NOTAS

GARANTÍAS FRENTE A LAS APLICACIONES DE RASTREO DE CONTAGIOS EN SITUACIONES DE PANDEMIA

ANTONI ROIG BATALLA
Profesor Titular Derecho Constitucional
Universidad Autónoma de Barcelona

TRC, n.º 48, 2021, pp. 527-542
ISSN 1139-5583

SUMARIO

I. Propósito lícito y con garantías. II. Aplicaciones de rastreo compatibles con la protección de datos personales. III. La aplicación gestionada por la administración sanitaria española se basa en la privacidad por el diseño. IV. Las dudas sobre el servicio de notificación de la exposición de Google/Apple V. Ventajas y límites de las aplicaciones de rastreo. VI. Conclusiones.

I. PROPÓSITO LÍCITO Y CON GARANTÍAS

Los sistemas de información geográfica (GIS, por sus siglas en inglés) aplicados a epidemias no son nuevos, y sus primeras versiones datan de los años 60 del siglo pasado[1]. Los cuadros basados en mapas sobre contagios confirmados, personas fallecidas y recuperados, en diferentes regiones y países, han sido ampliamente usados durante la gestión de esta pandemia[2]. Sin embargo, en este estudio vamos a centrarnos en las aplicaciones de detección y de rastreo de personas infectadas[3].

1 KAMEL BOULOS, M. N. y GERAGHTY, E.M., «Geographical tracking and mapping of coronavirus disease COVID-19/severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) epidemic and associated events around the world: how 21st century GIS technologies are supporting the global fight against outbreaks and epidemics», *International Journal of Health Geographics,* n.º 19, 2020, vol. 8, pp. 1-12.

2 Destaca en número de visitas el mapa del Center for Systems Science and Engineering de la Universidad Johns Hopkins (JHU CSSE) {consulta: 20.10.2021}. Disponible en https://coronavirus.jhu.edu/map.html.

3 La inteligencia artificial ofrece otras muchas posibilidades para la gestión de las pandemias, como por ejemplo la simulación de los efectos de las políticas públicas (DIGNUM, F., DIGNUM, V. DAVIDSSON, P.,

La Agencia Española de Protección de Datos ha tenido ocasión de indicar que la normativa de protección de datos es aplicable, pese a la situación de urgencia sanitaria[4]. Ciertamente, de acuerdo con el Considerando 46 del Reglamento General de Protección de Datos (en adelante, RGPD), la base jurídica para el tratamiento en tiempos de pandemia, además del cumplimiento de una obligación legal (art. 6.1.c) RGPD) como la prevención de riesgos laborales, puede ser también el interés público (art. 6.1e) y 9.2 g) e i) RGPD), o el interés vital del interesado o de otra persona física (art. 6.1.d) RGPD[5]. Ahora bien, al ser datos de salud, los arts. 9.1 y 9.2 del RGPD exigen circunstancias concretas que levanten la prohibición de tratamiento de los datos sensibles, previstas en el art. 9.2 b) RGPD —necesario para el cumplimiento de obligaciones en las relaciones entre empleador y empleado—, 9.2 g) e i) RGPD —interés público esencial o calificado—, y en el art. 9.2 h) RGPD —necesario para un diagnóstico médico o una evaluación de la capacidad laboral—. De acuerdo con esta habilitación, las autoridades sanitarias competentes podrán tratar datos de salud para salvaguardar a las personas de la posibilidad de contagio. Eso sí, los tratamientos deberán respetar tanto el RGPD como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD). De hecho, ni el estado de alarma, ni siquiera el estado de excepción o de sitio permiten suspender la protección de datos[6]. De manera destacada, dos principios merecerán especial atención: la minimización de datos que impone el tratamiento únicamente de los datos estrictamente necesarios para la finalidad que se pretende, así como la limitación de la finalidad, que impide que los datos sean usados por empresarios, por compañías de seguros o por entidades bancarias para fines distintos a la lucha contra la pandemia[7]. Si vamos a alegar el interés público para llevar a cabo esta vigilancia, deberemos ser claros sobre nuestra justificación, transparentes en cuanto al uso de los datos y honestos sobre la información —mínima— que necesitamos.

Ghorbani, A., Van Der Hurk, M., Jensen, M., Kammler, C., Lorig, F., Ludescher, L.G., Melchior, A., Mellema, R., Pastrav, C., Vanhee, L. y Verhagen, H., «Analysing the Combined Health, Social and Economic Impacts of the Corovanvirus Pandemic Using Agent-Based Social Simulation», *Minds and Machines,* 15-06-2020, 18 páginas).

4 Gabinete Jurídico de la Agencia Española de Protección de Datos, Informe N/REF: 0017/2020.

5 Considerando 46 RGPD: El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales *del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el* control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

6 Rodríguez Ayuso, J. F., «Control de la privacidad por parte de las autoridades sanitarias ante situaciones de emergencia», *Revista de Bioética y Derecho*, n.º 50, 2020, pp. 353-368.

7 Considerando 54 del RGPD.

II. APLICACIONES DE RASTREO COMPATIBLES CON LA PROTECCIÓN DE DATOS PERSONALES

1. **Recomendaciones generales**

La gestión de la crisis sanitaria en algunos países no ha reparado en medios tecnológicos tanto para hacer cumplir el confinamiento, como para la detección y el rastreo de las posibles infecciones. En algunos de estos países, el interés general —innegable— por limitar los efectos de la pandemia no ha tenido presente la necesaria garantía de los derechos, sobre todo la privacidad y la protección de datos personales[8]. Este no es el camino seguido, al menos abiertamente, por los países europeos, que abogan por herramientas de adopción voluntaria y que respeten la privacidad y la protección de los datos personales[9].

La duda entre el modelo centralizado o PEPP-PT (*Pan-European Privacy-Preserving Proximity Tracing*), adoptado por Francia y el Reino Unido —aunque este último país ha optado finalmente por el otro modelo— y el descentralizado, parece en la actualidad resuelta, al menos en Europa, en favor del segundo[10]. Existen prototipos alternativos basados en IoT y Blockchain, cuyos autores consideran respetuosos con la privacidad[11]. Sin embargo, la solución adoptada en la Unión Europea se ha basado en el protocolo DP-3T (*Decentralised Privacy-Preserving Proximity Tracing*), de contactos mediante Bluetooth, sin identificación ni geolocalización, sobre las plataformas de Apple y Google[12]. Además, se busca que las soluciones nacionales sean interoperables. En este sentido, los Estados miembros de la Unión Europea acordaron garantizar el intercambio de información segura entre las aplicaciones nacionales de rastreo de contactos que dispongan de una arquitectura descentralizada[13]. Se busca, con ello, que las aplicaciones nacionales funcionen ininterrumpidamente a pesar de los desplazamientos de los ciudadanos a otros países de la Unión Europea que tengan aplicaciones para móviles de rastreo con arquitectura descentralizada. Los identificadores arbitrarios de los usuarios detectados en las inmediaciones durante un período determinado se graban en el teléfono y se cotejan con los usuarios con infección declarada. La información se intercambiará de manera cifrada siguiendo las directrices de la Unión Europea sobre la protección de datos en las aplicaciones[14].

El Comité Europeo de Protección de Datos (en adelante, CEPD) recuerda, de entrada, no sólo la vigencia de los derechos fundamentales en época de pandemia, sino también la necesidad de generar confianza para obtener la aceptación social que requieren estas herramientas tecnológicas. El objetivo primordial de las

13 Comisión Europea (eHealth Network), *Interoperability guidelines for approved contact tracing mobile applications in the EU,* 13-05-2020.

14 Comité Europeo de Protección de Datos, *Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-1*, v.1.0, 21 de abril de 2020 y versión 1.1, 5 de mayo de 2020, correcciones menores.

aplicaciones y de los datos recopilados es aumentar las posibilidades puestas a disposición de los ciudadanos, más que controlar o reprimir conductas. Las finalidades deben ser específicas: (1) uso de datos de localización para modelizar la propagación del virus y evaluar así la eficacia de las medidas de confinamiento —detección— y (2) rastreo de contactos para romper cadenas de transmisión —rastreo—. El CEPD sugiere, además, que estas herramientas deben formar parte de una estrategia global de salud pública, con medidas de apoyo que garanticen la contextualización de la información facilitada a los ciudadanos y la utilidad de las alertas. Por lo demás, el uso de las aplicaciones de rastreo de contactos debe ser voluntario y no basarse en el rastreo de movimientos individuales, sino en la proximidad de los usuarios[15]. La voluntariedad no puede tampoco condicionarse o afectarse con exclusiones sociales o profesionales en caso de no adoptarse la aplicación[16].

2. **Recomendaciones concretas**

Una recomendación habitual cuando se trata de tecnología garante de derechos, o en este caso de tecnología al servicio de políticas públicas de salud, es involucrar a las autoridades sanitarias, los epidemiólogos y los responsables públicos de la lucha contra la pandemia en el proceso de desarrollo de las aplicaciones: estas últimas deben servir a la finalidad de rastreo tradicional de contactos.

Con el fin de calibrar y valorar la eficacia de los rastreos mediante la aplicación, conviene realizar pruebas piloto en una zona en la cual se haga igualmente rastreo manual, y comparar los resultados.

En esta línea, sería quizá deseable disponer de una plataforma digital que pueda servir para resolver las dudas de diseño y de funcionamiento de la aplicación, y poner en contacto a las autoridades sanitarias y a los diseñadores de la aplicación. Esta plataforma podría incluir las resoluciones de los órganos públicos de decisión, recopilar supuestos y servir de guía a los aplicadores públicos locales.

Sería recomendable realizar una evaluación de impacto de protección de datos (DPIA), como en Alemania[17]. En España la evaluación de impacto se publicó una vez la aplicación ya estaba en uso, como veremos.

15 Edwards, L., Veale, M., Lynskey, O., Coldicutt, R., Loideain, N., Kaltheuner, F., Oswald, M., Ducato, R., Schafer, B., Renieris, E., Mcharg A. y Bietti, E., *The Coronavirus (Safeguards) Bill 2020. Proposed protections fordigital interventions and in relation to immunity certificates,* 6 mayo 2020 {consulta: 20.10.2021}. Disponible en https://osf.io/preprints/lawarxiv/yc6xu/.

16 Klar, R. y Lanzerath, D., «The ethics of COVID-19 tracking apps — challenges and voluntariness», *Research Ethics*, vol. 16, n.º 3-4, 2020, pp. 1-9.

17 Evaluación de impacto alemana {consulta: 20.10.2021}. Disponible en https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf.

Sería conveniente incluir una indicación en la normativa de igualdad, como la Equality Act del Reino Unido de 2010, de que nadie será discriminado por haber tenido el Covid19.

Las personas con síntomas deben poder hacer pruebas y las infecciones confirmadas que dan lugar al aviso a los contactos debe requerir código o bien realizarse por las autoridades sanitarias[18].

Puede preguntarse a los infectados confirmados si quieren indicar el día a partir del cual empezaron a tener síntomas. Ello debería reducir los avisos a los contactos de 2 días previos a los síntomas, o el plazo alternativo que se considere conveniente[19]. También podría servir para considerar el intervalo justo antes y después de aparecer los primeros síntomas como el de contactos de alto riesgo.

En los casos asintomáticos, puede esperarse a informar a los contactos unos días para realizar pruebas de confirmación.

Conviene informar sobre el nivel de exposición. Así, en la medida que ello fuera técnicamente posible, habría que informar al ciudadano sobre el nivel del contacto, distinguiendo entre alto riesgo y bajo riesgo[20]. Para clasificar los niveles de exposición puede concebirse el contacto cumulativo de varios plazos reducidos de menos de 15 minutos, para considerarlo como un contacto de alto riesgo.

La fecha de aislamiento sugerida debería contar a partir de la fecha del último contacto indicado en la aplicación. Sin embargo, personalizar esta fecha puede comprometer la privacidad de la persona infectada en aquellos casos que el contacto puede llegar a individualizar con qué personas estuvo ese día[21]. Por ello, es mejor indicar varios días y contar el plazo a partir del último día.

Si el ciudadano ha consentido en indicar en la aplicación un número de teléfono, debería contactarse con él cuando la aplicación le envía un mensaje de que ha estado en contacto con un caso confirmado. Si no se ha indicado ningún número de teléfono, la posibilidad de añadir un número telefónico podría incluirse junto con el aviso de contacto enviado por la aplicación[22].

De manera general, hay que buscar el consentimiento del usuario sobre todos los datos que la aplicación y sus sensores puedan incorporar al expediente personal del contacto, para su posterior seguimiento convencional[23].

Hay que prever un botón de apagado de la aplicación para los supuestos en los cuales el usuario se encuentra en casa y no quiere falsos positivos de los

18 European Centre for Disease Prevention and Control, *Mobile applications in support of contact tracing for COVID-19 — A guidance for EU/EEA Member States*, Stockholm, 10 de junio de 2020, p. 4.

19 Ver nota anterior, p. 5.

20 European Centre for Disease Prevention and Control, *cit.,* p. 5.

21 European Centre for Disease Prevention and Control, *cit.*, p. 7.

22 European Centre for Disease Prevention and Control, *cit.*, p. 6.

23 European Centre for Disease Prevention and Control*, cit*., p. 7.

vecinos a través de las paredes, o bien para personal sanitario o cuidadores de personas infectadas que disponen de medidas protectoras eficaces[24].

No es deseable alertar a los contactos de segundo orden, es decir a las cadenas de contactos de contactos —no de infectados informados—. Ello se debe a que puede generar alarma social sin motivo y no ser útil para la gestión de los casos. Podría plantearse conservar la cadena de contactos de segundo orden inactiva, con todas las garantías que se consideren oportunas, hasta su activación cuando un contacto ha resultado finalmente infectado. En este caso, los contactos de segundo orden devienen contactos.

III. LA APLICACIÓN GESTIONADA POR LA ADMINISTRACIÓN SANITARIA ESPAÑOLA SE BASA EN LA PRIVACIDAD POR EL DISEÑO

Los primeros estudios sobre las aplicaciones gestionadas por distintas Administraciones sanitarias europeas concluyen que, salvo algunos aspectos mejorables, éstas suelen respetar la protección de datos. Se afirma, por ejemplo, que las versiones usadas en Irlanda, Polonia, Dinamarca y Letonia deberían mejorar sus garantías[25]. En el caso español, se sostuvo en su día la conveniencia de que RadarCovid usase certificados SSL para verificar que las comunicaciones fuesen seguras y que ofreciese el código en abierto. Este segundo punto, cuanto menos, parece haberse resuelto con la publicación del código fuente[26]. Por otro lado, en la versión de uso de RadarCovid, a diferencia de la primera versión de prueba, sí que se ha incorporado el certificado SSL. A pesar del cifrado de las comunicaciones, se ha detectado un agujero de seguridad, finalmente resuelto a principios de octubre de 2020, relativo a la identidad de las personas que informaban de un positivo. En este caso, a pesar de que no podía accederse al contenido, la empresa responsable de la aplicación de transmisión podía deducir que se trataba de un positivo. Para solventarlo, otras aplicaciones europeas enviaban falsos positivos para enmascarar a los reales. Ello no se hizo en la aplicación RadarCovid hasta el 9 de octubre de 2020. Tampoco se informó a los usuarios al no tener constancia de que se hubiera producido una violación real de la seguridad de los datos, siendo considerada así una vulneración potencial. En todo caso, existe un procedimiento abierto ante la

24 European Centre for Disease Prevention and Control, *cit., ibídem.*

25 Seguimos el studio de Leith, D.J. y Farrell, S., *Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps*, School of Computer Science & Statistics, Trinity College Dublin, Ireland, 18 de julio de 2020, pp. 1-22. Otros criterios para valorar el respeto a la intimidad y a la protección de datos en Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E. y Carrasco, A., «Privacy Assessment in Mobile Health Apps: Scoping Review», *JMIR MHealth and UHealth,* vol. 8, 2020, n.º 7, pp. 1-18.

26 Existe un repositorio sobre la aplicación {consulta: 20.10.2021}. Disponible en https://github.com/RadarCOVID/radar-covid-android/issues.

AEPD por posible brecha de seguridad de los datos. El poco uso de la aplicación hasta la fecha —octubre de 2021—, con únicamente el 2-4% de los casos positivos notificados, relativiza parcialmente esta vulnerabilidad[27]. En cuanto a los datos transmitidos por la aplicación cliente de RadarCovid, son básicamente los mismos que en la aplicación alemana (CoronaWarn), suiza (SwissCovid), italiana (Immuni), austríaca (StoppCorona) y danesa (SmitteStop)[28].

A pesar de la publicación del código en abierto, se ha criticado la falta de documentación explicativa complementaria para dar cumplimiento efectivo a la exigencia de transparencia. Aunque se publicó una vez la aplicación ya estaba en marcha —y no previamente como establece el art. 35.1 RGPD—, la evaluación de impacto de protección de datos (en adelante, EIPD) de noviembre 2020 concreta los riesgos y las soluciones adoptadas, lo cual quizá pueda contribuir a una mejor comprensión de la aplicación por parte de los usuarios[29].

Algunos de los aspectos discutidos, que han llevado a presentar denuncias a la Agencia Española de Protección de Datos, no resueltas a fecha de envío del presente trabajo, son los siguientes:

Los datos son pseudonimizados, no anónimos como parecía darse a entender cuando se afirmaba inicialmente que los datos recopilados por la aplicación no permitían la identificación directa del usuario o de su dispositivo. Se admite ahora en la EIPD que puede identificarse indirectamente a los usuarios mediante mapas de relaciones entre personas, reidentificación por localización implícita e identificación de los contagiados.

El responsable del tratamiento sería la Dirección General de Salud Pública, dependiente del Ministerio de Sanidad, aunque se sostiene igualmente que también lo serán las comunidades autónomas en el ámbito de sus competencias.

Es necesario obtener el consentimiento libre, específico, explícito e informado, mediante una clara acción afirmativa del usuario.

Aplicación del principio de minimización de datos y de la protección de datos por el diseño y por defecto: no se requiere un seguimiento de la ubicación de los usuarios, sino que se usan datos de proximidad. Los datos, además, se alojan en el terminal del usuario.

Los riesgos más notables, según el EIPD, serían la falta de información clara y concisa sobre las finalidades del tratamiento, lo cual afectaría al principio de transparencia en la información a los interesados; así como la falta de información y respuesta a la pretensión de ejercicio de los derechos de los interesados.

27 Estadísticas de uso de la aplicación RadarCovid {consulta: 20.10.2021}. Disponible en https://github.com/pvieito/Radar-STATS.

28 Leith, D.J. y Farrell, S., *cit.,* p. 6.

29 Ministerio de Asuntos Económicos y Transformación Digital, *Radar COVID. Informe de Evaluación de Impacto relativa a la Protección de Datos*, versión 2.0, noviembre 2020. La necesidad de una EIPD se basa en el uso de datos a gran escala, el control del interesado de forma sistemática y exhaustiva, el uso de categorías especiales de datos y la utilización de nuevas tecnologías.

Como veremos, estas aplicaciones son solamente uno de los componentes de un sistema más amplio; son la interfaz de contacto con el usuario y permiten interactuar con la Administración sanitaria. Concretamente, esta aplicación cliente permite recopilar las llaves de la persona cuando se detecta la infección, así como bajar las llaves publicadas de las personas infectadas para informar a sus contactos. Esta aplicación descentralizada aplica el principio de limitación de propósito y minimización de los datos por defecto, al permitir las notificaciones de proximidad, sin identificación ni GPS. Pero ello no evita todos los problemas. En efecto, existe además un segundo componente que analizaremos a continuación: el servicio de notificación de exposiciones de Google/Apple (GAEN, por sus siglas en inglés). Este servicio gestiona la transmisión y recepción mediante señales bluetooth, y juega así un rol central en el funcionamiento de la aplicación.

IV. LAS DUDAS SOBRE EL SERVICIO DE NOTIFICACIÓN DE LA EXPOSICIÓN DE GOOGLE/APPLE

Las aplicaciones nacionales se basan en un servicio de notificación de exposiciones de Google y Apple que fue lanzado de forma pública como API el 20 de mayo de 2020. La urgencia en su adopción podría explicar, al menos en parte, algunos de los riesgos para la protección de datos todavía existentes en su diseño. Conviene asegurarse que estos servicios cumplan con las necesarias garantías para la protección de datos, pues las autoridades fomentan su uso generalizado en la necesaria tarea de rastreo de los contactos de las personas infectadas.

Concretamente, cuanto menos en las versiones iniciales, se ha usado el servicio de Google Firebase, con la intención de borrarlo en las versiones sucesivas. El problema de usar estos servicios de análisis Google Play es que se conecta con los servidores de Google aproximadamente cada veinte minutos. Los datos que se pueden derivar de las conexiones son la dirección IP, una localización aproximada y otros identificadores que, sumados, pueden permitir el rastreo de la localización en el tiempo[30]. De hecho, se alega que algunas herramientas, como la disponible en www.coronadetective.eu, permiten re-identificar a las personas que notifican sus positivos.

Las posibles soluciones a tales problemas empezarían por una documentación comprensible para el usuario que incluya una evaluación de impacto de protección de datos, una posibilidad de *opt out* de los servicios de Google Play —para evitar que usuarios preocupados por su privacidad dejen de usar RadarCovid— y una revisión del mecanismo de gobernanza de estos sistemas GAEN, con obligaciones parecidas a las de las aplicaciones cliente, es decir con evaluaciones de

30 Leith, D.J. y Farrell, S., *cit.*, p. 2.

impacto de protección de datos[31]. Sin la confianza necesaria, el uso de tales aplicaciones puede no ser generalizado y mermar, con ello, su posible eficacia. Por otro lado, la gobernanza no puede quedar únicamente en manos de Google y Apple —aunque éstos deben estar presentes en la plataforma—, sino que debe compartirse con autoridades sanitarias públicas y representantes sociales.

Existen propuestas técnicas alternativas a los sistemas GAEN, como Pronto-C2 de la Universidad de Salerno (UNISA), PACT del MIT o un proyecto del NIST americano[32]. Sin embargo, aunque estos sistemas alternativos puedan ser técnicamente viables e incluso puedan ser mejores, no parece posible aplicarlos, sin más, para que funcionen en teléfonos móviles por razones de incompatibilidad y de consumo, entre otras. En definitiva, en la gestión de la Covid-19 no parecía posible escapar a la disyuntiva entre un modelo centralizado que recopilase los datos por parte del Estado, o un modelo descentralizado que se basase en las plataformas digitales de Apple y Google.

Quizá por ello podríamos preguntarnos, en primer lugar, si los teléfonos móviles son adecuados como herramientas médicas, debido a sus numerosos sensores y a los problemas derivados de esta capacidad de información. Existen tecnologías de rastreo y contacto que no se basan en teléfonos móviles, como en Singapur —dejando de lado el mandato obligatorio y los problemas de privacidad de este modelo—. Usan, en su lugar, las pulseras con sensores que únicamente se activan cuando el usuario notifica ser positivo. El NIST americano también opta por una tecnología de sensores portables o «wearables», como pulseras o relojes, para reducir los riesgos para la intimidad y la protección de datos[33].

En efecto, los riesgos para los derechos fundamentales podrían deberse principalmente a la infraestructura subyacente a las aplicaciones: la dependencia del GAEN limita las posibilidades de las aplicaciones nacionales y reduce las garantías para los usuarios. Ningún país se ha planteado, en la lucha contra la Covid-19, crear una infraestructura pública para las aplicaciones. En su lugar, se ha seguido la vía más rápida y barata de aprovechar las plataformas de Apple y Google. Construir una infraestructura alternativa podría ser una opción europea para la próxima pandemia y supondría una mejora significativa en las posibilidades de protección de los datos personales y de la intimidad de los usuarios. Mientras las aplicaciones se basen en plataformas GAEN, no se podrá garantizar que los datos de los usuarios se usen únicamente para la gestión de la pandemia y mientras

31 Leith, D.J. y Farrell, S., cit., p. 3.

32 Propuestas alternativas al modelo GAEN {consulta: 20.10.2021}. Disponible en https://eprint.iacr.org/2020/493, https://pact.mit.edu/, respectivamente. El modelo del NIST puede encontrarse en la nota siguiente.

33 Propuesta alternativa a la GAEN del NIST americano {consulta: 20.10.2021}. Disponible en https://www.nist.gov/system/files/documents/2020/09/08/NIST_ExposureNotificationMethod_2020901.pdf.

dure ésta. Es decir, el principio de limitación de propósito por defecto de la interfaz no queda preservado por la infraestructura GAEN.

V. VENTAJAS Y LÍMITES DE LAS APLICACIONES DE RASTREO

1. **Ventajas**

Las ventajas que ofrecen las aplicaciones de rastreo de infectados consisten en identificar más contactos que usando la memoria del paciente, así como notificar rápidamente contactos que el paciente desconoce, con el fin de poder rastrear y confirmar posibles casos[34]. Se ha sugerido que las aplicaciones permiten obtener datos más precisos, más rápidamente y a menor coste que el rastreo tradicional, incluso en zonas con poca cobertura y pocos recursos[35]. Ahora bien, el uso de la inteligencia artificial para la prevención de infecciones, por sí solo, no supone una ventaja definitiva. Es necesario un contexto de uso favorable, en el cual se integren los expertos en prevención de infecciones[36].

A la espera de valoraciones sobre la aplicación final de RadarCovid, disponemos de un estudio de seguimiento del prototipo durante 4 semanas, en un entorno controlado[37]. Entre el 29 de junio y el 22 de julio, en San Sebastián de la Gomera, se llevó a cabo un experimento con los residentes de la localidad que prestaron su consentimiento y se bajaron voluntariamente la aplicación. Se realizó una campaña de información y promoción del uso de RadarCovid y se simularon zonas de infección en cuatro localizaciones, tres urbanas y otra en una naviera que conecta la Gomera con Tenerife, con inicialmente 349 afectados. Un 10% de los 12.000 usuarios que se bajaron y siguieron activos con la aplicación resultaron finalmente infectados. De manera destacada, un 64% de los usuarios a los cuales se les envió un código lo introdujo, casi todos dentro de las 24h. El resultado final era esperanzador, pues se habían detectado 6,3 contactos por cada caso, de los cuales entre el 23 y 39% eran desconocidos. Como valoración final, los autores sostienen que es una herramienta útil como complemento a la detección y al rastreo tradicionales, aunque lamentan el bajo porcentaje de personas que comunican un contagio en la

34 European Centre for Disease Prevention and Control, *cit.*, p. 1-11.

35 Danquah, L.O., Hasham, N., Macfarlane, M., Conteh, F.E., Momoh, F., Tedesco, A.A., Jambai, A., Ross, D.A. y Weiss, H.A. «Use of a mobile application for Ebola contact tracing and monitoring in northern Sierra Leone: a proof-of-concept study», *BMC Infectious Diseases,* vol. 19, 2019, pp. 810-822.

36 Fitzpatrick, F., Doherty, A. y Lacey, G., «Using Artificial Intelligence in Infection Prevention», *Curr. Treat. Options Infect. Dis.*, vol. 12, 2020, pp. 135-144.

37 Rodríguez, P., Graña, S., Álvarez-León, E.E., Battaglini, M., Darias, F.J., Hernán, M.A., López, R., Llaneza, P., Martín, M.C., Ramírez-Rubio, O., Romaní, A., Suárez-Rodríguez, B., Sánchez-Monedero, J., Arenas, A. y LACASA, L., «A population-based controlled experiment assessing the epidemiological impact of digital contact tracing», *Nature Communications*, n.º 12, 2021, pp. 587-593.

aplicación definitiva. La diferencia con el prototipo puede deberse a que los usuarios sabían que era un experimento, con lo cual no les comprometía a ninguna actuación o test PCR posterior. Tampoco tienen información sobre el comportamiento de los contactos estrechos después de la notificación: ¿se autoaislaron para prevenir contagios o por el contrario siguieron haciendo vida normal? Finalmente, tampoco sabían si los usuarios seguirían activos durante un tiempo prolongado. Por todo ello, el número de bajadas de la aplicación —sobre los 7 millones— podría no ser un indicativo del todo fiable de los usuarios activos en la actualidad.

2. **Límites**

a) *Las aplicaciones no son la herramienta principal de rastreo y contacto*

Estas aplicaciones tienen límites que conviene remarcar. Así, las aplicaciones no deberían sustituir a los equipos físicos de rastreo sino, en todo caso, complementarlos[38]. No se trata de identificar a los contactos y de saber cuán cerca y por cuánto tiempo han estado en contacto con alguien, sino de permitir que personas que han estado cerca de una persona infectada sin saberlo, por ejemplo, en un medio de transporte público o en una dependencia pública, puedan saberlo. Se trata, por consiguiente, de permitir alertar y rastrear a los contactos con rapidez.

b) *Aspectos socioeconómicos*

Hay que tener presente, además, que las personas mayores pueden no disponer de teléfonos móviles o pueden no haberse bajado la aplicación. Las diferencias socioeconómicas y geográficas —zonas con poca cobertura— pueden también afectar al uso de las aplicaciones. Ello puede ser más acentuado en países en vías de desarrollo[39]. Hay que tener en cuenta, finalmente, que la persona puede no tener el móvil consigo todo el tiempo.

c) *Voluntariedad*

El uso de las aplicaciones de detección y rastreo debe ser voluntario y limitado en el tiempo[40]. Ello cobra importancia si los poderes públicos realizan campañas de

38 European Centre for Disease Prevention*, cit.,* p. 2.

39 Mbunge, E., «Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls», *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, 14, 2020, pp. 1631-1636.

40 European Centre for Disease Prevention, *cit.,* pp. 1-11.

concienciación para fomentar su uso y si la infraestructura sobre la que se basan no permite garantizar que Google y Apple no puedan usar los datos para otros fines.

d) *Falta de precisión*

Las aplicaciones deben ser precisas y avisar únicamente a los contactos de alto riesgo y no a los contactos separados por una barrera o un muro que impedía el contagio[41]. Por consiguiente, hay que distinguir los contactos de alto riesgo de aquellos otros que no lo son. Entre los primeros estarían, por ejemplo, personas en contacto de dos metros durante más de 15 minutos, sentados en un avión a dos asientos de distancia de una persona contagiada o cuidadores de personas infectadas sin las adecuadas medidas protectoras; en cambio, serían de bajo riesgo, los contactos que no superan los 15 minutos, en un medio de transporte público que no sea a dos asientos de distancia en un avión o cuidadores con las medidas adecuadas. Las aplicaciones, en muchos casos, no pueden discriminar entre los dos tipos de contactos. Quizá el parámetro «2 metros o menos durante 15 minutos» o combinaciones de distancia y tiempo puedan servir para clasificar como de alto riesgo. En todo caso, ello requiere un proceso de evaluación y calibrado de la aplicación[42]. Se sugiere tener en cuenta, entre otros, el porcentaje de contactos notificados que dan luego positivo, aunque ello pueda deberse a otro contacto. Otros datos, como la fecha del contacto, requieren consentimiento del afectado.

e) *Uso no autorizado o una vez la emergencia ha acabado*

Las aplicaciones de rastreo pueden llegar a usarse para otros fines distintos de la gestión de la pandemia o una vez ésta ya ha acabado[43]. Los principios de limitación del propósito y de límite temporal de la finalidad justificante obligan a una interpretación restrictiva en ambos casos. No deberían usarse los datos recopilados para fines no relacionados con la lucha contra la Covid-19, ni más allá del fin de la pandemia.

f) *Eficacia*

Dado que las aplicaciones de detección y rastreo plantean riesgos para varios derechos fundamentales como la protección de datos personales y la intimidad,

41 European Centre for Disease Prevention*, cit., p.* 3.

42 European Centre for Disease Prevention, *cit.*, p. 4 y anejo 1.

43 Floridi, L., «Mind the App—Considerations on the Ethical Risks of COVID-19 Apps», *Philosophy & Technology,* 13 de junio de 2020, 6 páginas.

el propósito público alegado debe quedar suficientemente acreditado. En efecto, de no ser una herramienta adecuada, se vulneraría el principio de proporcionalidad en su primer criterio: no sería una medida útil. Algunos estudios han intentado medir la eficacia de las aplicaciones en relación con la detección y el rastreo tradicional de infecciones. Sería necesario, al igual que sucede con el rastreo ordinario, que los datos fueran precisos y fiables, así como que la intervención fuese inmediata. Además, las aplicaciones de rastreo deben ser usadas por un porcentaje mínimo: se ha sugerido que incluso con un uso del 75-80% y un respeto de las cuarentenas del 90%, no sería suficiente sin medidas adicionales[44]. Por consiguiente, parecen medidas destinadas, en el mejor de los casos, a ser complementarias.

De manera general, se ha sostenido la utilidad de las aplicaciones con porcentajes mínimos de uso del 60% del total de los usuarios[45]. Ahora bien, otros estudios indican que pese a tener un porcentaje mucho más bajo, como el 15%, las aplicaciones podrían reducir hasta un 6-8% las infecciones e incluso las muertes[46]. En cambio, en el Reino Unido parece aceptado que, si el uso no llega al 20% de los usuarios, la aplicación no tiene sentido[47]. En España, el porcentaje de uso, en enero de 2021, podría estar entre el 2% y el 4%, aunque no son datos oficiales[48]. Las descargas de la aplicación podrían estar sobre los 8.000.000 a finales de 2021, según las estadísticas de la propia aplicación, siendo el número de casos positivos declarados a Radar COVID desde el 19 de agosto de 2020, de 76.000 aproximadamente, a finales de octubre de 2021.

En todo caso, ello pone de manifiesto que la aplicación puede llegar a ser desproporcionada, no sólo si es innecesaria, en el sentido de que podría haberse previsto una versión alternativa con las mismas finalidades que fuera más respetuosa con la privacidad y la protección de los datos personales; sino también, si es manifiestamente ineficaz, es decir, si su uso no aporta ventajas significativas en relación con la gestión de la detección y el rastreo manuales. A pesar de ser una aplicación respetuosa con la privacidad y la protección de datos, el riesgo para estos derechos no es nulo. Ello puede acarrear una inconstitucionalidad

44 Braithwaite, I., Callender, T., Bullock, M. y Aldridge, R.,W., «Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19», *The Lancet*, vol. 2, noviembre 2020.

45 Skoll, D., Miller, J.C. y Saxon, L.A., «COVID-19 Testing and Infection Surveillance: Is a Combined Digital Contact Tracing and Mass Testing Solution Feasible in the United States?», *Cardiovascular Digital Health Journal,* vol. 1, 2020, n.º 3, pp. 149-159.

46 Abueg, M., Hinch, R., Wu, N., Liu, L., Probert, W.J.M., Wu, A., Eastham, P., Shaf, Y., Rosencrantz, M., Dikovsky, M., Cheng, Z., Nurtay, A., Abeler-Dörner, L., Bonsall, D.G., Mcconnell, M.V., O'banion, S. y FRASER, C., «Modeling the combined effect of digital exposure notifcation and non-pharmaceutical interventions on the covid-19 epidemic», *Washington State. Tech. Rep*., Universidad de Oxford y Google, 2020.

47 Floridi, L., *cit,* p. 2.

48 Puede verse el proyecto de Vieito, P.J. {consulta: 20.10.2021}. Disponible en https://github.com/pvieito/Radar-STATS#last-results.

sobrevenida por no ser, finalmente, una medida adecuada para la finalidad que se propuso inicialmente. Por consiguiente, pasado un tiempo prudencial de uso de la aplicación, el porcentaje de usuarios que, finalmente, se han bajado la aplicación y han reportado estar infectados es relevante a efectos de la proporcionalidad de la medida. Y ello, no únicamente de acuerdo con el test de adecuación —pues alguna ventaja, cuanto menos teórica, tendrá la aplicación— sino, en definitiva, por la ponderación del test de proporcionalidad en sentido estricto, es decir si, una vez tomado todo en consideración, la medida aporta más ventajas o añade más riesgos.

De hecho, en el Reino Unido y en Noruega, las aplicaciones de rastreo centralizadas han sido finalmente suspendidas por falta de eficacia[49]. Quizá la falta de confianza que generan los modelos centralizados haya contribuido, al menos parcialmente, a la baja eficacia de estas aplicaciones. En todo caso, los usuarios deben poder tener confianza en las aplicaciones y para ello es imprescindible asegurar la protección de los derechos fundamentales[50].

g) *Gobernanza de las infraestructuras*

La gestión de la pandemia de Covid-19 se ha basado en aplicaciones de detección y rastreo de contagios instaladas sobre una infraestructura privada preexistente, llamada GAEN. Nadie se ha propuesto por el momento dotar a las futuras aplicaciones de un entorno que garantice los principios de privacidad por el diseño de la interfaz. La necesidad de gobernanza de las infraestructuras quizás pueda abordarse, cuanto menos parcialmente, en la actual discusión sobre la Digital Market Act europea. Mientras no se avance en esta gobernanza, parece posible la reidentificación última de los usuarios que informen de un positivo mediante las aplicaciones basadas en GAEN[51].

VI. CONCLUSIONES

Las posibilidades de la inteligencia artificial son innegables en la lucha contra las pandemias. Sin embargo, las aplicaciones y los sistemas usados en la

49 Consejo de Europa, *Digital Solutions to Fight COVID-19*. 2020 *Data Protection Report*, octubre de 2020, 36 páginas, esp. pp. 28-29.

50 Ranisch, O., Nijsingh, N., Ballantyne, A., Van Bergen, A., Buyx, A., Friedrich, O., Hend, T., Marckmann, G., Munthe, C. y Wild, V., «Digital contact tracing and exposure notifcation: ethical guidance for trustworthy pandemic management», *Ethics and Information Technology,* 21 de octubre de 2020.

51 Pueden encontrase incluso aplicaciones en línea {consulta: 20.10.2021}. Disponible en https://www.coronadetective.eu/.

actualidad parecen todavía preliminares o inmaduros[52]. Los riesgos para la protección de datos personales y la intimidad son también patentes. Sin una prioridad por las aplicaciones más respetuosas por la privacidad, la falta de confianza de los usuarios puede menoscabar la eficacia de las soluciones propuestas. En este sentido, unas aplicaciones que sean ineficaces pueden vulnerar la proporcionalidad de las medidas. Y el reto es también para la adopción de mejores aplicaciones de inteligencia artificial: sin una gobernanza de la inteligencia artificial, en general, y de la infraestructura, en particular, no se conseguirá garantizar la defensa de los derechos fundamentales de los usuarios. Queda mucho por hacer si queremos estar mejor preparados para la próxima pandemia, también desde el punto de vista de la regulación o de la gobernanza de las aplicaciones de detección y rastreo de personas infectadas. Para ello, conveniente aprovechar la experiencia de las actuales aplicaciones de rastreo de Covid-19, pues nos servirán para fijar los contenidos y las garantías mínimas que deberían caracterizar a las futuras aplicaciones de rastreo.

***

TITLE: *Safeguards for Contact Tracing during Pandemic Crisis*

ABSTRACT: *Contact tracing apps have thrived during the pandemic crisis. The need has led to unbalanced decisions that should be soon improved. In this paper, we shed light on the pros and cons of these apps, concretely the risks of apps like RadarCovid for data protection and privacy. We suggest lawmakers should settle a governance process of the infrastructure beneath the apps. Even though the medical interface should comply with data protection by design, the private platforms of Exposure Notification of Google and Apple (GAEN) do not provide equivalent safeguards. Moreover, the lack of efficiency of the apps, considering these risks, is relevant for the constitutional proportionality of the measure.*

RESUMEN: *Las aplicaciones de detección y rastreo de contagios se han multiplicado con la pandemia. La urgencia ha llevado a decisiones cuestionables o, en cualquier caso, mejorables. En este trabajo, se abordan algunas de las virtudes y también los indudables riesgos para la protección de datos y la intimidad que suponen aplicaciones como RadarCovid. Su estudio lleva a valorar la conveniencia de una gobernanza de las infraestructuras sobre las que se basan las aplicaciones. Aunque la interfaz aplique los principios de protección de datos por el diseño, las plataformas privadas de notificación de casos de Apple y Google (GAEN, por sus siglas en inglés) no ofrecen las mismas garantías. Por otro lado, la falta de eficacia de la herramienta, en este contexto de riesgo para los derechos, puede llegar también a tener consecuencias sobre la proporcionalidad de la medida.*

KEY WORDS: *contact tracing, mobile apps, Data Protection, Privacy, Governance.*

PALABRAS CLAVE: *rastreo de contactos, aplicaciones móviles, protección de datos, intimidad, gobernanza.*

FECHA DE RECEPCIÓN: *23.02.2021* FECHA DE ACEPTACIÓN: *20.09.2021*

52 NAUDÉ, W., «Artificial intelligence vs COVID-19: limitations, constraints and pitfalls», *AI & SOCIETY, 28 de abril de 2020,* 5 páginas.