour proposer leurs solution de prévention

En Corée du Sud, de nombreux éditeurs de logiciel se saisissent des données publiques sur les zones à risque. En s'appuyant sur ces dernières, ils produisent des applications informatives faciles d'usage et destinées au grand public. Ces applications, qui utilisent des données en *open data*, ne participent toutefois pas à enrichir la base.

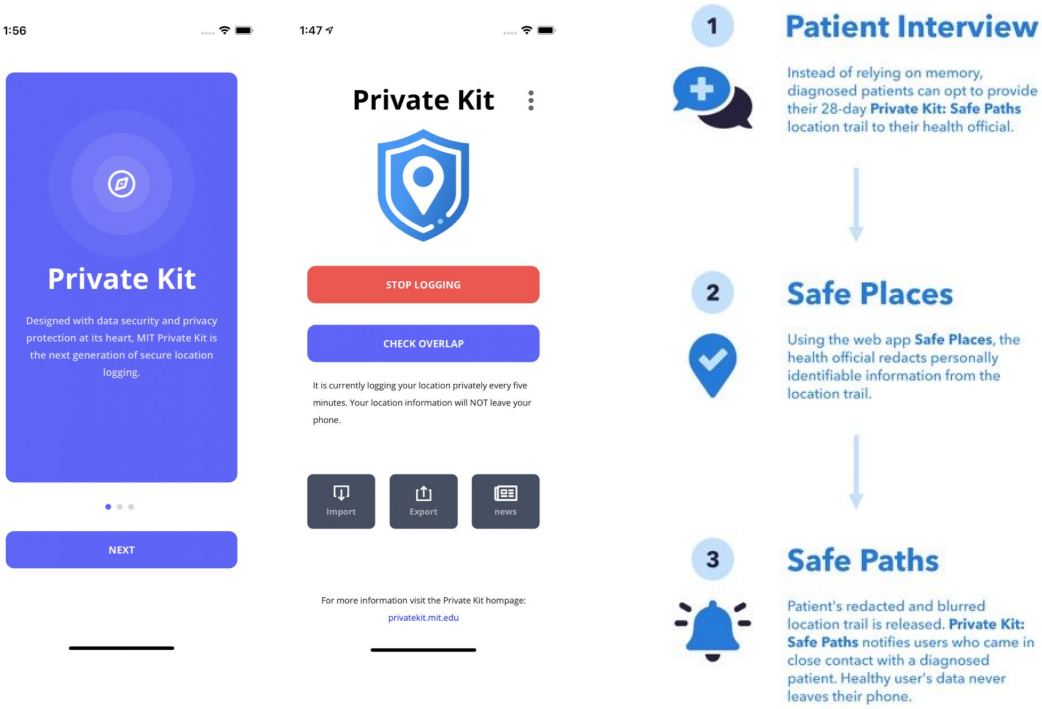


Captures d'écran

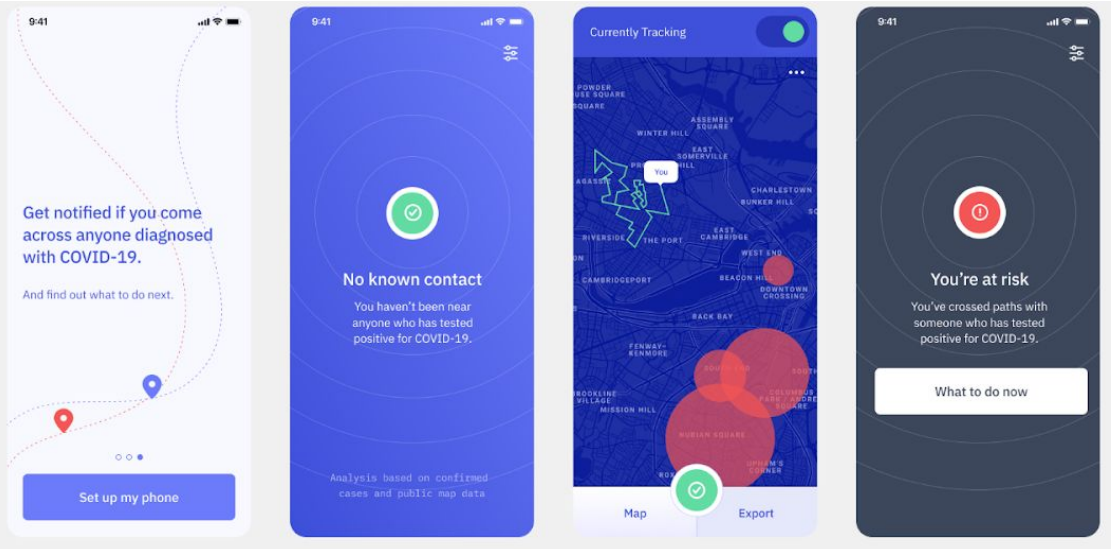
MIT [21] [22]

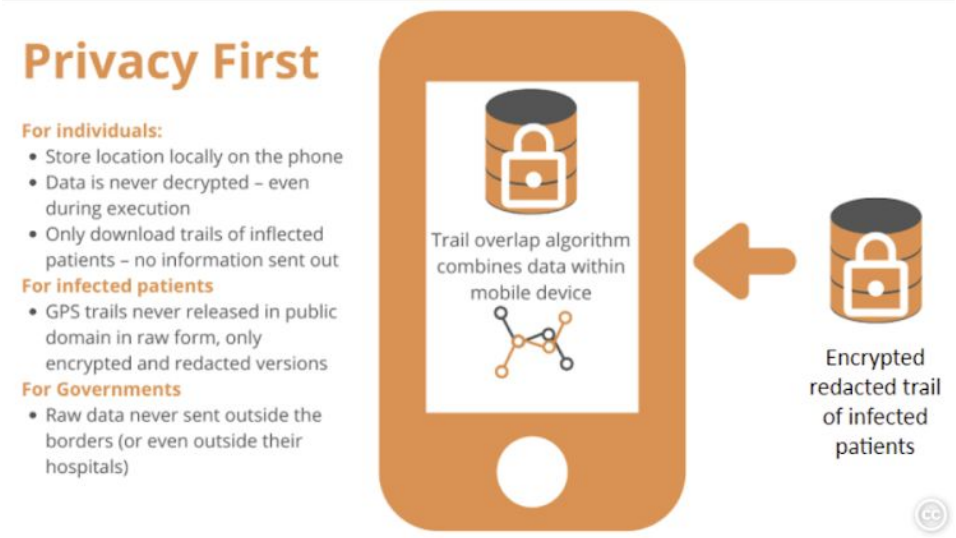
2 objectifs : stocker des informations fiables sur son parcours des 28 derniers jours et informer les personnes "contact" tout en protégeant ses données personnelles.

Au MIT, l'équipe du professeur Ramesh Raskar (composée d'épidémiologistes, de *data scientists* et d'ingénieurs de plusieurs institutions reconnues) a élaboré une application qui stocke 28 jours de données GPS sur le téléphone de l'utilisateur. La fréquence d'actualisation de ces données est de 5 minutes. Si l'utilisateur est détecté positif au virus, il peut, s'il le souhaite, communiquer ses données aux autorités de santé. Ceci permettrait d'identifier les zones à risque pour les autres utilisateurs. De plus, les individus ayant été à proximité du cas positif reçoivent une alerte leur signifiant qu'ils sont à risque. Ils n'ont cependant aucune information sur l'individu malade. L'approche *Privacy first* employée par l'équipe assure la confidentialité de toutes les données fournies. Après l'application singapourienne TraceTogether, c'est le second exemple de *contact tracing* le plus respectueux de libertés individuelles. Différence notable, l'application du MIT utilise des données de géolocalisation GPS alors que l'application Singapourienne utilise le Bluetooth. L'équipe de chercheurs affirme apporter un très haut niveau de protection des données.



[21] *Sciencemag.org. Cellphone tracking could help stem the spread of coronavirus. Is privacy the price?. 22 mars 2020*
[22] *Spectrum.ieee.org. Halting COVID-19: The Benefits and Risks of Digital Contact. 25 mars 2020*


9:41
Get notified if you come across anyone diagnosed with COVID-19.
And find out what to do next.
Set up my phone
9:41
No known contact
You haven't been near anyone who has tested positive for COVID-19.
Analysis based on confirmed cases and public map data
Currently Tracking
Map
Export
9:41
You're at risk
You've crossed paths with someone who has tested positive for COVID-19.
What to do now


Privacy First
For individuals:
• Store location locally on the phone
• Data is never decrypted – even during execution
• Only download trails of inflected patients – no information sent out
For infected patients
• GPS trails never released in public domain in raw form, only encrypted and redacted versions
For Governments
• Raw data never sent outside the borders (or even outside their hospitals)
Trail overlap algorithm combines data within mobile device
Encrypted redacted trail of infected patients

Technique 3 : TRAITEMENT DE CONNEXIONS BLUETOOTH ISSUES D'APPLICATIONS MOBILES

Comment ça marche ?

Le Bluetooth est un standard de communication de proximité entre appareils qui permet un échange de données entre téléphones à très courte distance en utilisant les ondes radio UHF.

Les utilisateurs doivent installer une application mobile et activer le *"mode bluetooth"* de leur téléphone. Ensuite, à chaque fois que deux téléphones avec l'application installée vont se trouver à proximité l'un de l'autre, ils vont réciproquement s'envoyer leurs coordonnées chiffrées. Ces données permettent d'identifier le téléphone mais non la personne.

En mesurant la force du signal Bluetooth entre deux téléphones, la distance peut être approximativement calculée. Cela est essentiel pour établir qu'il y ait bien eu contact entre deux personnes.

Un historique de tous les téléphones ayant été en contact avec la personne est enregistré dans le téléphone. Aucune donnée personnelle d'identification n'est nécessaire et aucune information de localisation géographique n'est enregistrée.

Lorsqu'un utilisateur est testé positif, il se déclare dans l'application et tous les utilisateurs tiers qui ont été à son contact sont informés en recevant une alerte sans qu'il y ait eu besoin de déclarer leur identité.

Quels sont les avantages ?

Près de 8 Français sur 10 possèdent un smartphone équipé d'un capteur Bluetooth.

La méthode est précise : elle relève des proximités de moins de 10 mètres.

Le Bluetooth ne géolocalise pas les utilisateurs.

Il fonctionne partout, notamment dans les espaces souterrains.

Quelles sont les limites technologiques ? [23]

Pour identifier efficacement les sujets *"contact"*, une application doit être utilisée par un nombre important d'utilisateurs dans la population. Selon le journal Les Echos une telle application est efficace si 60% de la population l'utilise et qu'une campagne de dépistage y est associée.[24] Or ce seuil est difficile à atteindre. Il est ainsi nécessaire de donner de la visibilité à l'application : appui officiel et fort du gouvernement, promotion dans les médias, recommandations des professionnels de santé… *"A défaut de taille critique, les utilisateurs pourraient pâtir d'un faux sentiment de sécurité. Ce n'est en effet pas parce qu'une zone est considérée "sans risque" qu'elle l'est réellement. Lorsque le nombre*

[23] *Sciencemag.org. Cellphone tracking could help stem the spread of coronavirus. Is privacy the price?. 22 mars 2020*
[24] *LesEchos. Benoît Georges. Quelles données, pour quel suivi ?1 avril 2020.*

d'utilisateurs est insuffisant, l'application ne rend compte que d'une petite fraction des sources d'infection potentielles."[25]

D'autre part, il existe peu d'exemples de succès d'application ayant utilisé le Bluetooth dans un contexte commercial et à une échelle aussi importante.

Quels enjeux éthiques ?

Informations montantes et descendantes

Les enjeux éthiques dépendent des spécifications de l'application suivant, par exemple, l'envoi automatique de données vers un serveur ou un stockage uniquement dans la mémoire interne du téléphone.

En cas d'envois automatiques, la réflexion éthique est similaire à celle de l'exploitation de données de bornage individuelles. En cas de données chiffrées et enregistrées dans le téléphone, les libertés des utilisateurs sont mieux protégées.

Concernant les historiques des proximités, ils peuvent être enregistrés de manière chiffrée sur la mémoire interne des téléphones et sans inclure l'identité de la personne (on utilise un code de référence lié à son téléphone). Des modèles de gestion associative ou décentralisée, peuvent aussi être envisagés.

En comparaison d'une utilisation des données GPS, faire appel à la technologie Bluetooth soulève moins de problèmes éthiques du fait de la nature des données recueillies : l'appareil n'est pas localisé et l'identité des personnes n'est pas révélée.

On pourrait envisager une complète transparence du code informatique et la réalisation d'un audit indépendant sur le caractère éthique, sur la qualité et sur la sécurité du code. Un conseil de surveillance avec participation des citoyens peut être envisagé.

Consentement à l'installation de l'application

Tout comme les applications reposant sur une exploitation des données GPS, celles utilisant le Bluetooth ne sont efficaces qu'à partir d'une certaine masse critique d'utilisateurs.

Atteindre ce seuil nécessite d'obtenir le consentement d'une partie importante de la population. Cela peut se faire en donnant de la visibilité à l'application (appui officiel et fort du gouvernement, promotion dans les médias, recommandations des professionnels de santé…). Mais les autorités pourraient aussi être tentées de recourir à des mesures coercitives pour motiver les installations, telles qu'une obligation d'usage. Cette obligation pourrait être rendue possible par l'intermédiaire des opérateurs mobiles ou des fournisseurs de système d'exploitation des téléphones.

Le problème du consentement se pose donc de la même manière pour une application utilisant la technologie Bluetooth que pour une application ayant recours aux données GPS.

[25] *Sciencemag.org. Cellphone tracking could help stem the spread of coronavirus. Is privacy the price?. 22 mars 2020*

Quels sont les exemples d'utilisation ?

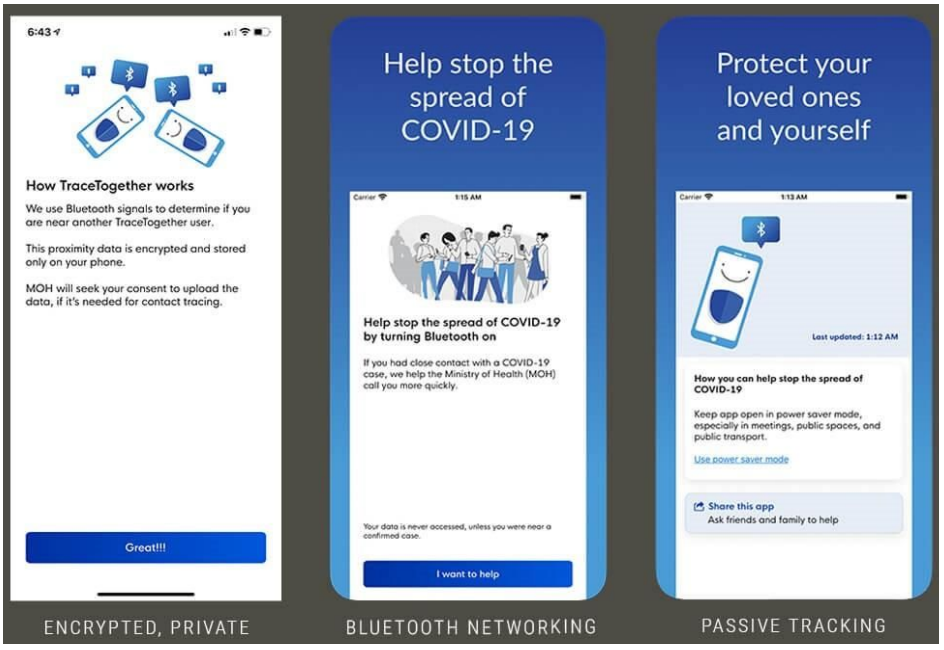
SINGAPOUR [26] [27]

TraceTogether : Une application gouvernementale en libre téléchargement

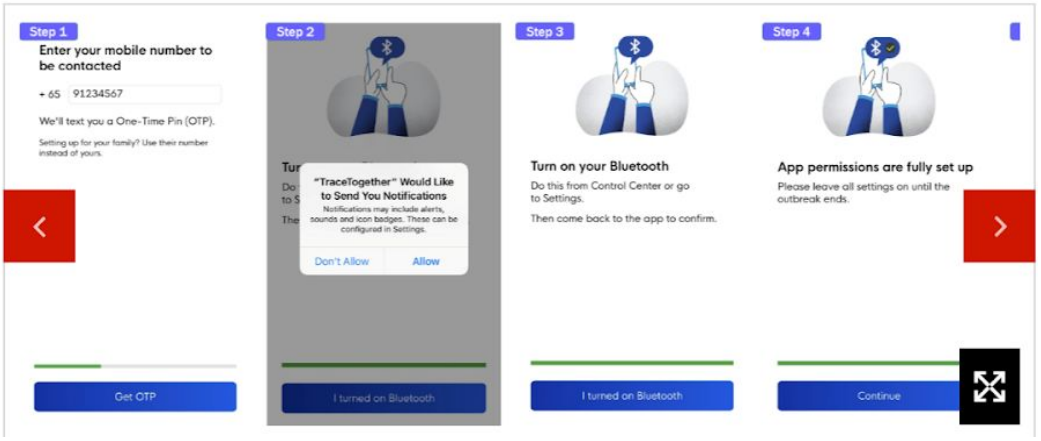
Le gouvernement singapourien a produit une application respectueuse des libertés individuelles : TraceTogether. Disponible depuis le 20 mars en libre téléchargement, 23%[28] des Singapouriens possédant un *smartphone* l'utilisent déjà.

Cette application repose sur le Bluetooth des *smartphones* pour enregistrer les proximités. Il n'y a donc pas de géolocalisation à proprement parler. Les données sont chiffrées et stockées sur les mobiles pendant 21 jours. Il n'y a pas de diffusion automatique. Lorsqu'un utilisateur apprend qu'il est infecté, il contacte les autorités sanitaires et leur transmet le fichier contenant les identifiants des téléphones croisés. Les sujets *"contact"* ainsi identifiés sont avertis du risque de contamination.

L'Etat a décidé de jouer au maximum la transparence en rendant public le code source de cette application pour permettre à d'autres pays de s'en saisir.[29]



[26] *Cnbc.com. Singapore says it will make its contact tracing tech freely available to developers. 25 mars 2020*
[27] *Ouest-france.fr. Coronavirus. À Singapour, la population est pistée de près. 25 mars 2020*
[28] *Site de l'application, faisant état d'1 millions d'utilisateurs au 09 avril 2020.*
[29] *Straitstimes.com. Hariz Baharudin. Coronavirus: Singapore Government to make its contact-tracing app freely available to developers worldwide. 23 mars 2020.*



ALLEMAGNE [30] [31]

En Allemagne, les opérateurs téléphoniques fournissent des données de bornage aux autorités pour leur permettre de vérifier le respect du confinement et de cartographier des zones à risque dans le respect du RGPD et de la directive ePrivacy. Deutsche Telekom, par exemple, a fourni à l'institut Robert Koch (l'équivalent allemand de l'Inserm) les données anonymisées et agrégées de 46 millions d'abonnés.

Le Ministre de la Santé allemand Jens Spahn a souhaité déposer une proposition législative rendant possible le *backtracking* par bornage téléphonique. Il l'a toutefois retirée suite à de vives critiques liées au caractère très général et peu restreint des données demandées. Certains dénonçaient des mesures potentiellement disproportionnées et remettaient en cause l'efficacité d'un tel *tracking*. D'autres souhaitaient que la récupération des données s'effectuent sur la base du volontariat et que leur durée de conservation soit clairement explicitée.

Désormais, les regards se tournent vers une application de *tracking* fonctionnant à l'aide de la technologie Bluetooth. En effet, l'Institut Fraunhofer Heinrich-Hertz prépare, en collaboration avec des partenaires européens, une application sur le modèle de TraceTogether (développée à Singapour) qui devrait être fonctionnelle au cours du mois d'avril. L'application conserverait *"la proximité et la durée des contacts entre les personnes pendant deux semaines sur des téléphones portables de manière anonyme et sans utiliser l'emplacement des données"*.

[30] *Spiegel.de. So ringt die GroKo um die Verwendung von Handydaten. 23 mars 2020*
[31] *20minutes.fr. Coronavirus : Collecte de données de santé, géolocalisation… A quoi le pistage numérique pourrait-il ressembler ? 26 mars 2020*

2ème usage : L'identification des sujets "contact"

Technique 4 : TRAITEMENT DES DONNÉES ISSUES DE L'USAGE DE CARTES BANCAIRES / DE TRANSPORT

Comment ça marche ?

À chaque paiement ou retrait par carte bancaire, une autorisation est transmise à la banque et le lieu de transaction est enregistré. Suivant cette information, les banques sont en mesure de retracer les déplacements de leurs clients.

Lorsqu'un abonné des transports en commun valide sa carte à une borne de bus, de station ou de métro, sa position d'entrée dans le réseau et celles des correspondances sont enregistrées par l'opérateur de transport. Dans les villes où il est obligatoire de valider à l'arrivée, comme à Londres, la position de sortie du réseau est également connue.

Quels sont les avantages ?

Les données existent dès lors que les individus utilisent leurs cartes de paiement et de transport.

Lorsque le personnel d'un point de vente (/usager des transports) est testé positif, la méthode permet d'identifier les clients *"contact"* (/usagers *"contact"*).

Les transports en commun sont des espaces à risque élevé (étroits, très fréquentés, position statique des personnes durant plusieurs minutes). Il est donc intéressant de pouvoir y observer les déplacements et les proximités entre usagers.

Quelles sont les limites technologiques ?

L'itinéraire récent des personnes ne peut être reconstitué que très partiellement pas ces biais.

Quels enjeux éthiques ?

Les considérations éthiques mènent à favoriser :

- l'obtention du consentement des personnes avant le *backtracking* ;
- une information des sujets *"contact"* mais non des autorités sanitaires ;
- une gouvernance de contrôle des usages.

Quels sont les exemples d'utilisation ?

SINGAPOUR, CORÉE DU SUD

L'usage permet d'identifier des boutiques, des transports et des stations à risque

Lorsque le personnel d'une boutique est testé positif, les autorités peuvent exploiter l'historique des transactions bancaires pour identifier les clients ayant été en contact.

France 2. Corée du sud. Carte interactive des zones sûres et à risque

2ème usage : L'identification des sujets "contact"

Technique 5 : TRAITEMENT DES DONNÉES ISSUES DE LA VIDÉOSURVEILLANCE

Comment ça marche ?

La vidéosurveillance couplée à un contrôle humain, ou à une intelligence artificielle, permet de distinguer les visages pour constater des proximités à risque au sein de l'espace public.

Quels sont les avantages ?

Les caméras positionnées à des endroits stratégiques (entrées et sorties de métro / d'hôpitaux, centres commerciaux…) contrôlent un maximum de citoyens.

Cette méthode est réalisée sans le consentement des personnes filmées.

Quelles sont les limites technologiques ?

Des questions se posent quand à l'efficacité réelle de la méthode :

- L'observation de vidéos par les humains est une tâche longue et complexe ;
- La performance des algorithmes d'identification automatique est en question (notamment, cela suppose une importante base de données sur les paramètres des visages) ;
- Le maillage de caméras doit être dense et disposer de vues qui se recoupent.

Si certains pays revendiquent son utilisation, aucun d'entre eux n'en a prouvé l'efficacité réelle.

Quels enjeux éthiques ?

Les enjeux éthiques sont majeurs. Cette technologie, pour être efficace, mène à créer une base de données biométriques des citoyens, ainsi qu'à analyser en permanence l'intégralité de l'espace public afin de les identifier.

Les utilisations des outils de reconnaissance faciale pour analyser les images de l'espace public, quand elles sont parfois envisagées dans les démocraties, ne le sont que pour les questions de lutte contre le terrorisme et dans le cadre d'une gouvernance de contrôle très importante avec une limitation du nombre de personnes présentes dans la base et une limitation des espaces publics analysés.

Ce débat est bien plus grand que le débat actuel lié au Covid. Au regard de l'absence de projets dans le cadre de la lutte contre le Covid, en dehors de la Chine, il est important que ce débat ne vienne pas perturber celui des autres usages dont il est ici question.

Quels sont les exemples d'utilisation ?

Chine

3ème usage

Le contrôle des confinements individuels

(i.e. tracking ou bracelet électronique virtuel)

Finalités : → *Veiller au respect des quarantaines (sujets malades et "contact")*
→ *Veiller au respect des confinements (population générale)*
→ *Développer un "permis de circuler"*

Techniques : *1) Traitement des données GPS issues d'une application mobile*
2) Traitement des données issues du bornage des opérateurs télécoms

En l'absence de contrôles, certaines personnes tenues à une quarantaine (porteuses du virus ou personnes *"contact"*) ou au confinement (personnes saines) ne respectent pas scrupuleusement la distanciation sociale, mettant ainsi en péril la santé d'autrui. Les technologies de traçage des données permettent de contrôler la présence effective des personnes à leur domicile, ou dans leur quartier.

Plusieurs finalités peuvent être constatées :

- Contrôler la présence de la personne à son domicile : position GPS, bornage mobile avec envoi d'un texto et contrôle de l'identité (demande d'un *selfie*, ou réponse de vive voix ou en vidéo à un appel).
- Développer un "*permis de circuler"* basé sur un ensemble de données et qui, lors de contrôles inopinés dans la rue, vous autorise à entrer dans certaines zones ou vous oblige à rentrer chez vous.

Dans les deux cas, les conséquences éthiques induites sont importantes et dépassent largement l'enjeu technologique. Si l'utilité de chacun de ces usages est incontestée, la question de son équilibre avec les libertés individuelles se pose gravement. Ce type de dispositif entre en contradiction avec de nombreuses valeurs des pays européens.

3ème usage : Le contrôle des confinements individuels

Technique 1 : TRAITEMENT DES DONNÉES DE GPS ISSUES D'UNE APPLICATION MOBILE

Comment ça marche ?

Suite à la décision des autorités de placer une personne en quarantaine, on lui impose d'installer une application mobile de suivi GPS sur son *smartphone* afin de contrôler les sorties de son domicile. Si la personne rompt son isolement en dehors des dispositions dérogatoires (aller travailler, faire les courses, une heure d'activité physique…), le service de surveillance en est averti et engage un dialogue. En cas de non respect manifeste des règles de distanciation, l'individu peut être sanctionné au travers d'une amende.

Quels sont les avantages ?

De nombreuses personnes disposent d'un *smartphone*.

Quelles sont les limites technologiques ?

Suivant un contrôle à partir du seul GPS, il est facile de frauder : il suffit en effet de laisser le téléphone chez soi alors que l'on est dehors. Des contrôles complémentaires et plus intrusifs sont souvent mis en place : appels inopinés (sans *selfie* ou avec comme en Pologne), bracelet électronique complémentaire, utilisation des données de bornage de l'opérateur mobile.

Quels enjeux éthiques ?

Les enjeux éthiques sont très importants mais ne sont pas particulièrement liés à la question technologique. La question posée est celle du degré de coercition décidée par les autorités pour veiller au respect des règles de confinement au niveau individuel. Jusqu'à quel point veut-on contraindre les personnes à respecter le confinement ?

En effet, en cas de non-respect du confinement, contrôlé ou non par une application, les enjeux éthiques ne sont pas les mêmes si la sanction est une peine de prison ferme comme en Corée du Sud, une amende de plus de 6000 euros en Pologne ou une amende de 135 euros en France.

La question éthique plus spécifiquement technologique est celle de l'extension du domaine du contrôle de la force étatique. Alors que l'Etat a le monopole de la contrainte physique, avec une application mobile de contrôle des mouvements, on ouvre symboliquement le champ à une nouvelle forme de contrôle sur la population. Le contrôle strict par application mobile rapproche le confinement individuel à une détention à domicile. Un débat qui s'approche de celui qui a eu lieu lors de la mise en place dans les démocraties des bracelets électroniques pour la détention à domicile. Ce type de dispositif entre en contradiction avec de nombreuses valeurs des pays européens.

Quels sont les exemples d'utilisation ?

Taïwan (appel inopiné), Pologne (avec *selfie*), Hong Kong (bracelet, sinon appel inopiné)

TAIWAN

Les personnes infectées ou susceptibles de l'être doivent se conformer à une quatorzaine contrôlée par la géolocalisation de leur téléphone. Un *tracker*, relié aux services de police, est imposé. Lorsqu'une personne à l'isolement s'éloigne de son domicile ou éteint son téléphone, elle est contactée dans les 15 minutes. Pour s'assurer que les personnes ne "trichent" pas en laissant leur téléphone à domicile alors qu'elles sont de sortie, des fonctionnaires les appellent 2 fois par jour. Les contrevenants s'exposent à une amende pouvant atteindre 30 000 euros et risquent la publication de leur identité.

Les autorités sanitaires utilisent un chatbot développé en partenariat avec HTC et la messagerie Line. Le bot demande régulièrement aux personnes surveillées de relever leur température et de reporter d'éventuels symptômes. En retour, les personnes peuvent poser des questions.

HONG KONG

Pour s'assurer du respect des périodes de quatorzaine par toutes les personnes venant de l'étranger, les autorités hongkongaises les équipent d'un bracelet électronique similaire à ceux des services de l'application des peines. Celui-ci est relié à une application que l'on télécharge sur son téléphone avant sa quatorzaine. Les autorités sont ainsi en mesure de s'assurer du respect du confinement individuel à chaque instant.

Au début de la quatorzaine, l'individu équipé d'un bracelet doit renseigner les coordonnées exactes de son espace de vie durant cette période en en faisant le tour. Est alors configurée une alerte qui se déclenche selon certaines situations (*smartphone* éteint, bracelet non fonctionnel, sortie de l'espace autorisé) et informe le Department of Health ainsi que la police.

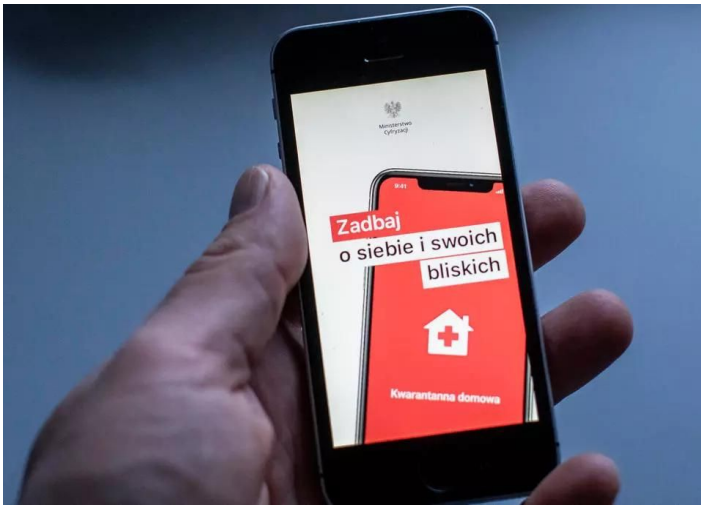
Il semblerait, selon le Government Chief Information Officer de Hong Kong, que le système ne conserve aucune information liée à la localisation des personnes. L'alerte se déclencherait seulement en cas de sortie d'une zone "autorisée", définie au préalable par l'individu lorsqu'il effectue un tour de son espace de vie.

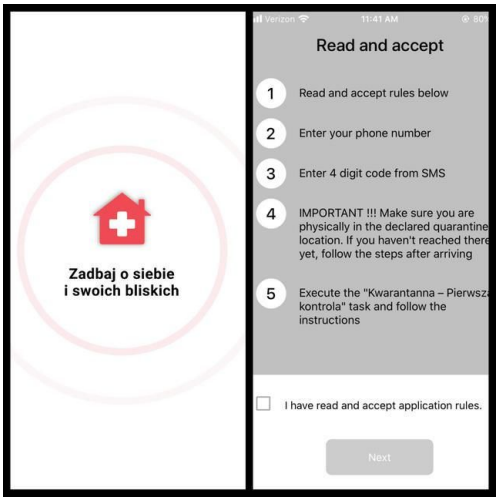
A l'issue de la quatorzaine, les individus sont encore sous surveillance médicale pendant deux semaines supplémentaires.

En parallèle, la police appelle quotidiennement les individus n'ayant pas été équipés d'un bracelet afin de vérifier le nombre de personnes présentes dans la zone de quatorzaine.

POLOGNE [32] [33]

La Pologne impose une quatorzaine aux sujets *"contact"* et aux personnes revenant de l'étranger. Pour s'assurer de leur isolement, elle utilise une application de géolocalisation dédiée. Les individus en quatorzaine reçoivent chaque jour plusieurs SMS, de façon inopinée, leur demandant de s'identifier par un *selfie*. L'identité et la localisation sont ainsi contrôlées. Faute de réponse aux SMS, la police se déplace. L'amende peut dépasser les 6000 euros.





[32] LeFigaro.fr. Samuel Kahn. *Les Polonais en quarantaine doivent se prendre en selfie pour prouver qu'ils sont chez eux.* 24 mars 2020.
[33] *Lepetitjournal.fr. Coronavirus en Pologne : Durcissement du confinement depuis mercredi. 29 mars 2020*

CHINE

Depuis le milieu du mois de février, un QR code tricolore (vert, jaune et rouge) guide les déplacements des utilisateurs de l'application Alipay Health Code dans la ville de Hangzhou (10 millions d'habitants). Des contrôles imposés s'appuyant sur cette application sont réalisés dans de nombreux quartiers, ce qui rend son usage obligatoire pour les personnes souhaitant s'y rendre. La couleur du QR code, actualisée quotidiennement, est définie en fonction des déplacements des 14 jours précédents :

- Vert : il est possible de circuler librement à travers les multiples points de contrôle.
- Jaune : un confinement au domicile de 7 jours est imposé.
- Rouge : aucun déplacement n'est autorisé pendant 2 semaines.

En cas de non respect, la police peut intervenir. Au 24 février, plus de 50 millions de Chinois avaient installé l'application, principalement dans la province de Zhejiang dans laquelle la pénétration est de 90%. Ce système serait en déploiement dans tout le pays. Malgré sa diffusion massive, l'absence de transparence sur les méthodes algorithmiques utilisées demeure.

3ème usage : Le contrôle des confinements individuels

Technique 2 : TRAITEMENT DES DONNÉES DE BORNAGE DES OPÉRATEURS

Comment ça marche ?

Suite à la décision des autorités de placer une personne en quarantaine, son numéro est inscrit dans une liste de numéros suivis.

La pratique est similaire à celle d'ores et déjà mise en place dans les démocraties mais sous contrôle d'un juge dans le cadre d'une enquête judiciaire pour détecter les mouvements d'un suspect.

Les données de bornage téléphonique de la personne en confinement sont surveillées afin de s'assurer qu'elle ne sort pas de chez elle, ou ne quitte pas son quartier. Le cas échéant, l'opérateur télécom alerte les autorités.

Quels sont les avantages ?

Elle ne nécessite pas d'installation particulière et fonctionne avec tous les téléphones.

La localisation est enregistrée automatiquement aussitôt que le téléphone se connecte à une borne relais et échange des informations, même passivement : réception d'un SMS, activation automatique d'une application utilisant Internet...

Quelles sont les limites technologiques ?

La précision peut être, dans certains contextes, insuffisante. Comme pour le contrôle par application de contrôle GPS, des moyens de contrôle complémentaires sont parfois mis en place pour éviter la triche.

Quels enjeux éthiques ?

Les enjeux éthiques sont majeurs et sont similaires à ceux du contrôle par application GPS. Cependant, dans cet usage, on peut considérer que le fait que tout le contrôle soit surveillé à distance par l'opérateur mobile rend le dispositif plus grave encore. Le rôle de l'opérateur mobile est de rester un acteur neutre dans l'usage des communications faites par ses utilisateurs, à la fois dans le secret des correspondances et des informations particulières détenues sur ses clients ; c'est la clé de la confiance des citoyens vis-à-vis des opérateurs de communication. Le mode de contrôle ici décrit est de nature à bouleverser à long terme la confiance des individus à communiquer et à utiliser un téléphone mobile. La pratique constituerait ainsi une atteinte à la liberté de communiquer.

Quels sont les exemples d'utilisation ?

La Corée du Sud et Taïwan semblent recourir à ce dispositif en complément des autres moyens, sans toutefois en faire une publicité particulière.

Résumé des Pratiques Internationales

	CHI	TAÏ	COR	SIN	ISR	RUS	POL	USA	ITA	ALL	FRA
Usages											
1) Observer les pratiques collectives											
- Obtenir une vision nationale et régionale	X	X	X	X	X	X	?	X	X	X	X
- Obtenir une vision affinée (i.e. quartiers)	?	?	?	?	?	?	?				
2) Identifier des sujets *"contact"*											
- Retracer le parcours récent des "positifs"	X	X	X	X	X					(4)	
- Informer la population des zones à risque		X	X								
- Relever directement les contacts récents				X				(5)		(5)	(5)
3) Contrôler des confinements individuels											
- Veiller aux quarantaines (malades+contact)	X	X	X		X	X	X				
- Veiller aux confinements (pop. générale)		(1)	(1)								
- Développer un *"permis de circuler"*	X										
Techniques											
Bornes téléphoniques	X	X	X	X	X	X	X	X	X	X	(3)
GPS	X	X	X	X	X	X					
Données bancaires / de transport	X	X	X	X		X					
Vidéo surv. + reconnaissance faciale	X	X	X	X		X					
Bluetooth				X						(5)	(5)
Données de géolocalisation											
Collectives / agrégées et anonymes	X	X	X	X	X	X	X	X	X	X	(3)
Individuelles sans consentement	X	X	X	X	X	X	X				
Individuelles avec consentement	X			X							
Accès à l'information sur les individus											
Autorités sanitaires	X	X	X	X	X	?	?				
Police	X	X	X		(2)	X	X				
Diffusion publique		X	X	X	X						
Stade de l'épidémie *(au 01/04)*											
Croissance faible et maîtrisée		X	X	X							
Croissance rapide					X	X	X				
Pleine épidémie								X	X	X	X
Pic dépassé, stabilisé	X										

(1) Pour l'heure, pas de confinement à Taïwan et en Corée du Sud.

(2) En Israël, la surveillance s'opère par le service de sécurité intérieur.

(3) Partenariat Orange / Inserm pour observer les mouvements de population et améliorer les prédictions.

(4) Le ministre allemand de la santé a voulu proposer un backtracking par bornage téléphonique. Suite à une levée d'oppositions, sa proposition a été retirée.

(5) Le MIT développe une application de backtracking par GPS respectueuse de la vie privée. La France et l'Allemagne réfléchissent à une application basée sur le Bluetooth, également respectueuse de la vie privée.

Revue de presse

Classement du plus récent au plus ancien

1. **Nature Medicine.** Marcello Lenca et Effy Vayena. 27/03/2020. On the responsible use of digital data to tackle the COVID-19 pandemic
2. **Mediapart.** Géraldine Delacroix et Jérôme Hourdeaux. 26/03/20. Surveillance de l'épidémie : la CNIL met en garde le gouvernement
3. **Le Parisien.** Damien Licata Caruso.25/03/20. Confinement : 5 questions sur la probable surveillance par nos *smartphones*
4. **Le Figaro.** 25/03/20. Coronavirus : huit opérateurs télécoms européens prêts à partager leurs données de géolocalisation
5. **Les Echos.** Isabelle Ficek. 25/03/20. Coronavirus : l'exécutif affiche la plus grande prudence sur le traçage numérique.
6. **La Croix.** AFP. 25/03/20. Données de géolocalisation contre coronavirus, le débat qui couve en France
7. **Atlantico.** Charles Reviens. 25/03/20. Covid- 19 : radioscopie des points clés de la méthode sud-coréenne
8. **Le Parisien.** Nathalie Schuck. 24/03/20. Coronavirus : pour vaincre l'épidémie, faut-il traquer les Français ?
9. **Ouest France.** 24/03/20. Coronavirus. 100 000 caméras surveillent les confinés à Moscou… Et tous les autres
10. **La Tribune.** 23/03/20.La Russie mise sur la géolocalisation pour endiguer le coronavirus
11. **Igen.** Sabrina Fekih. 23/03/20. A Taïwan, une clôture électronique entoure les personnes en quarantaine.
12. **Science Mag.** Kelly Servick. 22/03/2020. Cellphone tracking could help stem the spread of coronavirus. Is privacy the price?
13. **Le Figaro.** Valérie Segond. 22/03/20. Italie: contre le coronavirus, l'utilisation massive de la géolocalisation
14. **Usbek & Rica.** Annabelle Laurent. 20/03/20. COVID-19 : des États utilisent la géolocalisation pour savoir qui respecte le confinement
15. **L'Usine Nouvelle.** Adrien Simorre. 20/03/20. Covid-19 : comment Taïwan s'est appuyé sur la technologie pour contenir l'épidémie ?
16. **La Tribune.** Anaïs Cherif. 18/03/20. Faut-il craindre une surveillance des *smartphones* ?
17. **Le Monde.** Louis Imbert. 17/03/20. Coronavirus : Israël approuve des méthodes de surveillance électronique de masse
18. **Le Figaro.** Sébastien Falleti. 17/03/20. Le contre-modèle taiwanais irrite Pékin

19. **Usbek & Rica.** Pablo Maillé. 13/03/20. Il aurait fallu s'inspirer de Taiwan, mais c'est trop tard
20. **Sciences et Avenir.** AFP. 11/03/20. Covid-19 : Séoul, l'élève modèle dans la lutte contre le coronavirus ?
21. **Techcrunch.** Natasha Lomas. 10/03/20. Israel passes emergency law to use mobile data for COVID-19 contact tracing
22. **RFI.** Stéphane Lagarde. 09/03/20. Big Data contre big virus : des applications traquent les personnes en quarantaine
23. **The Guardian.** Nemo Kim. 06/03/20. More scary than coronavirus': South Korea's health alerts expose private lives
24. **BFMTV.** 02/03/20. Comment une application prive des millions de Chinois de déplacements
25. **Le Figaro.** Laura Andrieu. 15/02/20. La Chine accroît la surveillance de la population
26. **LCI.** Matthieu Delacharlery. 13/02/20. L'application qui localise les personnes infectées
27. **The Economist.** 02/02/20. To curb covid-19, China is using its high-tech surveillance tools
28. **Asialyst.** Emmanuel Pernot. 19/05/18. Comment l'Asie protège ses données personnelles