Covid-19 impact series

ETUI Policy Brief

Politiques économiques, sociales et de l'emploi en Europe

N°5/2020

Les applications de traçage des contacts pour le COVID-19 : comment éviter que la vie privée ne devienne la prochaine victime

Aída Ponce Del Castillo

Aída Ponce Del Castillo est chercheuse senior à l'Institut syndical européen à Bruxelles, Belgique.

Points clés

- **L'utilisation, pour lutter contre la diffusion du COVID-19, d'applications de traçage des contacts est intrusive et menace le droit des citoyens de l'UE au respect de leur vie privée. Pour défendre ce droit, les règles et les principes essentiels du droit de l'UE, en particulier ceux qui sont intégrés dans le règlement général sur la protection des données (RGPD) et dans la directive « vie privée et communications électroniques », doivent être respectés.**
- **Il est faux de soutenir que le souci de protéger les données à caractère personnel nuirait à la lutte contre la pandémie et à la relance de l'économie : pour que les applications de traçage des contacts soient efficaces, elles doivent être volontairement et librement téléchargées et utilisées par une majorité de citoyens. Cet objectif ne pourra être atteint que si les citoyens sont certains que le droit au respect de leur vie privée n'est pas menacé. Ces deux combats, pour le respect de la vie privée et contre le COVID-19, ne sont pas opposés, mais complémentaires.**
- **Les applications de traçage de contact ne peuvent être utilisées sur le lieu de travail que si des exigences spécifiques sont respectées (concernant, notamment, le but de l'utilisation de cette application, le type de données collectées, le délai de conservation de ces données, le consentement des travailleurs et l'implication des syndicats).**
- **Enfin, il est de la plus haute importance que les applications de traçage des contacts ne soient pas utilisées pour ouvrir la voie à la mise en place d'une culture de l'hypersurveillance sur le lieu de travail.**

Introduction

La pandémie de COVID-19 est loin d'être terminée et le nombre de ses victimes continuera malheureusement de croître. Toutefois, dans la seconde semaine d'avril 2020, plusieurs États membres de l'Union européenne (UE), notamment l'Autriche, l'Espagne et le Danemark, ont commencé à assouplir leurs mesures de confinement. D'autres pays commenceront à les imiter au début du mois de mai.

Parallèlement à ce processus de déconfinement, les applications de traçage sont de plus en plus fréquemment présentées comme des outils utiles pour accompagner et favoriser un retour à la normale, en dépit des nombreuses questions éthiques et juridiques qu'elles soulèvent. Le 14 avril, le Royaume-Uni a fait part de son intention de lancer une application permettant de tracer les personnes qui font état de symptômes du COVID-19 et d'alerter les autres personnes qui entrent en contact avec elles. Le 10 avril, Apple et Google (2020) ont annoncé qu'elles allaient s'associer pour lancer une « solution globale qui comporterait des interfaces de programmation d'application (API) et une technologie appliquée aux systèmes d'exploitation qui rendra possible le traçage des contacts ». Le 21 avril, le Premier ministre néerlandais Mark Rutte a déclaré que le développement des applications de traçage du COVID-19 se poursuivrait, en dépit du fait que sept de ces applications ont été testées et qu'aucune d'entre elles n'a réussi à répondre aux exigences en matière de sécurité, de respect de la vie privée et de fiabilité.

etui.

Les milieux d'affaires et les lobbys ont exercé d'intenses pressions pour faire redémarrer et « sauver » l'économie. Ce qui avait commencé comme une crise de santé publique s'est métamorphosé en crise économique et nous sommes aujourd'hui confrontés à un choix cornélien : accepter de « payer le prix » que représente l'utilisation d'applications de traçage envahissantes et, ce faisant, faciliter le redémarrage progressif de l'activité économique, ou bien lutter pour le respect de la vie privée et retarder le retour à la normalité.

Nous devons rejeter ce choix binaire. La défense du respect de la vie privée ne compromet pas la relance de l'économie : pour que les applications de traçage des contacts soient réellement efficaces, elles doivent être volontairement et librement téléchargées et utilisées par une majorité de citoyens. Cet objectif ne pourra être atteint que si les citoyens pensent que le respect de leur vie privée n'est pas remis en question. C'est précisément cet élément qui pourra faire la différence entre une utilisation de ces applications par un nombre limité de personnes, ce qui rendrait ces dispositifs inefficaces, et l'utilisation massive qui constitue un préalable indispensable pour garantir leur efficacité.

La relance de l'économie ne peut s'effectuer au prix de la perte de nos droits en matière de respect de la vie privée. Ce *policy brief* rappelle un certain nombre d'exigences essentielles qui doivent nous aider à garantir ce respect, aussi bien en tant que citoyen que sur notre lieu de travail.

Des applications multiples, des approches technologiques multiples, et des problèmes multiples de protection de la vie privée

Face au développement inévitable de la technologie du traçage dans la lutte contre le COVID-19, nous devons faire un choix. Voulons-nous vivre dans un monde « COVID-1984 » soumis à un système de surveillance autoritaire, orwellien, caractérisé par le traçage des citoyens à tous les niveaux et par la fin du respect de la vie privée ? Allons-nous commencer à utiliser des applications développées par des entreprises privées qui nous demanderont de leur faire confiance et de partager avec elles des données à caractère personnel et des données de localisation ? Ou bien allons-nous revendiquer une approche commune au niveau de l'UE et une application basée sur les règles du RGPD, notamment sur le principe de la protection des données dès la conception (« *privacy by design* »), afin de pouvoir à la fois combattre la diffusion du virus et garantir le respect de notre vie privée ?

À l'heure actuelle, le développement des applications s'effectue pratiquement sans aucune coordination et selon des approches très diverses : certaines applications collectent des données anonymisées et agrégées pour suivre les mouvements de la population, ou pour faire respecter le confinement, ou pour collecter des données statistiques ; d'autres sont axées sur l'autoévaluation. Plus récemment, les efforts se sont concentrés sur les applications de traçage des contacts qui localisent et suivent à la trace les personnes infectées et celles qui sont susceptibles de l'être, mais aussi les individus qui ont été en contact avec ces personnes.

Toutes ces applications présentent de graves défauts : elles sont envahissantes ; elles ne peuvent remplir leur rôle de signal d'alerte précoce que si un nombre important de personnes installent et activent l'application ; elles peuvent générer de fausses alertes ou créer la confusion en détectant à tort des personnes comme positives. Pire encore : elles ne sont pas toujours fiables. Tout d'abord, la portée du rayonnement du signal Bluetooth est plus importante dans les espaces ouverts que dans les environnements urbains, ce qui signifie que le dispositif peut considérer à tort que des personnes sont positives ou négatives. En outre, l'on peut se trouver sans risque à quelques mètres à peine d'une personne positive, par exemple si cette personne détectée par le signal se trouve de l'autre côté d'un mur, alors qu'un siège de métro peut rester une source de contamination pendant plusieurs heures.

Le défaut le plus criant de ces applications concerne le respect de la vie privée. La technologie et des mesures législatives d'urgence peuvent contribuer à contenir ou à limiter la crise du COVID-19, mais il est nécessaire de mener un débat démocratique sur le déploiement rapide de solutions technologiques qui semblent l'emporter sur certains droits fondamentaux, notamment le dialogue social ainsi que les droits à l'information, à la consultation et à la participation. L'adoption de ces technologies engendre des risques et des problèmes nouveaux et importants dans le cadre de la protection de la vie privée et des données à caractère personnel.

Des solutions extrêmes ont été mises en œuvre dans certaines parties du monde. À Singapour, le COVID-19 Dashboard, par exemple, partage des informations sur toutes les personnes infectées, en ce compris leur origine ethnique, leur âge, leur sexe, et dans certains cas le lieu où elles vivent, celui où elles travaillent, l'hôpital où elles se trouvent et l'identité des personnes qu'elles auraient pu contaminer (https://co.vid19.sg/singapore/). Tout aussi inacceptables sont les solutions qui font courir le risque de voir des données confidentielles d'un patient être partagées avec des entreprises technologiques américaines. Le 12 avril, le Guardian (2020a) a révélé que Palantir, une entreprise américaine de big data, et Faculty, une start-up britannique spécialisée dans l'intelligence artificielle, étaient impliquées dans une opération d'exploration de données (data mining) lancée par le gouvernement britannique. Cette opération comportait le stockage d'informations sensibles et confidentielles de santé dans une base de données centralisée reprenant notamment le contenu des appels des citoyens aux services d'assistance téléphonique du Service national de santé du Royaume-Uni.

Face à la multiplicité des applications et des approches technologiques développées à travers le monde pour faire face à la crise du COVID-19, l'ETUI a dressé une carte des initiatives lancées pour endiguer la pandémie (disponible en ligne sur le site www.etui.org à partir du 15 mai 2020), en se basant sur le travail effectué par gdprhub.eu et sur d'autres sources ; ce relevé sera régulièrement actualisé.

Ce *policy brief* présente également quatre cas d'utilisation de dispositifs technologiques : l'application *Self-Quarantine Safety Protection* en Corée du Sud, l'application *TraceTogether* à Singapour, la récente initiative conjointe d'Apple et de Google et la *Pan-*

European Privacy-Preserving Proximity-Tracing Initiative. Ces exemples ont été sélectionnés parce qu'ils décrivent quatre réalités différentes : Singapour et la Corée du Sud ont été cités en exemples à travers le monde pour leur efficacité à contenir la diffusion du virus (Mesmer 2020 ; McCurry 2020 ; Leung 2020). L'interface de programmation d'application (API) d'Apple/Google et la *Pan-European Privacy-Preserving Proximity-Tracing Initiative* ont été sélectionnées parce qu'il s'agit d'initiatives conjointes qui assurent placer le respect de la vie privée de l'utilisateur et la sécurité au cœur de leur projet.

Ce *policy brief* présente ensuite une liste de recommandations et d'exigences que les applications de traçage des contacts devraient respecter pour être à la fois efficaces et respectueuses de la vie privée de l'utilisateur.

Et en dernier lieu, il examine le cas spécifique des **applications de traçage des contacts utilisées dans le contexte de l'emploi.**

Quatre cas d'utilisation des technologies

1.Corée du Sud : l'application *Self-Quarantine Safety Protection*

De quoi s'agit-il ? Description du fonctionnement
Cette application, développée par le ministère de l'Intérieur et de la Sécurité, utilise la technologie GPS pour contrôler et suivre les citoyens infectés qui se sont mis en quarantaine volontaire. L'application permet à des fonctionnaires du gouvernement de localiser chaque patient qui s'est placé en quarantaine. En cas de violation de la quarantaine, une alerte est activée. En outre, une procédure de communication est mise en place entre les utilisateurs et les fonctionnaires : elle permet aux patients de faire deux fois par jour rapport sur leurs symptômes à un agent de l'administration locale. Toute personne qui quitte son lieu de quarantaine sans autorisation s'expose à une peine de prison pouvant aller jusqu'à un an ou à une amende de 7.500 €. Tout étranger qui refuse d'installer l'application ou qui quitte la zone de quarantaine sans autorisation peut être expulsé immédiatement (Central Disaster and Safety Countermeasures Headquarters 2020).

Caractéristiques et problèmes en matière de respect de la vie privée
L'application permet de collecter des informations personnelles dont le nom, la date de naissance, le sexe, la nationalité, le numéro de téléphone mobile, le numéro de téléphone mobile d'un membre de la famille et l'adresse où la quarantaine est effectuée. Il est intéressant de noter que le Centre coréen pour la prévention et le contrôle des maladies admet également que les patients sont d'abord interviewés puis, « pour vérifier les données qu'ils nous ont fournies et pour compléter ce qu'ils ne nous ont peut-être pas dit, nous utilisons les données GPS, les enregistrements des caméras de surveillance et les transactions effectuées avec des cartes de crédit pour recréer leur itinéraire la veille du jour où leurs symptômes se sont manifestés » (BBC 2020).

2. Singapour : l'application *TraceTogether*

De quoi s'agit-il ? Description du fonctionnement
L'application *TraceTogether* a été développée par l'Agence gouvernementale de Singapour pour les technologies (sous la direction du Premier ministre) et par le ministère de la Santé (source: tech.gov.sg/products-and-services/responding-to-covid-19-with-tech/). Cette application utilise les signaux Bluetooth pour déterminer si les téléphones mobiles des participants ont été en contact les uns avec les autres. L'application, basée sur un protocole appelé *BlueTrace* et sur un code source appelé *OpenTrace*, estime la distance entre les utilisateurs et la durée de leur rencontre. Les téléphones mobiles échangent les identifiants et l'application stocke l'historique des rencontres au niveau local (sur le téléphone mobile) pendant 21 jours. Ces données ne sont pas accessibles aux autorités. Si une personne est infectée, elle est invitée à partager l'historique de ses contacts avec les autorités sanitaires, qui peuvent ensuite s'assurer que la personne est isolée (Government Technology Agency of Singapore 2020).

Caractéristiques et problèmes en matière de respect de la vie privée
L'application présente un certain nombre de propriétés essentielles pour le respect de la vie privée, notamment le stockage local de l'historique des rencontres de l'utilisateur, l'utilisation d'identifiants temporaires et une autorisation révocable. Toutefois, pour télécharger et installer l'application, l'utilisateur doit donner explicitement son autorisation de participer au dispositif *TraceTogether* et accepter que son numéro de téléphone mobile et que les données de *TraceTogether* soient utilisées pour le traçage des contacts. En outre, si *l'encodage* des contacts est décentralisé (c'est-à-dire que les rencontres ne sont pas enregistrées dans une base de données centralisée), le *traçage* des contacts est centralisé : lorsqu'elle a conçu l'application, l'équipe *TraceTogether* a fait le choix fondamental de développer un système hybride (comportant une intervention humaine) plutôt qu'un système entièrement décentralisé. L'idée est que le diagnostic du COVID-19 doit être confirmé par un être humain pour éviter de faux rapports de contamination qui provoqueraient la panique. Le traçage centralisé des contacts commence lorsqu'un historique d'utilisateur est partagé avec le ministère dont les fonctionnaires classent ensuite ces contacts comme « étroits », « habituels » ou « éphémères », sur la base de la proximité et de la durée du contact, avant de prendre les mesures nécessaires.

3. Le traçage des contacts dans le respect de la vie privée d'Apple et Google

De quoi s'agit-il ? Description du fonctionnement
Google et Apple (2020a) ont annoncé leur intention de permettre l'utilisation de la technologie *Bluetooth Low Energy* pour aider les gouvernements et les services de santé à réduire la diffusion du COVID-19. Ces entreprises n'ont pas créé une application, mais une simple interface de programmation d'application (API) qui rendra possible l'interopérabilité entre les appareils Android et iOS et permettra plus facilement à d'autres acteurs de créer des applications de traçage. La plupart de ces applications utiliseront Bluetooth et opéreront de la manière décrite plus haut (TraceTogether). La prochaine étape pour Apple et Google

consistera à intégrer la fonctionnalité de l'API dans leurs systèmes d'exploitation (iOS et Android) (Apple 2020b).

Caractéristiques et problèmes en matière de respect de la vie privée

En privilégiant cette approche, Apple et Google ont choisi, non pas de lancer une application, mais de permettre à d'autres de le faire. Les risques décrits plus haut relatifs au respect de la vie privée sont toujours présents, en particulier ceux qui sont associés à la centralisation du traçage des contacts. La décentralisation de l'encodage et du traçage des contacts pourrait inciter davantage de personnes à participer à la formule, même si cela peut augmenter le risque de signalements positifs erronés.

Les niveaux d'adoption restent faibles, alors qu'ils devraient dépasser un certain seuil pour que l'application soit efficace : à Singapour, seulement 20% de la population a choisi d'utiliser *TraceTogether*. L'Australie estime qu'une application de traçage fonctionne si elle est utilisée par 40% de la population (Dalzell et Probyn 2020). Le ministère britannique de la Santé a fixé ce seuil à quelque 60 % de la population adulte.

Apple et Google affirment que « le respect de la vie privée, la transparence et le consentement sont de la plus haute importance ». Si, ce comme prévu, la technologie est intégrée dans leurs systèmes d'exploitation, nous pourrions être confrontés à une situation où un gouvernement, débordé par les cas de COVID-19 et les décès, ou frustré par le faible taux d'utilisation de l'application, ne demanderait plus l'autorisation des citoyens pour l'utiliser, mais les contraindrait à le faire.

4. L'initiative *Pan-European Privacy-Preserving Proximity-Tracing* (PEPP-PT)

Le projet de traçage de proximité paneuropéen préservant la confidentialité *(Pan-European Privacy-Preserving Proximity-Tracing* ou PEPP-PT) est conduit par un consortium réunissant plus de 130 membres dans huit pays européens.[1] Le projet porte sur le développement et la publication d'un code logiciel qui pourra être utilisé par les autorités nationales pour élaborer des applications de traçage du COVID-19. L'approche est très similaire à celle de *TraceTogether* et de l'initiative Apple/Google : elle est basée sur le signal Bluetooth, avec une garantie d'anonymisation des données et un souci d'interopérabilité transfrontalière. Thierry Breton, le commissaire européen pour le marché intérieur et les services, a récemment déclaré que la Commission européenne était en train de vérifier que l'emploi d'une application utilisant le logiciel PEPP-PT est bien conforme aux valeurs de l'UE.

Recommandations et exigences essentielles pour les applications de traçage des contacts

Les applications de traçage doivent respecter les règles et les principes essentiels du droit européen (c'est-à-dire le RGPD et la directive « vie privée et communications électroniques »), notamment la proportionnalité de la mesure en termes de durée et de champ d'application, la conservation limitée des données, la minimisation de ces données, leur suppression, la limitation de l'objet du traitement, une véritable anonymisation des données et une utilisation volontaire de l'application, basée sur un choix délibéré d'adhésion.

Lorsque des applications de traçage des contacts sont introduites, une évaluation des risques doit être effectuée.

Le pouvoir conféré à l'État de tracer les personnes doit être abrogé une fois que la crise est passée et une autorité indépendante doit être établie pour garantir le respect des règles (et pour intervenir si les règles ne sont pas respectées).

En outre, les États membres doivent également tenir compte des propositions formulées dans la « boîte à outils commune pour les États membres », présentée le 15 avril par le eHealth Network (2020), et dans la lettre du Comité européen de la protection des données (European Data Protection Board ou EDPB) à la direction générale de la justice et des consommateurs (EDPB 2020a).

La récente Stratégie européenne pour les données devrait tenir compte de la crise du COVID-19 pour établir un cadre de gouvernance qui tienne véritablement compte de la lutte contre la pandémie, afin d'éviter qu'en matière de gestion des données, le traçage des citoyens devienne la « nouvelle situation normale ».

Enfin, sur la base de la déclaration du Comité européen de la protection des données (EDPB 2020b), les douze exigences suivantes doivent être rencontrées :

1. Une législation doit avoir été adoptée avant qu'une application ne soit mise en place, et une surveillance parlementaire est nécessaire pendant le processus.
2. L'application doit être créée et mise en place par les pouvoirs publics plutôt que par des entreprises privées.
3. L'utilisation de l'application doit être assortie de garanties documentées et légalement établie.
4. Le code doit être de type open source et accessible gratuitement.
5. L'utilisation de l'application doit être proportionnelle, en termes de durée et de champ d'application. Comme l'indique le CEPD, « l'urgence est une condition légale qui peut légitimer des restrictions de liberté pour autant que ces restrictions soient proportionnelles et limitées à la période d'urgence ».
6. Limitation de l'objet : l'utilisation de l'application doit être limitée à l'arrêt de la diffusion du COVID-19. Seules des données de contacts minimales et pertinentes doivent être collectées et stockées.
7. Le système doit être totalement décentralisé, sans qu'aucune autorité centrale ne soit impliquée.
8. La conservation des données doit être limitée et les données collectées doivent être anonymes ou être rendues anonymes, cryptées et supprimées après un certain délai.
9. L'application doit être gratuite, basée sur une utilisation volontaire ; elle pourra être supprimée et elle ne sera pas intégrée dans le système d'exploitation de téléphones mobiles.
10. Les personnes qui refusent d'utiliser l'application ou qui

1 Ces pays sont l'Autriche, la Belgique, le Danemark, la France, l'Allemagne, l'Italie, l'Espagne et la Suisse.

décident de la supprimer après l'avoir installée ne peuvent être sanctionnées.
11. Les identifiants Bluetooth doivent changer régulièrement.
12. Aucun traçage de localisation ou de mouvement ne peut être rendu possible au départ du traçage des contacts.

Le traçage des contacts dans le contexte de l'emploi

Certains employeurs ont introduit ce qu'ils appellent des « solutions COVID » pour les travailleurs. En Belgique, le port d'Anvers a lancé l'utilisation de bracelets, ou de « preuves de santé » portables, développés par l'entreprise technologique Rombit, pour prévenir les infections au coronavirus dans l'environnement de travail (ATV 2020, Rombit 2020). Ce bracelet fonctionne de la même manière que les applications mobiles que l'on a décrites plus haut, sans connexion Internet. Si les travailleurs se rapprochent trop les uns des autres, une alarme se déclenche. Même si le site Internet de Rombit affirme que le dispositif « n'enregistre pas et ne stocke pas la localisation ou d'autres données confidentielles sensibles », l'outil permet de localiser et de suivre le travailleur individuel en temps réel. Le site Internet prétend que « toutes les informations personnelles sont totalement cryptées et conservées sur la plate-forme Romware, à laquelle seul l'employeur a accès. »

Dans le cas de travailleurs qui sont régulièrement ou fréquemment en contact avec des personnes potentiellement infectées, l'utilisation légitime et proportionnée d'applications de contrôle peut se justifier : par exemple, les travailleurs de la santé, les aides-soignants à domicile, les travailleurs des transports publics, le personnel des services d'urgence (dont les pompiers), les enseignants, les serveurs, etc. (Ellison 2020, Gamio 2020). Mais dans tous ces cas, les employeurs doivent toujours démontrer qu'il existe une raison impérieuse justifiant l'utilisation de systèmes de traçage des contacts sur le lieu de travail, qu'il n'existe aucune solution alternative moins envahissante, et que de telles initiatives n'ouvrent pas la voie à une culture de l'hypersurveillance.

Les syndicats ont également un rôle essentiel à jouer et ils doivent être impliqués à chaque étape du processus. Cela inclut l'évaluation des risques, une démarche nécessaire avant de pouvoir envisager l'utilisation d'une application. Le déploiement d'une application ne peut avoir lieu qu'à la condition que la mesure : (1) respecte les droits du travail, (2) soit négociée avec les représentants des travailleurs, (3) soit conforme aux règles du RGPD (4) et aux exigences indiquées ci-dessus, et qu'elle respecte les critères formulés ci-après :

1. Elle ne collecte les données personnelles que dans le seul but de prévenir la contagion du COVID-19, et pour aucune autre fin.
2. Elle exige le consentement explicite des travailleurs pour le traitement de leurs données spécifiques.
3. Elle fournit aux travailleurs des informations simples, claires et transparentes sur la manière dont leurs données vont être utilisées.
4. Elle ne collecte les données que dans la mesure de ce qui est strictement nécessaire à la protection de la santé des travailleurs, et non à des fins de surveillance ou à toute autre fin.
5. Elle s'accompagne de la mise en place de nouvelles mesures de gestion du risque et d'organisation au sein de l'entreprise pour évaluer les changements apportés aux conditions environnementales et de travail, et pour assurer la sécurité des données.
6. Elle fixe des limites à la durée de la conservation des données.
7. Elle implique la participation active des représentants des travailleurs et des délégués à la protection des données.

Remarques finales

La pandémie du COVID-19 a transformé l'impossible en réalité : la technologie et les applications de traçage se développent partout, sans coordination, sans débat démocratique et avec très peu d'opposition. Les circonstances sont exceptionnelles et peuvent justifier des mesures exceptionnelles, mais celles-ci ne peuvent devenir la nouvelle normalité. Ce risque est bien réel et la question du traçage des citoyens et des travailleurs doit être, et sera, une priorité essentielle et structurelle du mouvement syndical européen et international.

D'un point de vue juridique, le cadre légal européen – en ce compris le RGPD et la récente « Stratégie européenne des données » qui présente la vision de la Commission européenne sur l'accès aux données, leur utilisation et leur réutilisation – donne aux citoyens européens le droit de protéger leur vie privée et leurs données à caractère personnel. Le COVID-19 ne peut justifier une remise en cause de ce droit : les technologies de traçage et de surveillance ne sont pas une baguette magique qui permettra de résoudre le problème sans douleur ; elles ne peuvent être utilisées qu'à des fins légitimes, si et quand cela s'avère nécessaire et à condition que de véritables garanties soient mises en place.

Références

Apple et Google (2020a) Apple and Google partner on COVID-19 contact tracing technology, 10 April 2020. https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology

Apple et Google (2020b) Privacy-preserving contact tracing. https://www.apple.com/covid19/contacttracing

ATV (2020) Port of Antwerp test slimme armband om coronabesmettingen op de werkvloer te voorkomen, 17 April 2020. https://atv.be/nieuws/port-of-antwerp-test-slimme-armband-om-coronabesmettingen-op-de-werkvloer-te-voorkomen

BBC (2020) Coronavirus privacy: are South Korea's alerts too revealing? 5 March 2020. https://www.bbc.com/news/world-asia-51733145

Central Disaster and Safety Countermeasures Headquarters (2020) Guide on the installation of "self-quarantine safety protection app". http://ncov.mohw.go.kr/upload/ncov/file/202004/1585732793827_20200401181953.pdf

Dalzell S. et Probyn A. (2020) Convincing Australians to use government-sponsored coronavirus-tracing app a tough ask, ABC News, 15 April 2020. https://www.abc.net.au/news/2020-04-15/challenge-to-convince-australians-to-use-coronavirus-tracing-app/12151130

eHealth Network (2020) Mobile applications to support contact tracing in the EU's fight against COVID-19: common EU toolbox for Member States, 15 April 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

Ellison J. (2020) Millions of US workers at risk of infections on the job, UW researchers calculate, emphasizing need to protect against COVID-19, UW News, 6 March 2020. https://www.washington.edu/news/2020/03/06/millions-of-us-workers-at-risk-of-infections-on-the-job-uw-researchers-calculate-emphasizing-need-to-protect-against-covid-19/

European Data Protection Board (2020a) Letter to Olivier Micol, Head of Unit European Commission, DG for Justice and Consumers, 14 April 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

European Data Protection Board (2020b) Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

Fildes N. et Espinoza X. (2020) Tracking coronavirus: big data and the challenge to privacy, Financial Times, 8 April 2020. https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987

Gamio L. (2020) The workers who face the greatest coronavirus risk, The New York Times, 15 March 2020. https://www.nytimes.com/interactive/2020/03/15/business/economy/coronavirus-worker-risk.html

Government Technology Agency of Singapore (2020) 6 things about OpenTrace, the open-source code published by the TraceTogether team. https://www.tech.gov.sg/media/technews/six-things-about-opentrace

Knight W. (2020) How AI is tracking the coronavirus outbreak, Wired, 8 February 2020. https://www.wired.com/story/how-ai-tracking-coronavirus-outbreak/

Leung H. (2020) Why Singapore, once a model for coronavirus response, lost control of its outbreak, Time, 20 April 2020. https://time.com/5824039/singapore-outbreak-migrant-workers/

Lewis P., Conn D. et Pegg D. (2020) UK government using confidential patient data in coronavirus response, The Guardian, 12 April 2020. https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response

Manancourt V. (2020) Coronavirus tests Europe's resolve on privacy, Politico, 10 March 2020. https://www.politico.eu/article/coronavirus-tests-europe-resolve-on-privacy-tracking-apps-germany-italy/

McCurry J. (2020) Test, trace, contain: how South Korea flattened its coronavirus curve, The Guardian, 23 April 2020. https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve

Mesmer P. (2020) Endiguer le coronavirus : Singapour et la Corée du Sud, des exemples à suivre, L'Express, 18 mars 2020. https://www.lexpress.fr/actualite/monde/asie/endiguer-le-coronavirus-singapour-et-la-coree-du-sud-des-exemples-a-suivre_2121024.html

Rombit (2020) Smart bracelet to prevent coronavirus infections on the workfloor, 17 April 2020. https://rombit.be/smart-bracelet-to-prevent-coronavirus-infections-in-the-workplace/

Directeurs de publication de la série: Jan Drahokoupil, Philippe Pochet, Aída Ponce Del Castillo, Kurt Vandaele and Sigurt Vitols.
Responsable de ce numéro: Kurt Vandaele, kvandaele@etui.org
Les numéros précédents se trouvent sur le site www.etui.org/publications. D'autres informations sur l'ETUI sont également accessibles sur le site www.etui.org.

L'ETUI bénéficie du soutien financier de l'Union européenne. L'Union européenne ne peut être tenue responsable de l'utilisation qui pourrait être faite de l'information contenue dans cette publication.