confluências
revista interdisciplinar de sociologia e direito
| ARTIGO

NUEVAS TECNOLOGÍAS Y RETOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN EUROPA: EL RASTREO DE CONTACTOS DURANTE LA PANDEMIA POR COVID-19

Monica Arenas Ramiro
Universidad de Alcalá

RESUMEN

Vivimos un proceso de digitalización que se ha visto acelerado no sólo por los numerosos avances tecnológicos de los últimos años, sino por los acontecimientos relacionados con la pandemia que estamos viviendo a nivel mundial por COVID-19, y que nos han obligado a mantener medidas de distanciamiento social para combatir el virus. Pero como en toda pandemia o control de enfermedad infecciosa, más allá del distanciamiento social y otras medidas higiénico-sanitarias, se hace necesario identificar y rastrear los casos de las personas infectadas por coronavirus, conocer sus contactos y aislarlos para frenar la expansión del virus. Estas medidas suponen generalmente el conocimiento de datos tan sensibles como los relacionados con la salud y, por tanto, una clara injerencia en la vida privada de los ciudadanos. La cuestión es comprobar si dicha injerencia está o no justificada y es legítima. Este artículo se ocupa de dar respuesta a dicha cuestión, de analizar si las medidas de rastreo cumplen con los principios necesarios para tratar datos personales, y si el tratamiento que supone la identificación de los infectados y de sus contactos tiene una base de legitimación que las justifique.

Palabras-clave: COVID-19. Protección de datos personales. Rastreo de contactos.

NEW TECHNOLOGIES AND CHALLENGES FOR THE PROTECTION OF PERSONAL DATA IN EUROPE: CONTACT TRACING DURING THE COVID-19 PANDEMIC

ABSTRACT

We are living through a process of digitalisation that has been accelerated not only by the numerous technological advances of recent years, but also by the events related to the COVID-19 pandemic we are experiencing worldwide, which have forced us to maintain social distancing measures to combat the virus. But as in any pandemic or infectious disease control, beyond social distancing and other hygienic-sanitary measures, it is necessary to identify and trace cases of people infected by coronavirus, to know their contacts and isolate them in order to stop the spread of the virus. These measures generally involve the disclosure of such sensitive health-related data and, therefore, a clear interference in the private lives of citizens. The question is whether or not such interference is justified and legitimate. This article is concerned with answering this question, analysing whether the tracking measures comply with the necessary principles for processing personal data, and whether the processing that involves the identification of infected persons and their contacts has a legitimate basis that justifies it.

Keywords: COVID-19. Personal data protection. Contact tracing.

Recebido em: 16/06/2021
Aceito em: 03/07/2021

INTRODUCCIÓN

Vivimos en un entorno altamente digitalizado,[1] en continua transformación acelerada a marchas forzadas por las situaciones de confinamiento y distancia social establecidas como medidas para frenar la pandemia. Así lo hemos visto en el ámbito educativo, con la docencia *online*, o en el ámbito laboral, con el teletrabajo. En relación con la protección de la salud, más allá del uso de nuestra información personal, de nuestros datos médicos con fines de investigación médica durante la pandemia,[2] lo hemos visto con medidas como la toma de temperatura, las aplicaciones médicas para ayudarnos a autodiagnosticarnos y, muy especialmente, con las medidas manuales o automatizadas de rastreo o seguimiento de los contactos de personas infectadas con coronavirus. Estas últimas medidas constituyen, innegablemente, una herramienta eficaz para frenar la expansión de la pandemia por COVID-19 y no sólo a nivel nacional.

No obstante, si bien es evidente la necesidad de tratar datos personales en estos casos, por otro lado, son también incuestionables los peligros a los que el tratamiento de dichos datos personales se encuentra sometido: discriminación, manipulación o intromisión en la vida privada de los sujetos son algunos ejemplos. Con el tratamiento de datos personales nos encontramos ante la afectación de un derecho fundamental: el derecho fundamental a la protección de datos personales, que significa el control y poder de disposición de los datos personales y está íntimamente ligado al desarrollo personal, a la dignidad de la persona.

Para garantizar este derecho, para garantizar la privacidad de los sujetos y el control de su información personal y protegerlo, entre otros, frente a las amenazas de los avances tecnológicos

[1] En palabras del Supervisor Europeo de Protección de Datos (SEPD), hoy más que nunca debemos defender la privacidad como "piedra angular de la libertad individual y de la democracia". Vid. SEPD, *The EDPS Strategy 2020-2024. Shaping a Safer Digital Future: a new Strategy for a new decade*, 30 de junio de 2020. Disponible en: https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf. Accedido en: 26 e mar. 2021).

[2] Vid. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (Publicadas el 21 de abril de 2020. Disponibles en https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en. Accedido en: 26 mar. 2021).

diversos Tratados y normas internacionales,[3] europeas,[4] y nacionales[5] fueron reconociendo el derecho fundamental a la protección de datos y estableciendo los principios y reglas básicas para tratar datos personales. Estas normas establecieron entre otros, a saber, esencialmente, la transparencia en el uso de los datos personales; la información sobre quién, cómo y cuándo tratará la información personal; la necesaria existencia de una base que legitime dichos tratamientos, como el tan manido consentimiento; o la existencia de una Autoridad independiente de control que vigile el cumplimiento de la normativa de protección de datos y la protección del derecho fundamental.

Así las cosas, como en toda posible lesión de un derecho fundamental, los numerosos retos a los que se enfrenta el uso de la información personal -como es el caso concreto de las medidas de rastreo de contactos que aquí se estudian-, deben analizarse en conexión con los principios que las normas de tratamiento de datos personales exigen para hacer real y efectivo el poder de disposición: la transparencia, la información y el consentimiento, entre otros. Habrá que analizar si dichas medidas se ajustan a las exigencias de la normativa de protección de datos, sin perder de vista, ante todo, que lo que está en juego es un derecho fundamental vinculado intrínsecamente a la dignidad de la persona.

1. UN CAMBIO DE PARADIGMA A LA HORA DE TRATAR DATOS PERSONALES: LA APROBACIÓN DEL RGPD

El 25 de mayo de 2018 -tras un largo y complejo proceso hasta su aprobación y con una técnica legislativa cuestionable, conteniendo cincuenta y seis cláusulas abiertas o remisiones a los

[3] Citamos aquí por ser el germen del derecho a la protección de datos, garantizando la vida privada de los sujetos, el art. 12 de la Declaración Universal de Derechos Humanos (DUDH), y el art. 8 del Convenio Europeo de Derechos Humanos (CEDH). A nivel internacional destaca el conocido como Convenio 108, del Consejo de Europa. Vid. Convenio nº 108, del Consejo de Europa, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, aprobado el 28 de enero de 1981. El citado Convenio se ha visto reformado por una versión aprobada por el Consejo de Europa el 18 de mayo de 2018, siendo un Protocolo de enmienda nº 223, y pasando a ser conocido como Convenio 108+.

[4] Art. 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) y art. 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE), donde se reconoce el derecho fundamental a la protección de datos como un derecho fundamental autónomo para todos los ciudadanos europeos. Vid., también, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD). El RGPD se publicó el 4 de mayo de 2016 en el DOUE, dilatándose su aplicación hasta dos años más tarde, a partir del 25 de mayo de 2018 (art. 99 RGPD).

[5] Si bien los Reglamentos comunitarios no necesitan de transposición, en España, con el fin de completar lo previsto en el citado RGPD, crear seguridad jurídica y evitar confusión con la normativa nacional hasta entonces vigente, se aprobó la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD). La LOPDGDD derogó la anterior Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD) (sin perjuicio de lo previsto para los Tratamientos sometidos a la Directiva (UE) 2016/680 y de las Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE). Para un estudio de la citada LOPDGDD, vid. ARENAS; ORTEGA, 2019. Haciendo referencia a la Exposición de Motivos de la LOPDGDD, destacando el reconocimiento de toda una serie de derechos digitales, adaptando los derechos a la era digital, vid. GARCÍA, 2018, p. 63.

Estados (GARCÍA, 2018, pp. 71-72; y GARCÍA, 2019, pp. 95-131)-, entró en aplicación el ya citado RGPD. El RGPD se aprobó con el objetivo de empoderar a los ciudadanos respecto del control de sus datos personales sin limitar el libre flujo de los datos personales, contribuyendo de esta forma a fortalecer el mercado único digital.[6]

Destacamos aquí esta norma porque es de obligado cumplimiento en toda la Unión Europea sin necesidad de transposición a los ordenamientos jurídicos nacionales,[7] y porque marca los principios que deben regir todo tratamiento de datos personales, como los que se producen con las medidas de rastreo de contactos. Por ello, la tomaremos como norma a cumplir de referencia. Pero no solo por esto. Debemos subrayar el hecho de que con la aprobación del RGPD se produjo un cambio esencial en la forma en la que hasta ahora se venían tratando los datos personales en Europa, aportando un enfoque proactivo y no reactivo de la norma (TRONCOSO, 2016, p. 468; GARCÍA, 2018, pp. 72-73; y LÓPEZ, 2017, pp. 19 y 52-60). Se pasa de un sistema reactivo, que actúa frente a las infracciones, a un sistema proactivo, que busca prevenir y evitar la infracción. Ahora hay que cumplir y, en caso de ser requerido por las Autoridades competentes, poder demostrar que se cumple.[8] Todo esto ha convertido al RGPD en una norma de referencia a nivel mundial.[9]

Con la finalidad de hacer efectivo el cambio de paradigma a un modelo proactivo y garantizar así el derecho fundamental a la protección de datos personales en un mundo digitalizado, el RGPD introdujo no sólo nuevos principios a la hora de tratar los datos personales, sino que reforzó las bases de legitimación y reconoció nuevas facultades a los titulares de los datos personales, otorgando también nuevas potestades sancionatorias a las Autoridades de control con el fin de hacerlas más eficaces en su labor de garantes del derecho.[10] Dejamos aquí simplemente mencionadas, a modo de ejemplo, las novedades más significativas: la exigencia de un principio de transparencia

[6] Este es el doble objetivo de la reforma, tal y como lo manifestó la Comisión en la propuesta inicial de reforma de la materia y aprobación del RGPD iniciada en el año 2010: COM (2010) 609 final, "Un enfoque global de la protección de los datos personales en la Unión Europea", Bruselas, 4 de noviembre de 2010.

[7] De conformidad con el art. 288 TFUE, se ofrece una mayor seguridad jurídica al introducirse un conjunto armonizado de normas en esta materia.

[8] Art. 5.2 RGPD: "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

[9] Ya con motivo de la celebración del Día Europeo de la Protección de Datos de 2020, la Vicepresidenta de la Comisión Europea (VERA JOUROVÁ) y el Comisario europeo de Justicia (DIDIER REYNDERS) concluyeron que el RGDP se estaba convirtiendo en un "estándar global", sirviendo de inspiración a un gran número de normas en todo el mundo. Sobre dicha Declaración conjunta, vid. *Joint Statement by Vice-president Jourová and Commissioner Reynders ahead of Data Protection Daty*, 27 de enero de 2020 (Disponible en https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_120. Accedido el: 26 mar 2021. Y con motivo de sus dos años de vida y el análisis del mismo por la Comisión, vid. Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el Informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación (Resolución 2020/2717 (RSP) (Disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_ES.html. Accedido el: 28 mar. 2021).

[10] Capítulo VII RGPD.

respecto de los tratamientos de datos personales que se produzca;[11] la exigencia de un consentimiento informado expreso, invalidando cualquier tipo de consentimiento tácito;[12] la exigencia de nombrar un Delegado/a de Protección de Datos en determinadas circunstancias, siendo obligatorio en todo caso para las Administraciones públicas (SIMON y BACARIA, 2020);[13] la regulación detallada del consentimiento de los menores de edad (ARENAS, 2019, pp. 237-264); y el reconocimiento de nuevas facultades a los titulares de los datos como el conocido derecho al olvido, que es una versión modernizada del ya conocido derecho de cancelación o supresión (RALLO, 2014; ARENAS, 2014, pp. 537-558; y ÁLVAREZ, 2016, pp. 227-240),[14] o el derecho a la portabilidad de los datos.[15]

Las medidas destinadas a informar y rastrear a las personas infectadas por COVID-19 y sus contactos deben cumplir con la normativa de protección de datos. Pero, a la hora de analizar si la medida está o no justificada y es legítima, no debemos olvidar que el derecho fundamental a la protección de datos personales no es absoluto y debe analizarse con perspectiva, de forma sistemática, en el contexto social en el que se aplica y ejerce, y en equilibrio con el resto de derechos fundamentales e intereses en juego, analizando si las medidas que representan la injerencia son proporcionadas en una sociedad democrática.[16]

1.1. Los principios del tratamiento de datos personales

El derecho a la protección de datos personales descansa sobre una serie de principios esenciales y necesarios para que el tratamiento de dichos datos pueda llegar a producirse. Estos principios, recogidos en el artículo 5 RGPD, hacen referencia, en su conjunto, a las condiciones básicas para que los datos personales puedan ser tratados. Los citamos aquí brevemente con el fin de pasar luego a analizar si las medidas de rastreo de contactos los cumplen o no. Si no los cumplen todos, las medidas deberán ser consideradas ilícitas.

[11] Art. 5.1.a) RGPD.
[12] Art. 4.11) RGPD.
[13] Arts. 37 a 39 RGPD. Vid. *Directrices sobre los Delegados de Protección de Datos (DPD)*, aprobadas por el Grupo de Trabajo del artículo 29, el 13 de diciembre de 2016; revisadas y adoptadas el 5 de abril de 2017 (Disponible en https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf. Accedido en: 28 mar. 2021).
[14] Art. 17 RGPD.
[15] Vid. las *Directrices sobre el derecho a la portabilidad de los datos*, aprobadas por el Grupo de Trabajo del artículo 29, el 13 de diciembre de 2016, revisadas y adoptadas el 5 de abril de 2017 (Disponible en https://www.aepd.es/sites/default/files/2019-09/wp242rev01-es.pdf. Accedido en: 28 mar. 2021).
[16] Así lo recoge expresamente el Considerando 4 RGPD: "El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad", añadiendo que "el tratamiento de datos personales debe estar concebido para servir a la humanidad".

En primer lugar, debemos citar el principio de licitud, lealtad y transparencia del tratamiento. Conforme a este principio, para que un tratamiento de datos personales pueda considerarse lícito, el mismo deberá tener unas bases legítimas, como luego veremos y que se recogen en el artículo 6 RGPD. Los datos se tratarán de forma leal y transparente respecto del titular de los datos.

En segundo lugar, se encuentra el principio de limitación de la finalidad, conforme al cual los datos personales deben recogerse con una finalidad determinada, explícita y legítima, que permita a su titular controlar el uso que se hará de los mismos. Esto provoca que los datos personales no sean tratados con objetivos indeterminados o no explícitos; y, por otro lado, que no puedan ser utilizados para finalidades "incompatibles" con aquéllas para las que originariamente fueron recogidos. Se considera que siempre es compatible con la finalidad para la que son recogidos los datos personales, todo tratamiento que tenga como objetivo fines históricos, estadísticos o científicos, y, en todo caso con fines de archivo en interés público.

En tercer lugar, tenemos uno de los principios más importantes y una de las reglas básicas extraídas de la nueva normativa comunitaria que exige que los datos tratados se limiten a los mínimos necesarios para la finalidad perseguida.

En cuarto lugar, encontramos el principio de exactitud, conforme al cual los datos tratados deben ser exactos y estar puestos al día.

En quinto lugar, tenemos el principio de conservación de los datos: los datos personales deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recogidos. Se podrán conservar por más tiempo exclusivamente para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

En sexto lugar, el RGPD recoge el principio de integridad y confidencialidad conforme al cual los tratamientos deben garantizar la seguridad de la información, evitando un tratamiento no autorizado o ilícito aplicando las medidas técnicas u organizativas adecuadas. El RGPD remite, por ejemplo, a técnicas como la anonimización o la pseudonimización.

Por último, el RGPD se refiere al ya citado principio de responsabilidad proactiva.

1.2. Las bases de legitimación del tratamiento de datos personales

El artículo 6 RGPD hace referencia a todas aquellas circunstancias que legitiman el tratamiento de datos personales, que lo hacen lícito. Así, en primer lugar, sólo se podrán tratar datos que cumplan con los principios mencionados anteriormente, y una vez que se den dichos principios, se debe tener una base que los legitime.

El consentimiento sigue siendo una de las principales bases que legitiman el tratamiento de datos que se efectúe, pero debemos recordar que para poder tratar datos personales no siempre es necesario contar con el consentimiento de su titular, sino que se podrán tratar datos si existe otra base de legitimación. El consentimiento es la manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consiente al tratamiento de sus datos personales.[17] Este consentimiento debe ser, por un lado, un consentimiento libre e informado, esto es, el interesado debe conocer, como mínimo, la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados sus datos.[18] Y, por otro lado, y aquí está la gran novedad introducida por el RGPD, el consentimiento debe ser expreso: será el responsable de un tratamiento de datos el que deberá asegurarse de contar de forma expresa con el consentimiento del titular de dichos datos, obligándose así a contar con una declaración o una clara acción afirmativa del titular de los datos, no siendo válido un consentimiento tácito. Para el caso de que el consentimiento sea prestado por un menor de edad, se requerirá siempre el consentimiento de sus padres o tutores si éste tiene menos de 13 años; si tiene entre 13 y 16 (la edad concreta la debe definir el Estado miembro), el consentimiento del menor será el único necesario para tratar sus datos personales.[19] Como otra novedad relacionada con el consentimiento- y que en este caso afecta al caso aquí analizado sobre el rastreo de contactos de infectados por COVID-19-, encontramos el tratamiento de los datos sensibles o "categorías especiales de datos"; aquí, con el fin de evitar situaciones discriminatorias, más allá del consentimiento del titular de los datos, se deberá contar con otra de las bases de legitimación previstas.[20]

Más allá del consentimiento, en primer lugar, encontramos que el tratamiento será lícito si es necesario porque exista un contrato que requiera conocer dichos datos.

En segundo lugar, el tratamiento será lícito si el mismo es producto de una obligación legal, que bien puede ser la normativa general y horizontal sobre protección de datos, o bien las normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. Este tipo de

[17] Art. 4.11) RGPD. Sobre el requisito del consentimiento expreso merece especial atención la STJUE de 1 de octubre de 2019, asunto Planet49, sobre el uso de las llamadas *cookies*. Con el fin de aclarar los criterios exigibles al consentimiento a la hora de tratar datos personales, el Comité Europeo de Protección de Datos (CEPD) aprobó sus *Directrices 5/2020 sobre el consentimiento en el sentido del RGPD*, haciendo especial referencia al caso de las cookies (Publicadas el 4 de mayo de 2020. Disponibles en: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en. Accedido en: 26 mar. 2021).

[18] Recordamos aquí que el responsable del tratamiento es, como dice el RGPD "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros" (art. 4.7) RGPD).

[19] Art. 8 RGPD.

[20] Art. 9 RGPD.

legitimación guarda una estrecha relación con el tratamiento que realizan las Administraciones públicas en el ámbito de sus competencias, pues las mismas actuarán porque exista una norma que así lo establezca, por tener que cumplir con una obligación legal. En todo caso, la obligación legal debe tener como base el Derecho de la Unión o el propio del Estado miembro.

En tercer lugar, y esto guarda especial relevancia para el caso analizado, el tratamiento será legítimo si persigue proteger un interés vital. El interés vital debe entenderse como el interés esencial para proteger la vida del interesado o la de otra persona física.

En cuarto lugar, el tratamiento será lícito si concurre un interés público. Aquí debemos entender que el concepto de interés público, o de misión realizada en interés público, hace referencia al bien común de la sociedad entera. Los ejemplos más típicos son los ámbitos educativos y sanitarios. Y aquí nuevamente, debemos recordar esta base de legitimación para el caso que nos ocupa. En todo caso, dicho interés público debe tener una base en el Derecho de la Unión o en el de los Estados miembros.

En quinto lugar, debemos destacar el caso en el que el tratamiento es necesario para el ejercicio de poderes públicos, esto es, de las Administraciones públicas, incluidas las sanitarias. En este sentido, la actividad de las Administraciones Públicas estará, por regla general, legitimada por realizar el tratamiento de datos amparándose en una tarea en interés público o en el ejercicio de poderes públicos que deberán estar establecidos en una norma de rango legal.

Y, en último lugar, se podrán tratar datos de forma legítima siempre que exista un interés legítimo en dicho tratamiento y siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta sus expectativas razonables basadas en su relación con el responsable. Todo ello implica que es necesario analizar el caso concreto y realizar una ponderación para poder determinar si prevalece o no el interés legítimo.

Así las cosas, como ahora veremos de forma detallada, para el caso del rastreo de contactos, entre las bases de legitimación citadas, podemos encontrar desde las obligaciones legales hasta el interés público y el interés vital tanto de los interesados como de terceros.

2. LOS RETOS PARA EL TRATAMIENTO DE DATOS PERSONALES: EL RASTREO DE CONTACTOS DE INFECTADOS POR COVID-19

En marzo de 2020 la Organización Mundial de la Salud (OMS) declaró la pandemia mundial causada por COVID-19.[21] La aparición del virus y la forma de contenerlo conllevó que la mayoría de

[21] Vid. Declaración de pandemia internacional de la Organización Mundial de la Salud (OMS), aprobada el 11 de marzo de 2020, así como la alocución del Director General de la OMS en la rueda de prensa al efecto. Disponible en:

Estados a nivel mundial decretaran medidas de confinamiento, lo que provocó no sólo que nuestra forma de relacionarnos con los demás cambiara, sino que también afectó y ha transformado nuestra forma de trabajar, estudiar, investigar y, por lo tanto, de mover y compartir la información. Junto a esas medidas, los Estados de todo el mundo, entre otras cosas, fueron desarrollando sus medidas, procedimientos, y aplicaciones informáticas (apps), con el fin de hacer frente a la emergencia sanitaria que se acababa de declarar. En ese momento incluso la OMS instó a los países a que rastrearan y analizaran a cualquier persona que mostrara síntomas de COVID-19. De la misma forma, desde la Unión Europea, ante el levantamiento de las medidas de confinamiento, se adoptó una Hoja de ruta promoviendo el rastreo de contactos mediante el uso de aplicaciones móviles como una de las medidas complementarias que deberían servir de apoyo al levantamiento del confinamiento.[22]

Se producía así un nuevo reto al tratamiento de nuestros datos personales, para nuestra privacidad: analizar si dichas medidas, consideradas necesarias para evitar la propagación de la pandemia eran una medida justificada y proporcionada en una sociedad democrática. No todos los fines justifican los medios, ni un fin legítimo hace lícitos los medios empleados. Se hace indispensable encontrar el equilibrio entre la necesidad evidente de combatir el virus y respetar nuestra vida privada, dentro de la cual se engloba el tratamiento de nuestra información personal. Por ello, debemos analizar si técnicamente son medidas eficaces o existen medidas menos intrusivas en nuestros derechos fundamentales para combatir el virus. Aunque la cuestión parecerá centrarse en una elección entre seguridad y privacidad (HARARI, 2020),[23] como ahora plantearemos, no es necesario situarnos ante tal disyuntiva si las medidas de rastreo se llevan a cabo respetando los principios del tratamiento de datos personales, desde la privacidad. Debemos ser consciente de que "la protección de datos no es un derecho impertinente que "prohíba" sin más "hacer cosas", sino que más bien marca el camino que indica "cómo deben hacerse las cosas" (PIÑAR, 2020).

https://www.who.int/es/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020. Accedido el: 28 mar. 2021.

[22] Vid. Joint European Roadmap towards lifting COVID-19 containment measures, de 15 de abril de 2020. Disponible en: https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf. Accedido el: 28 mar. 2021. A la misma hace referencia nuestro RDL 21/2020 de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19, que se tradujo en el Plan para la Transición hacia una Nueva Normalidad, de 28 de abril de 2020. Disponible en: https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov-China/documentos/PlanTransicionNuevaNormalidad.pdf. Accedido el: 28 mar. 2021, donde se recoge la agilidad a la hora de identificar y contener las fuentes del contagio como una de las condiciones indispensables para levantar el confinamiento, incluyendo el "Trazado y cuarentena de contactos siempre garantizando el anonimato y la privacidad de la información" (p. 11).

[23] Desde un punto de vista ético, no jurídico, HARARI añade que, en este caso, "nos enfrentamos a dos elecciones particularmente importantes. La primera es entre vigilancia totalitaria y empoderamiento ciudadano. La segunda es entre aislamiento nacionalista y solidaridad mundial".

Llegados a este punto, antes de analizar si las medidas de control del seguimiento de contactos cumplen con los principios del tratamiento de datos y tienen una base que las haga legítimas, debemos destacar el hecho de que dicho tratamiento de datos puede implicar el tratamiento de los llamados datos sensibles o "categorías especiales de datos". Datos sensibles, son, entre otros, datos relacionados con la salud, como es el hecho de estar infectado por coronavirus.[24]

Recordamos igualmente que el tratamiento de los datos sensibles, o de los datos de salud, estará prohibido salvo que concurra alguna de las siguientes circunstancias: el consentimiento explícito del titular de los datos; el tratamiento es necesario para el cumplimiento de obligaciones y derechos en el ámbito laboral y de la seguridad o protección social; el tratamiento es necesario para proteger intereses vitales; el tratamiento es efectuado en el ámbito de las actividades legítimas de una asociación o fundación, como ha quedado dicho; el tratamiento se refiere a datos que el interesado ha hecho manifiestamente públicos; el tratamiento es necesario para la formulación, ejercicio o defensa de reclamaciones; el tratamiento es necesario por razones de interés público esencial; el tratamiento es necesario para fines de medicina preventiva o laboral; el tratamiento es necesario por razones de interés público en el ámbito de la salud pública; o el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.[25]

Debemos recordar aquí también, para lo que nos interesa, que para el caso de tratamientos de datos con fines de medicina preventiva o laboral, se podrán llevar a cabo si el tratamiento es realizado por profesionales médicos o por personas sujetas al secreto profesional según las normas que establezcan los organismos nacionales competentes. Asimismo, el propio RGPD dispone que respecto de los datos relativos a la salud, "los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones".[26]

Pero, como hemos señalado, las medidas de rastreo de contactos no tratan sólo datos sensibles o categorías especiales de datos, como los relativos a la salud, sino que muchas veces, especialmente en las apps informáticas, se tratan datos de localización o de geolocalización. La norma de referencia en este caso ya no será sólo el RGPD, sino que debemos tener en cuenta la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas (conocida como Directiva e-Privacy), que nos habla de datos de localización y de datos de tráfico.[27] En el caso de las apps de rastreo lo

[24] Datos de salud son "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" (art. 4.15) RGPD.
[25] Art. 9 RGPD.
[26] Art. 9.4 RGPD.
[27] Art. 2.b) Directiva e-Privacy que define los datos de tráfico como "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"; y Art. 2.c) Directiva e-Privacy que define los datos de localización como "cualquier dato tratado en una red de comunicaciones

importante es la proximidad de una persona con otra persona infectada o sospechosa de serlo, pero no su localización. Recordamos en este punto y para lo que aquí nos interesa, que sólo se podrá tratar o acceder a los datos de localización de una persona de acuerdo con lo previsto en la citada Directiva e-Privacy, esto es, siempre que los datos estén anonimizados o, si no lo están, en circunstancias estrictamente definidas, o con el consentimiento expreso del usuario, tras una información clara y completa.[28] Por lo tanto, se tratarán los datos anonimizados, lo cual debe estar presidido por el principio de transparencia, creando seguridad en los sujetos cuyos datos van a ser tratados; o bien, si no fuera posible tal anonimización, se requerirá el consentimiento expreso e informado del titular de los datos, o bien, como ha quedado dicho, en circunstancias estrictamente definidas que deberán ser, en todo caso, como todo tratamiento de datos personales, necesarias, apropiadas y proporcionadas en una sociedad democrática y con las garantías adecuadas.[29]

Así las cosas, con el fin de ofrecer una solución sobre los conflictos generados con el tratamiento de estos datos y arrojar algo de luz sobre la materia, tanto el Comité Europeo de Protección de Datos (CEPD) a nivel europeo como el Consejo de Europa a nivel internacional -y como en España, la AEPD- se han pronunciado al respecto sobre estas medidas de rastreo de contactos (ARENAS, 2020, nº 4).[30] Asimismo, no podemos dejar de citar, por un lado, el excelente y completo trabajo de la Comisión Europea en este terreno con su Recomendación, de 8 de abril de 2020, y con su Comunicación, de 17 de abril de 2020, para conseguir un enfoque común a nivel comunitario en cuanto al uso de aplicaciones y datos móviles en respuesta a la pandemia del coronavirus;[31] y, por

electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público".

[28] Arts. 5.3, 6 y 9 Directiva e-Privacy.

[29] Art. 15 Directiva e-Privacy y art. 23.1 RGPD. Sobre las limitaciones del art. 23 RGPD, vid. *Guidelines 10/2020 on restrictions under Article 23 GDPR*, adoptadas el 15 de diciembre de 2020 (Disponibles en https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202010_article23_en.pdf. Accesible en: 26 mar. 2021.

[30] Sobre las manifestaciones citadas, vid. las *Directrices 3/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19*, y las *Directrices 4/2020, sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19*, ambas aprobadas el 21 de abril de 2020. Disponibles en https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_es y en https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_es. Accesible en: 28 mar. 2021); y a nivel internacional, del Consejo de Europa, la *Joint Statement on Digital Contact Tracing*, publicada el 28 de abril de 2020. Disponible en: https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7), así como como el Informe, de octubre de 2020, sobre *Digital solutions to fight COVID-19* (Disponible en https://rm.coe.int/report-dp-2020-en/16809fe49c. Accedido en: 28 mar. 2021. Y, en España, el Estudio de la AEPD sobre *El Uso de las Tecnologías en la lucha contra el COVID-19. Análisis de costes y beneficios*, publicado en mayo de 2020. Disponible en: https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf. Accedido en: 28 mar. 2021.

[31] Vid. Recomendación (UE) 2020/518 de la Comisión, de 8 de abril de 2020, relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados (Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020H0518&from=ES. Accedido el:

otro lado, la importante labor del SEPD, tanto en el 2020 en relación con el rastreo mediante apps, como en el 2021 en relación con el rastreo manual (aunque centrado en las instituciones y organismos europeos).[32]

Todos estos organismos, de una u otra forma, destacaron los principios que el rastreo de contactos manual y, especialmente, automatizado mediante apps, debían cumplir para ser una herramienta legítima para combatir el coronavirus. Entre estos requisitos, con carácter general, se ha hablado de cumplir con unas "Garantías Esenciales Europeas", esto es, en primer lugar, que el tratamiento de datos debía basarse en normas claras, precisas y accesibles; en segundo lugar, se debía poder demostrar la necesidad y la proporcionalidad con respecto a los objetivos legítimos que se persiguen; en tercer lugar se debería acreditar la existencia de un mecanismo de supervisión independiente; y, en cuarto lugar, se debía poner a disposición de los ciudadanos los recursos efectivos para que pudieran ejercer sus derechos.

Más concretamente, con el fin de garantizar la privacidad de los sujetos implicados, se resalta no sólo la exigencia de una base legítima; sino su limitación temporal; la previsión normativa del intercambio de información o su comunicación de forma transparente; y, en el caso de utilizar datos de tráfico y de localización, se advierte del peligro de geolocalizar a las personas, recomendándose la utilización sólo de los datos de tráfico y su anonimización. Como mínimo se indicaban, para el caso de las apps, tres aspectos que deberían tenerse en cuenta: la anonimización de los datos (la cual consistía no sólo en eliminar los datos identificativos obvios como el número del teléfono o el número IMEI, recomendándose la agregación de los datos); las medidas de seguridad y el acceso (garantizando la confidencialidad); y la limitación de la retención de los datos (en tanto que, en el marco de un proceso transparente, se deberían retener los datos el tiempo estrictamente necesario que durase la pandemia, la situación de excepción).

Por último, en todos los organismos se hace hincapié en el enfoque paneuropeo de las medidas, en el hecho de una coordinación en las medidas de rastreo y de combatir el virus, basándose

28 mar. 2021 y Comunicación de la Comisión Europea sobre Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos (2020/C 124 I/01). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=ES. Accedido el: 28 mar. 2021).

[32] Vid. Comunicado del SEPD de 6 de abril de 2020, "EU Digital Solidarity: a call for a pan-European approach against the pandemic". Disponible en: https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf. Accedido en: 26 mar. 2021 y sus *Orientations on manual contact tracing by EU Institutions in the context of the COVID-19 crisis*, de 21 de febrero de 2021. Disponible en: https://edps.europa.eu/data-protection/our-work/publications/guidelines/orientations-manual-contact-tracing-eu_en. Accedido el 26 de marzo de 2021). Con fecha 25 de marzo de 2020, el SEPD dirigió una Carta a D. Roberto Viola, Director General de la Dirección General de Sociedad de la Información y Medios de Comunicación de la Comisión Europea "Monitoring spread". Disponible en: https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf. Accedido en: 28 mar. 2021.

en todo caso en el respeto a los derechos fundamentales y, en especial, en el respeto a la privacidad de los sujetos, evitando que éstos puedan caer en algún tipo de estigmatización o discriminación. En este terreno debemos criticar el hecho de que ese enfoque uniforme parece haberse sólo conseguido con el controvertido "Certificado verde digital", también llamado "Pasaporte COVID", que plantea serias dudas sobre su potencial efecto discriminador.[33]

Así las cosas, por último, los citados organismos, con carácter general, además de establecer las citadas directrices sobre cómo tratar los datos personales en un contexto de pandemia, manifestaron -especialmente, el Consejo de Europa-, sus dudas en relación a la efectividad de estas medidas y aplicaciones de rastreo, ya que, consideran que las mismas deben venir acompañadas de otra serie de estrategias o planes, por lo que se recomienda expresamente que el funcionamiento de las aplicaciones se hiciera público, informado y transparente, y, de una manera entendible para toda la población.

Consideramos, además, como ha quedado dicho, que, en todo caso, la decisión que se tome debe ser una decisión lo más global posible, pues nos encontramos ante una emergencia global de salud pública, "que precisa de una respuesta coordinada y en gran escala de los Gobiernos en todo el mundo".[34] La respuesta debería venir coordinada desde Europa, e incluso coordinada con la Organización Mundial de la Salud (OMS) para una proyección mundial. Sólo a través de unas medidas de carácter "paneuropeo" lograremos una lucha contra la pandemia mucho más efectiva (HARARI, 2020).[35] Pero es indispensable que dichas medidas tengan un enfoque ético que eviten cualquier tipo de efecto discriminador.[36]

[33] Sobre el citado Pasaporte, destaca el Dictamen conjunto entre el SEPD y el CEPD. Vid. Dictamen conjunto 04/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre un marco para la emisión, verificación y aceptación de certificados interoperables de vacunación, pruebas y recuperación para facilitar la libre circulación durante el COVID-19 pandemia (Certificado Verde Digital). Disponible en: https://edps.europa.eu/system/files/2021-04/21-03-31_edpb_edps_joint_opinion_digital_green_certificate_en_0.pdf. Accesible en: 1 abr. 2021). Asimismo, vid. la citada propuesta de Reglamento del Parlamento Europeo y del Consejo, de 17 de marzo de 2021. COM (2021) 130 final. Disponible en https://eur-lex.europa.eu/resource.html?uri=cellar:38de66f4-8807-11eb-ac4c-01aa75ed71a1.0014.02/DOC_1&format=PDF. Accesible en: 1 abr. 2021).

[34] *Declaración conjunta de la sociedad civil: Los Estados deben respetar los derechos humanos al emplear tecnologías de vigilancia digital para combatir la pandemia*, Amnistía Internacional, de 2 de abril de 2020. Disponible en: https://www.amnesty.org/download/Documents/POL3020812020SPANISH.pdf). Sobre esta respuesta global y el pronunciamiento de la ONU, vid. la noticia publicada el 31 de marzo de 2020 sobre "Dimensiones de derechos humanos en la respuesta al COVID-19". Vid. Comunicado de prensa ONU. Disponible en: https://www.hrw.org/es/news/2020/03/31/dimensiones-de-derechos-humanos-en-la-respuesta-al-covid-19).

[35] Así lo dijo también el SEPD en el citado Comunicado del 6 de abril de 2020.

[36] Vid. OMS, "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing", de 28 de mayo de 2020 (Disponible en https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf. Accesible en: 28 mar. 2021).

2.1. El cumplimiento de los principios del tratamiento de datos personales

Toda medida de rastreo debe cumplir con los ya citados principios recogidos en el RGPD para tratar datos personales, partiendo del principio de minimización de los datos y, por ello, no se debería recopilar información que pudiera incluir el estado civil, o, en el caso de las apps, los mensajes, registros de llamadas o los identificadores de dispositivos, siendo recomendable (como han hecho mucho de las apps) el empleo de un sistema de códigos o tokens que, además, vayan cambiando cada cierto tiempo, limitando así el riesgo de la reidentificación; así como siendo recomendable la anonimización de los datos y la utilización de técnicas criptográficas avanzadas que aseguraran los datos almacenados y sus necesarios intercambios.

Pero uno de los principios esenciales a cumplir es el de transparencia e información. Ante el supuesto peligro de caer en un caso de vigilancia ciudadana, la solución es la transparencia, que los ciudadanos confíen en que estamos en un Estado de Derecho en el que los poderes públicos están sometidos a las normas y a la responsabilidad en caso de incumplimiento (HARARI, 2020). Y para cumplir con la transparencia debe informarse de la trazabilidad del tratamiento de datos realizado, especialmente en lo relacionado con su conservación, siendo recomendable borrar los datos personales tratados pasado un mes desde que el usuario se realizara la prueba de autodiagnóstico, o bien después de que la persona hubiera dado negativo en la prueba (dado que se correspondía con el periodo de incubación más el margen) -solo pudiendo ser utilizados posteriormente con fines de investigación, siempre y cuando se adoptaran las correspondientes técnicas de anonimización. Más allá de esta cuestión, una forma de garantizar esta transparencia y la responsabilidad sobre las mismas se puede conseguir, en el caso de las apps de rastreo, empleando algoritmos auditables y revisados periódicamente por expertos independientes, publicando las evaluaciones de impacto, y poniéndose a disposición de todos el código fuente de la aplicación para un examen lo más amplio posible.

Junto a la necesidad de recoger el menor número de datos posible y hacerlo de forma transparente, las medidas de rastreo deben tener una finalidad legítima y las mismas, como hemos visto, la tienen: frenar la pandemia y cortar la transmisión del virus, esto es, proteger la salud pública, el interés vital del sujeto y de terceros y, por lo tanto, proteger un interés público.

Por último, para hacer efectivo el principio de proactividad, el RGPD introduce otros mecanismos como son la responsabilidad desde el diseño y por defecto,[37] lo que implica que desde

[37] Art. 25 RGPD. Vid. también, Vid., del CEPD, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* Disponible en: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es. Accesible en: 28 mar. 2021)

el momento en el que se vaya a diseñar una medida de rastreo de contactos, desde el inicio y por defecto se deben tomar las medidas técnicas y organizativas apropiadas que garanticen la privacidad de los sujetos. A lo que también puede ayudar realizar la correspondiente evaluación de impacto de la medida, también prevista por el RGPD en estos casos.[38] Las medidas de rastreo deben superar dichos procesos.

2.2. La existencia de una base de legitimación para tratar los datos personales

Cualquier injerencia en un derecho fundamental, como lo es evidentemente el uso de una aplicación de seguimiento o rastreo de nuestros contactos o de vigilancia digital, requiere ser legítima, necesaria y proporcionada.

Así las cosas, si buscamos una base legítima que establezca la posibilidad de utilizar estas medidas, más allá del consentimiento en el caso de las apps móviles -que deben descansar en la voluntariedad del sujeto, evitando así todo tipo de efecto discriminador-, entre las bases de legitimación analizadas podríamos considerar, como también ha quedado dicho, que la base que permitiría el tratamiento de estos datos sería la necesaria protección de intereses vitales del titular de los datos o de otra persona física, aunque necesitaríamos tener una norma de referencia que permitiera dicho tratamiento (MARTÍNEZ, 2020).[39]

En esta línea, como hemos visto, el RGPD contiene previsiones que permiten el tratamiento de datos relacionados con la salud -ya sea sobre la base del consentimiento, el interés vital del interesado o terceros, o el interés público por motivos de salud pública.[40]

3. A MODO DE CONCLUSIÓN: LA PROPORCIONALIDAD DE LAS MEDIDAS DE RASTREO DE CONTACTOS

Como hemos visto, tanto a nivel europeo como internacional se exige la necesidad de analizar el derecho fundamental a la protección de datos de forma sistemática y proporcionada, siendo

[38] Art. 35 RGPD; y *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*, adoptadas por el Grupo de Trabajo del artículo 29, el 4 de abril de 2017; revisadas por última vez y adoptadas el 4 de octubre de 2017 (WP 248 rev.01). Disponible en: https://www.aepd.es/es/documento/wp248rev01-es.pdf. Accesible en: 28 mar. 2021.

[39] En el caso español, dicha base normativa la encontraríamos en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública que permite en un contexto de pandemia "adoptar las medidas oportunas para el control de los enfermos"; así como en el RDL 21/2020, sobre (arts. 3 y 27.2) y Orden SND/404/2020 (art. 9), que habilitaron a que la Secretaria de Estado de Digitalización e Inteligencia Artificial (SEDIA) creara una app de rastreo de contactos, la llamada RadarCovid. Dicha app vió la luz en septiembre de 2020, pero sin mucho éxito y rodeada de mucha polémica, ante la escasa participación de la AEPD. Sobre la misma y este tipo de *apps*, vid. ARENAS, 2020, nº 5.

[40] Vid. Considerandos 46 y 54 y arts. 6 y 9 RGPD.

esencial el hecho de que cualquier medida que limite derechos en esta línea sea legal, necesaria y proporcionada, reiterándose la necesidad de que las medidas restrictivas de derechos deben tener una duración limitada y analizar el impacto en los grupos más desfavorecidos.[41]

Debemos analizar la proporcionalidad de dichas herramientas en función del fin legítimo que pretenden conseguir, que no es otro que frenar la expansión de la pandemia detectando a las personas infectadas y aislándolas, siendo, por lo tanto, con carácter general, un interés público el que legitimaría el tratamiento. Asimismo, vemos que el uso de estas medidas tiene una base legítima y que la misma está prevista legalmente. Hay normas que respaldan y justifican su uso (desde el RGPD como, a nivel nacional, en España, la LOPDGDD y las normas sanitarias existentes y la sucesión de reales decretos y órdenes ministeriales que prevén su puesta en marcha).

Por otro lado, ya hemos visto cómo estas medidas de control pueden cumplir sin mayor dificultad con los principios que marca el RGPD en cuanto a minimización de datos, finalidad determinada, plazo de conservación determinado y transparencia en todos sus extremos, garantizando además el anonimato de los sujetos. Así pues, estas medidas parecen útiles.

No obstante, el uso de las medidas de rastreo de contactos se debe abordar no sólo por sus implicaciones, sino también desde el punto de vista de las consecuencias éticas tanto por el método seguido a la hora de tratar datos personales -máxime al ser datos sensibles-, como por los objetivos y resultados previstos y sus posibles efectos discriminatorios. Al ser medidas que, en cierta forma, limitan derechos y suponen una forma de vigilancia ciudadana (especialmente las *apps*) se debería tener en cuenta la posibilidad de un mal uso, adoptándose medidas para evitar que esto se produzca y para proteger no sólo el derecho fundamental a la protección de datos, sino el resto de derechos fundamentales que pudieran verse afectados (MORLEY; COWLS; TADDEO; FLORIDI, 2020, pp. 16-17). No cumplir con valores y principios éticos puede provocar no sólo la lesión de derechos fundamentales, sino la pérdida de la confianza ciudadana en el Gobierno y en su capacidad para gestionar situaciones de crisis, más allá de los efectos directos sobre los ciudadanos afectados (MORLEY; COWLS; TADDEO; FLORIDI, 2020, pp. 1-2).

Por todo ello, en el análisis estricto de la proporcionalidad estos principios éticos deben tenerse en cuenta. Así, ante la cuestión de si estas medidas son necesarias en una sociedad

[41] Citamos aquí los conocidos Principios de Siracusa, adoptados por el Consejo Económico y Social de las Naciones Unidas en 1984, donde se recogen los principios conforme a los cuales los Gobiernos podrán limitar derechos por razones de salud pública o emergencia nacional. Entre los Principios de Siracusa, podemos citar: Imponerse y aplicarse de conformidad con la ley; responder a un objetivo legítimo de interés general; ser estrictamente necesarias en una sociedad democrática para alcanzar su objetivo; ser lo menos intrusivas y restrictivas posible para cumplir su objetivo; basarse en evidencia científica y no aplicarse de manera arbitraria ni discriminatoria; tener una duración limitada, ser respetuosas con la dignidad humana y estar sujetas a revisión. Disponible en: https://www.civilisac.org/civilis/wp-content/uploads/principios-de-siracusa-1.pdf. Accesible el: 28 mar. 2021).

democrática, a la luz de nuestros días, si la injerencia que provocan en nuestra vida privada es proporcional al bien que pretenden conseguir, deberíamos concluir que es innegable que, si cumplen con el RGPD, no hay medidas menos intrusivas que puedan conseguir el mismo fin en una situación extraordinaria de pandemia como en la que nos encontramos. Todos los Estados deberían apostar por estas medidas de rastreo de contactos manuales y, especialmente, automatizadas, pero con las debidas garantías, como hemos explicado, y, además, teniendo en cuenta tomar medidas para evitar efectos discriminatorios.

Pero debemos concluir recordando aquí que su necesidad y proporcionalidad dependerá en gran medida de su eficacia y estas medidas sólo pueden ser eficaces si -como nos han recordado organismos internacionales, europeos y nacionales- van acompañadas de otras medidas por parte de los poderes públicos. Esto es, el rastreo de contactos debe ir acompañado de un sistema de realización de tests, de aislamiento y de control de dicho aislamiento. Y si bien es cierto que hay una parte de responsabilidad personal en todo este proceso, hay cuestiones que deben ser resueltas por los poderes públicos, que deben reforzar sobre todo el sistema sanitario.

Así pues, este tipo de medidas sólo pueden ser eficaces si más allá del cumplimiento normativo, gozan de la confianza ciudadana, que debe descansar en la transparencia de las medidas, esencialmente, en la ausencia de medidas discriminatorias, y en la percepción ciudadana de que existe un aparato estatal capaz de hacer frente a la pandemia. Estamos en un momento democráticamente complicado para los Estados, donde los ciudadanos asisten a un proceso de desafección ciudadana basada esencialmente en la falta de capacidad de nuestros dirigentes para afrontar la pandemia y hacer frente a la crisis sanitaria, educativa, laboral y económica en la que estamos. Concluir que no hay medidas menos lesivas para nuestros derechos y que el rastreo de contactos es proporcional al fin legítimo que persigue sólo será posible si nuestros poderes públicos respetan las normas, las hacen eficaces realmente y no sólo lo aparentan. Quizá, en este caso, la mujer del César no sólo deba parecer ser honrada, sino serlo.

BIBLIOGRAFÍA

ÁLVAREZ CARO, María. XIV. El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas. En: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos.** Madrid: Editorial Reus, 2016, pp. 227-240.

ARENAS RAMIRO, Mónica. Unforgettable: a propósito de la STJUE de 13 de mayo de 2014. En: **Teoría y Realidad Constitucional**, n. 34, 2014, pp. 537-558.

ARENAS RAMIRO, Mónica. El impacto del Reglamento General de Protección de Datos europeo en el tratamiento de los datos personales de los menores de edad. En: GARCÍA MAHAMUT, Rosario; TOMÁS MALLÉN, Beatriz (Eds.). **El Reglamento General de Protección de Datos.** Valencia: Tirant lo Blanch, 2019, pp. 237-264.

ARENAS RAMIRO, Mónica; ORTEGA GIMÉNEZ, Alfonso (Dirs.). **Protección de Datos: c**omentarios a la ley orgánica de protección de datos y garantía de derechos digitales (en relación con el RGPD**)**. Madrid: Sepin, 2019.

ARENAS RAMIRO, Mónica. ¿Testing, Tracing, Isolation? A propósito de las Directrices 04/2020 del Comité Europeo de Protección de Datos. En: **La Ley Privacidad**, n. 4, abril-junio, 2020.
ARENAS RAMIRO, Mónica. ¿Rastrear o no rastrear? He ahí la cuestión. Las apps de rastreo de contactos y la protección de datos personales. En: **La Ley Privacidad**, n. 5, jul.- sept., 2020.

GARCÍA MAHAMUT, Rosario. El derecho fundamental a la protección de datos. El Reglamento (UE) 2016/679 como elemento definidor del contenido esencial del artículo 18.4 de la Constitución. En: **Corts -** Anuario de Derecho Parlamentario, n. extra 31, 2018**,** pp. 59-80.

GARCÍA MAHAMUT, Rosario. Del Reglamento General de Protección de Datos a la LO 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales. En: GARCÍA MAHAMUT, Rosario; TOMÁS MALLÉN, Beatriz. **El Reglamento General de Protección de Datos.** Valencia: Tirant lo Blanch, 2019, pp. 95-131.

HARARI, Yuval Noah. La falta de solidaridad global y de liderazgo representa un peligro inmenso para la humanidad. En: **La Nación,** de 5 de abril de 2020. Disponible en: https://www.lanacion.com.ar/el-mundo/yuval-noah-harari-la-falta-de-solidaridad-global-y-de-liderazgo-representa-un-peligro-inmenso-para-la-humanidad-nid2350906. Accedido el: 28 mar. 2021.

LÓPEZ CALVO, José. **Comentarios al Reglamento Europeo de Protección de Datos**. Madrid: Sepín, 2017.

MARTÍNEZ MARTÍNEZ, Ricard. Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública. En: **Diario La Ley**, n. 9604, 2020.

MORLEY, Jessica; COWLS, Johs; TADDEO, Mariarosaria; FLORIDI, Luciano. Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems. En: **SSNR Electronic Journal**, 1 mayo 2020. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582550. Accedido el: 28 mar. 2021.

PIÑAR MAÑAS, José Luis. La protección de datos durante la crisis del coronavirus. En: **Consejo General de la Abogacía Española**, 20 mar. 2020. Disponible en https://www.abogacia.es/actualidad/opinion-y-analisis/la-proteccion-de-datos-durante-la-crisis-del-coronavirus/. Accedido el: 28 mar. 2021.

RALLO LOMBARTE, Artemi. **El derecho al olvido en Internet.** Madrid: CEPC, 2014.

SIMON CASTELLANO, Pere; BACARIA MARTRUS, Jordi (Coord.). **Funciones del Delegado de Protección de Datos en los distintos sectores de actividad**. Barcelona: Bosch, 2020.

TRONCOSO REIGADA, Antonio. XXVI. Autoridades de control independientes. En: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento general de protección de datos.** Madrid: Editorial Reus, 2016.

AUTORA:
Monica Arenas Ramiro
RESUMO DA BIOGRAFIA:
Licenciada y Doctora en Derecho por la Universidad de Alcalá (1999 y 2005). Profesora de Derecho Constitucional de la Universidad de Alcalá desde 1999, y de diversos Másters y Cursos, y Formadora externa del Ayuntamiento de la Comunidad de Madrid, con un curso de protección de datos galardonado con el Premio Europeo Mejores Prácticas de Administraciones Públicas Europeas (2006). Junto a su labor docente, también participa en un Grupo de Innovación docente y en numerosos Proyectos y Jornadas de innovación; y ha desarrollado numerosas labores de gestión académica como la de Vicedecana de la Facultad de Derecho, o la de Inspectora Adjunta en la Inspección de Servicios. Actualmente es Delegada de Protección de Datos de la Universidad de Alcalá.
E-mail: monica.arenas@uah.es
Orcid: https://orcid.org/0000-0002-9329-2246