Covid-19 impact series

ETUI Policy Brief

European Economic, Employment and Social Policy

N°5/2020

Aplicaciones de rastreo de contactos del COVID-19: cómo evitar que la privacidad se convierta en la próxima víctima

Aída Ponce Del Castillo

Aída Ponce del Castillo es investigadora principal en el Instituto Sindical Europeo (ETUI) en Bruselas, Bélgica.

Mensajes clave

- **El uso de aplicaciones de rastreo de contactos para combatir la propagación de COVID-19 es intrusivo y amenaza el derecho a la privacidad de los ciudadanos de la Unión Europea (UE). Para defender este derecho, deben respetarse las normas y principios clave de la legislación de la UE, en particular los incluidos en el Reglamento General de Protección de Datos (GDPR, acrónimo de las siglas en inglés) y la Directiva de privacidad y comunicaciones electrónicas.**
- **Alegar que la defensa de la privacidad socava la lucha contra la pandemia y la reapertura de la economía es un error: para que las aplicaciones de rastreo de contactos sean efectivas, deben ser descargadas y utilizadas voluntaria y libremente por una mayoría de la ciudadanía. Esto solo sucederá si los ciudadanos confían en que su privacidad no está en juego. Las dos batallas, por la privacidad y contra la COVID-19, son complementarias, no opuestas.**
- **Las aplicaciones de rastreo de contactos solo deben usarse en el lugar de trabajo si se cumplen los requisitos específicos (en relación, entre otros aspectos, con el propósito de la aplicación, el tipo de datos recopilados, la duración de la retención de datos, el consentimiento de los trabajadores y la implicación de los sindicatos).**
- **Finalmente, es de suma importancia que las aplicaciones de rastreo de contactos no se usen para sembrar las semillas de una cultura futura de hipervigilancia en el lugar de trabajo.**

Introducción

La pandemia de la COVID-19 está lejos de terminar y el número de víctimas lamentablemente seguirá aumentando. Sin embargo, en la segunda semana de abril de 2020, varios Estados miembro de la Unión Europea (UE) como Austria, España y Dinamarca, entre otros, comenzaron a levantar sus confinamientos. Otros países están tomando medidas similares desde principios de mayo.

En paralelo, las aplicaciones de rastreo se han señalado de forma creciente como herramientas útiles para acompañar y contribuir a un retorno a la normalidad, a pesar de las muchas cuestiones éticas y legales que plantean. El 14 de abril, el Reino Unido reveló que lanzaría una aplicación para rastrear a las personas que informan de síntomas de la COVID-19 y para alertar a las personas que estuvieron en contacto con las mismas. El 10 de abril, Apple y Google (2020a) anunciaron que se asociarían para lanzar "una solución integral que incluye interfaces de programación de aplicaciones (API en su acrónimo en inglés) y tecnología de nivel de sistema operativo para ayudar a habilitar el rastreo de contactos". El 21 de abril, el primer ministro holandés, Mark Rutte, dijo que el desarrollo de las aplicaciones de rastreo de la COVID-19 continuaría, a pesar de probar siete y descubrir que todas fracasaron en cumplir con los requisitos de seguridad, privacidad y confiabilidad.

La presión ejercida por los círculos empresariales y los grupos de presión para reiniciar y "salvar la economía" ha sido intensa. Lo que comenzó como una crisis de salud pública se ha transformado en una crisis económica y ahora nos enfrentamos a una elección del tipo "*truco o trato*": aceptar "pagar el precio" y el uso invasivo de aplicaciones de rastreo y, al hacerlo, facilitar una reapertura gradual de los negocios; o luchar por la privacidad y retrasar el regreso a la normalidad.

etui.

Necesitamos rechazar esta elección binaria. Defender la privacidad no socava el reinicio de la economía: para que las aplicaciones de rastreo de contactos sean efectivas, deben ser descargadas y utilizadas voluntaria y libremente por una mayoría de la ciudadanía. Esto solo ocurrirá si las ciudadanas y ciudadanos confían en que su privacidad no está en juego. Esta puede ser la diferencia entre un número limitado de personas que usen las aplicaciones, lo que las haría inútiles, y su utilización masiva, el primer paso para asegurar su efectividad.

Perder nuestros derechos de privacidad no puede ser el precio que tenemos que pagar para reiniciar la economía. Este *Policy Brief* recoge varios requisitos clave que deberían ayudarnos a lograr esto, tanto como ciudadanas y ciudadanos como en nuestros lugares de trabajo.

Múltiples apps, múltiples enfoques tecnológicos, múltiples problemas de privacidad

Ante el inevitable despliegue de la tecnología de rastreo en la lucha contra la COVID-19, tenemos que tomar una decisión. ¿Estamos dispuestos a vivir en un mundo "COVID-1984", bajo un autoritario sistema de vigilancia orwelliana, con rastreo generalizado de la ciudadanía y el fin de la privacidad? ¿Comenzamos a usar aplicaciones desarrolladas por corporaciones privadas que nos pedirán que confiemos y compartamos con las mismas nuestros datos personales y de ubicación? ¿O llamamos a un enfoque común de la UE y a una aplicación basada en las normas GDPR, incluida la privacidad por diseño, que ayudará a combatir la propagación del virus y proteger la privacidad de las personas?

Las aplicaciones se desarrollan actualmente con muy poca o ninguna coordinación y enfoques muy diversos: algunas recogen datos anónimos y agregados para monitorear los movimientos de población, para imponer confinamientos, o para recopilar datos estadísticos; otras se centran en la autoevaluación. Esfuerzos más recientes se han centrado en aplicaciones de rastreo de contactos, que localizan y rastrean pacientes infectados, personas posiblemente infectadas y los individuos con los que han estado en contacto con las mismas.

Todas sufren de serios defectos: son invasivas; como herramientas de alerta temprano solo funcionan si un número significativo de personas instalan y activan la aplicación; pueden crear alarmas innecesarias o confusión al generar falsos positivos. Peor aún, no siempre son de confianza. En primer lugar, la señal Bluetooth viaja más lejos en espacios abiertos que en entornos urbanos, lo que significa que puede dar falsos positivos o falsos negativos. Además, se puede estar a pocos metros de alguien y no estar en riesgo – por ejemplo, si la señal alerta de alguien que está parado al otro lado de una pared – mientras que un asiento del suburbano puede seguir siendo un "punto de acceso" del virus durante varias horas.

La deficiencia más evidente de estas aplicaciones está relacionada con la privacidad. La tecnología y la legislación de emergencia pueden ayudar a contener o limitar la crisis de la COVID-19, pero es necesario tener un debate democrático sobre el rápido despliegue de soluciones tecnológicas que parecen anular derechos fundamentales, incluido el diálogo social, así como los derechos de información, consulta y participación. La adopción de estas tecnologías plantea nuevos problemas y riesgos graves en el contexto de la privacidad y la protección de datos.

En varios países del mundo, se han implementado soluciones a veces extremas. El panel de control COVID-19 de Singapur, por ejemplo, comparte información sobre cada individuo infectado, incluido su origen étnico, edad, sexo y, en algunos casos, dónde viven, donde trabajan, el hospital en el que están y a quién pueden haber infectado (https://co.vid19.sg/singapore/). Igualmente inaceptables son las soluciones que crean el riesgo de que los datos confidenciales del paciente sean compartidos con empresas tecnológicas de EE. UU. El 12 de abril, Lewis et al. (2020) reveló que Palantir, una empresa estadounidense de big data, y Faculty, una start-up británica de inteligencia artificial, están involucradas en una operación de minería de datos lanzada por el gobierno del Reino Unido que implica almacenar información de salud sensible y confidencial en una base de datos central, incluyendo el contenido de las llamadas de las personas al Servicio de línea de ayuda del Sistema Nacional de Salud del Reino Unido.

Dada la multiplicidad de aplicaciones y enfoques tecnológicos desarrollados a nivel mundial para abordar la crisis de la COVID-19, el Instituto Sindical Europeo (ETUI en su acrónimo en inglés) está creando un mapa de iniciativas de contención de COVID-19 (disponible en línea en www.etui. org), basándose en el trabajo realizado por gdprhub.eu y otras fuentes, que se actualizará periódicamente.

El presente *Policy Brief* aborda cuatro casos de uso de tecnología: la aplicación de Protección de Seguridad de Auto-Cuarentena de Corea del Sur; la aplicación *TraceTogether* (rastrear juntos) de Singapur; la reciente iniciativa conjunta de Apple y Google; y la Iniciativa de Rastreo Paneuropeo de Proximidad para Preservar la Privacidad. Estos casos de uso fueron seleccionados porque describen cuatro diferentes realidades: Singapur y Corea del Sur se han presentado como ejemplos en todo el mundo por su efectividad en contener la propagación del virus (Mesmer 2020; McCurry 2020; Leung 2020). La interfaz de programación de aplicaciones (API) de Apple / Google y la Iniciativa de Rastreo Paneuropeo de Proximidad para Preservar la Privacidad fueron seleccionadas porque son iniciativas conjuntas que afirman colocar la privacidad y seguridad del usuario en el núcleo de su diseño.

Este *Policy Brief* presenta a continuación una lista de recomendaciones y requisitos que las aplicaciones de seguimiento de contactos deben cumplir para que sean efectivas y asimismo garanticen la privacidad del usuario.

Finalmente, se examina el caso específico de las **aplicaciones de rastreo de contactos utilizadas en un contexto laboral.**

4 casos de uso de la tecnología

1. Corea del Sur: la Protección de Seguridad de Auto-Cuarentena

¿Qué es y cómo funciona?
Desarrollada por el Ministerio del Interior y Seguridad, esta aplicación utiliza la tecnología GPS para monitorear y rastrear

a los ciudadanos infectados en auto-cuarentena. La aplicación permite a los funcionarios del gobierno rastrear la ubicación de cada paciente en auto-cuarentena. En caso de incumplimiento, se activa una alerta. Además, un proceso de comunicación se establece entre usuarios y funcionarios, con los pacientes informando de sus síntomas a un funcionario de caso del gobierno local dos veces al día. Cualquiera que salga de su ubicación de cuarentena sin permiso se enfrenta hasta a un año de prisión o una multa de 7.500 euros. Cualquier persona extranjera que se niegue a instalar la aplicación o deje el área de cuarentena sin permiso enfrenta a la deportación inmediata (Central Disaster and Safety Countermeasures Headquarters, 2020).

Características y problemas de privacidad
La aplicación recopila información personal, incluido el nombre, la fecha de nacimiento, género, nacionalidad, número de teléfono móvil, número teléfono móvil número de un miembro de la familia y dirección donde la cuarentena está teniendo lugar. Curiosamente, el Centro de Corea para el Control y Prevención de Enfermedades también admite que los pacientes son entrevistados primero, luego "para completar las áreas que tal vez no nos han dicho, y también para verificar, utilizamos datos de GPS, cámaras de vigilancia y transacciones de tarjetas de crédito para recrear su ruta un día antes de que se mostraran sus síntomas" (BBC 2020).

2. Singapur: la aplicación *TraceTogether* (rastrear juntos)

¿Qué es y cómo funciona?
Desarrollado por la Agencia de Tecnología del Gobierno de Singapur (bajo la dirección del Primer Ministro) y el Ministerio de Salud (GOVTECH Singapur 2020), *TraceTogether* (rastrear juntos) es una aplicación que usa señales Bluetooth para determinar si los teléfonos móviles que participan han estado en contacto entre sí. La aplicación, basada en un protocolo llamado *BlueTrace* y una base de código llamado *OpenTrace*, estima la distancia entre usuarios y la duración del encuentro. Los identificadores del intercambio de teléfonos móviles y la aplicación almacena este historial de encuentros localmente (en el teléfono móvil) durante 21 días. Los datos no son accesibles para las autoridades. Si alguien se infecta, se les pregunta para compartir su historial de contactos con la autoridad sanitaria, que entonces puede asegurar que la persona esté aislada (Government Technology Agency of Singapore 2020).

Características y problemas de privacidad
La aplicación integra características de privacidad clave, incluido el almacenamiento local del historial de encuentros del usuario, identificadores temporales y consentimientos revocables. Sin embargo, para descargar y configurar la aplicación, el/la usuario/a debe dar su consentimiento explícito para participar en *TraceTogether* y aceptar que su número de teléfono móvil y los datos de *TraceTogether* sean utilizados para el rastreo de contactos. Además, mientras que el registro de contactos está descentralizado (es decir, no se cargan los encuentros en una base de datos central), el rastreo está centralizado: al diseñar la aplicación, el equipo de *TraceTogether* tomó la decisión fundamental de desarrollar un sistema híbrido ("humano en el circuito") en lugar de un sistema totalmente descentralizado. La idea es que los diagnósticos de la COVID-19 deben ser confirmados por un ser humano para evitar falsos informes de contagio, que podrían provocar pánico. El rastreo centralizado de contactos comienza cuando la historia de el/la usuario/a se comparte con el Ministerio, cuyos funcionarios luego clasifican los contactos en "cercanos", "casuales" y "transitorios", según la proximidad y duración, y luego toman las medidas necesarias.

3. El rastreo de contactos para preservar la privacidad de Apple y Google

¿Qué es y cómo funciona?
Google y Apple (2020a) han anunciado que quieren permitir el uso de la tecnología *Bluetooth Low Energy* para ayudar a los gobiernos y agencias de salud a reducir la propagación de la COVID-19. No están creando una aplicación, sino una Interfaz de Programación de Aplicaciones (API en su acrónimo en inglés) que permitirá la interoperabilidad entre dispositivos Android e iOS y hacer que sea más fácil para otros actores construir aplicaciones de rastreo. La mayoría de estas aplicaciones usarán Bluetooth y operan como se describe anteriormente (*TraceTogether*). El siguiente paso para Apple y Google será integrar la funcionalidad de la API en sus sistemas operativos (iOS y Android) (Apple 2020b).

Características y problemas de privacidad
En este enfoque, Apple y Google no están lanzando una aplicación sino permitiendo que otros lo hagan. Los riesgos de privacidad descritos anteriormente permanecen, en particular los asociados con la centralización del rastreo de contactos. La descentralización tanto del registro de contactos como del rastreo puede ser la forma en que más personas se convencerán de unirse, incluso si esto aumenta el riesgo de falsos positivos.

De hecho, las tasas de adopción siguen siendo bajas y deben estar por encima de cierto umbral para que la aplicación sea efectiva: en Singapur, solo el 20% de la población ha elegido usar *TraceTogether*. Australia estima que la aplicación de seguimiento funcionaría si se usara en un 40% (Dalzell y Probyn 2020). El Ministerio de Salud del Reino Unido ha establecido el umbral en torno al 60% de la población adulta.

Apple y Google afirman que la "privacidad, transparencia y consentimiento son de suma importancia". Si según lo planeado, la tecnología se integra en su sistema operativo, podríamos enfrentar una situación donde un gobierno – sobrecargado de casos y muertes de COVID-19 o frustrado por el bajo uso de su aplicación – ya no requeriría el consentimiento de los ciudadanos para usarlo, sino que les obligaría a hacerlo.

4. La Iniciativa de Rastreo Paneuropeo de Proximidad para Preservar la Privacidad (PEPP-PT)

La Iniciativa de Rastreo Paneuropeo de Proximidad para Preservar la Privacidad (PEPP-PT, en su acrónimo en inglés) es un proyecto liderado por un consorcio de la UE con más de 130 miembros en ocho países de Europa[1]. Tiene la intención de desarrollar y lanzar un código software que pueden usar las autoridades nacionales para

1 Estos países son Alemania, Austria, Bélgica, Dinamarca, España, Francia, Italia y Suiza.

construir las aplicaciones de rastreo de la COVID-19. El enfoque es muy similar al de *TraceTogether* y la Iniciativa Apple/Google basada en la señal Bluetooth, con datos seguros, anonimización e interoperabilidad transfronteriza. El Comisario de la UE para el Mercado Interior y los Servicios, Thierry Breton, ha declarado recientemente que la Comisión Europea está verificando si una aplicación que usa el software PEPP-PT realmente cumpliría con los valores de la UE.

Recomendaciones y requisitos clave para las aplicaciones de rastreo de los contactos

Las aplicaciones de rastreo deben respetar las reglas y principios clave del derecho de la UE (por ejemplo, el Reglamento General de Protección de Datos y la Directiva de privacidad electrónica) que cubren: la proporcionalidad de la medida en términos de duración y alcance; retención limitada de datos; minimización de datos; eliminación de datos; limitación de propósito; anonimización genuina de datos; y el uso voluntario de la aplicación y basado en las personas que optan por participar.

Si cuando se introduzcan las aplicaciones de rastreo de contactos, debe llevarse a cabo una evaluación de riesgos.

El poder otorgado al Estado para rastrear a las personas debe ser removido una vez que la crisis haya terminado, y una autoridad independiente debería establecerse para garantizar que se implementan las reglas (y para actuar si no lo son).

Además, lo que se propone en la "Caja de herramientas Común de la UE para los Estados miembros" publicada el 15 de abril por la Red de eSalud (2020), y en la carta de la Junta Europea de Protección de Datos (EDPB en su acrónimo en inglés) a la Dirección General de Justicia y Consumidores (EDPB 2020a) debería ser tenido en cuenta por los Estados miembros.

La recientemente lanzada Estrategia Europea de Datos debería tomar en cuenta la crisis COVID-19 y establecer un marco de gobernanza que realmente considera la dimensión de datos de la pandemia, para que el rastreo de los ciudadanos no se convierta en la "nueva normalidad".

Finalmente, sobre la base de la declaración del Consejo Europeo de Protección de Datos (EDPB 2020b), se deben cumplir los siguientes 12 requisitos:

1. Se debe aprobar la legislación antes de implementar una aplicación, y se necesita la supervisión parlamentaria durante el proceso.
2. La aplicación debe ser creada e implementada por las autoridades públicas, en lugar de por empresas privadas.
3. El uso de la aplicación debe basarse en la seguridad documentada y legalmente establecida.
4. El código debe ser de fuente abierta y libre acceso.
5. El uso de la aplicación debe ser proporcional en términos de duración y alcance. Según lo declarado por la EDPB, "la emergencia es una condición legal que puede legitimar restricciones de libertades, siempre que las restricciones sean proporcionadas y limitadas al período de emergencia".
6. Limitación del propósito: el uso de la aplicación debe limitarse a detener la propagación de la COVID-19. Solo los datos de contacto mínimos y relevantes deben ser recolectados y almacenados.
7. El sistema debe ser totalmente descentralizado, sin ninguna autoridad central involucrada.
8. La retención de datos debe ser limitada, y los datos recopilados deben ser anónimos o anonimizados, encriptados y eliminados después de una cierta cantidad de tiempo.
9. La aplicación debe ser gratuita, basada en el uso voluntario (opt in) y removible, no integrada en el sistema operativo de los teléfonos móviles.
10. Las personas que se niegan a usarla o deciden eliminarla después de la instalación no deben ser penalizadas.
11. Los identificadores de Bluetooth deben cambiar regularmente.
12. No debería ser posible derivar el rastreo de la ubicación o movimiento del rastreo de contactos.

El rastreo de contactos en el contexto laboral

Algunos empleadores han introducido lo que llaman "soluciones COVID" para los trabajadores. En Bélgica, el puerto de Amberes ha lanzado el uso de pulseras o *wearables* "prueba de salud", desarrollado por la empresa de tecnología Rombit, para prevenir las infecciones por coronavirus en su entorno de trabajo (ATV 2020, Rombit 2020). Esta pulsera funciona de manera similar a las aplicaciones móviles descritas anteriormente, pero sin ninguna conexión a internet. Si los trabajadores se acercan demasiado entre sí, se activa una alarma. Aunque el sitio web de Rombit dice que "no captura ni almacena la ubicación u otros datos privados delicados", la herramienta presenta la localización de trabajadores individuales en tiempo real y la monitorización. El sitio web afirma que "cualquier información personal está totalmente encriptada y guardada en la plataforma *Romware* y solo es accesible por el empleador".

De hecho, puede haber un caso para el uso legítimo y proporcionado de aplicaciones de monitoreo en el caso de trabajadores que mantienen un encuentro regular o frecuente con personas potencialmente infectadas: trabajadores de asistencia sanitaria; cuidadores domésticos; empleados de transporte público; agentes de la ley; socorristas (incluidos los bomberos); maestros; camareros, etc. (Ellison 2020, Gamio 2020). En esos casos, sin embargo, los empleadores aún deben demostrar que hay una razón sólida para justificar el uso de sistemas de rastreo de contactos en el lugar de trabajo, que no hay una solución alternativa menos intrusiva y que tales iniciativas no "siembran las semillas" de una cultura de hipervigilancia.

Los sindicatos también tienen un papel clave que desempeñar y deberían participar en cada paso del proceso. Esto incluye evaluar los riesgos, un paso necesario antes de poder prever el uso de una aplicación. El despliegue de la aplicación puede tener lugar, siempre que: (1) respete los derechos laborales; (2) se negocie con los representantes de los trabajadores; (3) siga las reglas del GDPR; y (4) así como los requisitos presentados anteriormente, en base a los siguientes criterios:

1. Recopila datos personales exclusivamente para evitar el contagio de COVID-19, y no para otros fines.
2. Requiere el consentimiento explícito de los trabajadores para procesar estos datos específicos.
3. Proporciona información simple, clara y transparente sobre cómo se van a utilizar los datos.
4. Recopila datos estrictamente necesarios para proteger la salud de trabajadores, y no para perseguir la vigilancia o para otros fines.
5. Pone en marcha nuevas medidas de organización y gestión de riesgos en la empresa, para evaluar los cambios en el medio ambiente y las condiciones de trabajo y para mantener los datos seguros.
6. Establece límites a la duración de la retención de datos.
7. Implica la participación activa de los representantes de los trabajadores y los responsables de protección de datos".

Consideraciones finales

La pandemia de la COVID-19 ha hecho realidad lo imposible: la tecnología de rastreo y las aplicaciones están surgiendo en todas partes, sin coordinación, sin debate democrático y con muy poca oposición. Las circunstancias son excepcionales y pueden requerir medidas excepcionales, pero éstas no deberían convertirse en la nueva normalidad. Este es un riesgo real y la localización de ciudadanos y trabajadores debería ser y será una prioridad clave y estructural para el movimiento sindical europeo y mundial.

Desde una perspectiva legal, el marco legal de la UE – incluyendo el GDPR y la reciente "Estrategia Europea de Datos", que establece la visión de la Comisión de la UE sobre el acceso, uso y reutilización de datos – otorga a los ciudadanos europeos el derecho a proteger su privacidad y datos personales. No se debe permitir que la COVID-19 amenace este derecho: las tecnologías de rastreo y monitoreo no son una varita mágica que resolverán el problema de forma indolora; solo deben usarse para fines legítimos, cuando y si se demuestra necesario, y con las salvaguardas reales en su lugar.

Referencias

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

Apple y 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-omcoronabesmettingen-op-de-werkvloer-te-voorkomen

BBC (2020) Coronavirus privacy: are South Korea's alerts too revealing? 5 March 2020. https://www.bbc.com/news/worldasia-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. y 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-coronavirustracing-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-ofinfections-on-the-job-uw-researchers-calculate-emphasizingneed-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. y 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 coronavirusrisk, The New York Times, 15 March 2020. https://www.nytimes.com/interactive/2020/03/15/business/economy/coronavirusworker-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-aboutopentrace

Knight W. (2020) How AI is tracking the coronavirus outbreak, Wired, 8 February 2020. https://www.wired.com/story/how-aitracking-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. y 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-incoronavirus-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-appsgermany-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-howsouth-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-lecoronavirus-singapour-et-la-coree-du-sud-des-exemples-asuivre_2121024.html

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

La traducción al español ha sido realizada gracias a la Fundación 1º de Mayo de la Confederación Sindical de Comisiones Obreras (CC.OO).

The *ETUI Policy Brief* series is edited jointly by Jan Drahokoupil, Philippe Pochet, Aída Ponce Del Castillo, Kurt Vandaele and Sigurt Vitols.
The editor responsible for this issue is Kurt Vandaele, kvandaele@etui.org
This electronic publication, as well as previous issues of the *ETUI Policy Briefs*, is available at www.etui.org/publications. You may find further information on the ETUI at www.etui.org.

The ETUI is financially supported by the European Union.
The European Union is not responsible for any use made of the information contained in this publication.