Documento de trabajo 9/2020
12 de mayo de 2020

La búsqueda de inmunidad digital frente a la pandemia: eficacia, privacidad y vigilancia

Andrés Ortega

La búsqueda de inmunidad digital frente a la pandemia: eficacia, privacidad y vigilancia

Andrés Ortega | Investigador sénior asociado,Real Instituto Elcano | @andresortegak

Índice

Resumen

El trazado por móvil de infectados por el coronavirus, para el que se han ideado una serie de aplicaciones y Apple y Google han lanzado una importante iniciativa conjunta, puede ser un elemento decisivo en la lucha contra la pandemia, sobre todo de cara al posconfinamiento, pero plantea retos de privacidad y confianza a los que es necesario responder, para su éxito, con pedagogía y respetando una serie de principios.

El trazado, o "rastreo y alerta" (*tracing*), por aplicaciones de móviles o por otros sistemas (o combinaciones de ellos) de infectados por el coronavirus puede ser una aportación decisiva en la lucha contra esta pandemia, sobre todo en el posconfinamiento y ante posibles nuevos brotes. El equilibrio entre seguridad y privacidad se puede romper a favor de la primera. Es necesario generar la confianza suficiente entre la población, para lo cual se requiere respetar la regulación y una serie de principios generales. La iniciativa conjunta de Apple y Google, dado el alcance de sus sistemas operativos, puede marcar un punto de inflexión. La UE ha propuesto unos principios y prioridades y ha establecido una hoja de ruta a los Estados miembros para asegurar la transparencia y la esencial interoperabilidad de las posibles aplicaciones. Se propone promover principios tales como el consentimiento social, voluntariedad, respeto de la ley y los derechos humanos, temporalidad y reversibilidad, transparencia, anonimidad, proporcionalidad y el *quid pro quo* de las empresas con los usuarios.

Introducción[1]

Gobiernos, epidemiólogos y tecnólogos están crecientemente interesados en el uso de las tecnologías de datos para luchar contra la pandemia de la COVID-19. Entre estas tecnologías destacan las de sistemas de trazado de poblaciones e individuos para controlar la expansión del virus en sus fases actuales o ante futuros nuevos brotes o pandemias. Puede ser una extraordinaria ayuda para gestionar la expansión del virus, reducir las infecciones y las muertes y quitar presión en las unidades de cuidados intensivos de los hospitales. El trazado o rastreo de contactos se hace en toda pandemia y es una práctica esencial, considerada prioritaria por la Organización Mundial de la Salud (OMS). Permitiría gestionar mejor y acortar los tiempos de confinamiento. Estas nuevas tecnologías posibilitarían sustituir una labor que habría que hacer manualmente, aunque parte de su utilidad también dependerá a su vez de las estrategias de salida que se sigan, sin ignorar que la solución será epidemiológica y médica, no tecnológica. Es una herramienta que puede ser muy útil para la gestión, pero no será una solución, aunque sí parte de ella, y se debería poner en marcha rápidamente –no en cuestión de meses, sino de semanas– para que esté presente en las primeras fases del desconfinamiento y le sirva de apoyo en su gestión.

Para España puede ser doblemente importante, por sí misma y para llegar a una nueva normalidad de cara al turismo, sobre todo europeo y extracomunitario, por lo que unas

[1] Quiero agradecer las aportaciones y comentarios de Rubén Cuevas Rumín (Universidad Carlos III de Madrid, UC3M), Ángel Cuevas Rumín (UC3M), Manuel Cebrián (Max Planck Institute for Human Development, Berlín), María Álvarez (Google) y Gloria Álvarez (UC3M y Dubitare), así como a los participantes en el Grupo de Trabajo sobre Transformaciones Tecnológicas del Real Instituto Elcano, que se reunió de forma virtual para abordar esta cuestión

aplicaciones (*apps*) de trazado instaladas en los móviles que fueran interoperables a escala de toda la UE –y, mejor aún, a escala mundial– serían de gran utilidad para reforzar la confianza –de los españoles y de los visitantes– en España como un país seguro.

Estas posibilidades, que ya se han puesto en práctica con relativo éxito en varios países, como Corea del Sur y Taiwán, demuestran que el conocimiento y análisis de los datos puede ser una herramienta útil en el diseño de políticas públicas y privadas para luchar contra el virus, pero, dependiendo de la solución adoptada, puede plantear quebrantos en la protección de datos personales sensibles más allá de su uso para aliviar esta crisis.

El trazado de contactos a través de individuos infectados, esencialmente mediante los móviles inteligentes, convertidos en "nuevas armas" contra el coronavirus[2], está demostrando ser una herramienta útil en la lucha contra la pandemia –siempre que se acompañe de test masivos sobre la infección y otras medidas– y también para medir el impacto de las políticas que se están siguiendo y ajustarlas. Por todo ello, los datos son necesarios. Desde hace tiempo, se sabe que el trazado de comunicaciones a través de los móviles puede servir para hacer un seguimiento de los contactos físicos[3] y para la reconstrucción de la historia de los contagios, aunque existen otras herramientas disponibles para medir el éxito de las medidas de distanciamiento social, confinamiento o restricción de movimiento.

Dependiendo de qué tipos de datos se usen, de las arquitecturas tecnológicas y de los agentes que intervengan en su tratamiento –y hay diversas opciones–, pueden plantearse problemas de privacidad si la situación se mantiene más allá de la pandemia o si se utilizan estas herramientas para otras finalidades, por lo que requerirán respetar ciertos principios, como el consentimiento social, anonimidad relativa, cumplimiento de la ley y los derechos humanos, finalidad, minimización de datos y proporcionalidad, temporalidad y reversibilidad, voluntariedad, transparencia, proporcionalidad y *quid pro quo* de las empresas con los usuarios.

Singapur, uno de los modelos más citados al principio en términos de trazado de contactos y usabilidad de los datos, marcó un camino, aunque en realidad no ha acabado de funcionar. Pero de él se puede aprender. Usa la aplicación TraceTogether[4], que puso rápidamente en marcha. En el móvil, cada uno recibe una señal por Bluetooth si el usuario está cerca de una persona infectada, lo que requiere que ambas personas tengan la aplicación instalada y la comunicación por Bluetooth activada. En esa ciudad

[2] Craig Timberg, Elizabeth Dwoskin y Drew Harwell (2020), "Governments around the world are trying a new weapon against coronavirus: Your smartphone", *The Washington Post*, 17/IV/2020, https://www.washingtonpost.com/technology/2020/04/17/governments-around-world-are-trying-new-weapon-against-coronavirus-your-smartphone.

[3] Katayoun Farrahi, Rémi Emonet y Manuel Cebrián (2014), "Epidemic Contact Tracing via Communication Traces", *Plos One*, 1/V/2014, https://doi.org/10.1371/journal.pone.0095133; "Predicting a Community's Flu Dynamics with Mobile Phone Data", *HAL archives-ouvertes*, 28 de abril de 2015, https://hal.archives-ouvertes.fr/hal-01146198/document.

[4] Michael Birnbaum y Christine Spolar (2020), "Coronavirus tracking apps meet resistance in privacy-conscious Europe", *The Washington Post*, 18/IV/2020, https://www.washingtonpost.com/world/europe/coronavirus-tracking-app-europe-data-privacy/2020/04/18/89def99e-7e53-11ea-84c2-0792d8591911_story.html.

Estado de 5,7 millones de residentes, poco más de millón y medio se la han instalado en sus móviles cuando el propio Gobierno señalaba que necesitaba que tres cuartas partes de la población la usase, y muchos de los que la tienen no han activado el Bluetooth[5]. La COVID-19 ha sufrido un rebrote en Singapur, aunque ahora parece estar controlada.

En Austria, un ejemplo más cercano, solo 230.000 ciudadanos –de una población de 8,9 millones– se habían descargado la aplicación Stopp Corona a mediados de abril. Investigadores de la Universidad de Oxford calculan que, para ser útil, una aplicación de este tipo tendría que descargarla y utilizarla al menos un 60% de la población[6]. En Australia, la desescalada dependerá del número de descargas de una aplicación de seguimiento. Taiwán tiene un sistema más directo: la policía registra el número de móvil de cada ciudadano o visitante y sus datos respecto a la COVID-19 y lo tiene geolocalizado. Las *Big Tech*, como Apple, Google y Microsoft, disponen ya de trazados de movilidad de un gran número de ciudadanos. Posiblemente, si se agregasen los datos de todas ellas y de otras empresas más pequeñas dedicadas a recoger información de geoposicionamiento, podríamos estar en esas cifras. No parece existir una alternativa tecnológica que permita alcanzar esta escala o aproximarse a ella. Esto justifica que sea la aproximación con mayor posibilidad de éxito.

El debate está centrándose en el uso de aplicaciones de trazado de contactos basadas en tecnología Bluetooth o en la geolocalización (lo que permite sumar datos demográficos de la zona en cuestión). Las aplicaciones basadas en el Bluetooth tienen dos problemas fundamentales: hoy en día no existen y tienen que desarrollarse –al menos en Europa– y, además, el debate sobre su desarrollo precisa un tiempo enorme. A lo que hay que sumar el ya citado escollo de su utilización masiva por el 60-70% de la población, como hemos mencionado en el caso de Singapur. Esto implica una amplia incertidumbre sobre su éxito. Por otra parte, la tecnología Bluetooth sólo sirve para detectar contactos directos y, por tanto, no los indirectos, cuando hay estudios que indican que el virus se mantiene en el aire y en superficies durante horas incluso.

Algunas de esas iniciativas se están poniendo en marcha en España, como el estudio DataCOVID que la Secretaría de Estado de Digitalización e Inteligencia Artificial anunció el 1 de abril[7], el cual recoge y agrega movimientos, nunca individualmente. Las aplicaciones CoronaMadrid y Stop Covid19 Cat también incluyen ya geolocalización y para poder usarlas es obligatorio que el usuario permita el acceso a su ubicación. La multiplicación de aplicaciones no contribuye a la útil y necesaria integración de la información si no se asegura la interoperabilidad entre plataformas.

[5] Manu Granda (2020), "La desescalada en Australia dependerá del número de descargas de una 'app' de seguimiento", *El País*, 4/V/2020, https://elpais.com/sociedad/2020-05-03/la-desescalada-en-australia-dependera-del-numero-de-descargas-de-una-app-de-seguimiento.html.

[6] Luca Ferreti y otros (2020), "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing", *Science*, 31/III/2020, https://science.sciencemag.org/content/early/2020/04/09/science.abb6936.

[7] La Orden SND/297/2020, de 28 de marzo, encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de actuaciones para la gestión de la crisis sanitaria ocasionada por la COVID-19.

Hay que partir de la base de que este tipo de tecnología es un elemento útil que puede contribuir a combatir la pandemia. Pero no hay que caer en el "solucionismo" [8] tecnológico y pensar que estas tecnologías por sí solas son la solución. Tampoco cabe ignorar que estas cuestiones resultan polémicas, aunque en las actuales circunstancias mucha gente esté dispuesta a dar primacía a las consideraciones de seguridad sobre las de privacidad. En el año 52 a. C. Cicerón ya consideraba en *De legibus* que "*salus populi suprema lex esto*" ('la salud del pueblo será la ley suprema'). Como recuerda Andrea Renda con esta cita[9], en situaciones de emergencia, el siempre delicado equilibrio entre la seguridad pública y la privacidad personal tiende a inclinarse algo más a favor de la primera, algo previsto incluso en el sistema más limitativo del mundo, que es el de la Unión Europea con el Reglamento General de Protección de Datos (RGPD en sus más conocidas siglas en inglés). Los artículos 6 y 9 del RGPD permiten el tratamiento de datos para un interés público preponderante, tal como lo ratifica la Agencia Española de Protección de Datos (AEPD)[10]. Las autoridades europeas de protección de datos han sido rotundas al afirmar que la lucha contra la actual situación pandémica es un claro interés público. En determinados contextos, el interés público es preponderante y no sería necesario el consentimiento del sujeto; por ejemplo, para el tratamiento de datos de salud en el ámbito de la relación empleador-empleado en el contexto de la COVID-19. Sin embargo, para el dato de la localización sería necesario el consentimiento o la anonimización de los datos.

Incluso con la mejor de las intenciones, se corre el riesgo de poner en marcha un sistema de vigilancia masiva que permanezca después y se utilice para otros fines, como pasó en EEUU. tras los atentados del 11S. El estado de vigilancia no es algo que únicamente se dé en sistemas autoritarios, como China, sino también en democracias, como quedó de manifiesto con las revelaciones de Edward Snowden sobre la Agencia de Seguridad Nacional (NSA) de EEUU. o por medio de las *Big Tech*, las grandes empresas tecnológicas, como expresa Shoshana Zuboff en su documentado libro *The age of surveillance capitalism*[11]. Más aún cuando la lucha contra la COVID-19 ha llevado a un grado de digitalización sin precedentes de la vida de los ciudadanos.

En todo caso, en la actual situación, el valor del *big data* (datos masivos) para el diagnóstico de situaciones y el diseño de estrategias inteligentes queda reforzado, al ir muchas veces por delante de los aparatos estadísticos oficiales[12]. Muchas empresas privadas se están lanzando al diseño de aplicaciones relacionadas con el virus para monitorizar los desplazamientos de sus trabajadores dentro de sus instalaciones de cara

[8] Evgeny Morosov (2020), "The tech 'solutions' for coronavirus take the surveillance state to the next level", *The Guardian*, 15/IV/2020, https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt.

[9] Andrea Renda (2020), "¿Será la privacidad otra víctima del Covid-19?", *Política Exterior*, 7/IV/2020, https://www.politicaexterior.com/se-convertira-la-privacidad-otra-victima-del-covid-19.

[10] AEPD, Informe del gabinete jurídico, REF: 0017/2020, https://www.aepd.es/es/documento/2020-0017.pdf.

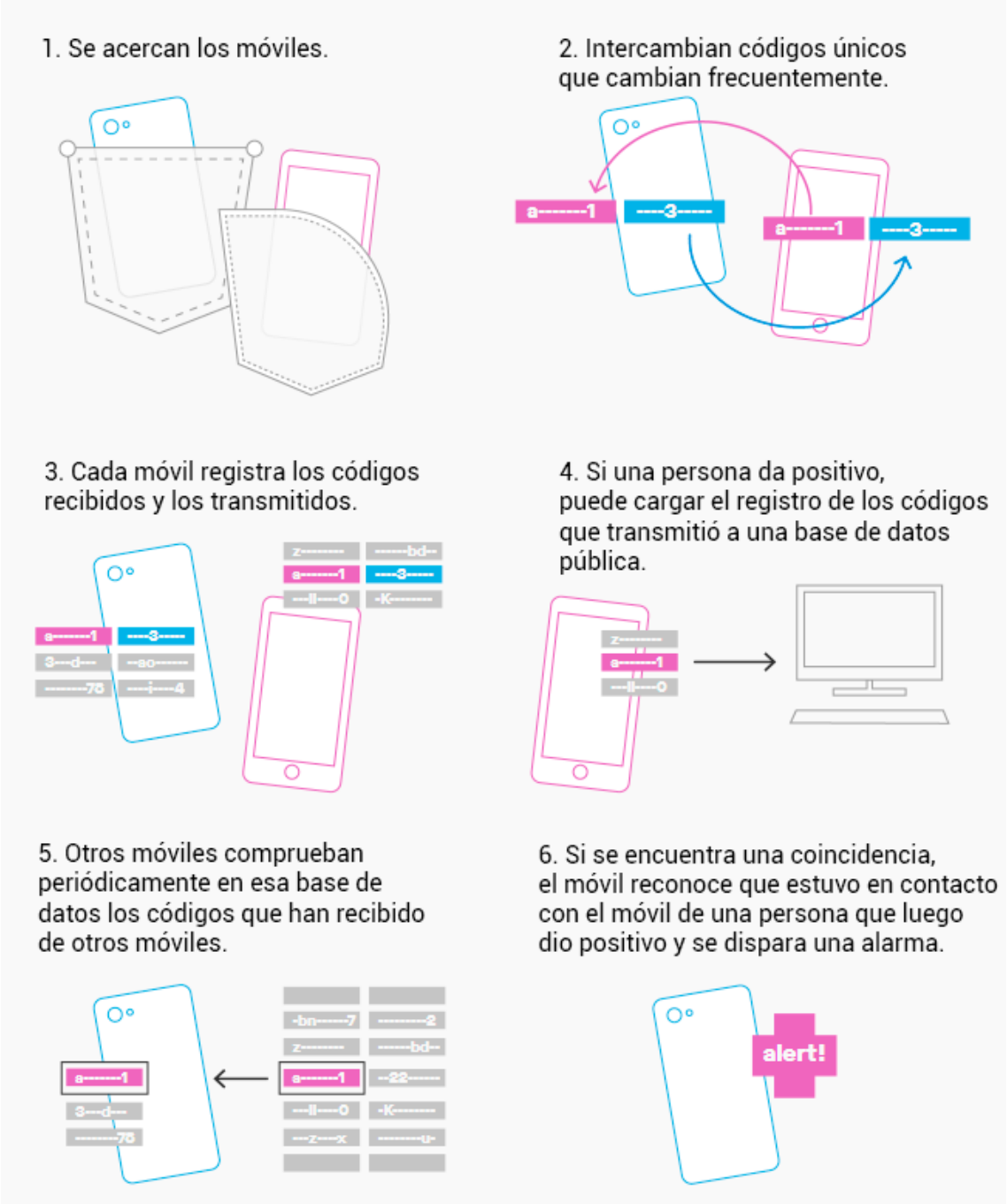
[11] Shoshana Zuboff, *The age of surveillance capitalism*, Profile, 2019.

[12] Álvaro Ortiz y Teresa Rodrigo (2020), "Coronavirus and Big Data: Economics in Real-Time and High-Definition", BBVA Research, 14/IV/2020,

https://www.bbvaresearch.com/en/publicaciones/coronavirus-and-big-data-economics-in-real-time-and-high-definition.

a una "nueva normalidad"[13]. Hay también una carrera entre Estados y, dentro de estos, entre regiones o estados federados.

Figura 1. Trazado de contactos por Bluetooth: cómo funciona



Fuente: Adaptación de *Quartz*.

[13] Hannah Murphy (2020), "Private sector races to build virus apps to track employees", *Financial Times*, 26/IV/2020, https://www.ft.com/content/caeb250b-8d8b-4eaa-969c-62a8b58464aa.

La utilidad de los datos y quién dispone de ellos

El uso de datos masivos de móviles donde ya se ha aplicado está demostrando, en general, ser una herramienta importante en la lucha contra el coronavirus, tanto para moldear como para modular las respuestas de los ciudadanos, que han de colaborar para que los sistemas funcionen. Ya hay muchos datos útiles disponibles para este tipo de seguimientos, desde los que aportan los operadores y las redes sociales hasta los proveedores de servicios, como Google (a través del sistema operativo Android para móviles), los buscadores o los informes a partir del sistema de geolocalización y mapas. La geolocalización se puede hacer vía GPS, pero también vía wifi, con una precisión de hasta dos metros[14]. Hay que señalar que el término *geolocalización* se confunde con el de *vigilancia* y despierta siempre temores, a menudo infundados, pues, como se ha explicado, diversas empresas tienen ya estos datos.

¿De qué tipo de datos se trata? Los principales datos que se van a recabar son la localización, las relaciones con contactos directos e indirectos, la identificación de personas, la información de condiciones de vida y sociodemográficas y los datos sanitarios. Algunos datos los pueden aportar los operadores de telefonía al amparo de la directiva europea sobre ePrivacy. Los datos estadísticos se pueden extraer del Instituto Nacional de Estadística (INE) y el Centro de Investigaciones Sociológicas (CIS). Los datos sanitarios están en el sistema sanitario público y privado y en los sistemas de prevención de salud e higiene en el trabajo. Hay también un problema de "burbujas sociales", que ya se detectó en Singapur y en Taiwán, al no haberse tenido en cuenta a trabajadores inmigrantes que viven en otras condiciones y no se conectan de la misma manera a los ecosistemas informativos locales, por lo que para futuras pandemias habrá que prever su inclusión en el sistema y asegurar el cruzado sistémico de datos.

Lo más habitual son los datos agregados. Diversos operadores de telefonía y servicios, incluidos Google y Facebook, están proporcionando este tipo de datos a sistemas de salud e investigadores. Al estar anonimizados, permiten la privacidad, pero no notificar a la gente de que pueden estar infectados (sólo los datos individualizados de proximidad o de GPS lo permitirían). Estos serían datos personalizados, que suponen una cierta intrusión, y las listas de contactos con gente que se ha tenido en la cercanía, localizados por geolocalización o por contacto Bluetooth, que son menos intrusivas en términos de privacidad.

[14] Michael Angerman y Marton Frassl, "Seamless and Smooth Location Everywhere with the new Fused Location Provider", Google Developers, https://www.youtube.com/watch?v=MEjFW_tLrFQ.

Estos datos se han utilizado hasta ahora de tres maneras:

- para el planeamiento estratégico por medio de la geolocalización para saber cómo y dónde se concentra la gente;
- para el trazado de individuos (posiblemente infectados)[15], y
- para aconsejar a los individuos afectados[16].

Desde un punto de vista técnico, hay un amplio consenso entre científicos en torno a que, cuanto más individualizados los datos de localización, más fácil es reducir el número de infecciones[17,] pero esto lleva a restar privacidad de los usuarios y a una elección, aunque sea temporal, entre privacidad y seguridad, una dicotomía que no se ha podido resolver del todo, aunque algunos científicos insistan en que es posible resolverla.

Como reitera la OMS[18], se trata de seguir (trazar) el desplazamiento de la persona infectada y localizar rápidamente sus contactos para testearlos o aislarlos. Para ello resulta esencial la capacidad de testear masiva y rápidamente, una capacidad de la que dispusieron desde un principio los países con más éxito en esta lucha y que se está alcanzando ahora en este país.

Se plantea también la cuestión de dónde almacenar estos datos y dónde procesarlos, además de la duración de este almacenamiento, pues para que el sistema funcione se necesita crear bases de datos con el máximo número posible de puntos de localización asociados a cada infectado durante el tiempo que sea transmisor del virus.

Hay dos tipos de soluciones:

1. **Centralizar** los datos en las Administraciones Públicas. Las grandes compañías de datos (*Big Tech*) y las operadoras de telecomunicaciones comparten estas bases de datos con las Administraciones Públicas encargadas de gestionar la crisis del coronavirus. Una vez superada la crisis, hay que garantizar que los datos se destruyen, salvo algunos agregados que se conserven con fines de investigación. Ahora bien, la Comisión Europea ha pedido que no se llame *centralizado* (una palabra llena de connotaciones negativas) al modelo que se basa en un servidor común.

[15] Por ejemplo, en Corea del Sur se han utilizado datos individuales de geoposicionamiento para ver si personas que debían guardar cuarentena se alejaban más de cien metros de sus casas.

[16] J. Scott Marcus (2020), “Big Data versus CoVID-19: opportunities and privacy challenges”, Bruegel, 23/III/2020, https://www.bruegel.org/2020/03/big-data-versus-covid-19-opportunities-and-privacy-challenges.

[17] Caroline O. Buckee y otros (2020), “Aggregated mobility data could help fight COVID-19”, *Science*, 10/IV/2020, https://science.sciencemag.org/content/early/2020/03/20/science.abb8021.full.

[18] Seguimos en parte el análisis de Kiko Llaneras, “Números del coronavirus: las medidas para volver a la vida normal”, *El País*, 15/IV/2020, https://elpais.com/politica/2020/04/14/actualidad/1586889164_929029.html.

2. **Descentralizarlos**, en el sentido de que toda la información se reparte entre, las Administraciones Públicas y las empresas de datos. Estas últimas desarrollan interfaces de programación de aplicaciones (*application program interfaces*, API) que permiten su utilización por diversos *softwares*. Son las empresas las que identifican los contactos y les pasan la información a las Administraciones, pero la información sobre geolocalización no sale de las citadas empresas. También en este caso se debería compartir la información con los científicos. Alemania, que era en un principio partidaria de la centralización, ha optado por la descentralización porque es lo que exigen Google y Apple, por cuya API apuesta[19].

En ambos casos, sería útil poder comparar la información, al menos a nivel europeo, y que los sistemas sean interoperables. Detrás de las diferencias hay un acuerdo en la UE sobre la necesidad y la urgencia de esta interoperabilidad.

El Foro Económico Mundial (World Economic Forum, WEF) está impulsando de forma general una tecnología que aumente la privacidad (*privacy enhancing technology*) al permitir capturar información confidencial sin revelarla por razones éticas, legales o comerciales[20]. Todo esto tiene también una dimensión cultural. Hay tres culturas diferentes en el mundo en lo relativo a la privacidad y la disciplina: la asiática, con China como uno de los casos más extremos de sociedad (sistema disciplinario); la europea, con su insistencia en la defensa de la privacidad, aunque dentro de Europa hay también distintas sensibilidades –la francesa es de las más acusadas–, y la americana, más laxa en algunos aspectos, pero con recelos ante las grandes empresas[21]. Por estas razones, y aunque tecnológicamente conviene que las soluciones sean interoperables, no es fácil lograr una solución uniforme para todo el mundo.

Críticas

Estas posibilidades han hecho sonar diversas alarmas en distintos sectores, incluso aquellos que piensan que el uso de la información de los teléfonos inteligentes para trazar la propagación del coronavirus puede ser una buena idea pero usarla para

[19] El protocolo DP3T propone que la información esté en los dispositivos finales. Lo único que compartiría un usuario infectado con un servidor central serían los identificadores aleatorios que él ha enviado a otros usuarios a través de Bluetooth. Luego los usuarios se bajan esos identificadores del servidor central y la verificación de si ha habido contacto se hace en el dispositivo móvil del usuario. Esto último es lo que se considera descentralizado desde un punto de vista técnico, aunque sigue habiendo un punto central: el servidor que guarda los identificadores de los usuarios infectados. Carmela Troncoso y otros, "Decentralized Privacy-Preserving Proximity Tracing (DP3T)", GitHub, 12 de abril de 2020, https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

[20] WEF, "The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value", septiembre de 2019, https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value.

[21] Una mitad de los estadounidenses con teléfonos inteligentes dicen que probable o definitivamente no están dispuestos a descargar aplicaciones que están desarrollando Google y Apple para alertar a los que están cerca de que entraron en contacto con alguien infectado, sobre todo porque no confían en que las empresas traten sus datos de forma segura y privada. Joseph Marks y Tonya Riley (2020), "Americans are wary of the coronavirus tracking apps being produced by big tech", *The Washington Post*, 29/IV/2020, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/29/the-cybersecurity-202-americans-are-wary-of-the-coronavirus-tracking-apps-being-produced-by-big-tech/5ea89da7602ff14578420bee.

rastrear los movimientos de individuos específicos no**.** Por ejemplo, un grupo de científicos de varios países ha publicado una declaración conjunta en la que señala que "la actual crisis de la COVID-19 no tiene precedentes y necesitamos formas innovadoras de superar bloqueos actuales. Sin embargo, nos preocupa que algunas 'soluciones' a la crisis puedan (…) dar lugar a sistemas que permitan una vigilancia sin precedentes de la sociedad en general", y se pronuncian más bien a favor de sistemas de trazado vía Bluetooth que por la geolocalización para preservar esa privacidad. Otros investigadores también se han pronunciado en una tribuna conjunta a favor del modelo descentralizado de esta tecnología para el trazado de contactos al respetar mejor los principios de privacidad desde el diseño, minimización de datos y retención de los datos e implicar menor compartición de estos.

Amnistía Internacional, junto con otras organizaciones civiles, ha hecho público un manifiesto en el que reconoce que la pandemia de la COVID-19 es "una emergencia global de salud pública que precisa de respuestas coordinadas y en gran escala de los gobiernos en todo el mundo. Sin embargo, las iniciativas de los Estados para contener el virus no deben servir para encubrir el inicio de una nueva era marcada por una enorme expansión de los sistemas de vigilancia digital invasiva".

Las críticas más notables han partido de grupos de defensa de la privacidad y de intelectuales como el historiador israelí Yuval Noah Harari[22] o el filósofo coreano afincado en Berlín Byung-Chul Han, que alerta contra lo que llama la "sociedad disciplinaria"[23], ante la cual no hay resistencia. En Asia, afirma, "apenas se habla ya de protección de datos, incluso en Estados liberales como Japón y Corea del Sur. Nadie se enoja por el frenesí de las autoridades para recopilar datos". Esto se puede ver sumado o integrado con la tecnología de reconocimiento facial con bases biométricas que incorpora termómetros digitales para detectar a individuos con fiebre.

Aunque ya hemos visto lo que ocurre en Singapur en cuanto a los límites de la colaboración ciudadana, algunas élites son en general más reacias a este tipo de sistemas que las propias poblaciones, incluso en Europa. Como señala Adam Przeworski, "ante el peligro, la gente acepta someterse a este tipo de escrutinio", y añade que, "en la provincia china de Zhejiang, el 90% se unió al sistema AliPay Health Code, que rastrea sus movimientos. E incluso los franceses, fóbicos respecto a la privacidad, están dispuestos a someterse a ella: en una encuesta reciente, el 80% declaró que instalaría una aplicación de este tipo"[24]. Dos terceras partes de los británicos se muestran a favor de dejar usar al Gobierno aplicaciones para móviles para rastrear

[22] Yuval Noah Harari (2020), "The world after coronavirus", *Financial Times*, 20/III/2020, https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

[23] Byung-Chul Han (2020), "La emergencia viral y el mundo de mañana", *El País*, 22/III/2020, https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html, y "La pandemia y el regreso a la sociedad disciplinaria", *La Vanguardia*, 4/IV/2020, https://www.lavanguardia.com/internacional/20200403/48287439354/la-pandemia-y-el-regreso-a-la-sociedad-disciplinaria.html.

[24] Adam Przeworski (2020), "Life in the Time of COVID19", Reddit, abril de 2020, https://www.reddit.com/r/IRstudies/comments/fwl316/life_in_the_time_of_covid19_adam_przeworski.

a infectados de coronavirus e informar a otros de que pueden estar en riesgo, según una encuesta de mediados de abril en el *Financial Times*[25].

Claro que regímenes autoritarios pueden utilizar este tipo de sistemas invasivos para reforzar su control sobre sus ciudadanos, una tentación de la que no están exentas las democracias liberales. "Este laboratorio de experimentos permanecerá permanentemente en el arsenal de los Gobiernos. Pueden o no usar lo que hayan aprendido, pero habrán aprendido", concluye Przeworski. En este sentido, coincide, por citar otro ejemplo de crítica, con Marietje Schaake, directora de Política Internacional del Stanford Cyber Policy Center y exeurodiputada, cuando señala: "La verdad incómoda es que un mayor acceso a los datos también ayuda convenientemente a los Gobiernos a controlar a su gente y que las empresas tecnológicas aprovechan la abertura para estirar los límites de lo posible. La triste realidad es que, además de la erosión de los derechos de la privacidad, las aplicaciones pueden crear una falsa sensación de seguridad, lo que puede hacer que las personas sean imprudentes en el momento en que deben estar atentas"[26].

Excepciones ya existentes –por ejemplo, el terrorismo– habilitaban a los Gobiernos a tener acceso a estos datos. Realmente, el riesgo que supone la situación creada por la pandemia, aun no siendo inexistente, es relativamente mucho menor, puesto que no está facilitando a los Gobiernos ninguna información de la que no pudiesen disponer ya por otros medios, como se ha señalado al citar los casos de Snowden y la visión de Zuboff. Hay otro peligro añadido y es un aspecto de la privacidad novedoso, a saber: cómo se aprovecha la urgencia de la comunicación para extraer datos fuera de los canales protegidos habituales. Hay mayor vulnerabilidad a filtraciones y hackeos para explotar esas aplicaciones y su información, individual o colectiva, con diversos fines –entre otros, los de dar la impresión de más casos de los que realmente hay, generar caos o sacar beneficio–, lo que obliga a extremar las medidas de ciberseguridad.

La apuesta de Apple, Google y Facebook

Apple y Google, competidores acérrimos en lo que a móviles y otras dimensiones se refiere, anunciaron a principios de abril en un comunicado su asociación para desarrollar conjuntamente un sistema con estos fines, una solución a bajo nivel para que ambos sistemas operativos registren otros dispositivos en proximidad a través de Bluetooth independientemente del sistema operativo que usen. Se trata de una solución mundial y transfronteriza que lleve a la interoperabilidad de diferentes aplicaciones que se diseñen sobre esta API. Entre ambas empresas suman los sistemas operativos de 3.000 millones de usuarios (iOS y Android, respectivamente), con lo cual pueden revolucionar

[25] Helen Warrell (2020), "Majority in the UK support use of mobile phones for coronavirus contact tracing", *Financial Times*, 17/IV/2020, https://www.ft.com/content/1752affb-24dc-4ad9-8503-78f9ce1adca9; Simon Dennis y otros (2020), "Social Licensing of Privacy-Encroaching Policies to Address the COVID-19 Pandemic", GitHub, 27/IV/2020, https://stephanlewandowsky.github.io/UKsocialLicence/index.html.

[26] En servicios de geolocalización, la adopción masiva de herramientas de nicho y la débil encriptación encabezan la lista de las preocupaciones de algunos expertos. Kevin McAllister, "What are the biggest holes in data privacy that have been exacerbated by coronavirus?", *Protocol*, 9 de abril de 2020, https://www.protocol.com/Braintrust/data-privacy-holes-coronavirus-pandemic?rebelltitem=1#rebelltitem1.

este mercado. Aunque faltan detalles, ambos sistemas operativos están aunando esfuerzos para lanzar, a mediados de mayo, unas API que garanticen la interoperabilidad entre dispositivos Android e iOS que utilicen aplicaciones de Gobiernos para el trazado de contactos y, en los próximos meses, incorporarán este trazado de contactos como funcionalidad en sus sistemas operativos. Posteriormente, se incluirían con las actualizaciones de los sistemas operativos, aunque activarlas requeriría consentimiento explícito y, para la información de proximidad, activar el Bluetooth en los móviles. Una interpretación de este sistema es que, si un usuario da positivo para coronavirus y decide participar en el sistema, otros usuarios que a su vez participen podrán ser notificados o alertados en caso de haber estado expuestos al virus, es decir, físicamente próximos al dispositivo de una persona que ha dado positivo. Otra es que Google y Apple ofrecerán esta funcionalidad y estará disponible para las aplicaciones oficiales desarrolladas por Gobiernos u otro tipo de autoridades, pero es responsabilidad de esas aplicaciones –y de las instituciones garantes del tratamiento y uso de los datos– conseguir la participación activa de los usuarios, lo que puede frenar su instalación masiva, como ya se ha visto en el caso de Singapur.

Aunque es la solución en la que están trabajando Apple y Google, no parece posible que las agencias de salud pública creen aplicaciones móviles que puedan detectar y registrar a todas las personas que entren en contacto durante la pandemia. Si una de esas personas da positivo para coronavirus, recibiría una alerta en la que se le notificaría que hable con un médico. Apple y Google aseguran que van a crear *software* que permita a los teléfonos transmitir códigos únicos generados criptográficamente a través de Bluetooth. Los códigos no incluirán información de identificación o datos de ubicación y la criptografía está diseñada para que sea imposible vincular los códigos a una persona en particular. A este respecto, un elemento en relación con la privacidad es que el proceso de *matching* de los códigos que envían los dispositivos (para reconocer si un teléfono ha estado próximo físicamente a otro) ocurre en el propio dispositivo (*on device*) y no en un servidor o nube. En un movimiento nada habitual, ambas empresas han publicado parte del código propuesto detrás del *software* para que los investigadores puedan analizarlo. El código muestra, entre otras cosas, que todos los datos del usuario se borran si un individuo decide más adelante eliminar la aplicación y que las conexiones con operaciones publicitarias de las empresas están deshabilitadas. Dado el citado alcance de ambas *Big Tech*, podemos estar ante un salto cualitativo en el uso de los datos de los usuarios. No obstante, para ser efectivas necesitan que un 60-70% de la población tenga activadas dichas aplicaciones y, además, los epidemiólogos advierten de que el trazado de contactos digitales puede no ser una panacea para el coronavirus, porque en gran parte del mundo se reservan los test para los pacientes con síntomas claros, aunque se tienda cada vez más a comprobar a los asintomáticos[27].

Google, que tiene una red para informes de movilidad sobre la pandemia, también coopera con Facebook a la hora de compartir datos para pronosticar casos de coronavirus. Facebook tiene un programa llamado Data for Good (‘datos para el bien’) con herramientas e iniciativas que pueden servir para responder a la pandemia de la COVID-19. Además, forma parte de la Red de Datos de Movilidad COVID-19, una red

[27] Sidney Fusell (2020), “The Apple-Google Contact Tracing Plan Won’t Stop Covid Alone”, *Wired*, 14/IV/2020, https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone.

de epidemiólogos de enfermedades infecciosas en universidades de todo el mundo que trabajan con empresas tecnológicas para utilizar datos agregados de movilidad para apoyar la respuesta a la COVID-19. Se trata, esencialmente, de contribuir a pronosticar, pero no a detectar[28].

Directrices y direcciones europeas

La regulación de la UE es muy garantista en materia de privacidad, por lo que vigilará que las aplicaciones relacionadas con la COVID-19 respeten los principios europeos. El RGPD es quizás, junto con el reglamento vigente en California, uno de los sistemas legales que más protegen la privacidad digital en el mundo, incluso en situaciones excepcionales como la que vivimos. Las normas de la UE, en particular el RGPD y la Directiva sobre la privacidad y las comunicaciones electrónicas (ePrivacy), ofrecen las mayores garantías de fiabilidad –es decir, carácter voluntario, minimización de los datos y limitación temporal– para que se extienda el uso de estas aplicaciones y para garantizar la privacidad de los datos y metadatos y la confidencialidad de las comunicaciones. A ello hay que sumar la Declaración Universal de los Derechos Humanos y sus derivados y, en el ámbito europeo, la Convención Europea de Derechos Humanos y la Carta de los Derechos Fundamentales de la UE, más las Constituciones y otras leyes nacionales[29].

La cuestión del trazado, especialmente por geolocalización, está provocando un debate en muchos países; por ejemplo, entre constitucionalistas en España o claramente entre Gobierno –partidario de estas aplicaciones– y oposición en un país como Francia[30]. En España, según el ministro del Interior, los datos procedentes de la geolocalización se utilizarán "cuando haya que utilizarlos, si se llegan a utilizar, en los términos legales". Según *eldiario.es*, el ministro dijo no "descartar" el uso de la geolocalización personal, "siempre con amparo legal y judicial" para comprobar el grado de cumplimiento de las normas elaboradas por la pandemia del coronavirus. Los datos móviles se utilizarán para fines sanitarios y para "tareas de vigilancia, de supervisión o incluso sanción".

[28] Karen Hao (20202), "How Facebook and Google are helping the CDC forecast coronavirus", *MIT Technology Review*, 9/IV/2020, https://www.technologyreview.com/2020/04/09/998924/facebook-and-google-share-data-to-forecast-coronavirus.

[29] Así, el artículo 18 de la Constitución Española reza: "1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

[30] Por ejemplo, Reyes Rincón y José María Brunet (2020), "Una norma de 1945 para una crisis del siglo XXI", *El País*, 10/IV/2020, https://elpais.com/espana/2020-04-09/una-norma-de-1945-para-una-crisis-del-siglo-xxi.html, y Alexandre Lemarié (2020), "Coronavirus: le gouvernement favorable au traçage numérique de la population, une partie de la majorité s'y oppose", *Le Monde*, 9/IV/2020, https://www.lemonde.fr/politique/article/2020/04/09/coronavirus-le-gouvernement-favorable-au-tracage-numerique-de-la-population-une-partie-de-la-majorite-s-y-oppose_6036051_823448.html.

El RGPD no incluye el uso de datos identificables recogidos por los Gobiernos para propósitos de lucha contra la criminalidad, pues se trata de una competencia nacional[31]. El Reglamento tiene, como ya se ha apuntado, una cláusula que permite excepciones en casos de interés público como es el de una pandemia. Ambos elementos los ha reconocido el Comité Europeo de Protección de Datos en una declaración del pasado 20 de marzo. Pero el uso de datos anonimizados no plantea problemas, pues la norma señala que las reglas de protección de datos personales no se aplican a datos que han sido adecuadamente anonimizados. De hecho, las autoridades sanitarias de España, Noruega, Bélgica, Reino Unido, Portugal y Grecia ya han utilizado datos de geolocalización para localizar concentraciones de enfermos, con un conocimiento que no parte de cero: Telefónica se ha asociado con Facebook para geolocalizaciones ante desastres naturales en América Latina y en 2017 con Unicef y la Universidad de Notre Dame (EEUU.) para modelos epidemiológicos con que predecir el virus del Zika en Colombia. Vodafone también lo ha hecho en África[32].

En la UE, algunos países han instaurado sistemas invasivos. Así, una aplicación llamada Cuarentena en el Hogar exige a los ciudadanos polacos en cuarentena confirmar por medio de una foto en su casa que están respetando la medida, si así se les requiere, en menos de 20 minutos, so pena de multa. La aplicación usa reconocimiento facial para comprobar la identidad y la geolocalización. La Comisión Europea, tras consultas con el Comité Europeo de Protección de Datos, publicó el pasado 16 de abril una comunicación con directrices para la protección de datos y la limitación del grado de injerencia sobre el desarrollo de nuevas aplicaciones móviles que contribuyan a la lucha contra el coronavirus. Las directrices siguen la anterior recomendación de la Comisión sobre un enfoque común de la UE para el uso de aplicaciones y datos móviles y van acompañadas de un conjunto de instrumentos de la UE para las aplicaciones móviles de trazado de contactos.

El documento "EU toolbox for members States", publicado el 15 de abril por la eHealth Network y respaldado por la Comisión, establece una aproximación común para los Estados miembros sobre el uso de aplicaciones móviles para el trazado y aviso de contagios. La Comisión los emplaza a seguir una hoja de ruta y a la consecución de cuatro hitos entre finales de abril y junio de 2020. Es importante este curso de acción de la Comisión no solo con vistas a conseguir los objetivos de salud pública, sino también para facilitar una movilidad segura entre Estados, factor clave para una rápida reactivación del sector turístico en España.

Las directrices de la UE se centran en aplicaciones de uso voluntario con una o más de las siguientes funciones: información precisa para los usuarios sobre la pandemia de coronavirus, cuestionarios de autodiagnóstico y orientación individualizada (función de comprobación de síntomas), alertas dirigidas a personas que han estado cerca de una

[31] Pero sí la "Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo".

[32] Nic Fildes y Javier Espinosa (2020), "Tracking coronavirus: big data and the challenge to privacy", *Financial Times*, 8/IV/2020, https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987.

persona infectada para que se hagan una prueba o se aíslen (función de localización de los contactos y de alerta) y un foro de comunicación entre médicos y pacientes en aislamiento voluntario en el que se ofrece asesoramiento adicional en materia de diagnóstico y tratamiento (telemedicina).

Ahora bien, según algunos expertos consultados, no se puede tener aplicaciones que garanticen completamente el trazado por proximidad y preserven totalmente la privacidad, aunque sí garantiza ambas cosas el protocolo DP3T, que propone que el móvil de una persona –no una entidad central– la avise si ha estado en contacto con un infectado. Es decisión del individuo tomar las medidas oportunas para, por ejemplo, aislarse, tal y como se ha explicado.
Hay, sin embargo, un problema fundamental en el debate, a saber, que se está centrando exclusivamente en el desarrollo y uso de aplicaciones. Esto deshabilita de manera inmediata el uso de datos disponibles como los de localización de Google, Apple, Facebook y otros. Para la comisaria de Competencia y Digital, Margrethe Vestager, no se trata de tener que elegir entre luchar contra el virus y proteger la privacidad; ambos fines son compatibles[33].

Las principales condiciones que plantea la Comisión para el desarrollo de aplicaciones móviles de lucha contra el coronavirus son las siguientes:

- **El papel de las autoridades sanitarias nacionales:** Se debe establecer claramente desde el principio qué instancia debe rendir cuentas sobre el cumplimiento de las normas de protección de datos personales de la UE. Dada la alta sensibilidad de los datos y la finalidad última de las aplicaciones, esta responsabilidad debe recaer sobre las autoridades sanitarias nacionales.

- **Los usuarios conservan el pleno control de sus datos personales:** La instalación de una aplicación en el aparato de un usuario debe ser voluntaria; los usuarios deben tener la posibilidad de dar su consentimiento para cada una de las funciones de la aplicación móvil. Si se utilizan datos de proximidad, deben almacenarse en el dispositivo del usuario.

- **Uso limitado de datos personales:** Una aplicación debe respetar el principio de minimización de los datos, que requiere que solo puedan tratarse los datos personales pertinentes y limitados a los fines en cuestión. La Comisión considera que los datos de localización no son necesarios a efectos de trazado del contacto y recomienda no utilizarlos en este contexto.

- **Límites estrictos al almacenamiento de datos:** Los datos personales no deben conservarse más tiempo del necesario. Los plazos deben fijarse en función de su pertinencia médica.

[33] Samuel Stolton (2020), “Vestager: it`s not a choice between fighting the virus and protecting privacy”, Euractiv, 1/IV/2020, https://www.euractiv.com/section/digital/news/vestager-its-not-a-choice-between-fighting-the-virus-and-protecting-privacy.

- **Seguridad de los datos:** Los datos deben almacenarse en el dispositivo del usuario y estar cifrados.

- **Garantía de la exactitud de los datos tratados:** Con arreglo a las normas de la UE sobre protección de datos personales, aquellos tratados por un tercero deben ser exactos. Para ello han de emplearse tecnologías, como Bluetooth, que proporcionen una evaluación más precisa de los contactos entre las personas. No obstante, cabe prever que así no se llegará al 60% de la población. Los sistemas por Bluetooth, además, presentan algunas limitaciones importantes, como su incapacidad para detectar infecciones indirectas (que un infectado toque un envase en un supermercado y diez minutos después lo toque otra persona). La tecnología GPS no es inexacta: dice dónde ha estado un usuario, y en eso es exacta. Otra cosa es el uso que hagamos de ella: si lo que se pretende es que identifique únicamente a los infectados positivos, no lo va a hacer; va a tener un alto número de falsos positivos, porque una mayoría de los contactos que se detecten no habrán incurrido en un proceso de transmisión de la enfermedad. Pero esto mismo –posiblemente en menor medida– ocurre con la tecnología Bluetooth. Es una recomendación de la UE poco consistente.

- **Participación de las autoridades nacionales de protección de datos:** Las autoridades de protección de datos deben participar plenamente y ser consultadas en el desarrollo de una aplicación y deben encargarse de revisar su implementación.

El comisario de Mercado Interior, Thierry Breton, pidió a los operadores que dieran datos agregados de localización para rastrear cómo se expande el virus e identificar los lugares en los que más se necesita ayuda. Pero "no vamos a rastrear a individuos", ha afirmado[34]. Las directrices buscan también armonizar algunos principios ante la carrera que se ha desatado a todos los niveles por lograr estas aplicaciones. En Europa –en los países y a veces en las regiones– se están desarrollando varias aplicaciones. La más prometedora, porque ha juntado a más socios, parece ser el llamado PEPP-PT (Rastreo Paneuropeo de Proximidad para Preservar la Privacidad) –más que una aplicación, un sistema de aplicaciones–, un consorcio con sede en Suiza en el que participan de momento Austria, Bélgica, Dinamarca, España, Francia, Italia y Suiza. Alemania parece estar distanciándose a favor de la opción Google-Apple. El consorcio ha aprobado un protocolo que han desarrollado varios grupos de investigación en el área de la privacidad para el trazado de contactos con COVID-19, pero ya empiezan a entreverse intereses políticos encontrados. La aplicación, según explica el consorcio, funcionaría por sistema de proximidad (Bluetooth), aunque no hay un acuerdo total al respecto, pero no se transmitirían geolocalización, información personal ni ningún otro dato que permitiera la identificación del usuario. La instalación sería voluntaria. El proyecto no ha entrado en la estrategia para conseguir instalaciones masivas de las aplicaciones que utilicen el protocolo propuesto por PEPP-PT. El proyecto europeo alternativo es el ya citado DP3T, sobre una base descentralizada, que parecen apoyar Apple y Google.

[34] Nic Fildes y Javier Espinosa (2020), "Tracking coronavirus: big data and the challenge to privacy", *Financial Times*, 8/IV/2020, https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987.

El reto de Apple y Google es mayúsculo, pues entre ambos sistemas operativos reúnen, como ya se ha mencionado, unos 3.000 millones de usuarios de móviles en el mundo. A Europa le va a resultar difícil competir en escala y alcance, por lo que habrá de plantearse vías de cooperación. Tiene también una dimensión de colaboración público-privada, aunque estemos hablando de empresas de talla gigantesca, superior a la de muchos Estados. Detrás hay también una competencia geopolítica que tiene que ver con la actual idea europea –por lo menos de la Comisión Europea y de algunos Estados miembros de peso– de lograr una "soberanía digital europea". Algunas voces de desarrolladores en Alemania[35], por ejemplo, se han alzado contra lo que ven como una cesión de la soberanía europea a Silicon Valley con estas aplicaciones para rastrear las infecciones por coronavirus. Sin embargo, el Gobierno de Merkel parece haber elegido el camino de la colaboración con Google y Apple.

La OCDE, por su parte, califica esta información y las tendencias de las aplicaciones o la información que en algunos casos proporcionan las operadoras como "inestimable" para los Gobiernos que buscan rastrear la pandemia[36], pero considera que "deberían integrarse en el diseño soluciones de preservación de la privacidad totalmente transparentes y responsables para equilibrar los beneficios y los riesgos asociados con la recopilación, el procesamiento y el intercambio de datos personales. Los datos deben conservarse sólo durante el tiempo que sea necesario para cumplir el propósito específico para el que fueron recopilados".

Principios convenientes, con cierta flexibilidad

Partiendo de la utilidad del uso de *big data* personal, el uso de estas tecnologías en diversas formas tiene que someterse a varios principios que forman parte de una legitimidad democrática no basada únicamente, aunque sí necesariamente, en la eficiencia. En algunos aspectos, vamos más allá de lo que propone la UE; en otros, por debajo. Son condiciones que se aplicarían en un escenario "normal" y que en esta situación de excepcionalidad requieren refuerzo y a la vez flexibilización por su alcance. Son una combinación de lo que se puede hacer (la ley) y lo que se debe hacer (la ética) necesaria para lograr el convencimiento. Dicho esto, una exigencia al 100% de estas condiciones, su maximización conjunta, paralizaría cualquier intento de lograr sistemas de trazabilidad operativos con un elevado grado de éxito, por lo que se requiere cierta flexibilidad en su aplicación.

Interoperabilidad

Como ya se ha señalado, es condición indispensable en Europa y, desde luego, para un país como España, dada la importancia del turismo, que estas aplicaciones sean interoperables, es decir, que funcionen entre sí y al cruzar fronteras. Que sean diferentes, si se mantiene esta condición, acaba siendo secundario.

[35] Reuters, "German tech startups say sovereignty of corona-tracking apps can't be left to Google, Apple", *Daily Sabah*, 14/IV/2020, https://www.dailysabah.com/business/tech/german-tech-startups-say-sovereignty-of-corona-tracking-apps-cant-be-left-to-google-apple.

[36] OCDE, "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics", 23 de abril de 2020, https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics.

Consentimiento social informado

La legitimidad y el derecho moral de un Gobierno a utilizar el poder del Estado sólo está justificado y es lícito cuando lo consiente el pueblo o la sociedad sobre los que se ejerce ese poder político (definición de Wikipedia). El uso de estas tecnologías en nuestros sistemas democráticos requiere el consentimiento de los gobernados o usuarios, y el consentimiento implica convencimiento, para lo que se requiere disponer de la suficiente información si se desea. Para lograr la necesaria colaboración de los ciudadanos, se requeriría tal consentimiento. Entendemos *consentimiento* en un sentido amplio y general –es decir, social– de la teoría anglosajona sobre el *consent*; no nos referimos al concepto jurídico (europeo o nacional) de consentimiento explícito individual.

Voluntariedad

Además del consentimiento social o general, la cesión de este tipo de datos por parte de los ciudadanos debe responder a un ejercicio voluntario, fruto de la confianza en los Gobiernos y en las empresas que lo llevan a cabo y del convencimiento de la contribución al bien común. Por ello, aunque las aplicaciones se instalen de forma automática en los sistemas operativos de los móviles o se descarguen, su activación, así como la de otros elementos, requerirá previsiblemente una acción voluntaria.

Respeto a la ley y a los derechos humanos

La aplicación de estas tecnologías debe respetar la ley vigente –en España el orden constitucional– y los derechos humanos en sus diversas acepciones, más restrictivas en Europa, como ya se ha explicado. No ceñirse a la ley –por ejemplo, a la Constitución Española– podría llevar algunas de estas iniciativas ante los tribunales.

Temporalidad y reversibilidad

Harari, por ejemplo, expresa una preocupación bastante extendida cuando señala que "las medidas temporales tienen el desagradable hábito de convertirse en duraderas, especialmente porque siempre hay una nueva emergencia al acecho en el horizonte"[37]. Según Adam Schwartz, abogado en la Electronic Frontier Foundation (EEUU.)[38]: "Entendemos que, dado que estamos en esta crisis, puede ser necesario un ajuste temporal de nuestras libertades digitales; sin embargo, es muy importante que esos ajustes sean temporales". Debe garantizarse que el uso de estas tecnologías sea limitado en el tiempo[39], es decir, que se interrumpa cuando se supere la pandemia, que no se convierta en la norma, y que los datos personales no agregados se destruyan, lo

[37] Yuval Noah Harari (2020), "The World after Coronavirus", *Financial Times*, 20/III/2020, https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

[38] Cit. en Kirsten Grid, Robert McMillan y Anna Wilde Mathews, "To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits", *The Wall Street Journal*, 17/III/2020, https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841.

[39] Ver también Mateo Valero, Josep Martorell y Ulises Cortés (2020), "El poder de los datos", *La Vanguardia*, 10/IV/2020, https://www.lavanguardia.com/vida/20200410/48407655850/el-poder-de-los-datos.html.

que haría reversible la situación[40]. Tiene que establecerse una cláusula de suspensión (*sunset clause*) para evitar que este tipo de controles sobre el comportamiento de las personas se convierta en un instrumento de vigilancia masiva por parte de Gobiernos y empresas, aunque también hay que prever la posibilidad de que se pueda reactivar –probablemente con tecnologías renovadas– ante nuevas alertas pandémicas. Sin temporalidad, el consentimiento social puede ser más difícil de lograr.

Transparencia

La transparencia por parte de los poderes públicos y de las empresas sobre el uso y control de estos datos es esencial. Como indica el ya mencionado J. Scott Marcus, es necesario que el Gobierno deje claro qué datos se recogen, por qué, con quién se van a compartir, cómo se van a asegurar frente a terceros y durante cuánto tiempo se retendrán. Lo es para mantener la confianza en las autoridades, como ejemplifica el caso de Taiwán. La transparencia es un mecanismo de protección y garantía de los datos privados.

Anonimidad

En la medida de lo posible, hay que mantener la anonimidad o desidentificación de los datos, al menos una pseudoanonimidad. La anonimidad requeriría de una solución en la que es el individuo y no las autoridades el notificado sobre un posible contagio, lo que dejaría a decisión de ese individuo el protocolo de actuación, que puede ir desde ocultarlo hasta lo deseable, que sería informar de ello y confinarse. Por el contrario, si se facilita a las autoridades la identidad del individuo –mediante, por ejemplo, su número de teléfono–, existirá un protocolo de actuación único para todos los potenciales positivos que seguramente responda a solicitarles que se confinen y hacer un test con la mayor brevedad posible, como ocurre en el caso de Taiwán. En todo caso, como considera el comisario de Justicia de la UE, Didier Renders, esta información sólo debe almacenarse durante la emergencia sanitaria y sólo de forma muy agregada para posibles estudios y mejoras posteriores.

Proporcionalidad

Como pide el supervisor europeo de Protección de Datos, la captación de estos datos debe ser proporcional a sus fines y no entrar en otros que nada tienen que ver con la lucha contra el virus. Quizás haya que sustituir el análisis predictivo de macrodatos (*big data*) por datos más pequeños y controlados (*small controlled data*)[41].

'Quid pro quo' de las empresas con los usuarios

Las grandes compañías, ya sean operadores de aplicaciones o de sistemas operativos, deben compartir los datos para salvar vidas, como propone Ángel Cuevas Rumín al hablar de una "privacidad decente", que en el fondo son los datos de los usuarios,

[40] Samantha Stein (2020), "How to restore data privacy after the corona virus pandemic", WEF, 31/III/2020, https://www.weforum.org/agenda/2020/03/restore-data-privacy-after-coronavirus-pandemic.

[41] James Guszcza (2015), "The last-mile problem: How data science and behavioral science can work together", *Deloitte Review*, 16, 2015, https://www2.deloitte.com/content/dam/insights/us/articles/behavioral-economics-predictive-analytics/DR16_last_mile_problem.pdf.

quienes deben recuperar así su condición de ciudadanos. Es necesario que esos datos se pongan al servicio de la sociedad. En esto estamos en una situación diferente a la de otros sectores, dado el tenor de los datos de los que se trata; es un modelo "centrado en el usuario". En otros sectores el usuario o consumidor delega en entidades de control, que también son necesarias, mas no suficientes.

Conclusiones

Este tipo de tecnología no lo resuelve todo, sobre todo sin test masivos, pero puede ayudar mucho en la lucha contra esta pandemia y otras futuras. Las tecnologías de trazado pueden ser un requisito previo a una vida posconfinamiento y antes de que el virus haya sido derrotado, pero tienen que acompañar a test masivos. Los sistemas de trazado requieren además mucho personal y, para que los ciudadanos los descarguen en sus móviles, una confianza que solo es posible si se respetan una serie de principios sobre la privacidad, aunque esta se vea comprometida de forma temporal. Todo con una cierta flexibilidad, pues la urgencia está en derrotar la pandemia, en este caso con la ayuda de la tecnología digital de datos. No vayamos, en términos de Rafael del Águila, a avanzar hacia lo implacable o imposible en nombre de lo impecable.

En este debate e iniciativas, hay que adaptar el lenguaje al fin perseguido: no todo –desde luego no la geolocalización, como se ha apuntado– equivale a vigilancia. En vez de hablar de "vigilancia por parte del Gobierno", es más conveniente hacerlo de "seguimiento por parte de las autoridades sanitarias". Del mismo modo, las aplicaciones, que tienen muy mala prensa, deben considerarse "sistema de emergencia de salud pública".

Más allá del lenguaje, el éxito de estas opciones tecnológicas requiere también el cumplimiento de tres condiciones: la colaboración público-privada –cruzar datos entre las aplicaciones y las autoridades sanitarias es esencial, como lo es la colaboración con las empresas–; el liderazgo político para implantarlas, explicarlas y convencer –la pedagogía y el debate de cara a la opinión pública son esenciales–, y la interoperabilidad de las aplicaciones, por supuesto a escala nacional, pero también europea y, si es posible, mundial.