Revista de Bioética y Derecho
Perspectivas Bioéticas
www.bioeticayderecho.ub.edu - ISSN 1886-5887

DOSSIER CUESTIONES BIOÉTICAS DE LA PANDEMIA COVID-19

La COVID-19 y los desafíos de la vigilancia digital para los derechos humanos: a propósito de la *app DataCOVID* prevista en la Orden Ministerial SND/29/2020, de 27 de marzo

COVID-19 and the challenges of digital surveillance for human rights: Analysis of the app *DataCOVID* foreseen in the Ministerial Order SND/29/2020, of March 27th

La COVID-19 i els desafiaments de la vigilancia digital pels drets humans: a propòsit de l'*app DataCOVID* prevista a l'Ordre Ministerial SND/29/2020, del 27 de març

CARMEN MÁRQUEZ CARRASCO, JUAN ANTONIO ORTEGA RAMÍREZ *

* Carmen Márquez Carrasco. Catedrática de Derecho Internacional Público y Relaciones Internacionales, Facultad de Derecho, Universidad de Sevilla (España). Email: cmarque@us.es.

Juan Antonio Ortega Ramírez. Catedrático de Lenguajes y Sistemas Informáticos, E.T.S. de Ingeniería Informática, Universidad de Sevilla (España). Email: jortega@us.es.

Esta publicación se enmarca dentro de las actividades que desarrollan los grupos de investigación PAIDI "Nuevos sujetos, nuevos derechos, nuevas responsabilidades: derechos humanos en la sociedad global" (SEJ-055) e "Investigación, Desarrollo e Innovación en Informática" (TIC-223). Este trabajo se ha desarrollado parcialmente dentro de los proyectos de investigación "Gobernanza y Aplicación de la a Responsabilidad Social Empresarial en la Unión Europea" (DER2017-85834-R) y EDITH (PGC2018-102145-B-C21,C22 (AEI/FEDER, UE)), financiados por el Ministerio de Ciencia, Innovación y Universidades del Gobierno de España.

Resumen

La pandemia de la COVID-19 ha demostrado la fragilidad del mundo globalizado y se está combatiendo mediante una combinación de técnicas y herramientas de ámbitos muy diferentes, desde clínico hasta tecnológico. La aplicación de las nuevas tecnologías ha suscitado el actual gran debate europeo sobre la privacidad. Una de sus manifestaciones es la Orden SND/29/2020, de 27 de marzo, del Ministerio de Sanidad, en la que se prevé el desarrollo de la *app DataCOVID* de seguimiento digital. Este trabajo tiene por objeto examinar la legalidad y alcance de estas medidas desde la perspectiva del respeto al derecho a la privacidad en el marco de las garantías para los derechos humanos y la protección de datos.

Palabras clave: COVID-19; nuevas tecnologías; seguimiento digital; derecho a la privacidad; protección de datos personales; limitaciones de derechos y libertades fundamentales.

Abstract

The COVID-19 pandemic has demonstrated the fragility of the globalized world and is being fought through a combination of techniques and tools, among which new contact tracing technologies play a fundamental role. These new tracking technologies have sparked the current great European debate on privacy. One of its manifestations is Order SND/29/2020, of March 27, approved by the Ministry of Health of the Government of Spain, which provides for the development of a website and a contact tracing app *DataCOVID*. This work aims at examining the legality and scope of the measures adopted in the Ministerial Order considering its implications for the respect of the right to privacy and data protection from the perspective of human rights guarantees.

Keywords: COVID-19; new technologies; digital monitoring; contact tracing; right to privacy; protection of personal data; limitations of human rights and fundamental freedoms.

Resum

La pandèmia de la COVID-19 ha demostrat la fragilitat del món globalitzat i s'està combatent mitjançant una combinació de tècniques i eines d'àmbits molt diferents, des del clínic fins al tecnològic. L'aplicació de les noves tecnologies ha suscitat l'actual gran debat europeu sobre la privacitat. Una de les seves manifestacions és l'Ordre SND/29/2020, del 27 de març, del Ministeri de Sanitat, en la qual es preveu el desenvolupament de l'*app DataCOVID* de seguiment digital. Aquest treball té per objecte examinar la legalitat i abast d'aquestes mesures des de la perspectiva del respecte al dret a la privacitat en el marc de les garanties pels drets humans i la protecció de dades.

Paraules clau: COVID-19; noves tecnologies; seguiment digital; dret a la privacitat; protecció de dades personals; limitacions de drets i llibertats fonamentals.

1. Introducción

La crisis sanitaria global de la COVID-19 ha afectado profundamente a España[1] y al continente europeo, foco de la pandemia en los meses de marzo y abril de este *annus horribilis* 2020. Los gobiernos han ensayado diferentes enfoques para "aplanar la curva" y se ha procedido a valorar la efectividad de las medidas de choque adoptadas. Hasta ahora, los gobiernos que han reaccionado más eficazmente parecen ser aquellos que han invertido en una infraestructura de salud sólida, han sometido a pruebas masivas e identificaron y aislaron a las personas infectadas, y pusieron en cuarentena sus contactos.[2]

Buscar soluciones a este problema global requiere de las nuevas tecnologías de la información y la comunicación y la ingeniería de datos. En efecto, como han indicado varias organizaciones de derechos humanos, las funciones que la tecnología puede y debe desempeñar son imprescindibles. Ahora bien, el aumento de los poderes de vigilancia digital de los Estados, como el acceso a los datos de localización de los teléfonos móviles, amenaza la privacidad, la libertad de expresión y la libertad de asociación de una manera que podría conducir a violaciones de derechos humanos y a reducir la confianza en las autoridades públicas, con el consiguiente menoscabo de la eficacia de las repuestas de salud pública. Además, tales medidas también pueden conllevar un riesgo de discriminación que afecte de forma desproporcionada a comunidades ya marginadas.[3]

Los países europeos, que pertenecen al círculo de la llamada *Europa de los derechos* y que cuentan con amplias garantías constitucionales democráticas y de derechos y libertades fundamentales, hasta la fecha han sido reacios a imponer restricciones que impacten en el núcleo esencial de los derechos, como el derecho a la vida privada y la libre circulación de personas.

En este contexto, el gran debate europeo sobre la privacidad y sobre las salvaguardias con que los derechos humanos ya cuentan tiene que ver con la utilización de las nuevas tecnologías de seguimiento y rastreo digital para la contención de la COVID-19. Y ello por varias razones. En primer lugar, la UE ha desarrollado un marco cuasi-autónomo sobre Derecho digital y protección de datos personales que se entrecruza con la protección y garantías de los derechos y libertades

1 A fecha de 13 de junio del 2020, según el Ministerio de Sanidad hay 243928 personas contagiadas por el coronavirus en España y 2354844 de casos en Europa, de los 7670887 en el mundo. Véase https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov-China/home.htm [Consulta: 13 de junio 2020].

2 Estos países son Alemania, Taiwan, Nueva Zelanda, Islandia, Finlandia, Noruega y Dinamarca, todos ellos con gobiernos presididos por mujeres. Véase https://www.forbes.com/sites/avivahwittenbergcox/2020/04/13/what-do-countries-with-the-best-coronavirus-reponses-have-in-common-women-leaders/ [Consulta: 1 de junio 2020].

3 Disponible en: https://www.hrw.org/print/340477 [Consulta: 13 de junio 2020].

fundamentales en la propia Unión; en segundo lugar, porque la respuesta de la UE a la pandemia, a la vista de que varios países miembros (como Alemania, Francia, Italia) ya tienen proyectos acabados o en pruebas con miras a gestionar el complejo reto del desconfinamiento, ha promovido el desarrollo de una *app* europea de geolocalización (Rastreo Paneuropeo de Proximidad para Preservar la Privacidad/*Pan-European Privacy-Preserving Proximity Tracing*)[4] que estará operativa en breve.[5]

Este debate tiene su manifestación en España con la aprobación por el Ministerio de Sanidad de la Orden SND/29/2020, de 27 de marzo (BOE de 28 de marzo)[6], en la que figuran una serie de encomiendas de gestión a la Secretaría de Estado de Digitalización e Inteligencia Artificial para el desarrollo, entre otros, de la *app* DataCOVID19 para monitorizar a la población con el fin de contener la pandemia.

En este trabajo se examina la legalidad y alcance de las medidas adoptadas en la Orden Ministerial de acuerdo al marco jurídico europeo y su implementación nacional sobre el Derecho digital, la protección de datos personales y el respeto a la privacidad, incluyendo las garantías de los derechos humanos, en la actual situación de crisis sanitaria. Este trabajo tiene un enfoque multidisciplinar. Por ello, primeramente, se presentarán las características de las herramientas tecnológicas que se están desarrollando frente a la pandemia.

2. Desarrollo de tecnologías de seguimiento digital frente a la pandemia

La rápida expansión del coronavirus determina su alta capacidad de contagio. No es un virus con un índice de letalidad elevado, pero sí ha demostrado la fragilidad de la globalidad. Esta pandemia puede tener unas consecuencias aún difíciles de pronosticar y que pueden ser más graves que la Gran Recesión de 2008 que comenzó con la quiebra de Lehman Brothers o la de la Gran Depresión del 1929 que comenzó con el lunes negro de la bolsa neoyorquina.

4 https://www.pepp-pt.org/ [Consulta: 23 de abril 2020].

5https://elpais.com/tecnologia/2020-04-20/la-guerra-de-la-app-de-rastreo-del-virus-investigadores-y-gobiernos-europeos-compiten-por-su-opcion.html [Consulta: 23 de abril 2020].

6 https://www.boe.es/boe/dias/2020/03/28/pdfs/BOE-A-2020-4162.pdf [Consulta: 1 de abril 2020].

Un aspecto del contagio es que el virus puede estar presente en personas asintomáticas que son portadoras y por tanto pueden trasmitirlo al resto de la población, sin ni siquiera saberlo. Esto supone un reto que aún dificulta más su control y propagación.

Entre las nuevas tecnologías, son varias las iniciativas en marcha, y algunas de ellas están dando respuestas evidentes, combinadas con otras, como la realización masiva de test de detección, el confinamiento, el uso de mascarillas y guantes y otras medidas de higiene personal y reducción de la movilidad y la proximidad entre las personas. Entre ellas cabe mencionar los portales y plataformas digitales, los *gadgets*, la inteligencia artificial y la robótica, y la utilización de drones. Son las aplicaciones móviles y los *chatbots* los que están contemplados en la Orden Ministerial que analizamos en este trabajo y por ello nos referiremos a ellos a continuación.

2.1 Aplicaciones móviles

El desarrollo de big data y de *apps* de geolocalización para optimizar la vigilancia sanitaria en varios países de Asia ha tenido consecuencias positivas en el control de la crisis epidemiológica. Sin embargo, el uso de datos personales no ha estado exento de críticas y desconfianzas puesto que los gobiernos utilizan la combinación de estas *apps* móviles con otros portales web especializados y plataformas digitales para el control de los ciudadanos. Así, agencias gubernamentales chinas han desarrollado y operan un sistema que asigna a cada persona un código QR de movilidad[7]. El sistema obliga a que tras registrarse en las plataformas desarrolladas el usuario debe incluir sus datos personales, además de ubicación actual, los lugares en los que ha estado, unido a información sobre síntomas propios de la COVID-19. Para conseguir la difusión global del código, se incluyen como una funcionalidad adicional en dos plataformas chinas muy utilizadas, Alipay y Wechat[8], con las que el gobierno chino se ha asociado, fruto de lo cual ha llegado a manejar una enorme cantidad de datos. Se cuestiona además si estos datos conciernen solo a la salud o la ubicación, o si también comprenden datos de tráfico en internet, compras, etc.

En Corea del Sur la *app Corona100m*[9] ha sido muy importante para el control de la propagación de la pandemia. Esta *app* utiliza un sistema de localización GPS a través del cual los usuarios son informados cuando se encuentra a menos de 100 metros de un lugar que haya sido

7https://www.bloomberg.com/news/articles/2020-03-23/to-pass-go-in-china-you-need-a-green-light-from-alipay-app [Consulta: 20 de mayo 2020].

8https://www.finance.yahoo.com/news/alibaba-spinoff-alipay-surged-past-1-billion-accounts-in-2019-150728030.html [Consulta: 20 de mayo 2020].

9https://thediplomat.com/2020/03/a-democratic-response-to-coronavirus-lessons-from-south-korea/ [Consulta: 20 de mayo 2020].

frecuentado visitado por un contagiado, dentro de su periodo de contagio; también le informa si ha transitado por lugares donde previamente se han detectado casos de COVID-19. La responsabilidad en este caso es solo de una empresa tecnológica que construye los datos a través de información pública, o sea, entregados por las autoridades y a disposición de la ciudadanía.

De manera similar, otros gobiernos también han desarrollado *apps* para combatir el virus, como la lanzada por el Gobierno de Singapur (*TraceTogether)*. Esta es la solución tecnológica que ha inspirado a muchos países europeos para el desarrollo de sus propias aplicaciones y de la *app* europea. La *app* de Singapur almacena cuándo y con quién ha estado a menos de un metro cada usuario de la aplicación[10]. De esta manera, si alguien presenta síntomas es fácil avisar a los contactos con los que ha estado de esta circunstancia y aconsejarle (u obligarle) a realizar el confinamiento a aquellas personas que hayan estado expuestas a pacientes con sintomatología de la COVID-19. Se trata por lo tanto de detección individualizada, no de una localización por antenas o ámbitos de geolocalización. En cualquier caso, las autoridades pueden obtener información encriptada en casos de riesgo.

Este modelo ha servido de base para otras iniciativas. El Gobierno japonés ha puesto en marcha un sistema similar que informa al usuario de su proximidad a un infectado sin indicarle cuándo.[11]

De manera análoga, la histórica alianza Google y Apple para combatir el virus, desarrollan una iniciativa que ha comenzado a fines de mayo para inter-operar teléfonos con sistemas iOS y Android que a través de Bluetooth LE almacenará de manera anónima los dispositivos cercanos con los que se ha estado durante los últimos 14 días para notificar en caso de que haya un positivo y avisar a los que estuvieron próximos al mismo[12]. Las serias dudas acerca de la privacidad de los usuarios se resuelven según ambas empresas porque el sistema la garantizará con identificadores únicos de privacidad, que se almacenarán en los dispositivos, no en la nube y por el uso de Bluetooth y el carácter "voluntario" de la participación de los usuarios.[13]

10https://elpais.com/sociedad/2020-04-14/el-movil-avisa-has-estado-en-contacto-con-alguien-positivo-de-coronavirus.html [Consulta: 29 de mayo 2020].

11https://digitalpolicylaw.com/gobierno-de-japon-desarrolla-app-de-rastreo-de-covid-19/ [Consulta: 29 de mayo 2020].

12https://digitalpolicylaw.com/google-y-apple-desarrollaran-app-de-rastreo-de-covid-19-en-ios-y-android/ [Consulta: 29 de mayo 2020].

13 https://www.republica.com/2020/04/28/la-alianza-de-apple-y-google-para-luchar-contra-el-covid-19/ [Consulta: 29 de mayo 2020].

2.2 Chatbots

Los *chatbots* o *bots* conversacionales son programas que emulan tener una conversación con una persona. En el ámbito de la COVID-19 se han desarrollado algunos para realizar el seguimiento de los pacientes que hayan contraído la enfermedad y se encuentren en su hogar o bien aquellos otros que hayan presentado síntomas y se le haya informado a la autoridad sanitaria competente.

Estos sistemas comienzan a trabajar una vez que un usuario contacta con el servicio de salud informando sobre el padecimiento y la sintomatología de la enfermedad, o también cuando se utiliza una *app* para informar a un usuario que se encuentra dentro de los posibles infectados por el virus. Utilizando los sistemas de geolocalización o proximidad, según corresponda, se recibe una alerta informando que la persona debe autoimponerse una cuarentena si ha estado próximo a una persona contagiada y se realiza el seguimiento de los síntomas y/o la evolución de la enfermedad de la persona aislada.

Entre ellos se puede destacar Carina[14] que utilizando inteligencia artificial responde a preguntas sobre la COVID-19 en castellano, y otros *chatbots* como Pegg[15] de SAGE Group que se centra en prestar información sobre la protección y bienestar de los empleados, o el *chatbot*[16] de la empresa AvantgardeIT y Abarca que presta asistencia en la preparación de la solicitud de ayudas propuestas por el gobierno para personas físicas o autónomos.

3. Las medidas de seguimiento digital aprobadas en España y su incardinación en el Derecho de la Unión Europea

3.1 Medidas de vigilancia digital aprobadas en España

La Orden SND/29/2020 comprende dos grupos de medidas. El primero consiste en encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial el desarrollo urgente de soluciones tecnológicas y aplicaciones móviles con el fin de mejorar la eficiencia operativa de los servicios de salud del país y ofrecer la mejor atención a los ciudadanos.

Ello se ha concretado en la creación de una página web y una *app* que permite al usuario autoevaluarse sobre COVID-19 a partir de síntomas y ofrecerle información y consejos prácticos.

14https://1millionbot.com/chatbot-coronavirus/ [Consulta: 29 de mayo 2020].
15https://www.sage.com/es-es/productos/pegg/ [Consulta: 29 de mayo 2020].
16http://www.subsidioscovid19.es/ [Consulta: 29 de mayo 2020].

Esta *app* ya existe y se denomina AsistenciaCOVID19[17]. Dados los diferentes teléfonos y direcciones de cada Comunidad Autónoma, la *app* debe "permitir la geolocalización del usuario a los solos efectos de verificar que se encuentra en la Comunidad Autónoma en que declara estar" (Orden SDN/29/2020:2)[18]. La instalación de la *app* y la autorización de la geolocalización son *voluntarias*. Los sistemas operativos de los teléfonos móviles piden siempre el permiso del usuario si una *app* intenta acceder al GPS o a cualquier otro sensor, como la cámara de fotos o el micrófono.

La Orden también prevé el desarrollo de un asistente conversacional (*chatbot*) para ser utilizado vía aplicaciones de mensajería instantánea, así como el de una *web* para proporcionar información oficial ante las preguntas de la ciudadanía (Orden SDN/29/2020: 2)[19].

En cuanto a los datos recopilados, el Gobierno subraya que:

> *"los datos personales serán conservados durante el tiempo que perdure la crisis sanitaria y, una vez finalizada, serán agregados de forma anónima para tratarlos con fines estadísticos, de investigación o de planteamiento de políticas públicas, durante un período máximo de dos años"*.[20]

El segundo grupo de medidas encarga un estudio de movilidad de usuarios que se realizará por medio de la Secretaría de Estado de Digitalización e Inteligencia Artificial junto con el INE, siguiendo el modelo que éste ya aplicó el año pasado, y las principales operadoras de telefonía de España, con el fin de analizar los efectos de las medidas de confinamiento aplicadas durante la pandemia "a través del cruce de datos de los operadores móviles, de manera agregada y anonimizada" (Orden SDN/29/2020 2). Se llama *DataCOVID19*. Según la Orden ministerial, el periodo de análisis de la movilidad se ceñirá "a los días previos y durante el confinamiento" (Orden SDN/29/2020:2).

En estos momentos existen varios proyectos de desarrollo de tecnologías de seguimiento digital ya en marcha en diferentes Comunidades Autónomas[21]. Según el Gobierno español, se trata de tecnologías que sólo permiten manejar de manera confidencial, agregada y anónima datos voluntariamente proporcionados por los ciudadanos, y que, a nivel estadístico, serán útiles para

---

17https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2020/060420-asistencia-covid19.aspx [Consulta: 29 de mayo 2020].

18 https://www.boe.es/boe/dias/2020/03/28/pdfs/BOE-A-2020-4162.pdf [Consulta: 29 de mayo 2020].

19https://www.boe.es/boe/dias/2020/03/28/pdfs/BOE-A-2020-4162.pdf [Consulta: 29 de mayo 2020].

20https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2020/060420-asistencia-covid19.aspx [Consulta: 29 de mayo 2020].

21 Asturias, Canarias, Cantabria, Castilla-La Mancha y Extremadura serían los nuevos puntos que se sumarían a la Comunidad de Madrid (pionera) en la implementación de medidas de seguimiento digital. Sobre este proyecto: https://www.coronamadrid.com [Consulta: 29 de mayo 2020].

trazar –en tiempo real y con predicciones basadas en modelos matemáticos y algorítmicos– la movilidad de las personas y comprender así su influencia en la tasa real de contagio. Ahora bien, superada la crisis de la COVID-19, se entiende que esos datos deberían ser destruidos por completo.

En la ejecución del previsto estudio de movilidad, la Orden ministerial subraya que se velará por el cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)[22] y por el que se deroga la Directiva 95/46/CE; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPD)[23] y "los criterios interpretativos" de la Agencia Española de Protección de Datos (AEPD). La AEDP ha subrayado que:

> *"esta situación de emergencia no puede suponer una suspensión del derecho fundamental a la protección de datos personales. Pero, al mismo tiempo, la normativa de protección de datos no puede utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades competentes, especialmente las sanitarias, en la lucha contra la epidemia…"*[24]

La Orden ministerial de 27 de marzo pone de manifiesto, de acuerdo con Rivas (2020, p.1) "el interés del Gobierno español por apostar por las nuevas tecnologías como una herramienta más para la concreción de medidas excepcionales y urgentes que faciliten la contención del COVID-19"[25] Asimismo, estas medidas suponen que, en esta situación excepcional, se permitirá a la Administración la geolocalización de los usuarios de los móviles por motivos de salud y la monitorización de la población.

Para un sector de opinión[26], las medidas de rastreo digital representan una forma de intromisión ilegítima estatal en el ámbito de la mayor intimidad y privacidad de las personas.

22https://www.boe.es/doue/2016/119/L00001-00088.pdf [Consulta: 29 de mayo 2020].

23https://www.boe.es/eli/es/lo/2018/12/05/3 [Consulta: 29 de mayo 2020].

24https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad; sobre la noticia véase https://www.ituser.es/seguridad/2020/03/las-webs-y-apps-de-autodiagnostico-del-covid19-ante-la-proteccion-de-datos-estas-son-las-normas [Consulta: 29 de mayo 2020].

25Rivas, M. (2020) Implicaciones legales del seguimiento digital en España [en línea]. Disponible en: https://www.fidefundacion.es/Implicaciones-legales-del-seguimiento-digital-del-COVID-19-en-Espana_a1272.html [Consulta: 29 de mayo 2020].

26 Así, la Asociación Española de Derechos Humanos expresa que "es preocupante el hecho de que medidas como la de geo-localizar individualmente entran ya en el control de la esfera individual de la persona sin su consentimiento". El 19 de abril de 2020, 300 científicos y académicos han firmado una carta sobre los problemas de vigilancia masiva que entrañan estas tecnologías. En: https://digitalpolicylaw.com/cientificos-y-academicos-desconfian-de-apps-de-rastreo-de-contactos-para-combatir-covid-19/ [Consulta: 2 de mayo 2020]. Amnistía Internacional han elaborado recomendaciones para que se respeten plenamente los derechos

Desde esta perspectiva es preciso evaluar su conformidad con los marcos jurídicos en los que se encuadran.

3.2 Conformidad con el marco europeo y su implementación nacional sobre protección de datos personales

Se ha de subrayar la importancia que tienen los principios de finalidad y proporcionalidad en la protección de datos de carácter personal, como establece en su artículo 6 la Directiva 95/46/CE, adoptada el 24 de octubre de 1995[27]. El artículo 8 de la Carta de los Derechos Fundamentales de la UE contempla que el tratamiento de los datos personales tiene que realizarse conforme a unos criterios o principios que lo legitimen (fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley) y que deberá existir una autoridad de control independiente que se encargue de supervisar el respeto de las normas sobre esta materia[28]. Sobre esta base, las medidas anunciadas deben tener un ámbito temporal: el que marque la crisis sanitaria y el estado de alarma.

Las medidas contempladas en la Orden ministerial SND/297/2020 encuentran su encuadre legal en el Real Decreto 463/2020, de 14 de marzo, por el que se declara en España el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por la COVID-19[29]. Asimismo, se basan en la Ley Orgánica 3/1986, de 14 de abril, sobre Medidas Especiales en Materia de Salud Pública[30], y en la Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio[31]. Tal y como específica la misma orden, estas medidas han de cumplir además con lo dispuesto en el RGPD y con la LOPD.

---

humanos al utilizar estas tecnologías. En: https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/los-estados-deben-respetar-los-derechos-humanos-al-emplear-tecnologias-de-vigilancia-digital-para-co/ [Consulta: 29 de mayo 2020].

27 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos: https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678 [Consulta: 2 de mayo 2020].

28Este artículo dispone "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2.Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley…". En: https://www.boe.es/doue/2010/083/Z00389-00403.pdf [Consulta: 2 de mayo 2020].

Véase Ruiz Miguel, C. (2003). El derecho a la protección de datos en la Carta de Derechos Fundamentales de la Unión Europea. Un análisis crítico. Revista de Derecho Comunitario Europeo 14 (7-43) [en línea]. Disponible en: https://recyt.fecyt.es/index.php/RDCE/article/download/48377/29850 [Consulta: 2 de mayo 2020].

29 BOE 14/03/2020: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-3692 [Consulta: 2 de mayo 2020].

30 BOE 29/04/1986: https://www.boe.es/buscar/act.php?id=BOE-A-1986-10498 [Consulta: 2 de mayo 2020].

31 BOE 05/06/1981: https://www.boe.es/buscar/act.php?id=BOE-A-1981-12774 [Consulta: 2 de mayo 2020].

Teniendo en cuenta el contenido de la orden y su fundamento jurídico, la conformidad con el marco legal de las medidas de seguimiento digital dependerá de si son medidas temporales, necesarias y adecuadas en función de un propósito claramente previsto y delimitado (la gestión de la situación de crisis sanitaria ocasionada por la COVID-19).

También debe determinarse si constituyen una fórmula menos invasiva de retención limitada de datos. Esto es, que el procesamiento de los datos que se obtengan mediante dichas medidas permitirá la geolocalización del usuario a los solos efectos de verificar que se encuentra en la Comunidad Autónoma en que declara estar; y, por otro, que el análisis de la movilidad de las personas en los días previos y durante el confinamiento se hará únicamente de manera agregada y anonimizada, en el entendido de que, en realidad, se trata de datos seudo-anónimos. En efecto, anonimizar datos requiere de algo más que eliminar identificadores obvios (como números de teléfono y números IMEI).[32]

Entre los criterios técnicos elaborados por el Comité Europeo de Protección de Datos[33] y la AEPD, se subraya que dichas medidas deben respetar las leyes nacionales que implementan la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva europea de privacidad electrónica o *eDirective*)[34]. En principio, los datos de ubicación solo pueden ser utilizados por el operador cuando se hacen anónimos o con el consentimiento de las personas.

Sin embargo, el artículo 15 de la Directiva sobre privacidad electrónica, en línea con lo que establecía la Directiva 95, permite a los Estados miembros introducir medidas legislativas para salvaguardar la seguridad pública. Dicha legislación excepcional, que puede tener el efecto de introducir limitaciones en los derechos humanos, solo es posible si constituye *una medida necesaria, apropiada y proporcional en el marco de una sociedad democrática*.

Por tanto, son aplicables los requisitos que a este respecto contemplan el Convenio Europeo de Derechos Humanos y su interpretación por el Tribunal Europeo de Derechos Humanos (TEDH),

---

32 Se considera que un dato ha sido procesado de manera anónima cuando se tomen medidas adicionales para considerar el conjunto de datos como tal, incluida la eliminación y generalización de atributos o la eliminación de los datos originales, al menos hasta el punto de llevarlos a un nivel altamente agregado. Véase Grupo de Trabajo del artículo 29 (2014). Opinion 05/2014 on Anonymisation Techniques, nro. 0829/14/EN WP216, adoptado el 10/04/2014, en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Consulta: 2 de mayo 2020].

33 Statement on the processing of personal data in the context of the COVID-19 outbreak, adoptado el 19/03/2020, en: https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en [Consulta: 2 de mayo 2020].

34 https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32002L0058 [Consulta: 2 de mayo 2020].

en lo que afecten al derecho a la vida privada (artículo 8), así como con las condiciones de la Carta de Derechos Fundamentales de la UE, en lo que afecte al derecho autónomo de protección de datos personales del artículo 8 (artículo 52). Las limitaciones o restricciones de derechos reconocidos en estos dos instrumentos se encuentran sujetas al control judicial del Tribunal de Justicia de las Unión Europea[35] y del TEDH. En caso de una situación de emergencia, en la que fueran adoptadas medidas de suspensión o derogaciones de derechos, también deben limitarse estrictamente a la duración de la emergencia en cuestión.[36]

La *eDirective* y el RGPD establecen que los datos personales que son necesarios para alcanzar los objetivos perseguidos deben procesarse para fines específicos y explícitos. Además, los interesados deben recibir información transparente sobre las actividades de procesamiento y sobre sus características principales, incluido el período de retención para los datos recopilados y los fines del procesamiento. Al introducir el procesamiento de datos de ubicación no anonimizados, un Estado miembro está obligado a establecer garantías adecuadas, como proporcionar a los usuarios de servicios de comunicación electrónica el derecho a un recurso judicial.

El Comité europeo ha insistido en que la información proporcionada debe ser fácilmente accesible y debe proporcionarse en un lenguaje claro. Es importante adoptar medidas de seguridad y políticas de confidencialidad adecuadas para garantizar que los datos personales no se divulguen a partes no autorizadas. Las medidas implementadas para gestionar la emergencia actual y el proceso de toma de decisiones subyacente deben documentarse adecuadamente.

Respecto al uso de datos de ubicación móvil como una posible forma de monitorear, contener o mitigar la propagación de COVID-19, esto es, para geo-localizar a individuos o enviar mensajes de salud pública a individuos en un área específica por teléfono o mensaje de texto, las autoridades públicas deben, en primer lugar, tratar de procesar los datos de ubicación de forma anónima (es decir, procesar los datos agregados de una manera que los individuos no pueden ser re-identificados), lo que podría permitir generar informes sobre la concentración de dispositivos móviles en una determinada ubicación ("cartografía" o "mapeo"). Hay que recordar a este respecto que las normas de protección de datos personales no se aplican a los datos que se han anonimizado adecuadamente, entendiendo que un dato ha sido procesado de manera anónima cuando se tomen medidas adicionales para considerar el conjunto de datos como tal, incluida la eliminación y generalización de atributos o la eliminación de los datos originales, al menos hasta

35 Artículo 52 de la Carta de Derechos Fundamentales de la UE y artículos 8-11 CEDH.

36 Oraá Oraá, J. (1997). Derechos humanos, estados de emergencia y Derecho internacional. En *Cursos de Derecho Internacional de Vitoria Gasteiz* (pp. 17-46). Vitoria Gasteiz: Universidad del País Vasco.

el punto de llevarlos a un nivel altamente agregado. En cuanto al principio de proporcionalidad, son preferibles las soluciones menos intrusivas, dado el propósito específico que se debe lograr. Cabe preguntarse si las medidas invasivas, como el "seguimiento digital" (es decir, el procesamiento de datos históricos de ubicación no anonimizados) podrían considerarse proporcionales en estas circunstancias excepcionales, y ello dependerá de las modalidades concretas del procesamiento. Para tales casos, esta tecnología deberá estar sometida a mayor escrutinio y mayores salvaguardas para garantizar el respeto de los principios de protección de datos: proporcionalidad de la medida en términos de duración y alcance, retención limitada de datos y limitación de propósito.

Estas garantías han sido subrayadas desde diversas instancias europeas, tales como el Supervisor Europeo de Protección de Datos (SEPD)[37], la Comisión[38] y el Parlamento Europeo (PE).

La Comisión Europea ha especificado que las *apps* descargadas en los dispositivos móviles deberían utilizar una tecnología ya existente, como el *Bluetooth*, para establecer la proximidad de otro dispositivo, encriptar la información, almacenarla de una forma segura y permitir un acceso seguro de las autoridades sanitarias. Esta solución se diferencia del GPS en que *no almacena los datos de ubicación*. Según la Comisión, el teléfono móvil tendría ya cargados los datos de proximidad y si alguno de los usuarios comunica una infección habría métodos para advertir a las personas que han estado en contacto cercano con el infectado, preservando los requisitos de confidencialidad. De ahí el debate más actual sobre estas herramientas centrado en torno a su almacenamiento centralizado o no centralizado[39], y la posición del PE expresada en su Resolución de 17 de abril de 2020 a favor del almacenamiento descentralizado y de mantener todas las cautelas.[40]

Teniendo lo anteriormente expuesto, se puede afirmar, que, en principio, las medidas decretadas en la Orden SND/297/2020 son ajustadas a Derecho, ya que a través de ellas las autoridades públicas españolas sólo podrán procesar "anónimamente" los datos de ubicación proporcionados libremente por los ciudadanos, es decir, procesar los datos agregados de manera

37https://www.mobileworldlive.com/spanish/el-supervisor-europeo-de-proteccion-de-datos-propugna-una-actuacion-paneuropea-contra-la-covid-19/ [Consulta: 2 de mayo 2020]. Según el actual Supervisor Europeo, los más adecuado sería la coordinación con la Organización Mundial de la Salud para asegurar la protección de datos globalmente.

38https://ec.europa.eu/info/files/recommendation-apps-contact-tracing_es [Consulta: 29 de mayo 2020]. La Recomendación de la CE establece que son preferibles las medidas menos intrusivas pero efectivas.

39https://elpais.com/tecnologia/2020-04-26/las-tecnologias-de-la-covid-19-marcaran-nuestro-manana.html [Consulta: 29 de mayo 2020]. Francia es partidaria de la solución centralizada. Información disponible en: https://elpais.com/tecnologia/2020-04-23/francia-pide-a-apple-y-google-que-limiten-la-privacidad-de-los-usuarios-para-crear-su-app-de-rastreo.html [Consulta: 29 de mayo 2020].

40Resolución de 17 de abril del 2020 del PE sobre la acción coordinada de la UE para combatir la pandemia de la COVID-19 y sus consecuencias. En: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf [Consulta: 2 de mayo 2020].

tal que las personas no puedan volver a identificarse, y exclusivamente para la gestión de la crisis del coronavirus. Coincidimos con Rivas (2020: p.1) en que dichas medidas "no tienen por qué representar una intromisión ilegítima en la vida privada de las personas, la vulneración a los derechos de protección de su propia imagen, protección de datos, intimidad y libre circulación". Ahora bien, habrá que esperar a ver cómo se implementan operativamente.

4. Conclusiones

La COVID-19 va a obligarnos a decidir lo que es "la nueva normalidad", y lo que no, en muchísimos ámbitos, y no solo en materia sanitaria sino, además, en los terrenos jurídico, social y económico.

Es bastante probable que los gobiernos tengan dificultades para responder a las preguntas de cómo determinar qué es necesario y qué es proporcional en las limitaciones del derecho a la privacidad ante las pandemias. Es poco probable que se consideren necesarias restricciones de privacidad que no demuestren ser esenciales para salvar vidas, o que permitan la continuación de una actividad económica esencial. La disponibilidad de alternativas viables para preservar la privacidad debería descartar la posibilidad de implementar políticas intrusivas, aunque sea temporalmente, ya que no cumplirían con el test de proporcionalidad. Exigir garantías cuando se extraiga información de móviles en la lucha contra la COVID-19 es lo adecuado, y así se ha hecho desde diversas instancias europeas[41] y nacionales.

La crisis de la COVID-19 pone de manifiesto cuan fundamental es articular un equilibrio entre la necesidad de salvaguardar la salud pública y la limitación de ciertas libertades fundamentales, aunque sin perder de vista que los valores y derechos a la vida y la salud deben ser prioritariamente salvaguardados en tal coyuntura. Varios países miembros del Consejo de Europa han notificado la aplicación del artículo 15 del CEDH para la suspensión de determinados derechos y libertades fundamentales[42]. No es el caso de España, que, *desde una perspectiva jurídico-internacional*, ha preferido centrarse en la figura de las limitaciones y restricciones a los derechos reconocidos, y ante el dilema de suspender o no suspender, ha optado por favorecer el

41https://www.europarl.europa.eu/spain/barcelona/es/prensa/el-pe-pide-garant%C3%ADas-de-que-se-respeta-la-protecci%C3%B3n-de-datos-al-recabar-informaci%C3%B3n-de-m%C3%B3viles-contra-el-covid-19. [Consulta: 2 de junio 2020]. El SEPD también ha emitido una guía dedicada sobre los tests de necesidad y proporcionalidad, pero la necesidad de actuar rápidamente en una pandemia puede llevar a los gobiernos a apresurar las pruebas en su intento de aplicar todas las medidas posibles.

42https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/62111354 [Consulta: 5 de junio 2020].

principio de normalidad ya que ha gestionado la crisis sin proceder a derogar derechos reconocidos ni proclamar un estado de emergencia.

Por todo ello, es imperativo realizar un ejercicio de reflexión ciudadana sobre la tecnología que queremos. Sin duda, las medidas de seguimiento digital son herramientas valiosas en estos tiempos de pandemia. También demuestran ser un instrumento de control, cuya utilización en el marco de una crisis sanitaria debe estar sometida a información, transparencia, rendición de cuentas públicas y control judicial.

Bibliografía

- Agencia de Derechos Fundamentales de la Unión Europea (2018). *Manual de legislación europea en materia de protección de datos*. Luxemburgo: Oficina de Publicaciones de la Unión Europea.
- Agencia de Derechos Fundamentales de la Unión (2020). *Coronavirus pandemic in the EU — fundamental rights implications*, Boletín nro. 1, del 1 de febrero al 20 de marzo de 2020[en línea]. Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin_en.pdf [Consulta: 29 de mayo 2020].
- Carrillo Salcedo, J.A. (2003). *El Convenio Europeo de Derechos Humanos*. Madrid: Tecnos.
- Carrillo Salcedo, J.A. (2001). *Soberanía de los Estados y Derechos Humanos en Derecho Internacional* (2ª ed). Madrid: Tecnos.
- European Center for Digital Rights (2020). *Ad hoc Paper (V0.3) SARS-CoV-2 Tracking under GDPR* [en línea]. Disponible en: https://noyb.eu/sites/default/files/2020-04/ad_hoc_paper_corona_tracking_v0.3.pdf [Consulta: 29 de mayo 2020].
- Comité Europeo de Protección de Datos (2020). *Statement on the processing of personal data in the context of the COVID-19 outbreak*, [en línea]. Disponible en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf [Consulta: 29 de mayo 2020].
- González Fuster, G. (2009). Tribunal Europeo de Derechos Humanos: TEDH- Sentencia de 04.12.2008, S y Marper c. Reino Unido, 30562/04 y 30566/04- Artículo 8- Vida privada- Injerencia en una sociedad democrática- Lo límites del tratamiento de datos biométricos de personas no condenadas. *Revista de Derecho Comunitario Europeo 33*, 619-633.

- Grupo de Trabajo del artículo 29 (2014). *Opinion 05/2014 on Anonymisation Techniques, nro. 0829/14/EN WP216*, [en línea]. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Consulta: 2 de mayo 2020].
- Hustinx, P. (2017). EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. En M. Cremona (ed) *New Technologies and EU Law*. Oxford: Oxford University Press.
- Mangas Martín, A. et al (2008). *La Carta de Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo*. Bilbao: Fundación BBVA.
- Madrid, A. (2020). Vigilancia digital: antes y después del COVID-19, *Revista Mientras Tanto* [en línea]. Disponible en: http://www.mientrastanto.org/boletin-189/notas/vigilancia-digital-antes-y-despues-del-covid-19 [Consulta: 24 de abril 2020].
- Oraá Oraá, J. (1997). Derechos humanos, estados de emergencia y Derecho internacional. En *Cursos de Derecho Internacional de Vitoria Gasteiz* (pp. 17-46). Vitoria Gasteiz: Universidad del País Vasco.
- Piñar Mañas, J.L. (2020). *La protección de datos durante la crisis del coronavirus* [en línea]. Disponible en: https://www.abogacia.es/actualidad/opinion-y-analisis/la-proteccion-de-datos-durante-la-crisis-del-coronavirus/ [Consulta: 2 de mayo 2020].
- Rivas, M. (2020). *Implicaciones legales del seguimiento digital en España* [en línea]. Disponible en: https://www.fidefundacion.es/Implicaciones-legales-del-seguimiento-digital-del-COVID-19-en-Espana_a1272.html [Consulta: 2 de mayo 2020].
- Ruiz Miguel, C. (2003). El derecho a la protección de datos en la Carta de Derechos Fundamentales de la Unión Europea. Un análisis crítico. *Revista de Derecho Comunitario Europeo* 14, 7-43. [en línea]. Disponible en: https://recyt.fecyt.es/index.php/RDCE/article/download/48377/29850 [Consulta: 2 de mayo 2020].

Fecha de recepción: 30 de abril de 2020
Fecha de aceptación: 15 de junio de 2020