CEFD

Cuadernos Electrónicos de Filosofía del Derecho

| ARTÍCULO

Consecuencias de la STC 76/2019, de 22 de mayo en la privacidad y uso de apps para el control de la COVID. El caso de Radar COVID•

Consequences of STC 76/2019, May 22 on privacy and apps to monitorize COVID. The case of Radar COVID

Rafael Rodríguez Prieto
Universidad Pablo de Olavide

Fecha de recepción 31/05/2020 | De aceptación: 29/09/2020 | De publicación: 28/12/2020

RESUMEN.

En este artículo se estudiará las consecuencias que tiene para la dialéctica entre preservación de la privacidad y la oportunidad de aprovechar las posibilidades que la tecnología nos ofrece para el control de epidemias como la del COVID. En la STC 76/2019, de 22 de mayo se establecen una serie de garantías adecuadas para ser tenidas en consideración en el diseño de aplicaciones que control y vigilancia, justificadas por la entidad de la crisis epidemiológica, pero que en ningún caso debieran servir para limitar o restringir derechos constitucionalmente garantizados. Se analizará el caso de Radar COVID.

PALABRAS CLAVE.

privacidad; derechos fundamentales; blockchain; Radar COVID.

ABSTRACT.

This paper focusses on the consequences for the dialectic between preservation of privacy and the opportunity to take advantage of the possibilities that technology offers us to control epidemics such as COVID. STC 76/2019, of May 22 rules a set of accurate guarantees to be taken into consideration in the design of applications that control and surveillance, justified by the entity of the epidemiological crisis, but which in no case should serve to limit or restrict constitutionally guaranteed rights. This paper will analyze the case of Radar COVID.

KEY WORDS.

privacy; basic rights; blockchain; Radar COVID

• Este trabajo es resultado de los proyectos de investigación dirigidos por el Prof. Pablo Antonio Fernández Sánchez de la Universidad de Sevilla, Las Respuestas del Derecho Internacional y Europeo a los Nuevos Riesgos y Amenazas Contra la Seguridad Humana (RASEGUR), Plan Nacional de I+D+I (Ref.: DER2015-65906-P) y de la Red de Excelencia sobre Los actuales desafíos del Derecho Internacional, del Plan Estatal de Investigación Científica y Técnica y de Innovación (DER15-69273-RED).

1. Introducción

La novela de Julio Verne olvidada, *Paris en el siglo XX* nos traslada a un mundo hipertecnificado donde no hay lugar para el humanismo o el arte. El control que se establece es opresivo, conformando una brillante narración disutópica. El arte ha descrito estas amenazas, probablemente con la intencionalidad de que no se lleguen a cumplir. Una metaconciencia que nos advierte de los peligros inherentes al gusto humano de jugar a ser dios.

Periódicamente, aparecen noticias vinculadas a internet que comprometen derechos que considerábamos fuertemente garantizados en nuestras democracias. Casos como la sustracción de datos de tarjetas de crédito o troyanos que se insertan en los ordenadores para espiar a los usuarios, han generado que, en cierta medida, el halo de ingenuidad que cubría internet se vaya lentamente desvaneciendo. Con la irrupción de la pandemia de la COVID[1] se ha vuelto a poner en primer plano la dialéctica entre seguridad y privacidad[2]. A lo largo del mundo, se han introducido aplicaciones para el control de la epidemia. Unas cuentan con un carácter meramente informativo o de autodiagnóstico; otras suministran información sobre los movimientos de las personas[3] y controlan si se ha podido estar expuesto a un posible contagio. A efectos del derecho fundamental a la protección de datos, la primera no tiene consecuencias. La segunda pudiera tenerlas[4]. Su uso se justifica para afrontar un problema de la salud pública. La privacidad

[1] De acuerdo a la Fundéu RAE, la grafía elegida es una de las dos consideradas correctas, v. RAE https://www.fundeu.es/recomendacion/covid-19-mayusculas-minusculas/

[2] Esta dialéctica no es nueva. La protección contra el terrorismo es uno de los primeros ejemplos de la retórica que sitúa la renuncia a derechos individuales como una vía de lograr una mayor seguridad.

[3] Los estudios de movilidad, no son nuevos. En los primeros meses de la pandemia, el Ejecutivo central puso en marcha una app denominada 'Asistencia COVID', para el autodiagnóstico. Esta aplicación se descarga voluntariamente y geolocaliza solo en caso de que se active esta opción. A primeros de abril de 2020, la Secretaría de Estado de Digitalización e Inteligencia Artificial junto con el Instituto Nacional de Estadística (INE) anunció un estudio de movilidad para analizar datos anónimos y agregados de desplazamientos de la población durante el tiempo necesario hasta que se restablezca la normalidad. Este estudio cuenta con ciertas similitudes con uno programado meses antes con el fin de analizar los desplazamientos de los españoles en fechas críticas por el Instituto Nacional de Estadística. En noviembre de 2019 el Instituto Nacional de Estadística (INE) inició un estudio para analizar son los desplazamientos de los españoles utilizando los datos de los teléfonos móviles durante ocho días (cuatro días laborales de noviembre, del 18 al 21; el domingo 24 de noviembre, el festivo del 25 de diciembre, y dos días de verano: el 20 de julio y el 15 de agosto). V. https://www.ine.es/covid/covid_movilidad.htm

[4] Sobre un análisis sistemático de las apps. puestas en marcha para el control de la COVID, LEITH, D., FARRELL, S.; "Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps", https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf y DAVALBHAKTA, S., ADVANI, S., KUMAR, S., et al.; "A

de los datos debería implicar que sean recolectados y procesados de acuerdo a límites[5], aunque el derecho a la protección de los datos personales debe conciliarse con su tratamiento en caso de epidemias, tal y como exige la legislación vigente[6].

Los Estados miembros de la UE buscaron soluciones tecnológicas que posibilitaran el rastreo de contactos y avisaran si se había estado cerca de un infectado[7]. Durante el diseño de estas aplicaciones se generó un intenso debate entre los partidarios de un modelo denominado como 'centralizado', con un servidor central operado por las autoridades sanitarias que calcularía los riesgos e informaría a los usuarios afectados, y un modelo 'descentralizado' en el que cada teléfono almacenaría y procesaría los datos y subiría el código, en caso de ser positivo, a un servidor *backend*. Durante el proceso, Apple y Google se aliaron con el fin de que sus sistemas operativos iOS y Android formarán una plataforma única para el rastreo de la expansión del coronavirus por el mundo. Las compañías mostraron su compromiso con la privacidad y el consentimiento informado de los individuos, al garantizar que el cliente tendría que descargarse la app y, para ello, se precisa del consentimiento del individuo[8]. Una de las condiciones de estas compañías fue el no uso de un sistema centralizado. La incursión de estas megaempresas en el debate sobre el modelo de app produjo una controversia con el Gobierno francés, que fue de los pocos que optó por un sistema centralizado y por tanto sin la tecnología de ambas, y una fuerte discusión en el seno del alemán. Sin embargo, en este último país se optó por modificar el proyecto inicial y adoptar la *Google-Apple Exposure Notification application programming interface*. El 26 de mayo de 2020, Suiza se convirtió en el primer país en que se lazaba una app basada en la tecnología de Google y Apple. Posteriormente, otros Estados diseñaron su app con esta tecnología[9]. Radar COVID la integra, junto con el DP-3T (*Decentralized Privacy-Preserving Proximity Tracing*). Sus impulsores han afirmado que no vulnera la privacidad de las personas, pero una serie de hechos, que posteriormente se estudiarán, generan

Systematic Review of Smartphone Applications Available for Corona Virus Disease 2019 (COVID19) and the Assessment of their Quality Using the Mobile Application Rating Scale (MARS)", *Journal of medical systems*, 44, N.º 9, 2020.

[5] DE LA TORRE RODRÍGUEZ, P.; "Protección de datos: conceptos, objetivos y principios básicos", ELDERECHO.COM, https://elderecho.com/proteccion-de-datos-conceptos-objetivos-y-principios-basicos

[6] Tal y como se establece en considerando 46 del 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 sus datos personales y a la libre circulación de estos datos.

[7] Estas aplicaciones seguirían las recomendaciones de la iniciativa europea PEPP-PT (*Pan-European Privacy-Preserving Proximity Tracing*), menos invasiva que los modelos de Corea del Sur o China.

[8] Un mensaje informaría al dueño del *smartphone* si ha estado en contacto con un infectado.

[9] Para una lista pormenorizada v. Davalbhakta, S.,Advani, S., et al.; "A Systematic Review of Smartphone Applications Available for Corona Virus Disease 2019 (COVID19) and the Assessment of their Quality Using the Mobile Application Rating Scale (MARS)", *Journal of Medical Systems*, tomo 44, 9, 2020.

dudas. A todo ello se debe añadir la reciente investigación sobre Google auspiciada por el Departamento de Justicia de EE.UU. por abuso de posición dominante en el mercado[10].

Se ha de plantear la cuestión de si estas aplicaciones, ya sea mediante bluetooth o por GPS –las más invasivas-, pudieran ser una amenaza a los derechos fundamentales. Los Gobiernos afirman que no hay peligro. De hecho, una lectura de la política de privacidad de Radar COVID parece ser respetuosa con los derechos fundamentales. Apple y Google defienden que su tecnología garantiza la privacidad. Como señala PEREZ LUÑO, "uno de los desafíos más importantes de la época en que vivimos consiste en establecer una ecuación exacta, correspondiente a los apremios del tiempo, en las relaciones entre los avances tecnológicos y la tutela de las libertades"[11]. ¿Pueden el miedo y la crisis generada por la pandemia provocar unas prisas que rebajen estándares respecto a derechos fundamentales? Hay razones para ser cautelosos. Existen demasiados ejemplos de intrusiones ilegítimas de Gobiernos y corporaciones en nuestra privacidad. Uno de los últimos casos, en el ámbito estatal, fue la reforma de la ley de protección de datos, apoyada por todo el arco parlamentario, para que los partidos políticos pudieran enviar propaganda electoral a los ciudadanos en función del rastro que dejan en internet.

También se producen injerencias por parte del sector privado. El último caso conocido ha sido el de asistentes de voz que graban las conversaciones de los usuarios. Como señala MORENO MÚÑOZ, los datos son hoy el propulsor de crecimiento y transformación, como lo fue el petróleo en su momento[12]. Los datos son dinero y, por consiguiente, poder e influencia. Su tratamiento y el uso de algoritmos pudieran generar graves consecuencias en los derechos fundamentales. Los algoritmos no son inocentes y pueden contener sesgos que promuevan la discriminación y la desigualdad, por ejemplo el racismo[13]. Los algoritmos se nutren de datos que presentan realidades personalizadas, como ha señalado BALLESTEROS[14]. De hecho, como afirma COHEN, los algoritmos generan decisiones personalizadas, *ad hoc*, basadas en patrones y no en principios *erga omnes*. No dan razones de las decisiones que se toman, que mutan y no se someten a un escrutinio público, lo que implica una profunda tensión con las

[10] https://www.nytimes.com/2020/10/20/technology/google-antitrust.html
[11] PEREZ LUÑO, A. E.; "Internet y los Derechos Humanos", *Anuario de Derechos Humanos*, 12, 2011, pp. 287-330.
[12] MORENO MUÑOZ, M. "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", *Dilemata*, 24, 2017.
[13] SWEENEY, L.; "Discrimination in Online Ad Delivery", *Communications of the ACM*, 56,5, 2013.
[14] "No se trata ya solo de personalizar por usuario, sino de personalizar según el instante mismo en que la tecnología presenta la realidad deformada", BALLESTEROS, A.; "Tecnología digital:¿realidad aumentada o deformada?", *CEFD*, 42, 2020.

articulaciones tradicionales de las características institucionales, que un compromiso con el Estado de Derecho requiere[15].

En este artículo se analizará la dialéctica entre preservación de la privacidad y la oportunidad de aprovechar las posibilidades que la tecnología nos ofrece para el control de epidemias como la COVID[16]. En concreto, se tomará como referencia la STC 76/2019, de 22 de mayo[17], donde nuestro alto tribunal resolvía un recurso de inconstitucionalidad presentado por el Defensor del Pueblo mediante escrito presentado el 5 de marzo de 2019, contra el apartado 1 del art. 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado a esta por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Esta sentencia es de especial interés para el debate mencionado por dos razones: la primera es que se trata de una reforma que fue respaldada por todos los grupos políticos de nuestro parlamento. Desde una perspectiva política, gozaba por tanto de una enorme legitimidad y unánime consenso. Todos los representantes de los ciudadanos afirmaron que no suponía ningún ataque a la privacidad de los votantes. Pero desde la perspectiva jurídico constitucional y de preservación de los derechos fundamentales, verdadera espina dorsal de nuestra democracia, la norma fue recurrida por el Defensor por razones más que suficientes, gracias también a la movilización de parte de la sociedad civil. Finalmente, el Tribunal Constitucional dio la razón al recurrente, lo que debería hacernos desconfiar de nuestros representantes. En segundo lugar, la sentencia establece una serie de garantías que pueden ser muy útiles para ser tenidas en cuenta en un momento en el que se diseñan aplicaciones que control y vigilancia, justificadas por la entidad de la crisis epidemiológica, pero que en ningún caso debieran servir para limitar o restringir tácita o explícitamente el contenido esencial de derechos constitucionalmente garantizados. En Radar COVID, interviene el sector privado, en concreto, la compañía Alphabet, dueña de Google, con un controvertido historial en lo que respecta al derecho a la privacidad de las personas, lo que también debería hacernos desconfiar de las grandes empresas de internet. Se analizará la app Radar COVID (donde se combina el sector público con el privado) sobre la base del principio de confianza y

[15] COHEN, J.; "Internet Utopianism and the Practical Inevitability of Law", *Duke Law & Technology Review*, 18, 2019, pp. 85-96.
[16] Como señala PÉREZ LUÑO, la seguridad de los datos, frente a su posible manipulación o destrucción, implica que la seguridad jurídica se sitúe como un concepto clave de los sistemas informáticos y una garantía del propio derecho. V. PÉREZ LUÑO, A. E.; *La seguridad jurídica*, Barcelona, Ariel, 1994, p. 10.
[17] Esta STC es además una fuente sistemática y ordenada de jurisprudencia sobre la relación entre derechos fundamentales y privacidad, cuyas referencias han fortalecido jurisprudencialmente este trabajo.

la no renuncia ni expresa ni tácita de derechos fundamentales y se establecerán una serie de propuestas para la preservación del equilibrio entre mejoras tecnológicas y garantía de la privacidad.

2. La STC 76/2019, de 22 mayo. Contenido esencial

2.1. Contexto regulatorio y delimitación del derecho a la privacidad

Las nuevas tecnologías han tenido unos beneficios evidentes en muchas áreas de la vida social. No obstante, hay elementos que generan inquietud y que se aprecian con mayor claridad a medida que nos relacionamos más con estas tecnologías y se eleva la tecnificación de las mismas. La aprobación del Reglamento de Protección de Datos por la UE (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 sus datos personales y a la libre circulación de estos datos -en adelante RGPD- trató de responder a este desafío[18]. Con la irrupción de internet el derecho a la intimidad se convierte en uno de los más vulnerados, como señala BELLOSO, junto con otros principios constitucionales similares lo que dificulta el control de nuestros datos personales[19]. Así, como afirma SANCHO, la obtención de información personal se facilita gracias a la tecnología, así como "la fragmentación legislativa o incluso la desregulación, lo que da rienda suelta al *mercadeo* de datos personales sin demasiados problemas"[20]. En este sentido, habría que realizar una breve aclaración y delimitación de índole conceptual sobre datos personales e intimidad.

Tal y como señalan ARELLANO y OCHOA, las diversas tradiciones jurídicas tienen un peso importante en este debate. La tradición jurídica continental ha reservado una fuerte protección a la intimidad. En EE.UU. se ha usado el concepto de privacidad vinculado a la información personal como un valor constitutivo de la identidad individual[21], que se ha ido desarrollando a lo largo del tiempo, gracias al precedente judicial, "incorporando principios como la inviolabilidad del domicilio, la correspondencia o, más recientemente, las telecomunicaciones"[22]. MARTÍNEZ DE PISÓN entiende la composición de la

[18] Su aplicación fue de carácter obligatorio desde el 25 de mayo de 2018, aunque, no hubo una norma española hasta la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
[19] BELLOSO MARTÍN, N.; "La protección de los derechos fundamentales en la era digital: su proyección en la propiedad intelectual", *CEFD*, 18, 2009.
[20] SANCHO LÓPEZ, M.; "Internet, Big data y nuevas tecnologías: repercusiones y respuestas del ordenamiento jurídico", *CEFD*, 39, 2019.
[21] ARELLANO TOLEDO, W., OCHOA VILLICAÑA, A. M.; "Derechos de privacidad e información en la sociedad de la información y en el entorno TIC", *Rev. IUS*, 7, 31, 2013.
[22] SALGADO SEGUIN, V.; "Intimidad, privacidad y honor en Internet, *Telos: Cuadernos de comunicación e innovación*, 85, 2010, pp. 69-79.

intimidad ligada a las diferentes esferas a partir de las cuales el individuo manifiesta sus intereses personales y la voluntad de estructurar su vida[23]. Tal y como señala SALGADO, "la privacidad sería así una nueva esfera, mucho más amplia que la de la propia intimidad, que contendría ni más ni menos que todos los datos vinculados a un individuo, sean éstos sensibles o no, los cuales deben ser controlados y protegidos en su tenencia y tratamiento por parte de terceros"[24]. Tanto el propio art. 18.4 de la C.E. como la propia jurisprudencia del Tribunal Constitucional la definieron como un derecho fundamental autónomo[25]. El RGPD contempló una serie de principios entre los que destaca el de minimización de datos, cuyo objetivo es que los datos de carácter personal que se colecten deban ser los adecuados, pertinentes y limitados al propósito para los que son tratados. Este principio obliga a aplicar las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento (art. 25.2); se trata de una consideración clave para el procesamiento que hagan de nuestros datos las apps de control epidemiológico[26].

En este contexto regulatorio, el proyecto de ley de Protección de Datos y Garantías de Derechos Digitales, modificó la Ley Orgánica del Régimen Electoral General[27] por una enmienda presentada por el PSOE y respaldada por todos los grupos, que permitía a los partidos políticos, coaliciones y agrupaciones electorales utilizar datos personales obtenidos en webs y otras fuentes de acceso público con fines de comunicación política durante el período electoral. Una de las cuestiones más controvertidas, junto con la indefinición de términos como 'interés público' o 'garantías adecuadas',[28] fue que no hacía falta el

[23] MARTÍNEZ DE PISÓN desarrolla la célebre fórmula de WARREN y BRANDEIS, *the right to be alone*. El derecho a la intimidad es concebido como el derecho a estar sólo. "Warren y Brandeis lograron un rápido éxito con su propuesta de reconocimiento de un derecho a la *privacy,* recogido prontamente por los tribunales americanos y después por la Declaración Universal de Derechos Humanos". MARTÍNEZ DE PISÓN, J.; "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional", *AFD*, XXXII, 2016, pp. 409-430.

[24] Id.

[25] Un derecho que implica tanto la intimidad personal, como el resultado del proceso tecnológico en la protección de los datos personales de los individuos.

[26] El RGPD amplió el deber de informar al usuario en torno a la base legal para el tratamiento de los datos, su periodo de conservación, la posibilidad de reclamar y los derechos con los que cuenta. Otros elementos reseñables para nuestro objeto de estudio serían tanto la necesaria obtención del consentimiento expreso para el tratamiento de datos, como la comunicación de los fallos de seguridad a la autoridad de protección de datos durante las 72 horas posteriores al incidente y a la persona interesada, si es que existe un riesgo para ella (posteriormente, se tratarán las brechas de seguridad de Radar COVID). Se establece la figura del Delegado de Protección de Datos, cuyo objetivo es la coordinación y control del cumplimiento de la normativa sobre protección de datos en la empresa.

[27] La parte más criticada fue el apartado primero: "1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas."

[28] Ya HART hablaba de la textura abierta del derecho para referirse a cierto grado de abstracción de la norma. Como señala MARTÍNEZ STAY, siempre existe un cierto grado aceptable de indeterminación en el derecho, pero en asuntos que impliquen derechos y libertades fundamentales se debe ser cuidadoso, especialmente para garantizar cierta previsibilidad y la seguridad jurídica de la ciudadanía,

consentimiento expreso de los ciudadanos para que los partidos políticos usaran los datos[29]. Algunos juristas y asociaciones consideraron que esta reforma recordaba a *Cambridge Analytica*[30]. La razón es que el derecho a la participación política en los asuntos públicos que garantiza el art. 23 CE, se encontraría conectada con libertad ideológica en la medida que, tal y como señaló el Defensor del Pueblo en el recurso planteado "esta libertad difícilmente puede darse en un entorno tecnológico en el que las modernas técnicas de análisis de la conducta sobre la base del tratamiento masivo de datos y la inteligencia artificial permiten procedimientos complejos orientados a modificar, forzar o desviar la voluntad de los electores y sin que estos sean conscientes de ello" (…) por lo que "la inconcreción del art. 58 bis.1 LOREG respecto de los límites precisos en los que los partidos políticos pueden recopilar datos personales relativos a opiniones políticas de los ciudadanos y el uso que puedan darle a esa recopilación genera una afectación negativa de la libertad de sufragio, contraria al art. 23.1 CE". Las actividades de *Cambridge Analytica* se basaron en el uso de los datos procesados para condicionar al electorado. Existen muchas técnicas para manipular las creencias más personales de una persona. Si se pueden identificar los valores mediante algoritmos, se pueden también cambiar también estas creencias[31].

La recopilación de datos personales con fines políticos va al núcleo de lo que entendemos por privacidad. Son datos personales especialmente sensibles. De hecho, las presuntas intervenciones de *hackers* en elecciones o referenda han generado honda preocupación porque erosionan la legitimación del sistema

MARTÍNEZ STAY, J. I.; "Los conceptos jurídicos indeterminados en el lenguaje constitucional", *Revista de Derecho Político*, 105, 2019, pp. 161-196.

[29] Un grupo de abogados y organizaciones, entre las que destaca la Plataforma para la Libertad de Información (http://libertadinformacion.cc/la-pdli-considera-escandaloso-el-acuerdo-de-todos-los-partidos-para-legalizar-el-spam-electoral-y-la-realizacion-de-perfiles-ideologicos/) redactó un formulario para que la ciudadanía pudiera solicitar el acceso a los datos personales que se encontraran en las bases de datos de los partidos políticos. "En el supuesto de que dichos datos se encuentren almacenados en una base de datos de perfiles ideológicos" se solicitaba expresamente "la eliminación de dicha base de datos por ser manifiestamente ilícita". V. https://confilegal.com/20181207-expertos-en-privacidad-crean-un-formulario-para-que-los-partidos-no-creen-bases-de-datos-con-opiniones-de-los-ciudadanos/?utm_medium=social&utm_source=twitter&utm_campaign=shareweb&utm_content=footer&utm_origin=footer Además, estas personas y colectivos establecieron una lista a la que denominaron "Viernes", con el fin de que los ciudadanos puedan manifestar su oposición al envío de propaganda electoral a los correos electrónicos y teléfonos que se facilitaran. El 25 de febrero de 2019 presentaron un escrito ante el Defensor del Pueblo para que interpusiera un recurso de inconstitucionalidad contra la reforma de la Ley Orgánica del Régimen Electoral General (LOREG). El recurso interpuesto por el Defensor del Pueblo impugnó dicha modificación normativa por lo que respecta a su apartado 1 del art. 58 bis, por considerar que vulnera diversos preceptos constitucionales, en concreto los arts. 9.3, 16, 18.4, 23 y 53.1 CE. Por su parte, el abogado del Estado solicitó la desestimación integra del recurso.

[30] *Cambridge Analytica* se fundó 2013 gracias al mecenas del Partido Republicano Robert Mercer, quien invirtió 15 millones de dólares con la finalidad de que se desarrollara una herramienta para identificar potenciales votantes e influir en sus decisiones. V. HINDMAN, M.; *The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy*, Princeton, Princeton University Press, 2018.

[31] SMIT, A.; *Identity Reboot: Reimagining Data Privacy for the 21st Century*, London, MintBit, 2020, p. 32.

gracias a procesos electorales. En mayo de 2020, se publicaba que los servicios de información españoles investigaban campañas de manipulación extranjeras en las elecciones de 2019[32].

2.2. El pronunciamiento del Tribunal Constitucional

El 22 de mayo de 2019 fue resuelto el recurso presentado por el Defensor del Pueblo. El Alto tribunal consideró que el asunto se centraba en dirimir si el legislador había cumplido con los requisitos constitucionales en el caso del apartado 1 del art. 58 bis LOREG, que constituye una injerencia en el derecho fundamental a la protección de datos personales garantizado por el art. 18.4 CE[33]. La disposición legal recurrida permitía que los partidos políticos recopilasen datos personales relativos a las opiniones políticas dentro de sus actividades electorales. En el recurso de inconstitucionalidad se señaló también una posible infracción de derechos fundamentales sustantivos, vinculados a la libertad ideológica (art. 16 CE), de participación política (art. 23 CE) y el principio general de seguridad jurídica (art. 9.3 CE). El TC solo entró a dirimir si se habían producido tres vulneraciones del art. 18.4 CE en conexión con el art. 53.1 CE, de carácter autónomo e independiente entre sí y vinculadas a la insuficiencia de la ley, "redundando las tres en la infracción del mandato de preservación del contenido esencial del derecho fundamental que impone el art. 53.1 CE". Para el TC la norma legal impugnada adolece de una grave vaguedad o indeterminación que representa una amenaza para los ciudadanos cuyos datos personales son recopilados y procesados. El hecho de que exista una clara indeterminación de la finalidad del tratamiento y no se establezcan de forma precisa "*garantías adecuadas* o las *mínimas exigibles a la Ley* constituyen en sí mismas injerencias en el derecho fundamental de gravedad similar a la que causaría una intromisión directa en su contenido nuclear"[34]. El TC señaló que existiría una vulneración del contenido esencial de principios reconocidos tanto por la legislación supranacional -el Reglamento Europeo- como por la legislación española de protección de datos. La norma objeto del recurso incluye una remisión a dos textos normativos - RGPD y la LOPDGDD- "sin reglas claras y precisas". Ambas carecen de garantías

[32] ARALUCE, G.; "Los servicios de información investigan campañas de manipulación extranjeras en las elecciones de 2019", *Voz Populi*, 02/05/2020 en https://www.vozpopuli.com/espana/elecciones-injerencia-extranjera_0_1360364293.html

[33] El TC señala que su jurisprudencia sobre el derecho fundamental a la protección de datos personales, y en concreto el pronunciamiento específico sobre las garantías adecuadas que a este respecto se contiene en la STC 292/2000, de 30 de noviembre.

[34] En este sentido, la STC de referencia señala que "la disposición legal recurrida no haya determinado por sí misma la finalidad del tratamiento de datos personales que revelen opiniones políticas, más allá de la genérica mención al "interés público"; (ii) que no haya limitado el tratamiento regulando pormenorizadamente las restricciones al derecho fundamental; y (iii) que no haya establecido ella misma las garantías adecuadas para proteger los derechos fundamentales afectados".

adecuadas para proteger datos relativos a las opiniones políticas de la ciudadanía, lo que constituiría una grave indefensión y una intromisión ilegítima en la esfera privada de la persona.

Esta insuficiencia legal no puede garantizarse por el concurso de órganos como la Agencia de Protección de Datos, cuyo papel a lo largo del proceso resulta, al menos, cuestionable. El propio TC considera que, aunque con posterioridad a la interposición del recurso del Defensor del Pueblo, la Agencia Española de Protección de Datos aprobara la Circular 1/2019, de 7 de marzo con el fin de abordar ese vacío, "no puede subsanar la insuficiencia constitucional de la que adolece el art. 58 bis LOREG". Una de las claves de la STC de referencia es que una interpretación distinta del principio de reserva legal consagrado en la Constitución lo vaciaría de contenido. Esta afirmación constituye un verdadero aviso en temas tan sensibles como la protección de datos y la irrupción de las nuevas tecnologías de la información. De hecho, el propio TC recuerda que el RGPD establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales y no establecen por sí mismas el régimen jurídico aplicable a los tratamientos de datos personales especiales. En su fallo, el TC sostiene que la Ley Orgánica 3/2018 no ha fijado, de acuerdo al art. 53.1 CE, las garantías adecuadas que preserven los derechos fundamentales de los españoles cuando los partidos políticos recopilen sus datos personales relativos a las opiniones políticas. No hay, por tanto, reglas claras y precisas que los protejan.

2.3. Garantías adecuadas y reglas claras y precisas para preservar la privacidad. Consecuencias de la doctrina constitucional

La STC 254/1993, de 20 de julio, afirmó que el uso de la informática se encuentra limitada por el respeto a la intimidad de las personas y el pleno ejercicio de sus derechos. La explotación del rastro de los ciudadanos en la Red podría comprometer el control de la ciudadanía de sus datos, lo que limitaría su libertad ideológica. El propio Alto Tribunal en STC 20/1990 señaló que dicha libertad, por ser esencial para la efectividad de los valores superiores del ordenamiento jurídico no puede limitarse. Solo podría recortarse en razón de medidas que fueran necesarias para el mantenimiento del orden público protegido por la ley. Nos situamos, por tanto, ante el reto de preservar la igualdad de acceso bienes jurídicos básicos de nuestro ordenamiento que como la privacidad requiere de garantías adecuadas y reglas precisas. Sin privacidad no hay libertad ideológica. Ha sido el propio TC el que en su jurisprudencia ha afirmado que el artículo 18.4 CE supone el reconocimiento constitucional del derecho fundamental a la "autodeterminación informativa", entendida como la facultad conferida a sus titulares de disposición y

control de sus datos personales que implica el derecho a conocer los datos que poseen terceros, quiénes los poseen y la finalidad con la que los poseen (STC 292/2000). En este sentido, PERALTA señala el carácter democrático-personalista del ordenamiento constitucional español y la jurisprudencia constitucional, sitúa a los derechos fundamentales en una dimensión tanto subjetiva como objetiva. Así, "la consideración de un derecho fundamental como garantía institucional exige un reforzamiento en su protección jurídica, un debilitamiento de sus limitaciones en orden a garantizar el mayor alcance respecto de su efectividad en el seno del ordenamiento positivo"[35]. Como afirma KLIEMT, la norma de igualdad ha significado dos cosas respecto al orden jurídico del Estado; la primera se identifica con el Estado de Derecho; la segunda era aquella que implicaba que el orden jurídico debía otorgar a los individuos derechos, procurando establecer la igualdad fáctica que posibilitara una participación igual en el goce de bienes sociales[36]. Para apoyar este enfoque, contamos además con alguna jurisprudencia en el ámbito europeo muy significativa[37]. Así pues, no resultaría aventurado afirmar que cualquier intervención ilegítima en la vida de las personas que implique la creación de perfiles de las mismas, afecta a la libertad ideológica y a la participación, ya que se trataría de un límite al libre ejercicio de estos derechos. Tal y como señala SOLER PRESAS, los límites a los derechos fundamentales constitucionalmente reconocidos deben mantenerse independientemente de lo cambiante del medio a través del cual se ejerciten[38].

En cualquier caso, y como elementos básicos de la STC con consecuencias en el tema objeto de este trabajo, se ha de señalar que es necesario que se establezcan garantías adecuadas al bien jurídico a proteger, o de lo contrario se estará facilitando la vulneración de derechos fundamentales, ya que el TC entiende que serían equivalente a una intromisión directa en su contenido esencial. El diseño de una app que ayude al control de una enfermedad no puede constituirse en una amenaza al derecho a la privacidad. El TC ha afirmado que cualquier injerencia estatal en la esfera de los derechos fundamentales y las

[35] PERALTA MARTÍNEZ, R.; "Libertad ideológica y libertad de expresión como garantías institucionales", *Anuario iberoamericano de justicia constitucional*, 16, 2012, pp. 251-283.
[36] KLIEMT, H.; *Filosofía del Estado y criterios de legitimidad*, Barcelona, Alfa, 1983, p. 152.
[37] Es el caso de la Sentencia de la Gran Sala de 8 de abril de 2014, *Digital Rights Ireland*, consecuencia de una petición de decisión prejudicial sobre la interpretación de los artículos 3, 4 y 6 de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006. En esta sentencia se afirmó que la obligación impuesta por los artículos 3 y 6 de la Directiva 2006/24, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones constituye en sí misma una injerencia en los derechos garantizados por el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea. El tribunal estimó que, de acuerdo al artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley y respetar su contenido esencial.
[38] SOLER PRESAS, A.; "Am I in Facebook? Sobre la responsabilidad civil de las redes sociales on-line por la lesión de los derechos de la personalidad, en particular por usos no consentidos de la imagen de un sujeto", *InDret,* 3, 2011.

libertades públicas debe conciliarse con un fin constitucionalmente legítimo o proteger un bien constitucionalmente relevante. En el caso de una app para el control del COVID el fin sería la salvaguarda de la salud pública, cosa que la Constitución no impide, de tal forma que el legislador imponga limitaciones al contenido de los derechos fundamentales o a su ejercicio por protección de otros derechos o bienes constitucionales (STC 104/2000, de 13 de abril). Sin embargo, como también ha señalado el TC en la sentencia de referencia y en su jurisprudencia, tales limitaciones deben ser proporcionadas al fin perseguido con ellas (STC 11/1981). Cualquier injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas precisa una habilitación legal que garantice la seguridad jurídica en el ámbito de los derechos fundamentales implica una "suma de legalidad y certeza del Derecho (STC 27/1981)"[39]. Invocar el conocimiento de las opiniones de los electores, sin la salvaguardas adecuadas o confiando en que los partidos no harán mal uso de los mismos, recuerda a controlar los movimientos de los ciudadanos y los resultados de sus test de COVID, pero sin establecer políticas de privacidad claras y precisas que garanticen adecuadamente su privacidad y donde el software usado sea auditable en su totalidad.

Este es el elemento substantivo que el alto tribunal identifica con el mandato de que existan reglas claras y precisas que establezcan garantías adecuadas cuando están en juego derechos fundamentales como la privacidad. Es precisamente la vaguedad e inexistencia de las mismas las que comprometía gravemente la constitucionalidad de la reforma objeto del recurso del Defensor del Pueblo[40]. De no establecerse este tipo de medidas que garanticen el contenido esencial de estos derechos, las apps para el control de epidemias pueden afectar a la privacidad de las personas.

Es interesante la mención del TC a la doble función de la reserva de ley. Considera que se debe entender como necesaria la intervención de una ley que habilite la injerencia que "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención"[41]. Esta referencia del TC nos debiera compeler a

[39] En la STC de referencia se invoca la STC 292/2000, en la que se enjuició una injerencia legislativa en el derecho a la protección de datos personales, en la que expresamente se rechazó "que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas".

[40] Señala el TC que se remite a dos normas "sin reglas claras y precisas que delimiten efectiva y eficazmente las garantías adecuadas que se consideran aplicables (…) y ninguna de ellas se refiere específicamente a las garantías adecuadas para la protección de la categoría especial de datos que son los relativos a las opiniones políticas de las personas".

[41] En la STC de referencia se citan las SSTC 49/1999, 292/2000 y 49/1999 que apoyan esta exigencia y se afirma que "a la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental."

abrir un debate sobre la reevaluación jurídica de las apps de control sanitario, donde rigen políticas de privacidad que se aceptan a través de unos 'Términos y Condiciones de Uso'. Una pregunta legítima en una sociedad democrática es si resulta adecuado el uso de un contrato de adhesión para una herramienta de control epidemiológico. ¿Se está usando la técnica legislativa adecuada? ¿Se podría entender que hay un troceamiento de la soberanía? ¿No cabría cuestionarse esta ingente cantidad de contratos de adhesión?

En todo caso, de las dudas sobre la regulación de herramientas tecnológicas se infiere la relevancia de la privacidad como sostén del Estado de Derecho y un sistema democrático, donde debiera primar el principio de confianza y la no renuncia de derechos fundamentales. La experiencia indica que los ciudadanos debemos ser cautelosos. El diseño de apps para el control de la pandemia son especialmente sensibles por dos razones: el primer lugar, cuentan con el marchamo o prestigio de venir avaladas por el propio Estado. En segundo lugar, se entiende que por esta razón, cuentan con garantías que evitan una intromisión ilegítima en la privacidad de las personas.

3. El principio de confianza y la "no renuncia" ni expresa ni tácita a derechos fundamentales. La app Radar COVID.

No cabe duda de que es necesario tomarse en serio la libertad ideológica y, por tanto, la privacidad de las personas. La posibilidad de ser objeto de abusos, algunos de los cuales se sustentan en la renuncia a derechos de los usuarios, no es nada excepcional. Al contrario. Existen 'Términos y Condiciones de Uso' que pueden vulnerar derechos personalísimos. Tal vulneración se concreta en la imposición en un contrato de adhesión de cláusulas que implican la renuncia de derechos inalienables. El resultado debería ser la nulidad del acuerdo. Nuestro Código Civil especifica que para que se produzca la renuncia de derechos tiene que ser de manera expresa y taxativa. En consecuencia, no cabe interpretación tácita de la misma (art. 6). En concreto, respecto a la renuncia, por ejemplo, de derechos sucesorios. Así lo ha afirmado el Tribunal Supremo en la STS 25/2005, al declarar "que las renuncias no se presumen; que han de resultar de manifestaciones expresas a tal fin, o de actos o conductas que de modo inequívoco, necesario o indudable lleven a la afirmación de que ha existido una renuncia". La Sala de lo Civil del Tribunal Supremo establece que en la medida que la transmisión *mortis causa* es uno de los negocios jurídicos más determinantes en nuestro ordenamiento debe estar sujeto a una especial protección, cuya

consecuencia es la necesidad de que cualquier renuncia tenga que ser incontrovertida y explícita[42]. Una aceptación acrítica implica alienar los derechos de la personalidad de la parte más débil, y un desamparo manifiesto ante grandes corporaciones que imponen su voluntad en contratos de adhesión. Se han dado casos en que los usuarios han tenido que litigar en una jurisdicción extranjera. Cuestiones semejantes son la pérdida de control sobre contenidos que, originalmente, son de nuestra propiedad, cuando el usuario cuelga una foto o un vídeo en una red social. De hecho, el TC ha afirmado recientemente en un caso de uso de por un tercero de una foto publicada en Facebook que "el ciudadano desconoce la mayor parte de las veces el contenido real y las consecuencias del otorgamiento de la autorización exigida para su registro y utilización, pues resultan de no fácil comprensión para cualquier usuario medio que no disponga de conocimientos jurídicos y tecnológicos (…), difícilmente en este caso puede hablarse de un consentimiento basado en información fiable o confiable" (STC 27/2020).

Como señala LARENZ, el principio de confianza tiene tanto un componente de ética jurídica como otro de seguridad del tráfico que son inseparables. El primero está presente en la buena fe. Suscitar la confianza se encuentra ligado a saber, o deber saber, que otra parte va a confiar. El principio de confianza sobrepasa al de buena fe en la medida de que demanda un respeto recíproco ante todo en aquellas operaciones jurídicas que requieran una continuada colaboración, en general el comportamiento que se puede esperar entre los sujetos que intervienen en el tráfico jurídico[43]. Este principio implicaría que las relaciones en internet vinculadas a cualquier tipo de intercambio de datos deberían estar presididas por este principio ético y de seguridad del tráfico. Los usuarios de aplicaciones, por ejemplo de redes sociales, mantienen a lo largo de años relaciones donde se colabora entre empresa y usuario. Lo mismo sucede con la administración pública. Esta relación precisa de confianza y respeto; este último se gana evitando abusos o incluso compensando adecuadamente a las personas por sus datos. Este principio precisa de una arquitectura adecuada que evite vulneraciones en el derecho a la protección de datos que puedan ser producto de conductas abusivas o negligentes y, por tanto, *contra legem* de empresas y Gobiernos.

Los seguimientos masivos de población o las apps que se han desarrollado para el control de la pandemia de la COVID deberían estar sujetas a ambos parámetros de análisis y escrutinio. Cualquier control de nuestras actividades debe estar tasado y no implicar una renuncia ni expresa ni tácita de nuestros derechos

[42] RODRÍGUEZ, R., MARTÍNEZ, F.; "Herencia digital, términos y condiciones de uso y problemas derivados de la praxis social. Un análisis desde la filosofía del derecho", *Revista internacional de pensamiento político*, 12, 2017, pp. 77-104.
[43] Este principio aparece recogido tanto en el Código Civil alemán (art. 157 y 242) como suizo (art. 2). V. LARENZ, K.; *Derecho justo. Fundamentos de ética jurídica*, Madrid, Civitas, 1985, pp. 95-96.

fundamentales. Medir la temperatura de las personas que, por ejemplo, entran en recintos cerrados, no deja de ser una intromisión en su intimidad que al recabar datos biométricos, debe estar sujeta a un serio escrutinio y sometida al principio de confianza[44]. La carrera por el diseño de aplicaciones para el control de la COVID se desencadenó en todo el mundo a la vez que se extendía el virus.

En relación a este instrumentos se deben señalar una par de cuestiones con carácter previo. La primera es que faltan datos sobre estas aplicaciones a causa de su escaso tiempo de implementación. Algunas como la española, han sido puestas en marcha muy recientemente, lo que ha generado algo de sorpresa por su retraso[45]. La segunda es que podemos distinguir una triple dimensión de estudio de las mismas, que comprendería lo que nos dicen los Gobiernos o empresas sobre las apps, la percepción que tienen los ciudadanos de las mismas y, finalmente, la evaluación crítica de estas herramientas en relación a la privacidad de las personas. Sobre la primera de las perspectivas, los Ejecutivos han recurrido a la excepcionalidad de la situación como justificación para la toma de medidas que pudieran ser cuestionadas. Sobre la falta de garantías y la intromisión ilegítima de empresas de internet en nuestra privacidad existe ya una abultada experiencia. De hecho, los defensores de estas apps para el control de la COVID suelen invocar que la mayoría de las aplicaciones que tenemos en nuestros teléfonos móviles son mucho más intrusivas. Este argumento, siendo correcto, no debería implicar no tomarnos en serio nuestra privacidad; justo al contrario. Los estándares de exigencia se deberían elevar tanto para apps de Gobiernos como de empresas privadas. La segunda implica la percepción del ciudadano corriente sobre la app. Se han realizado investigaciones en ese sentido[46]. Esta percepción es limitada, ya que seguimos sin un debate o deliberación rigurosa sobre internet en nuestras sociedades[47]. La tercera es la que interesa a este trabajo. Se trata de analizar si estas apps pudieran suponer una intromisión ilegítima en la privacidad y, por tanto, vulnerar derechos fundamentales.

[44] Organizaciones de la sociedad civil como Xnet advirtieron de la existencia de problemas de actualización de una parte de la legislación española al RGPD en dos sentidos: falta de adaptación eficaz al principio de minimización de datos y carencias en la conciliación entre la protección de datos personales y la libertad de expresión e información. Para Xnet la Ley 39/2015 incrementó la recogida de datos personales cuya motivación y necesidad es de difícil justificación en el marco del RGPD. V. https://xnet-x.net/identificacion-minimizacion-datos-datosporliebre/

[45] Radar COVID se basa, en parte, en software validado y libre, que ya ha sido desarrollado y está en funcionamiento. Para los expertos ha sido una sorpresa que se haya tardado tanto en su implementación o en la publicación de su código.

[46] KAPTCHUK, G., GOLDSTEIN, D. G., HARGITTAI, E., HOFMAN, J., REDMILES, E. M.; "How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt", *arXiv:2005.04343*, 2020, https://arxiv.org/abs/2005.04343 Se trata de una investigación financiada por Microsoft y en la que participan tanto empleados de la compañía como de las universidades John Hopkins y de Zurich. Se pregunta a 4500 estadounidenses sobre las apps de control de la pandemia y, en concreto sobre si sienten que sus aplicaciones garantizan su privacidad.

[47] Se ha propuesta una asignatura sobre internet que ayude a comprender los riesgos y beneficios de su uso, v. RODRÍGUEZ PRIETO, R.; *Retos jurídico-políticos de Internet*, Madrid, Dykinson, 2019.

Los casos de Corea del Sur, Singapur o China han sido citados como ejemplos de control cibernético de la epidemia. El problema reside en que las aplicaciones de los tres países, en diferentes grados, son muy intrusivas en la esfera personal de los ciudadanos. De hecho, merece la pena recordar que China es una dictadura que cuenta con un 'programas de puntos' para sus habitantes, en función de su adhesión al régimen y Corea del Sur es un Estado basado en un nacionalismo etnicista que restringe derechos fundamentales. Los Estados europeos se han dividido entre aquellos que han optado por el *software* ofrecido por Apple y Google –caso de Italia o Alemania- y aquellos que han optado por soluciones propias –el caso de Francia. Como se señaló en la introducción, Apple y Google ofrecieron su colaboración, siempre que el modelo fuera 'descentralizado', frente a un enfoque 'centralizado', cuyo servidor quedaría bajo la supervisión de las autoridades sanitarias. Aún es pronto para un análisis solvente de estas decisiones. Podemos analizar los argumentos de uno y otro lado para esta decisión. Los indicios que tenemos nos deberían mover a la cautela y la precaución. Los casos de abusos de Gobiernos y corporaciones privadas no son extraños y deben estar sujetos a un estricto control jurisdiccional[48]. Cabe incluso señalar la existencia de una soterrada batalla entre Gobiernos y la iniciativa de Apple-Google, de la que han resultado victoriosos estos últimos. Esta cuestión plantea preguntas sobre el papel de las grandes empresas de internet en determinar la forma en que los Estados hacen frente a una crisis sanitaria o de cualquier otro tipo[49].

El primer grupo de Estados sostiene que el modelo escogido permite un mayor respeto a la privacidad de los individuos. Consideran que el almacenamiento de todos los datos en un único servidor es un riesgo para la privacidad de los ciudadanos. La tecnología ofrecida por Google y Apple, permite una mayor protección de la privacidad al ser un modelo descentralizado donde los datos están encriptados, anonimizados y no accesibles por terceros. Además, se usa un protocolo en código abierto denominado DP-3T, desarrollado de manera independiente por un equipo interdisciplinar. La aplicación no realiza los cálculos por sí mismos, sino que utiliza el sistema creado por Google y Apple, que incorporó este protocolo en su API. Este modelo calcula, de acuerdo a la información emitida por los distintos dispositivos móviles encontrados y en función de los contactos, el nivel de riesgo del usuario. El sistema

[48] Los usuarios de Facebook recibieron un mensaje en las últimas elecciones animándoles a compartir 'que habían ido a votar'. La explicación era que el sistema geolocalizaba al usuario y si había pasado por delante de un colegio electoral enviaba el mensaje. Esa actividad supone una intromisión ilegítima en la privacidad de las personas, que desgraciadamente no tuvo trascendencia judicial.
[49] De hecho, la revista POLITICO publicó en mayo un artículo en el que usó el término militar "outflanked" para describir esta batalla por el uso del software de estas megaempresas en las apps del COVID. V. https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/

se basa en la conectividad Bluetooth. Cada usuario comunique a la app que ha dado positivo y el resto de usuarios recibirán la información de forma anónima. En suma, con la arquitectura descentralizada es el teléfono el que extrae los datos y realiza todas las coincidencias de contactos y análisis de riesgos.

El segundo grupo considera que es peligroso incluir a compañías privadas en una cuestión de políticas públicas y más en caso de una pandemia. Aunque Android pudiera ser en parte *open source*[50] -aunque esta afirmación sostenida por algunos expertos es muy discutible- y pudiera usarse sin interactuar con Google (especialmente, por las restricciones que impuso el Gobierno chino), pero lo que está fuera de toda discusión es que *Google Play Services* no es software libre[51]. El sistema usa también bluetooth. En caso de dar positivo en un test de COVID, el usuario escanea un código QR. La app alertará a otros usuarios del peligro al que han estado expuestos. Se garantiza que los datos serán anonimizados y se borraran posteriormente. Los defensores del enfoque centralizado argumentan que este método permite a los funcionarios de salud identificar redes de contactos y superdifusores o puntos críticos[52].

En ambos modelos la cuestión de los datos, su minimización, anonimización y privacidad son elementos centrales. Se debe, por tanto, analizar su relación con la privacidad. Con ese fin, se analizará la herramienta tecnológica por la que ha optado nuestro país, en el marco de una arquitectura descentralizada.

3.1. Radar COVID.

La app española pertenece al primero de los grupos y cuenta con las características generales ya referidas. Entre el 29 de junio y el 31 de julio se realizó una prueba en la Gomera en el que se pretendía analizar la viabilidad de una app para el control de la COVID. Después de que Radar COVID fuera aprobada por las autoridades sanitarias, el Gobierno la puso a disposición de las Comunidades Autónomas. Además, planificó su interoperatividad con el resto de apps implantadas en los principales países europeos que

[50] Android aprovecha Linux y su código fuente en las versiones 1 y 2 fue liberado por Google, aunque es insuficiente para que sea considerado software libre y además algunas de las aplicaciones que generalmente vienen con Android son software privativo. V. https://www.theguardian.com/technology/2011/sep/19/android-free-software-stallman

[51] *Google Play Services* es una *closed-source proprietary app* que suministra analíticas, anuncios, localización, etc.

[52] V. SKOLL, D., MILLER, J. C., SAXON, L. A.; "COVID-19 Testing and Infection Surveillance: Is a Combined Digital Contact Tracing and Mass Testing Solution Feasible in the United States?", Cardiovascular Digital Health Journal, pre-proof available October 2, 2020, https://www.sciencedirect.com/science/article/pii/S2666693620300360 Este artículo contiene gráficos de gran claridad y muy didácticos sobre ambas arquitecturas.

funcionan con la API de Google y Apple y DP-3T[53]. La app fue desarrollada por Indra[54] para la Secretaria de Estado para la Digitalización y la Inteligencia Artificial.

El 9 de septiembre se hizo publicó su código fuente, tan solo 6 días antes de que estuviera disponible para todo el territorio nacional. Sin embargo, la versión que se colgó en GitHub no era la misma que los españoles llevaban en su móvil. Uno de las primeras controversias generadas por Radar COVID fue el uso de un software de Google denominado Firebase. Como señala Pérez Colomé, "se habían dejado en el código presuntamente limpio de GitHub una referencia a Firebase que delataba su uso. Empero con un análisis de la propia aplicación, podía comprobarse que seguía enviándole información"[55]. Firebase[56] es un software de Google que no se mencionaba en su política de privacidad y que implicaba una vulneración del deber de declarar la presencia de código externo, de acuerdo a la legislación vigente. La Secretaría de Estado de Inteligencia Artificial, admitió su uso en la fase de prueba. Pero lo cierto es que la actualización de la app en la que desaparecía no se realizó hasta bien entrado septiembre para Apple (primero) y Android (posteriormente). Pero esta controversia no sería la última.

El 22 de octubre de 2020, la sección de tecnología del diario *El País* publicaba que la app Radar COVID había tenido una brecha de seguridad desde su lanzamiento. El problema afectaba a la confirmación del positivo de usuarios de la app. El código que dan las autoridades de cada comunidad autónoma a los positivos, se inserta en la app que enviará a un servidor las claves que ha compartido en los últimos días cuando ha estado cerca de otros usuarios. Esas claves permitirán al resto de usuarios comprobar si han estado cerca del nuevo positivo. Este tráfico está cifrado y el contenido de la comunicación es anónimo, pero si existe una subida de datos al servidor se infiere que el usuario es positivo, lo que implica que si

[53] DP-3T está en código abierto, lo que significa que cualquiera puede estudiarla y detectar errores o incorporarla a una app. Existe una salvaguarda: aquellos que usen este código deben también liberar el código de la app que se beneficie del mismo. Es importante también señalar que Google y Apple no abrirán su código con el fin de comprobar si en realidad están obrando de acuerdo a los compromisos que han expresado en relación a la privacidad. Lo lógica sería que tuvieran una auditoría independiente que confirmara su respeto a la privacidad de las personas.

[54] Hasta el 11 de agosto a las 15:37 no fue publicado el contrato con Indra en la plataforma de contratación del sector público. Tomado de https://www.newtral.es/radar-covid-app-rastreo-espana/20200810/

[55] PÉREZ COLOMÉ, J.; "La app Radar COVID no advierte de todos los riesgos para la privacidad de sus usuarios", https://elpais.com/tecnologia/2020-09-17/la-app-radar-covid-no-advierte-de-todos-los-riesgos-para-la-privacidad-de-sus-usuarios.html Cuando se publicó la nueva versión para el ecosistema de Apple, desarrolladores externos advirtieron de que no funcionaba. Se había subido una versión de prueba vinculada a servidores ficticios. Posteriormente, fue corregida.

[56] Este software permite compilar datos sobre el uso de la app que englobarían tanto el modelo de teléfono que la descarga como el tiempo de uso. Podría tener sentido en la fase de prueba. Como señala Douglas Leith, "Google es una organización con ánimo de lucro cuyo negocio es usar datos para anuncios personalizados, lo que levanta preocupaciones obvias. Además, en móviles Android, el uso de Firebase habilita *Google Play Services*, que comparten información con Google (email, número de teléfono, número de SIM) y hace que un móvil envíe mensajes frecuentes a servidores de Google". Compartir datos con sensibles con una gran empresa privada como Google no es la mejor forma de preservar la privacidad de los usuarios. Citado en https://elpais.com/tecnologia/2020-09-17/la-app-radar-covid-no-advierte-de-todos-los-riesgos-para-la-privacidad-de-sus-usuarios.html

alguien tiene acceso al tráfico puede conocer quién ha dado positivo. El *quid* de la cuestión es que el software usado para subir los datos pertenece a Amazon, lo que tiene como consecuencia que esta empresa pueda saber quién es positivo. Una compañía que está bajo vigilancia de la UE por praxis que comprometen precisamente la privacidad[57]. Pero aun es peor: cualquiera con la opción de entrar a la misma red wifi desde la que se envían las claves podría haber tenido acceso a esos datos[58].

Según el Gobierno, el problema fue subsanado el 9 de octubre. Sin embargo, como señala PÉREZ COLOMÉ, aunque la Secretaria de Estado de Inteligencia Artificial explicara que no se había comunicado al público en general, porque esa posible vulnerabilidad tenía un alcance muy limitado, "dado que solo podría ser explotada por el operador de comunicaciones", la posibilidad de acceder a esos datos tan sumamente sensibles "no implica que se haya explotado, aunque en realidad no se sabe. No hay pruebas de que la brecha haya sido aprovechada, pero existía y, como tal, debía ser reparada"[59].

Durante el proceso los desarrolladores independientes reclamaron participar para ayudar. Sin embargo, el Gobierno no se lo permitió. De hecho, en un documento firmado por importantes académicos se reclamaba textualmente que "Radar COVID precisa de la cooperación de toda la sociedad, lo que la convierte en una aplicación de carácter masivo y de alto impacto social. Democratizar no solo implica permitir a la ciudadanía el acceso a la infraestructura, sino la cocreación de dichas infraestructuras junto a la sociedad"[60]. Al haberse financiado con fondos públicos debería está sujeta tanto a escrutinio público, como a posibles mejoras. En el caso de Radar COVID ha faltado además información sobre su proceso de desarrollo. Estos problemas pueden o no afectar a la privacidad de la app, pero genera un malestar que no es positivo en ningún caso para la confianza.

3.2. Radar COVID en cuestión.

[57] La Comisión Europea tiene dos investigaciones abiertas contra Amazon: por aprovechar en beneficio propio los datos confidenciales de los minoristas que venden en su plataforma y por la forma en que la compañía elige al ganador de la Buy Box, Además, la Comisión Europea obligó a Amazon en 2017 a devolver 250 millones de euros a Luxemburgo por haberse beneficiado de un pacto fiscal que le permitió eximir del fisco el 75% de sus ganancias en Europa entre mayo de 2006 y junio de 2014, https://elpais.com/economia/2020-11-10/bruselas-mantiene-el-pulso-asi-esta-la-batalla-de-la-ue-contra-los-gigantes-tecnologicos.html

[58] PÉREZ COLOMÉ, J.; "La app Radar COVID ha tenido una brecha de seguridad desde su lanzamiento", https://elpais.com/tecnologia/2020-10-22/la-app-radar-covid-ha-tenido-una-brecha-de-seguridad-desde-su-lanzamiento.html

[59] Id. La Agencia Española de Protección comunicó que había recibido la comunicación de la vulnerabilidad en la semana del 5 de octubre, de acuerdo a la legislación vigente. La Secretaría de Estado afirmó que "la vulnerabilidad no se hizo pública porque no ha habido constancia de una violación de la seguridad de los datos personales, tal como recoge el artículo 33 del Reglamento".

[60] https://transparenciagov2020.github.io/

El grupo de más de cien académicos españoles[61] que firmaron el manifiesto para exigir más transparencia a la aplicación Radar COVID entendían que la publicación del código de la aplicación era un signo de democratización de las infraestructuras digitales del Estado. Lamentablemente, no se publicó su código fuente con el histórico de la aplicación y el progreso completo, habiendo incluso partes del código que diferían entre la versión GitHub y la de Android[62].

El texto suscrito por los investigadores reclamó un repositorio con el código que permitiera analizar todos los elementos del sistema incluyendo el historial desde el inicio del desarrollo, aportando detalles sobre los posibles cambios de versión, y un informe del diseño del sistema con los detalles que han llevado a decidir los parámetros de configuración y uso de las API. También plantearon la necesidad de un informe de los mecanismos propios de monitorización para asegurar el cumplimiento de la normativa de protección de datos. Uno de los aspectos más interesantes del documento es la petición de una evaluación de impacto en la protección de datos basada en el informe del diseño y en los análisis de riesgos. Desde la perspectiva de los expertos, nos encontramos ante la posibilidad de concretar los principios de privacidad basada en el diseño y otros presentes en el RGPD, como el de responsabilidad proactiva, pero "sin un procedimiento abierto que posibilite la implicación de toda la comunidad y de los destinatarios de la app, esta no gozará de la confianza necesaria para su adopción masiva"[63].

Si bien, existen elementos que minimizan las posibles vulneraciones de la privacidad como la utilización del Bluetooth, el accidentado *iter* de Radar COVID puede resultar sospechoso y además debía regir el célebre principio de *public money, public code*[64]. No cabe duda de que existen indicios que pueden generar cierta preocupación[65]. Como señala PÉREZ LUÑO, internet ha abierto posibilidades nuevas y

[61] Entre los firmantes se encontraban Ricardo Baeza-Yates, miembro del Consejo Nacional de la Inteligencia Artificial del Gobierno; Miguel Luengo-Oroz, jefe de datos de Global Pulse de Naciones Unidas o Carme Torras, profesora en el Instituto de Robótica del CSIC y también miembro del Consejo Nacional de Inteligencia Artificial, v. https://www.computerworld.es/tendencias/un-centenar-de-expertos-espanoles-exige-mas-transparencia-a-radar-covid

[62] https://www.xatakandroid.com/analisis/radar-covid-analisis-a-fondo-su-codigo-como-funciona-que-esta-bien-que-esta-mal-que-falta Como señala esta revista, existe "un listado de *endpoints* más extenso en la versión de *Google Play*, servicios internos que no existen en el código de GitHub y código detectado no presente en la versión de GitHub. Respecto a los *endpoints*, son aquellas URLs a las que la aplicación realiza llamadas para interactuar con el servidor. Por otro lado, hay detalles curiosos, como que la versión para Android utiliza código para detectar root (el cual está bastante obsoleto al basarse en el antiguo SuperSU y no en Magisk). Dicho código no se encuentra en la versión subida a GitHub."

[63] https://transparenciagov2020.github.io/ De hecho, carecemos de datos completos y fiables sobre su uso o sobre los errores que ha dado la app y que también han generado desconfianza en el usuario sobre su eficacia.

[64] https://github.com/hjacobs/public-money-public-code

[65] La legislación vigente exige evaluaciones de datos cuando haya alto riesgo para los derechos y libertades de las personas Se requiere consultar a la Agencia Española de Protección de Datos (AEPD), en caso de no poder limitar los riesgos. Otro elemento que ha producido preocupación ha sido que en la versión para dispositivos Android se requiere la activación por defecto la función GPS. La explicación técnica es que la tecnología *Bluetooth Scanning* del sistema operativo de Google, usada por Radar COVID, necesita localización activa para rastrear por Bluetooth, v. https://www.xatakandroid.com/analisis/radar-covid-analisis-a-fondo-su-codigo-como-funciona-que-esta-bien-

preocupantes para los sistemas de control social y político, que permiten a Gobiernos y multinacionales una monitorización sin precedentes de la ciudadanía[66]. Un datismo, que de acuerdo a BYUNG-CHUL HAN, conduce a un control total sobre lo que somos y seremos[67]. Una de las manifestaciones más evidentes de este nuevo tipo de control que facilita la Red la encontraríamos en la "conectividad"[68]. Esta radical conectividad, que incluso genera problemas psicológicos[69], y exposición a la posibilidad constante de una injerencia en nuestra privacidad debe ser tratada jurídicamente como una cuestión vinculada a los derechos fundamentales y, por tanto, sobre la que se deben expresar todo tipo de prevenciones y garantías[70]. Como se ha señalado, estas cautelas deben pasar por la satisfacción de dos parámetros básicos: el principio de confianza y la no renuncia a Derechos fundamentales.

En el caso de Radar COVID existen dos elementos que, al menos deberían generar una razonable dosis de prevención. No encontramos con elementos sustantivos de la app que permanecen ocultos, sobre los que los expertos no pueden opinar ni auditar. La participación de empresas privadas que, al mismo tiempo, se encuentran incursas en graves acusaciones de abuso de posición dominante[71] o de invasión de la privacidad de los individuos[72], hace que, como mínimo, se deba ser cauteloso, ante una app en la que la ciudadanía deposita su confianza porque sus responsables políticos les dicen que puede ayudar a controlar una pandemia que está costando miles de vidas y la ruina económica de amplios sectores. Una de las acusaciones que se hacían a las apps de arquitectura centralizada era que los datos quedaban en un

---

que-esta-mal-que-falta Google y Apple afirman que han desarrollado salvaguardas que garantizan que las apps de los Gobiernos basadas en *Exposure Notifications System* no podrán inferir la localización del usuario, lo que implicaría que aunque el servicio tenga que activarse no significa que la app lo use.

[66] PEREZ LUÑO, A. E.; "Internet y los Derechos Humanos", *Anuario de Derechos Humanos*, 12. 2011.

[67] HAN, B. C.; *Psicopolítica: Neoliberalismo y nuevas técnicas de poder*, Barcelona, Herder, 2014, p. 88. Los escritos de ANDREW KEEN o de BYUNG-CHUL HAN, entre otros, cuestionan esta obsesión por el dato frente al conocimiento. KEEN, A.; *The Internet Is Not The Answer*, London, Atlantic Books, 2015, p. 218. KEEN señala que las grandes empresas de internet tiene como único fin crear valor para sus fundadores y accionistas. Se diferencian de las otras en que éstas emplean a menor cantidad de gente, disfrutan de márgenes de beneficio mayores y son además menos controlados por los gobiernos que sus predecesoras.

[68] Sería la ideología que marca la obsesión por estar conectado en todo momento a Internet, que incluiría además un deber de estar siempre disponible, lo que implica tanto una mayor producción de datos como de exposición de nuestras esferas de intimidad. Así BOLTANSKI y CHIAPELLO estiman que el capitalismo contemporáneo ha conseguido dotar de prestigio a una disponibilidad que diluye las fronteras entre el tiempo privado y profesional o el del trabajo y el del consumo; v. BOLTANSKI, L., CHIAPELLO, E.; *El nuevo espíritu del capitalismo*, Madrid, Akal, 2002.

[69] Como señala RENDUELES, todo ello se desarrolla en un marco donde tanto la sentimentalización de relaciones mercantiles y la gestión gerencial de emociones personales y familiares hacen de los afectos un elemento más de la lógica neoclásica y la psicología positiva. En nuestro mundo, la democratización emocional ha allanado el camino para la subordinación gerencial y terapéutica. V. RENDUELES, C.; "La gobernanza emocional en el capitalismo avanzado. Entre el nihilismo emotivista y el neocomunitarismo adaptativo". *Revista de Estudios Sociales*, 62, 2017, 82 y ss.

[70] Por ejemplo, la previsión del considerando 56 del Reglamento Europeo 2016/679/UE.

[71] Google ha sido acusada de haber dejado de ser un buscador para convertirse en un repositorio donde coloca sus productos y servicios y marginar los resultados, en función de si la empresa les pertenece o les paga. Su actividad se desarrolla en un régimen de monopolio en España (99'09% en teléfonos móviles).

[72] En septiembre de 2019, Google fue multada con 170 millones de dólares por las acusaciones de la Comisión Federal de Comercio y la fiscal general de Nueva York por violar la Ley de Protección de la Privacidad Infantil en Internet (COPPA).

servidor centralizado bajo el control del Gobierno. Pero en el modelo descentralizado hay que hacer un acto de fe y creer a dos corporaciones transnacionales. ¿Cuál puede ser el mal menor? ¿Dos grandes empresas tecnológicas o un Gobierno democrático? No es admisible que se ponga a la ciudadanía ante una disyuntiva así. La erosión del principio de confianza se encuentra relacionada con la renuncia expresa o implícita de derechos fundamentales. Esta renuncia se está naturalizando de forma creciente en internet, al presentarse contratos de adhesión sobre los que la ciudadanía puede actuar de forma limitada. La legislación europea y española reciente ha mejorado una situación que está aún lejos de ser la ideal, particularmente porque los controles sobre el respeto a las cláusulas de privacidad son muy laxos. Sin embargo, poco a poco la jurisprudencia constitucional parece tomar conciencia de los peligros de la Red para los derechos fundamentales y establecer garantías más exigentes.

Como señala FLORES ANARTE, el TC apuesta en su jurisprudencia más reciente por la solución más garantista desde la perspectiva de la protección jurídica del usuario de una red social[73]. En consecuencia, es preciso establecer controles más sólidos y rigurosos. Como afirman LEITH y FARRELL, la actual situación en la que Google y Apple son guardianes de la Red y cuenta con una gran influencia en el comportamiento de estas apps no es deseable. Se debiera imponer un nivel similar de escrutinio sobre todos los que intervienen en una app que puede comprometer la privacidad de las personas[74]. Así como el TC afirmaba que la mera referencia a interés público' o 'garantías adecuadas' sin reglas claras y precisas que protegieran el derecho fundamental a la protección de datos personales, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales, podemos entender que la referencia a una política de privacidad donde ni tan siquiera se cita una API que no está sometida a escrutinio público, no es una garantía suficiente. De hecho, una de las reclamaciones de los expertos consiste en "la evaluación de impacto en la protección de datos basada en el informe de diseño y los análisis de riesgo asociados a la aplicación y su uso en las plataformas Android y iOS"[75]. Lógico.

[73] FLORES ANARTE, L.; "Facebook y el derecho a la propia imagen: reflexiones en torno a la STC 27/2020, de 24 de febrero", *Estudios de Deusto*, vol. 68, 1, 2020. Se refiere al caso de la publicación de una imagen en una red social y su posterior uso. No puede interpretarse como consentimiento para su reproducción por terceros a los efectos del art. 2.2 LO 1/82, aunque el grado de privacidad establecido en el perfil permita el acceso público a la imagen y el usuario acepte cláusulas que autoricen tal cesión.
[74] LEITH, D., FARRELL, S.; "Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps", https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf
[75] Además reclamaron al Gobierno tanto un "informe de diseño del sistema (aplicación y servidores), detallando los análisis que han llevado a decidir los parámetros de configuración y uso de la API de Exposición de Notificaciones de Google y Apple, los mecanismos implementados y las librerías y servicios utilizados para evaluar la seguridad y privacidad de los datos, así como la evaluación de la inclusión y accesibilidad del diseño".

En el plano jurídico-político, los organismos públicos, deberían optar por un software que pueda ser auditado en su integridad y que se encuentre sujeto a mejoras. La intervención de entes privados debiera quedar limitada al grado de compromiso que tengan con la transparencia. Entendemos que abrir el código puede colisionar con su modelo de negocio, pero en ese caso no debería avalarse su participación en herramientas que pueden potencialmente afectar a derechos fundamentales. Todo ello ligado a una deliberación pública sobre el internet que queremos y al papel que sus diferentes actores deben jugar. Como hemos señalado el Prof. MARTÍNEZ CABEZUDO y yo, el establecimiento de una ingente cantidad de contratos de adhesión puede implicar un menoscabo estructural de la ciudadanía y los derechos y libertades públicas que acompañan a esta. Una fragmentación jurídica que bloquea el desarrollo de una normativa rigurosa y *erga omnes* que garantice de una forma ordenada y sistemática los derechos fundamentales de los ciudadanos.

En el plano técnico se han de adoptar soluciones validables, auditables y potencialmente respetuosas con los derechos fundamentales. Las aplicaciones vinculadas al *blockchain* puede ser una salida para el dilema entre privacidad y el uso de aplicaciones tecnológicas que nos permitan mejorar el control de pandemias como la provocada por el virus SARS-CoV-2. No se trata de la panacea, pero su filosofía puede ser de ayuda para afrontar con garantías este tremendo desafío. Blockchain es la plataforma que usan criptomonedas o bitcoins por razón de su "inmutabilidad, trazabilidad, descentralización, transparencia y veracidad de los datos en ella contenidos"[76]. Hay razones de índole técnica y otras de carácter *ius* filósofico. En lo referido a las tecnológicas, el uso de la tecnología del *blockchain* permitiría establecer mecanismos de control sobre la enfermedad sin necesidad de ceder datos personales. Las identidades cuentan con una serie de atributos. Tal y como señala el experto ANTONIO SOTOMAYOR, con el uso del *blockchain* podemos pedir a entidades que conozcan nuestra identidad que generen una credencial verificable que el usuario pueda descargar en el teléfono móvil con el fin de utilizar esos datos en cualquier otro contexto sin revelar la verdadera identidad, la identidad completa. De esta manera sería el usuario el que controlaría los datos personales que expone. Se puede generar una identidad diferente para cualquier relación o conjunto de atributos. Se trataría de una identidad descentralizada, lo que

[76] MUÑOZ CASQUERO, I. "Blockchain vs COVID 19", https://www.elsaltodiario.com/1984/blockchain-vs-covid19-una-realidad-y-una-solucion#comentarios La utilidad de esta tecnología alcanza tanto a entidades financieras, instituciones públicas en diversos países, multinacionales, firmas legales u ONGs. La Unión Europea está desarrollando el European Blockchain Services Infrastructure (EBSI). Para Muñoz Casquero, "la tecnología blockchain tiene una serie de características técnicas que le confieren una veracidad y fiabilidad total sin necesidad de que exista un tercero de confianza que gestione y supervise dichos datos". Tanto la imposibilidad de modificar los datos en ella contenidos, como la trazabilidad y fiabilidad del registro son características que hacen muy atractiva a esta tecnología.

implica que en vez de que todas las características de una identidad estén centralizadas en un solo lugar (por ejemplo la cuenta de Facebook, que progresivamente se van nutriendo de más datos sobre el usuario), son las organizaciones o empresas que ceden credenciales verificables sobre la identidad para que el usuario las use como considere conveniente[77]. Actualmente, existen dos proyectos que usan esta tecnología para el control de la COVID. El primero es HashLog; desarrollado por la empresa Acoer, ayuda a los investigadores y particulares a comprender la propagación del coronavirus y sus tendencias mediante imágenes que se presentan en el tablero HashLog de Acoer, incluyendo datos en tiempo real[78]. La segunda es MiPasa, cuyo fin es reforzar y garantizar la información global y el correcto seguimiento de la pandemia, mediante el uso de fuentes fiables y contrastadas a las que se les respeta su privacidad[79]. De una perspectiva meramente técnica, las posibilidades de esta tecnología pareen ajustarse a las necesidades que impone la pandemia de la COVID. De hecho, recientemente se han publicado trabajos que refuerzan esta idea[80]. ¿Qué se puede decir desde la óptica de los derechos fundamentales?

El uso de blockchain para gestión de datos personales puede suponer un verdadero cambio en la forma en que nos relacionamos con internet. Uno de los problemas que existen en la actualidad, y que generan más controversia desde la perspectiva jurídica, es la gestión y control de los datos personales. Elementos destacados de la legislación vigente como el consentimiento o la privacidad son resueltos por blockchain con una elevada solvencia. La introducción de esta tecnología podría reemplazar el uso de los *passwords*, si el usuario cuenta con identidades digitales encriptadas[81]. De esta forma, el ciudadano gestionaría su información *on line*, lo que supone un relevante avance en el plano tecnológico. En los tiempos de la Odisea, las manchas o cicatrices eran la forma más habitual de determinación de la identidad de una persona[82]. En la modernidad, la mayoría de los marcos de determinación de la identidad se sustentaron en la existencia de una autoridad central que controla el procesamiento de todas las identidades y que representa un punto crítico, ya que alguien que quiera sustraer o manipular datos de los usuarios puede

[77] SOTOMAYOR, A.; "¿Como es la Identidad Descentralizada en APPs contra COVID-19?", *Blockchain Economía*, https://www.blockchaineconomia.es/como-es-la-identidad-descentralizada-en-apps-contra-covid-19/ Es interesante ver su vídeo explicativo sobre el uso de la tecnología blockchain para preservar la identidad que se encuentra en https://www.youtube.com/watch?v=t9ONc6Hoq4I&feature=youtu.be

[78] WOLFSON, R.; "La tecnología DLT se vuelve viral a medida que el seguimiento en tiempo real del coronavirus se extiende a la Blockchain", en https://es.cointelegraph.com/news/dlt-goes-viral-as-live-coronavirus-tracking-spreads-to-the-blockchain

[79] SÁNCHEZ, A., "La tecnología blockchain hace frente al COVID-19", Blog Cuatrecasas, https://blog.cuatrecasas.com/propiedad-intelectual/tecnologia-blockchain-hace-frente-al-covid-19/

[80] MARBOUH, D., ABBASI, T., MAASMI, F. et al.; "Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System", *Arabian Journal for Science and Engineering*, 2020.

[81] RIDGWAY Y JOSEPH BAMBARA. "Data privacy amid coronavirus: Blockchain to the rescue!" https://www.withersworldwide.com/en-gb/insight/data-privacy-amid-covid-19-blockchain-to-the-rescue

[82] ABOUT, I., DENIS, V.; *Historia de la identificación de las personas*, Madrid, Ariel, 2011, p. 38.

actuar contra ese nodo centralizado[83]. Las posibilidades de los dispositivos actuales, junto con el avance del software tanto positivo, como malicioso, requerirían que se garantizara a los usuarios la propiedad de los datos que sus dispositivos generan y, por tanto, sería necesario un sistema descentralizado y eficiente que garantizara tanto el negocio como el aspecto regulatorio[84]. El resultado sería que existiría una red *peer to peer* donde los nodos se intercambian, direcciones, bloques y transacciones con el resto de la Red[85]. Las cadenas de bloques usan seudónimos y algoritmos de cifrado para garantizar la privacidad.

Estas previsiones tecnológicas podrían encajar con un enfoque centrado tanto en el principio de confianza como en la no renuncia tácita o expresa a derechos fundamentales. Aplicar la precaución en nuestras relaciones virtuales y establecer mecanismos tasados de garantía de respeto a la privacidad de las personas no solo podría mejorar estatus como ciudadanos, sino que además permitirían un mejor conocimiento de la Red y una concienciación de nuestros derechos y de nuestras responsabilidades. No obstante, hay cuestiones que jurídicamente deben resolverse.

Desde la perspectiva de algunos expertos, existiría una colisión con la legislación vigente de protección de datos en lo que respecta a identificar al responsable del tratamiento, la conservación limitada de los datos o el derecho al olvido. El primero podría colisionar con la propia esencia de *blockchain*, por su carácter descentralizado. Al tratarse de un protocolo no existe un responsable del tratamiento a menos que se considere a todo internet como responsable, lo que conculcaría la legislación vigente. No obstante, como ha recordado MARCELINO TAMARGO, la CNIL (*Commission nationale de l'informatique et des libertés*) autoridad francesa de protección de datos personales - la primera en pronunciarse sobre blockchain y la normativa europea- afirma que "podrán ser responsables del tratamiento todos aquellos que introduzcan datos personales en la cadena de bloques, siempre y cuando, quien los introduzca sea una persona física o jurídica y el tratamiento de datos personales esté relacionado con una actividad profesional o comercial"[86].

[83] SGHAIER, A., BASIR, O.; "Capability-Based Non-Fungible Tokens Approach for a Descentralized AAA framework in IoT", in Reza M. Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, *Blockchain Cybersecurity, Trust and Privacy*, Springer, Cham, 2020, p. 9.

[84] VOSHMGIR señala que el uso de las apps y P2P aumentan día a día, mientras la amenazas también por lo que los tokens criptográficos pueden significar una revolución semejante a cuando Tim Berner introdujo un nuevo estándar que permitió crear páginas web con unas pocas líneas de código y moverse por Internet con links en vez de usar command line interfaces, VOSHMGIR, S.; *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*, BlockchainHub Berlin, 2019, p. 15.

[85] BUCHANAN, W. J.; *Cryptography*, River Publishers Series in Information Science and Technology, 2017, p. 309.

[86] TAMARGO, M.; "Conflicto entre la tecnología blockchain y la normativa de protección de datos", https://www.economistjurist.es/noticias-juridicas/conflicto-entre-la-tecnologia-blockchain-y-la-normativa-de-proteccion-de-datos/ La CNIL finaliza el informe "advirtiendo de la necesidad de una regulación más específica de la normativa a nivel europeo para facilitar el tratamiento de datos personales en la blockchain. Y que los derechos de los interesados se cumplan". Como apuntan varios expertos, una vía de solución podría ser operar en una red Blockchain privada.

En cuanto a los derechos de rectificación y el derecho al olvido, se ha de señalar que la inmutabilidad de los datos de blockchain -los datos ingresados no son borrables ni rectificables- es otra de sus características distintivas. En este caso, de acuerdo a ASSUMPTA ZORRAQUINO Y ALEJANDRA MATAS, existiría la posibilidad de "aplicar procesos de anonimización irreversibles, de modo que el dato sea tan inaccesible que pudiera equivaler a la supresión del mismo" [87]. ZORRAQUINO Y MATAS también aportan una solución a la rectificación, "dada la inmutabilidad de los bloques, la atención del derecho ejercitado comportará la introducción de un nuevo registro que modifique el anterior. Así, el último registro que incluye los datos más actualizados anularía la información del anterior, siendo el último el válido"[88]. El propio derecho al olvido tiene límites que han sido establecidos en la una sentencia del Tribunal de Justicia de la UE (C-507/17,) de 24 de septiembre de 2019[89].

En suma, se debe concluir que el uso de Blockchain puede ser conciliable con la normativa vigente[90], si esta tecnología se configura atendiendo a los requisitos que se establecen, que además debieran ser revisados en periodos de tiempo razonables, con el fin de adaptarla tanto a las necesidades que se presenten, como al fortalecimiento de los derechos fundamentales.

4. Reflexiones finales

Guadalinex fue un sistema operativo - distribución de Linux- libre y sin costo frente a otros softwares privativos como Windows de Microsoft. A su alrededor se estableció una comunidad de personas capaz de mejorarlo y resolver los problemas gratuitamente. Su última versión salió en 2014. A partir de ahí, el proyecto quedó olvidado por la administración autonómica andaluza del PSOE-IULV-CA[91] y, posteriormente no fue retomado por la del PP- Cs[92]. En 2020 su web oficial fue cerrada. Guadalinex en

[87] Ambas expertas consideran que suprimir la clave secreta del hash- un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija- tendría como consecuencia que no se pudieran conocer los datos que había dentro del hash. V. ZORRAQUINO, A., MATAS, A.; "Blockchain y la protección de los datos personales", https://www.expansion.com/especiales/pwc/2019/07/03/5d1c9db9e5fdeafd318b45ab.html

[88] Id. Otro de los elementos en que se detienen en su análisis es en la automatización de blockchain. La configuración actual de los *smart contracts* contravendría la legislación vigente (art. 22 RGPD), pero no sería difícil adaptarlos con el fin de que cumplan con la exigencia de intervención humana.

[89] Esta sentencia abolía de facto el derecho al olvido, ya que este queda restringido al ámbito de la UE, lo que hace que incluso dentro de la UE se pueda acceder a la información restringida a través del uso de redes privadas virtuales (VPN).

[90] Para compañías como Grant Thornton la función hash y canales privados con datos cifrados serían la solución para conciliar blockchain con la legislación vigente. V. https://www.grantthornton.es/globalassets/1.-member-firms/spain/folletos/rgpd-y-blockchain-final.pdf

[91] En la segunda administración correspondiente al PSOE no participó IULV-CA.

[92] https://usandoguadalinexedu.wordpress.com/2018/09/24/quien-mato-a-guadalinex-el-fracaso-de-susana-y-ciudadanos-con-el-software-libre-andaluz-y-como-cargarte-al-cga-con-tu-carne-socialista-sin-ser-siquiera-funcionario/ En un post se señala que "aunque en un principio el desarrollo de Guadalinex V10 parece haber concluido en el repositorio de GitHub, nada ni nadie informa sobre ninguna evolución a corto y medio-largo plazo." V. https://usandoguadalinexedu.wordpress.com/2018/06/21/la-muerte-de-guadalinex-se-acerca-con-la-llegada-de-gecos-v4/

su versión ciudadana dejo de existir. Se había perdido una nueva oportunidad de abrir al conocimiento común infraestructuras públicas claves.

Una de los argumentos que se han dado para aceptar el software de Google y Apple ha sido su experiencia y capacidad. Algunos comentarios van incluso a asegurar que no hay otra salida. De ser cierto, los Estados, sus funcionarios y su capacidad de acción medida en sus presupuestos, e incluso sus alianzas estratégicas, no significarían nada al lado de una gran corporación. No hay razones para pensar que, al menos de momento, sea así. No solo los Gobiernos cuentan con personal muy formado y cuantiosos recursos, sin que también existen herramientas informáticas y multitud de desarrolladores independientes de la sociedad civil capacitados para afrontar estos retos. Una vez más, se trata de voluntad política y de que estos asuntos sean parte de una deliberación pública y democrática.

Google y Apple son conocidos en organismos regulatorios por prácticas que no son muy sostenibles desde la perspectiva de la competencia en el mercado y los derechos de los ciudadanos. El cuidado y la precaución no están de más en apps, que como Radar COVID, cuentan con una participación de estas empresas. La enorme sensibilidad de los datos y cierta fe en que se va a cumplir lo que se promete, debería generar prevención.

La STC estudiada nos alerta sobre la banalización de los riesgos de permitir vías que incursionen en nuestra privacidad de forma ilegítima. Nos sitúa frente a la necesidad de reivindicar tanto una regulación exigente como una técnica legislativa que no fragmente y no trocee nuestra soberanía. Las apps no pueden convertirse en un vehículo para la violación de derechos fundamentales. El principio de confianza y la no renuncia de derechos fundamentales han de ser parámetros con los que se evalúen las herramientas tecnológicas en relación a la privacidad.

La desigualdad y la correlativa erosión de los valores que conforman el modelo liberal de democracia han generado una crisis, cuyos síntomas más evidentes son el crecimiento del populismo y la degradación institucional. Internet parece haberla acelerado y agudizado en ciertos aspectos, gracias al control de los datos, la vigilancia y el poder desmesurado de gigantes empresariales. Procesos como el *brexit* o populismos como el de Bolsonaro o Trump y el desarrollo de los nacionalismos regionales en Europa y en España denotan un problema que, en buena parte, proviene de la articulación de políticas neoliberales que han incrementado los conflictos sociales. Internet nos puede ayudar a resolver este grave desafío, pero siempre acompañado de mayor democracia tanto política como económica, que pasa por un reforzamiento de nuestras instituciones y de la educación cívica.

Bibliografía

Todas las páginas web accedidas el 13/11/2020.

ABOUT, I., Denis, V.; *Historia de la identificación de las personas*, Ariel, Madrid, 2011.

ARALUCE, G.; "Los servicios de información investigan campañas de manipulación extranjeras en las elecciones de 2019", *Voz Populi*, 02/05/2020 en https://www.vozpopuli.com/espana/elecciones-injerencia-extranjera_0_1360364293.html

ARELLANO TOLEDO, W., OCHOA VILLICAÑA, A. M.; "Derechos de privacidad e información en la sociedad de la información y en el entorno TIC", *Rev. IUS* vol.7 no.31 Puebla ene./jun. 2013.

BALLESTEROS, A.; "Tecnología digital: ¿realidad aumentada o deformada?", *CEFD*, 42, 2020.

BELLOSO MARTÍN, N.; "La protección de los derechos fundamentales en la era digital: su proyección en la propiedad intelectual", *CEFD*,18, Junio 2009.

BOLTANSKI, L., CHIAPELLO, E.; *El nuevo espíritu del capitalismo*, Madrid, Akal, 2002.

BUCHANAN, W. J.; *Cryptography*, River Publishers Series in Information Science and Technology, 2017.

Chance & Necessity, https://chanceandnecessity.net/2017/01/01/people-who-tell-computers-what-to-do-and-people-who-are-told-by-computers-what-to-do/

COHEN, J.; "Internet Utopianism and the Practical Inevitability of Law", *Duke Law & Technology Review*, 18, 2019, pp. 85-96.

DE LA TORRE RODRÍGUEZ, P.; "Protección de datos: conceptos, objetivos y principios básicos", ELDERECHO.COM, https://elderecho.com/proteccion-de-datos-conceptos-objetivos-y-principios-basicos

FLORES ANARTE, L.; "Facebook y el derecho a la propia imagen: reflexiones en torno a la STC 27/2020, de 24 de febrero", *Estudios de Deusto*, vol. 68, 1, 2020.

HAN, B. C.; *Psicopolítica: Neoliberalismo y nuevas técnicas de poder*, Barcelona, Herder, 2014.

HINDMAN, M.; *The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy*, Princeton, Princeton University Press, 2018.

http://libertadinformacion.cc/el-recurso-del-defensor-del-pueblo-contra-la-nueva-ley-de-proteccion-de-datos-confirma-el-atropello-que-representa-esta-norma-para-los-derechos-fundamentales/;

http://libertadinformacion.cc/la-pdli-considera-escandaloso-el-acuerdo-de-todos-los-partidos-para-legalizar-el-spam-electoral-y-la-realizacion-de-perfiles-ideologicos/

https://elpais.com/tecnologia/2019/02/01/actualidad/1549027026_079052.html https://medium.com/@Arianee_Espanol/el-%C3%BAltimo-hackeo-de-facebook-significa-que-ya-es-hora-de-abandonar-el-almacenamiento-de-datos-6f1d56a4afd0

https://www.nytimes.com/2020/02/20/technology/new-mexico-google-lawsuit.html

KEEN, A.; *The Internet Is Not The Answer*, Atlantic Books, London, 2015.

KLIEMT, H.; *Filosofía del Estado y criterios de legitimidad*, Barcelona, Alfa, 1983.

LA ROSA, F.; "Blockchain y bases de datos descentralizadas: ¿son la misma cosa?", Criptonoticias, https://www.criptonoticias.com/tecnologia/blockchain-y-bases-de-datos-descentralizadas-son-la-misma-cosa/

LARENZ, K.; *Derecho justo. Fundamentos de ética jurídica*, Madrid, Civitas, 1985.

LEITH, D., FARRELL, S.; "Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps", https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf

MARTÍNEZ DE PISÓN, J.; "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional", *AFD*, XXXII, 2016.

MARTÍNEZ STAY, J. I.; "Los conceptos jurídicos indeterminados en el lenguaje constitucional", *Revista de Derecho Político*, 105, 2019, pp. 161-196.

MARBOUH, D., ABBASI, T., MAASMI, F. et al.; "Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System", *Arabian Journal for Science and Engineering*, 2020.

MORENO MUÑOZ, M. "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", *Dilemata*, 24, 2017.

MUÑOZ CASQUERO, I. "Blockchain vs COVID 19", https://www.elsaltodiario.com/1984/blockchain-vs-covid19-una-realidad-y-una-solucion#comentarios

PERALTA MARTÍNEZ, R.; "Libertad ideológica y libertad de expresión como garantías institucionales", *Anuario iberoamericano de justicia constitucional*,16, 2012, pp. 251-283.

PÉREZ COLOMÉ, J.; "La app Radar COVID ha tenido una brecha de seguridad desde su lanzamiento", https://elpais.com/tecnologia/2020-10-22/la-app-radar-covid-ha-tenido-una-brecha-de-seguridad-desde-su-lanzamiento.html

PÉREZ COLOMÉ, J.; "La app Radar COVID no advierte de todos los riesgos para la privacidad de sus usuarios", https://elpais.com/tecnologia/2020-09-17/la-app-radar-covid-no-advierte-de-todos-los-riesgos-para-la-privacidad-de-sus-usuarios.html

PEREZ LUÑO, A. E.; "Internet y los Derechos Humanos", *Anuario de Derechos Humanos*, 12. 2011, pp. 287-330.

PÉREZ LUÑO, A. E.; *La seguridad jurídica*, Barcelona, Ariel, 1994.

RENDUELES, C.; "La gobernanza emocional en el capitalismo avanzado. Entre el nihilismo emotivista y el neocomunitarismo adaptativo". *Revista de Estudios Sociales* 62, 2017, pp. 82-88.

RIDGWAY, M., BAMBARA, J.; *Data privacy amid coronavirus: Blockchain to the rescue!* https://www.withersworldwide.com/en-gb/insight/data-privacy-amid-covid-19-blockchain-to-the-rescue

RODRÍGUEZ, R., MARTÍNEZ, F.; "Herencia digital, términos y condiciones de uso y problemas derivados de la praxis social. Un análisis desde la filosofía del derecho", *Revista internacional de pensamiento político*,12, 2017, pp. 77-104.

RODRÍGUEZ PRIETO, R.; *Retos jurídico-políticos de internet*, Madrid, Dykinson, 2019.

SALGADO SEGUIN, V.; "Intimidad, privacidad y honor en Internet", *Telos*: *Cuadernos de comunicación e innovación*, 85, 2010, pp. 69-79.

SÁNCHEZ, A., La tecnología blockchain hace frente al COVID-19, Blog Cuatrecasas, https://blog.cuatrecasas.com/propiedad-intelectual/tecnologia-blockchain-hace-frente-al-covid-19/

SANCHO LÓPEZ, M.; "Internet, Big data y nuevas tecnologías: repercusiones y respuestas del ordenamiento jurídico", *CEFD*, 39, 2019.

SGHAIER OMAR, A., BASIR, O.; "Capability-Based Non-Fungible Tokens Approach for a Descentralized AAA framework in IoT", in Reza M. Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, *Blockchain Cybersecurity*, Trust and Privacy, Springer, Cham, 2020.

SMIT, A.; *Identity Reboot: Reimagining Data Privacy for the 21st Century*, London, MintBit, 2020.

SOTOMAYOR, A.; "¿Como es la Identidad Descentralizada en APPs contra COVID-19?", *Blockchain Economía, https://www.blockchaineconomia.es/como-es-la-identidad-descentralizada-en-apps*-contra-covid-19/

SWEENEY, L.; "Discrimination in Online Ad Delivery", *Communications of the ACM*, 56,5, 2013, pp. 44-54.

V. SKOLL, D., MILLER, J. C., SAXON, L. A.; "COVID-19 Testing and Infection Surveillance: Is a Combined Digital Contact Tracing and Mass Testing Solution Feasible in the United States?", *Cardiovascular Digital Health Journal*, pre-proof available October 2, 2020, https://www.sciencedirect.com/science/article/pii/S2666693620300360

TAMARGO, M.; "Conflicto entre la tecnología blockchain y la normativa de protección de datos", https://www.economistjurist.es/noticias-juridicas/conflicto-entre-la-tecnologia-blockchain-y-la-normativa-de-proteccion-de-datos/

VOSHMGIR, S.; *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*, BlockchainHub Berlin, 2019.

WOLFSON, R.; La tecnología DLT se vuelve viral a medida que el seguimiento en tiempo real del coronavirus se extiende a la Blockchain https://es.cointelegraph.com/news/dlt-goes-viral-as-live-coronavirus-tracking-spreads-to-the-blockchain

ZORRAQUINO, A., MATAS, A.; "Blockchain y la protección de los datos personales", https://www.expansion.com/especiales/pwc/2019/07/03/5d1c9db9e5fdeafd318b45ab.html