Revista catalana de dret públic

#especial

www.rcdp.cat

LA PANDEMIA Y EL DERECHO A LA INTIMIDAD*

Miguel Revenga**

Resumen

La lucha contra el virus de la COVID-19 ha sometido al sistema constitucional a importantes tensiones y mutaciones. En particular, el derecho a la intimidad y a la protección de los datos de salud se ha visto cuestionado por el uso de tecnologías dirigidas a hacer frente a la pandemia de manera eficaz. En el artículo se repasan algunos de los principales problemas que se han planteado al respecto, prestando particular atención a las aplicaciones de rastreo de contactos.

Palabras clave: pandemia; derecho a la intimidad; derecho a la salud; tecnología; rastreo de contactos.

THE PANDEMIC AND THE RIGHT TO PRIVACY

Abstract

The fight against the COVID-19 virus has subjected the constitutional system to significant tensions and mutations. In particular, the right to privacy and the protection of health data have been questioned by the use of technologies aimed at effectively dealing with the pandemic. The article reviews some of the main issues that have arisen in this regard, paying particular attention to contact tracing apps.

Key words: pandemic; privacy; right to health; technologies; contact tracing.

* Trabajo realizado en el marco del Proyecto RTI2018-098405-B-I00, sobre seguridad pública, seguridad privada y derechos fundamentales.

** Miguel Revenga, catedrático de derecho constitucional en la Universidad de Cádiz. Facultad de Derecho, av. de la Universidad, 4, 11406 Jerez de la Frontera (Cádiz). miguel.revenga@uca.es.

Artículo recibido el 15.09.2020.

Citación recomendada: Revenga, Miguel. (2020). La pandemia y el derecho a la intimidad. *Revista Catalana de Dret Públic*, (número especial), 125-136. https://doi.org/10.2436/rcdp.i0.2020.3521.

Sumario

1 La Constitución y los derechos en tiempos de pandemia

Transcurridos varios meses desde la declaración de la pandemia por la Organización Mundial de la Salud, aún es pronto para calibrar el impacto que la misma está teniendo sobre el sistema constitucional. Lo que podemos decir sin sombra de duda es que no hay parcela de la actuación pública que no se haya visto afectada de la manera más rotunda por una situación excepcional que no acabó, ni mucho menos, con el levantamiento del estado de alarma, tras seis prórrogas sucesivas, en junio de 2020. Desde el 14 de marzo y hasta este mismo momento, hemos visto cómo se acentuaban ciertos rasgos de nuestro sistema constitucional que se presentan en línea de continuidad con tendencias ya asentadas bastante antes de la declaración de la pandemia; por ejemplo, el declive a ojos vistas de las genuinas funciones del Parlamento como sede primigenia de la representación, y el correlativo realce de la figura del presidente del Gobierno, erigido en portavoz de una razón pública manifestada directamente a la ciudadanía a través de comparecencias televisadas. Y, en correlato con ello, el desplazamiento de la ley como figura normativa central y de referencia en nuestro sistema de fuentes, sustituida ahora por una legislación de urgencia que apenas sirve como cobertura de una frenética producción de normas de diferente rango y procedencia que no hacen sencilla la aproximación a una realidad en extremo fluida y cambiante.

Junto a la Constitución *formal* —si se nos permite la licencia— tenemos una constitución *en sentido material* compuesta por una pléyade de decretos leyes (también en el ámbito autonómico) y normas de rango reglamentario, en la que ocupa una posición paramétrica el Decreto Ley 21/2020, de 9 de junio, la disposición que transpuso al mundo del derecho el Plan para la Transición hacia una Nueva Normalidad aprobado en Consejo de Ministros. Desafortunadamente, los indicadores de transmisión del coronavirus tras las "desescaladas" y la superación de las "fases de transición", que siguen en aumento cuando escribo estas líneas, delinean un panorama en el que lo de la normalidad, por muy nueva que sea, resulta todavía más un desiderátum que una realidad.

En materia de derechos fundamentales, todo lo acaecido durante estos últimos meses invita también a reflexionar sobre las mutaciones y cambios de paradigmas que se nos aparecen a partir de la de la declaración del estado de alarma. Por lo pronto, la idea de la gradación de situaciones de excepcionalidad nucleada en torno a la disponibilidad para limitar o suspender derechos ha quedado en entredicho desde el momento en que la menos incisiva de tales situaciones sirvió de cobertura para establecer como regla general el confinamiento domiciliario de toda la ciudadanía. El debate sobre si lo procedente hubiera sido el estado de excepción, en lugar del estado de alarma, ha quedado en todo caso sobrepasado por una situación epidemiológica que persiste y en la que lo que ahora importa es quién puede hacer qué, desde el punto de vista competencial, para hacer frente a la pandemia. La titularidad autonómica de las competencias en materia de sanidad, las facultades estatales de supervisión y control, y la obsolescencia de un marco normativo sobre salud pública que no estaba diseñado para enfrentar una situación como la que padecemos, conforman un cóctel explosivo (desde el punto de vista de la seguridad jurídica) en el que muchos de los derechos reconocidos en la Constitución como fundamentales quedan al albur de iniciativas dispares condicionadas a un respaldo caso por caso (que a menudo es contradictorio) de la jurisdicción.

En tales condiciones, una garantía "de arquitectura" como la de la reserva de ley para el desarrollo de los derechos con respeto del contenido esencial queda un tanto desdibujada. Lo decisivo ahora no es la ubicación de este o de aquel derecho en una u otra parte de la Constitución. Lo verdaderamente importante es la aparición de un interés público de relevancia constitucional —la preservación de la salud pública a la que se endereza la lucha contra el virus— que hace que los juicios de ponderación en materia de disposición y limitaciones de los derechos graviten en torno suyo, prefigurando ineluctablemente el resultado de la ponderación. Se trata de una fuerza de gravitación poderosa, justificada y ubicua, y que por lo demás no deja precisamente en buen lugar las jerarquizaciones de los derechos que realiza, con base en las garantías de estos, el artículo 53 de la Constitución. Tampoco habla bien, por cierto, de la escasa atención que los juristas, y especialmente los que nos situamos en la esfera del derecho constitucional, hemos prestado al significado y a la proyección normativa de los deberes constitucionales, con aproximaciones que (salvo excepciones) se han centrado sobre todo en resaltar los condicionantes de tipo formal a que se hallan sometidos los deberes, como consecuencia de una cultura constitucional tan comprometida con los derechos individuales y sus garantías, que ha tendido a pasar por alto las implicaciones de una comunidad de ciudadanos vinculados en torno al apego hacia valores fundacionales de carácter compartido.

2 El derecho a la intimidad: inconsistencias y paradojas

Hace unos años publiqué un trabajo sobre el derecho a la intimidad, al que me atreví a calificar como un derecho "en demolición y necesitado de reconstrucción" (Revenga, 2016). En aquella ocasión, la preocupación por la suerte de este derecho provenía principalmente de los programas de vigilancia masiva sobre nuestras comunicaciones electrónicas aplicados por ciertos Servicios de Inteligencia, que acababan de ser denunciados ante la opinión pública.[1] El Tribunal Europeo de Derechos Humanos ha tenido ya ocasión de pronunciarse al respecto en una sentencia, *Big Brother Watch and others v. the United Kingdom*[2] (aceptada para ser revisada ante la Gran Sala), que no es muy tranquilizadora, ni acaso en absoluto crítica, con respecto al "estado de vigilancia" que hemos visto consolidarse durante los últimos años (Foessel, 2010). La sentencia es sobre todo una reivindicación del valor de la seguridad jurídica; exige a la legislación británica que da cobertura a las intervenciones masivas un grado más de precisión en cuanto a los criterios que se siguen para seleccionar el material digno de una revisión en profundidad por su interés para la seguridad. Ciertamente, lo que hace el TEDH en esa sentencia dista mucho de ser un análisis sustantivo sobre el valor de la vida privada del artículo 8 del Convenio. Más bien viene a aceptar que, como la vigilancia es inevitable, y dado que pertenece al ámbito de decisión de cada Estado determinar qué es lo que conviene para salvaguardar su seguridad, al menos es exigible un esfuerzo dirigido a que el ciudadano pueda conocer, con la mayor precisión posible, cuáles son las reglas a las que atenerse.

Esa aproximación al derecho a la intimidad es descarnada. Podría decirse incluso que está imbuida de cinismo y que deja de lado todo lo que representa el viejo *to be let alone*, quizá la definición del derecho a la vida privada más famosa de todos los tiempos. Esta no viene contemplada como un derecho de la esfera personal susceptible de defensa patrimonial como hace nuestra Ley Orgánica 1/1982, mezclando el valor de la intimidad con la defensa del honor y de la propia imagen. Tampoco parece muy preocupada por la erosión irreversible que supone para la intimidad el hecho de que todo aquello que compartimos con terceros a través del uso del teléfono o de Internet, sea cual sea el sentido de la comunicación o el carácter y el alcance de la misma, haya dejado de ser algo que pertenece a la esfera privada.[3] No hay dignidad oponible a la invasión creciente de las tecnologías de la comunicación en nuestras vidas, hasta el punto no ya de darles un nuevo sesgo o condicionarlas, sino de crear todo un universo paralelo de realidad *virtual* en el que no nos incomoda habitar con otro yo vigilado y, pese a ser consciente de ello, comunicativo y transparente hasta lo trivial.

En un contexto así cobran más sentido que nunca toda una serie de cuestiones que no tienen nada de retóricas: ¿qué queda del derecho a la intimidad?; ¿es equivalente a la *privacy* anglosajona?; ¿coincide con la vida privada y familiar del derecho positivo europeo?; ¿guarda una relación absorbente, de género a especie, con respecto a la inviolabilidad del domicilio y el secreto de las comunicaciones?, o ¿tiene sustantividad propia? Son las preguntas de siempre que los juristas solemos responder utilizando argumentos de *lege data* (y expresando deseos de *lege ferenda*), así como recurriendo a sentencias y otros documentos de *hard law* o *soft* law, que nos permiten dar respuestas aproximadas y formular guías de conducta.

1 Resultan de gran interés al respecto las memorias de Edward Snowden (Snowden, 2019), el analista y consultor de la CIA que reveló la existencia de los programas de vigilancia.

2 *Big Brother Watch and others v. the United Kingdom* (*applications* núms. 58170/13, 62322/14 y 24960/15), sentencia de 13 de septiembre de 2018.

3 Véase, no obstante, la Sentencia 27/2020 del Tribunal Constitucional dictada por su Sala Segunda el 24 de febrero. En ella se desestima el amparo interpuesto por una publicación periódica, poniendo coto al empleo de la imagen captada en Facebook del protagonista de un suceso luctuoso. La sentencia se centra sobre todo en el derecho a la propia imagen, pero contiene interesantes precisiones sobre los derechos fundamentales en la sociedad digital. "Contemplado de esta manera el panorama tecnológico actual —se señala en el FJ 1.3— y aceptando que la aparición de las redes sociales ha cambiado el modo en el que las personas se socializan, hemos de advertir, sin embargo —por obvio que ello resulte—, que los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica. Por consiguiente, salvo excepciones tasadas, por más que los ciudadanos compartan voluntariamente en la red datos de carácter personal, continúan poseyendo su esfera privada, que debe permanecer al margen de los millones de usuarios de las redes sociales en Internet, siempre que no hayan prestado su consentimiento de una manera inequívoca para ser observados o para que se utilice y publique su imagen".

En lo que se refiere al derecho a la intimidad, lo que ha acontecido de relevante en los últimos tiempos proviene no tanto del intento de alzar un claustro personal íntimo e inexpugnable frente a la interesada curiosidad de los Estados y los gigantes de la comunicación digital, sino de la voluntad de poner orden en el magma inabarcable de los datos y megadatos que origina nuestro comportamiento del día a día, y que representan para ambos un caudal inagotable de información sobre nosotros. Baste recordar las contribuciones del Tribunal de Justicia anulando disposiciones —precisamente la Directiva sobre conservación de datos— que sentaban las bases de posibles abusos de las autoridades públicas en aras de la seguridad,[4] "descubriendo" el derecho al olvido frente al gran almacenador/proveedor de la información a nuestro alcance,[5] o exigiendo de manera indirecta a las autoridades norteamericanas un nivel de protección de los datos transferidos equivalente al dispensado en el espacio jurídico de la Unión Europea.[6] Puede parecer exagerada la afirmación de que el régimen jurídico de la protección de datos —el sistema de los llamados *derechos ARCO*— sintetiza y agota hoy el contenido realmente exigible de la intimidad, pero que la vorágine de los datos tiene desde esa perspectiva un potencial absorbente nos parece indudable. Comparando este aspecto de la experiencia europea con el sesgo constitutivo y preferente de la libertad de expresión en la norteamericana, se ha llegado a decir (Petkova, 2019) que la defensa de la *privacy* ha resultado ser, al cabo, nuestra Primera Enmienda.[7]

3 Tecnología e intimidad en la lucha contra el virus

El artículo 18.4 de la Constitución, que es uno de los que no admite suspensión en el marco de los estados excepcionales, representa un caso de *serendipia constitucional* realmente admirable. Lo que en él se reclama está en sintonía con las exigencias del TEDH: leyes que nos protejan de los abusos de la informática para garantizar nuestros derechos. Es algo que formula de manera sintética lo que el artículo 8 de la Carta de Derechos Fundamentales de la UE ("Protección de datos de carácter personal") convierte en todo un programa paramétrico sobre el régimen de los datos en la sociedad digital: tratamiento leal, finalidad legítima, consentimiento del afectado y/o fundamento previsto por la ley, derechos de acceso y rectificación, y control de todo ello por autoridades independientes.

Hablando en líneas generales puede decirse que el uso de la tecnología en la lucha contra el virus está siendo, en nuestro caso y, en general, en el caso de los sistemas europeos, un uso conforme a los imperativos recién señalados. Y, sin embargo, considerando todo a la luz de unas inercias donde la lucha por la protección de datos coexiste con un auge de la vigilancia estatal descontrolada y el abandono de consideraciones de sustancia sobre el valor de la intimidad —y sobre la intimidad como valor—, no es de extrañar que las actitudes de temor y de recelo frente a las iniciativas públicas dirigidas a un uso selectivo e inteligente de la tecnología en la lucha contra el virus sobrepasen claramente a las que tienden a percibirlas como limitaciones razonables de algunos derechos que merecen un apoyo decidido en función de los beneficios que pueden aportar a la preservación del derecho a la salud y la contención del virus. El célebre *dictum* de Foucault sobre la peste como el estado ideal para ver funcionar la disciplina perfecta (Foucault, 2002: 183)[8] acaso vale para describir las formas de hacer frente al virus que hemos visto poner en práctica en China y en algunos países asiáticos, pero —más

4 Casos C-293/12 y C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources & Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238.

5 Caso C-131/12, *Google Spain v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

6 Caso C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650.

7 Hay que apresurarse a añadir que también el Tribunal Supremo norteamericano, por cinco votos contra cuatro, en el caso *Carpenter contra Estados Unidos*, realizó, en el año 2018, una importante contribución a la defensa de la vida privada frente al acceso a los datos telefónicos de ubicación. Rectificando una línea de razonamiento que se remonta a bastantes años atrás, centrada en las bajas expectativas de privacidad con relación a todo aquello que se comparte voluntariamente con terceros (*third party doctrine*), la mayoría del Tribunal ha tenido allí como una intromisión personal contraria a las garantías de las pesquisas irrazonables de la Cuarta Enmienda el acceso directo por parte de la policía, sin autorización judicial, a los datos de ubicación del teléfono celular durante los últimos seis meses almacenados por el proveedor del servicio.

8 La cita completa es así: "Para hacer funcionar de acuerdo con la teoría pura los derechos y las leyes, los juristas se imaginaban en el estado de naturaleza; para ver funcionar las disciplinas perfectas, los gobernantes soñaban con el estado de peste".

allá que como *licencia política*— creo que resulta una observación que no hace justicia a las condiciones, llenas de prevención y cautela, con las que, bajo la supervisión del garante europeo de protección de datos y las demás instituciones de la Unión, se ha recurrido hasta ahora a la tecnología en los países de la UE.

En el caso de España, las técnicas susceptibles de ser utilizadas aparecieron recogidas tempranamente en la Orden 297/2020, de 27 de marzo, del Ministerio de Sanidad.[9] Además del Real Decreto 463/2020, mediante el que se declaró el estado de alarma, la disposición cita en apoyo de lo previsto en ella el artículo 3 de la Ley Orgánica 3/1986, de Medidas Especiales en Materia de Salud Pública. Hay allí una amplísima habilitación en favor de la autoridad sanitaria dirigida a "adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible". A día de hoy tal sigue siendo la endeble base jurídica sobre la que gravita principalmente la lucha contra el virus, algo que no dice mucho en favor de la capacidad del titular del poder legislativo para amoldarse a las circunstancias. Las actuaciones contempladas en la orden consisten básicamente en el desarrollo de una aplicación informática para transmitir información sobre la COVID-19, además de propiciar a partir de la misma, y según los síntomas médicos comunicados por el usuario, la realización de un autodiagnóstico sobre la probabilidad de que esté infectado, y la transmisión de recomendaciones. Además —y esto es quizá lo más polémico— la orden prevé que la aplicación posibilite la geolocalización del usuario "a los solos efectos de verificar que se encuentra en la comunidad autónoma en que declara estar". En tercer lugar, la orden ministerial prevé el desarrollo de una web informativa, así como de un chatbot para ser utilizado vía WhatsApp u otras aplicaciones de mensajería instantánea. Y, por último, encomienda a la Secretaría de Estado, coordinada con el Instituto Nacional de Estadística, un análisis de la movilidad de las personas en los días previos y durante el confinamiento "a través del cruce de datos de los operadores móviles, de manera agregada y anonimizada". La orden identifica en cada caso los titulares del tratamiento de los datos e invoca como fuentes de referencia para el desarrollo de las actuaciones previstas en ella el Reglamento (UE) núm. 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como los criterios interpretativos proporcionados por la Agencia Española de Protección de Datos (AEPD).

En su Informe 17/2020, la AEPD va desgranando los fundamentos legales que permiten el tratamiento de datos, en general, y de datos sensibles, como son los de salud, incluso sin consentimiento previo del interesado, en situaciones de emergencia sanitaria como las causadas por la pandemia. Obviamente, tales fundamentos legales existen[10] y son una prueba de aquello que suele afirmarse siempre sobre la superior inteligencia de la ley con respecto a la del legislador. Como afirma la doctrina especializada, bien están las cautelas y prevenciones que eviten un deterioro del régimen de protección de datos al socaire de la pandemia, pero sin olvidar nunca que el régimen jurídico de la protección de los datos, y la propia existencia de autoridades independientes encargadas de custodiarlo, más que para prohibir y cerrar vías, están para recordar a todos el modo de transitarlas.[11] Por su *auctoritas* y por el esmero con el que, en general, están realizados los informes y las tomas de posición de las agencias, deberían aportar legitimidad a las iniciativas, contribuyendo a romper la dinámica de la desconfianza. Hay que tener en cuenta, además, que datos personales con capacidad de afectar a la vida privada son solamente aquellos que posibilitan la identificación de personas físicas concretas, que es lo que

9 Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por la COVID-19.

10 Véanse especialmente el considerando 46 del RGPD ("El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano"), el artículo 6.2, apartados *c*, *d* y *e*, así como el artículo 9.2, apartados *c*, *g*, *h* e *i* del propio REPD. Y véase también la kilométrica disposición adicional 17.ª de la Ley Orgánica 3/2018, dedicada al tratamiento de datos de salud.

11 Martínez (2020a, 2020b y 2020c) y Piñar (2020). Véase también, con amplias referencias jurisprudenciales, Timón (2020).

determina la aplicación de la normativa de protección. Si tal es el caso (datos individualizados), o bien cuando la identificación es factible mediante la agregación y tratamiento de nuevos datos (datos "seudonimizados"),[12] es cuando, como consecuencia de la afectación real o potencial, rigen en plenitud los principios que enuncia, con carácter general, el artículo 5 del RGPD, y, entre ellos, el de proporcionalidad (adecuación, pertinencia, no exceso).

A la luz de tales principios, la AEPD emitió a finales de marzo un comunicado resaltando la vigencia del régimen de protección *en condiciones de plena normalidad*, pero advirtiendo al mismo tiempo contra la utilización del mismo como pretexto u obstáculo para impedir la adopción de medidas eficaces contra el virus. A tales efectos la AEPD ofreció a las autoridades su leal colaboración y tomó una posición claramente favorable a la obtención de estadísticas con datos de geolocalización agregados para obtener "mapas que informen sobre áreas de mayor o menor riesgo".[13] Igualmente, y con idéntica finalidad de control de la pandemia, el seguimiento de la localización de las personas en cuarentena se condiciona a la previa facilitación voluntaria del número de teléfono móvil. Y, en cuanto al uso de las aplicaciones y páginas webs de información y autodiagnóstico, se establece también la condición de que el usuario sea mayor de 16 años.

Posteriormente, la Unidad de Evaluación y Estudios Tecnológicos de la AEPD ha realizado un informe más completo sobre el uso de las tecnologías en la lucha contra la COVID-19, que subtitula con el rótulo "Un análisis de costes y beneficios".[14] En él la AEPD, además de ocuparse brevemente de las *apps* de seguimiento de contactos, a las que nos referimos en el siguiente epígrafe, se ocupa de los siguientes extremos: a) geolocalización mediante la información recogida por los operadores de telecomunicaciones; b) geolocalización en redes sociales; c) *apps*, webs y chatbots para autotest o cita previa; d) *apps* de recogida de información de contagiados, y e) pasaportes digitales de inmunidad y cámaras infrarrojas.

a) En lo que se refiere a la geolocalización de acuerdo con la información almacenada por los operadores, la AEPD recuerda que es algo que ya está previsto en nuestro ordenamiento, pero condicionada, cuando se pretende utilizar en el curso de una investigación criminal con respecto a un determinado usuario, a la obtención de la correspondiente orden judicial. Por contraste, de lo que aquí se trata es de obtener información anonimizada al solo objeto de analizar estadísticamente los movimientos de la población. Los riesgos potenciales que ello acarrea, se dice, siempre que la gestión sea cuidadosa y el acceso propiamente anonimizado, no sobrepasan los beneficios que cabe esperar de este tipo de análisis, si bien habría que "evaluar de forma continua su utilidad frente a los escenarios cambiantes de confinamiento global o parcial".

b) En cuanto a la geolocalización de móviles a partir de los datos de redes sociales y las direcciones IP desde las que accedemos a Internet, la AEPD considera que se trata de una práctica amenazante para la privacidad, sobre todo si la información se complementa con la que se deriva de la actividad del usuario. Por ello, estima que las autoridades tendrían que demostrar, antes de recurrir a la geolocalización basada en datos de este tipo, la razón de ser y la utilidad por las que se espera mejorar la información ya disponible a través de otras vías.

c) Las *apps*, las páginas webs y los chatbots de autodiagnóstico, consulta y cita previa —lo que se ha dado en llamar *telemedicina*— son instrumentos en auge a los que la pandemia parece haber dado un impulso decisivo, y que plantean considerables problemas desde el punto de vista del procesamiento de datos personales relacionados con la salud (Cotino, 2020). Lo que la AEPD pide a la Administración sanitaria es que no se deje llevar por la urgencia de descargar una demanda de atención saturada y que ponga especial cuidado en el diseño de tales

12 El artículo 4 del RGPD, sobre definiciones, se refiere a la "seudonimización" como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

13 Comunicado de 26 de marzo de 2020, de la AEPD, sobre *apps* y webs de autoevaluación del coronavirus.

14 El documento, con finalidades claramente divulgativas, consta de 13 páginas y está fechado en mayo de 2020.

instrumentos. Y, por otra parte, previene contra los peligros de la brecha digital en un ámbito, el de la atención sanitaria, en el que el riesgo de invisibilidad de ciertos sectores de la población, que son probablemente los que más necesitan de ella, es especialmente acuciante.

d) En cuanto a las *apps* de información voluntaria de contagios, los peligros para la intimidad provienen del carácter dispar, público y privado, de tales iniciativas, y del carácter en extremo sensible de los datos que se ponen a disposición de los servidores de Internet, así como de la posibilidad de ofrecer información maliciosa o poco veraz, con los consiguientes resultados distorsionados y con un fuerte potencial de estigmatización. Lo que la AEPD denuncia a este respecto es que estamos ante un ámbito de actuaciones que, además de adolecer de un déficit de regulación y control, resultan de muy dudosa eficacia.

e) Los pasaportes digitales de inmunidad y el uso de cámaras de infrarrojos para la toma individual y generalizada de temperatura nos evocan escenarios que, de no adoptar cautelas, podrían situar a nuestras sociedades en un lugar cercano a la pesadilla orwelliana o al escenario foucaultiano al que antes nos referíamos. En cuanto a lo primero, la AEPD trae a colación la experiencia china de códigos QR asociados a colores (al modo de semáforos) en función del grado calculado de exposición al virus, de utilización obligatoria, y con efectos de salvoconducto o de prohibición de acceso.[15] Se trata de una tecnología que podemos calificar de efectiva para detener la propagación del virus, pero cuyo carácter imperativo no parece que cuadre con el entendimiento a la europea de la posición de los individuos frente al poder. Prefigura, no obstante, rasgos y tendencias hacia los que podríamos encaminarnos; esperemos que no para establecer jerarquías entre las personas en función de su encuadramiento digital, pero sí para hacer de nuestros *smartphones* un apéndice o repositorio relacionado con nuestra salud, por ejemplo, incorporando el historial clínico de cada uno con posibilidad de ser actualizado en tiempo real. Aunque se trata de algo puramente especulativo, la AEPD anticipa un juicio favorable a esto último, siempre y cuando el acceso a la información sea estrictamente reservado y con finalidades relacionadas con las políticas públicas para el control de la pandemia. En cuanto a las cámaras de infrarrojos, en fin, se trata de cámaras con capacidad para identificar el rostro de las personas mediante algoritmos de inteligencia artificial a las que se incorpora un sistema para medir y revelar la temperatura corporal. Al respecto, la AEPD se muestra decididamente cautelosa no solo por el carácter poco concluyente que tiene ese dato aislado, sino por los riesgos de discriminación, estigmatización y más que probable exposición pública de un dato de salud que comportan para el sujeto afectado.[16]

Fuera de las técnicas de las que se ocupa el informe quedan cuestiones como la identificación y registro de las personas que participan en (o acuden a) ciertos actos, lugares o eventos. Se trata de procedimientos que vienen proliferando al abrigo de normativas autonómicas adoptadas apresuradamente bajo la presión de la evolución de los datos de contagio. Sería interesante que, antes de actuar para dar la impresión de que se hacen cosas, cada medida en particular fuera precedida de un análisis detenido sobre el impacto que puede comportar sobre el ejercicio de derechos, optando de entre todas las alternativas por aquella que resulte menos gravosa.

15 Para un panorama comparativo de respuestas a la pandemia desde el punto de vista de la incidencia sobre los derechos, véase Saetta (2020), con un análisis del modelo chino.

16 "Aplicar estas medidas" —concluye el informe— "sin un criterio establecido por las autoridades sanitarias con relación a qué valor de fiebre es significativo, sobre qué otros síntomas han de ser comprobados, con una manipulación que puede carecer de precisión suficiente en manos de personal no cualificado, podría crear una falsa sensación de seguridad que facilita el contacto con personas realmente infectadas". Véase también el Comunicado de la propia AEPD, de fecha 30 de abril de 2020, sobre tomas de temperatura en los comercios, centros de trabajo y otros establecimientos. El autor no se resiste a contar, a modo de anécdota (reveladora quizá de una categoría), que el acceso a la piscina pública frecuentada por él está condicionado a la aplicación de una normativa municipal en la que se dispone la toma de temperatura realizada por la persona encargada del control de acceso y a la vista del resto de los usuarios.

4 En especial, las aplicaciones de rastreo de contactos

Ninguna de las iniciativas adoptadas para contribuir a reducir las tasas de contagio parece haber despertado tanto interés como el recurso a aplicaciones o *apps* de rastreo de contactos. Utilizadas por vez primera en Singapur a los pocos días de la declaración de la pandemia (TraceTogether), las *apps* de rastreo han sido objeto desde entonces de acalorados debates sobre sus supuestos beneficios y debilidades. Se ha esperado de ellas que permitan a una gran parte de la población conocer de continuo, y en tiempo real, el nivel de su exposición al virus. Pero, como resulta obvio, se trata de un beneficio sujeto a condición: para cumplir las expectativas, las *apps* tendrían que ser descargadas y activadas masivamente. Además, sus rendimientos positivos solo serían posibles si todos los usuarios actuaran con conciencia cívica, es decir, con plena disposición para cumplir cabalmente las indicaciones de las autoridades sanitarias, sometiéndose a las correspondientes pruebas y cumpliendo los períodos de cuarentena que resultaran necesarios. Por su parte, las autoridades sanitarias deberían haber integrado esta modalidad de rastreo en su esquema genérico de combate contra el virus, asegurando la suficiencia de recursos humanos y materiales como para poder responder con prontitud y eficacia a las situaciones que se plantearan en cada caso. Si no se dan tales condiciones, las *apps* de rastreo parecen abocadas a convertirse en un expediente más bien anecdótico o marginal dentro de las estrategias dirigidas a frenar los contagios.

Cabría preguntarse entonces si está justificado tanto "ruido" a propósito de ellas. En unos casos se presentan como una panacea, un ejemplo elocuente de lo importante que puede resultar para la salud pública el recurso a las nuevas tecnologías. Por el contrario, otros contemplan las *apps* de rastreo de contactos como peligrosos artefactos que no harán sino incrementar el control sobre nuestras vidas e infligir otra vuelta de tuerca en la erosión irreversible del derecho a la intimidad.

Las *apps* de rastreo representan un arquetipo de todo aquello que estamos viendo transformarse a ojos vistas durante estos últimos meses. Incorporar a nuestros teléfonos una aplicación que nos pone en contacto permanente con los otros y permite a las autoridades sanitarias alertarnos de situaciones de riesgo según lo que resulte de tal contacto no es cosa baladí. Por lo pronto, nos viene a mostrar que la telemedicina está ya aquí, y, como suele decirse con la recurrente frase hecha, ha venido para quedarse. Por ahora se trata de una telemedicina que es solo muy genérica y de carácter preventivo, pero, nos guste o no, a través de las *apps* de rastreo se acaba realizando un prediagnóstico sobre nuestra exposición al virus basado en el control permanente de nuestra conducta.

Nada tiene, pues, de extraño que instituciones públicas y organizaciones no gubernamentales interesadas por la suerte de los derechos se hayan apresurado a tomar posiciones con respecto a las *apps* de rastreo. Entre las primeras, puede citarse la Recomendación de la Comisión de la Unión Europea 518/2020, de 8 de abril, a la que siguió de inmediato la Comunicación sobre *apps* de *contact tracing*, de 17 de abril.[17] El Parlamento Europeo, en su Resolución de 17 de abril de 2020 sobre la acción coordinada de la Unión para luchar contra la pandemia de COVID-19 y sus consecuencias, insistió en la necesidad de desarrollar un enfoque común de la Unión para el uso de las aplicaciones de rastreo de contactos, y estableció al respecto (puntos 52 y 53 de la resolución) una serie de principios que, en líneas generales, sigue muy de cerca el tipo de aplicación por la que se ha optado en el caso de España.[18] El Consejo Europeo de Protección de Datos aprobó el 21 de abril de

17 Recomendación de la Comisión 2020/518, de 8 de abril de 2020, relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados; Comunicación de la Comisión 2020/C 124 I/01, relativa a orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos. En el marco de la E-Health Network de la Directiva sobre derechos de los pacientes en la asistencia sanitaria transfronteriza, fueron aprobados también los documentos *Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States*, de 15 de abril, e *Interoperability guidelines for approved contact tracing mobile applications in the EU*, de 15 de mayo.

18 Tales puntos de la resolución afirman literalmente lo siguiente: "52. Toma nota de la aparición de aplicaciones de localización de contactos en dispositivos móviles con el fin de alertar a las personas si se encuentran cerca de una persona infectada, y la recomendación de la Comisión de desarrollar un enfoque común de la Unión para el uso de dichas aplicaciones; señala que cualquier uso de aplicaciones desarrolladas por las autoridades nacionales y de la Unión no puede ser obligatorio y que los datos generados no deben almacenarse en bases de datos centralizadas, que son proclives a un riesgo potencial de abuso y pérdida de confianza y pueden

2020 las Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, y la Agencia de Derechos Fundamentales de la Unión, las suyas.[19]

No escasean, como se ve, las tomas de posición y las normas de *soft law* sobre la cuestión de las aplicaciones de rastreo. Lo que en todo ello subyace no es quizá tanto el papel que tales *apps* puedan desempeñar *en este momento concreto* para frenar las tasas de contagio —de hecho, alguno de los documentos citados muestra bastante escepticismo al respecto—, sino la novedad y el salto cualitativo que pueden llegar a tener sobre los usos sociales relacionados con la vigilancia de la salud. Hay planteamientos de tipo ético que resaltan la importancia de realizar en sede de debate político un detenido análisis coste-beneficio antes de impulsar una medida como la de las *apps* de rastreo; y ello porque, como se ha señalado, hablando en términos generales (Taddeo, 2020) y en términos más específicos (Floridi, 2020; McGregor, 2020), una vez que se dan determinados pasos la vuelta atrás resulta más bien difícil.

En el caso de la aplicación española (Radar COVID), el sistema se ha ido implantando de manera progresiva en las últimas semanas sin más cobertura legal que la genérica para todas las actuaciones relacionadas con la lucha contra el virus. Esto contrasta con lo ocurrido en otros países, como, por ejemplo, Italia, donde la aplicación cuenta con una previsión legal *ad hoc* que reproduce las exigencias y las garantías de funcionamiento de la *app* en consonancia con lo establecido por las autoridades europeas.[20] La falta de un debate suficiente en la esfera pública ha difuminado, en cambio, entre nosotros las potencialidades y la propia implantación de la aplicación. La impresión personal del autor de este trabajo es que el desconocimiento, la desconfianza y el escepticismo son los tres términos que describen fielmente una experiencia que todavía está en ciernes, pero a la que hasta ahora le ha faltado manifiestamente un apoyo desde instancias oficiales dirigido a explicar el sentido y el funcionamiento de la *app*, así como las cautelas que se han incorporado a la misma para evitar que pueda convertirse en un instrumento generador de control y discriminación.

La propia AEPD, en el informe al que antes nos hemos referido, apunta a la implicación de un número elevado de usuarios de la *app* como un factor decisivo, y considera que en la situación actual de España y de otros países europeos "no parece que estas aplicaciones vayan a tener éxito a corto plazo como una estrategia global de lucha contra la pandemia". Ello no obstante, la propia AEPD tendrá que pronunciarse más pronto que tarde sobre Radar COVID, pues ya obra en su registro una denuncia contra la Secretaría General de Administración Digital, a la que se achaca haber puesto en marcha la aplicación sin el previo estudio de impacto sobre protección de datos y sin haber definido con la suficiente precisión las finalidades del tratamiento, las funciones y las responsabilidades de las autoridades sanitarias de las comunidades autónomas, y los plazos de conservación de los datos.[21] En el momento de escribir estas líneas, tenemos también noticia de que la Secretaría de Estado de Digitalización e Inteligencia Artificial ha abierto al público, mediante un enlace de

poner en peligro su adopción en toda la Unión; pide que todo almacenamiento de datos esté descentralizado, que se brinde una plena transparencia ante los intereses comerciales (no comunitarios) de los desarrolladores de estas aplicaciones, y que se ofrezcan proyecciones claras sobre cómo el uso de aplicaciones de localización de contactos por una parte de la población, en combinación con otras medidas específicas, dará lugar a un número significativamente menor de personas infectadas; pide que la Comisión y los Estados miembros sean plenamente transparentes en el funcionamiento de las aplicaciones de localización de contactos, a fin de que las personas puedan verificar tanto el protocolo de seguridad y privacidad subyacente como el propio código, para comprobar si las aplicaciones funcionan con arreglo a lo que afirman las autoridades; recomienda que se establezcan cláusulas de extinción y se respeten plenamente los principios de protección de datos desde el diseño y de minimización de datos". "53. Pide a la Comisión y a los Estados miembros que publiquen los detalles de estos sistemas y que permitan el control público y la plena supervisión por parte de las autoridades de protección de datos; señala que los datos de localización móvil solo pueden procesarse de conformidad con la Directiva sobre la privacidad y las comunicaciones electrónicas y el RGPD; destaca que las autoridades nacionales y de la Unión deben cumplir plenamente la legislación en materia de privacidad y protección de datos, así como la supervisión y orientación de las autoridades de protección de datos nacionales".

19 *Coronavirus pandemic in the EU – Fundamental Rights implications: With a focus on contact-tracing apps*. Entre las posiciones de las ONG puede citarse la de Privacy International: "COVID-19 response: overview of data and technology".

20 Se trata del artículo 6 del Decreto Ley 28/2020, de 30 de abril. La implantación de la *app* fue además precedida de un extenso informe redactado por un grupo de trabajo sobre "Tecnología para el gobierno de la emergencia". Véanse Colapietro y Iannuzzi (2020), así como Bergonzini (2020).

21 "Denuncian a la Secretaría General de Administración Digital ante la Agencia Española de Protección de Datos por Radar COVID", *ElDerecho.com*, 10 de septiembre de 2020.

GitHub, el código fuente de la aplicación.[22] Ello puede contribuir a despejar muchas de las dudas que aún puedan persistir con respecto al diseño y al esperable funcionamiento de la aplicación, pero no revierte por sí solo la situación de cierto estancamiento que se percibe con respecto a ella, plasmada en los déficits de información a los que ya nos hemos referido y en los retrasos de incorporación plena de la misma en el sistema sanitario de todas las comunidades autónomas.

5 Conclusiones

La intimidad es, como se ha dicho (Eiermann, 2020), un concepto "vaporoso" y lleno de connotaciones ambiguas. Al final, lo que lo dota de sentido son las circunstancias que rodean su entrada en escena, a menudo para descartar, por consideraciones de principio basadas en ella, comportamientos o vías de acción que nos parecen amenazantes para la idea de intimidad que a la mayoría le resulta razonable y defendible. En el caso de lo que se ha dado en llamar *biovigilancia*, y en una situación de grave emergencia sanitaria como lo que padecemos, confluyen circunstancias que ponen a prueba muchas cosas y, entre ellas, nuestra concepción de la intimidad como un derecho y como un principio sometido a presión, pero que nos sigue resultando inescindible de los valores de dignidad y autodeterminación personal que fundamentan, junto a otros, nuestra convivencia organizada. Ello no significa que tengamos que optar entre intimidad o salud. No es eso lo que enseña una historia de lucha contra las enfermedades infecciosas (tuberculosis, polio, viruela y tantas otras) que no hizo de la intimidad un concepto de museo arrumbado por la necesidad de actuar; al contrario, la salud pública y los derechos fueron de la mano creando lógicas de actuación y sistemas públicos cada vez más sofisticados y eficaces. El presente es un momento que podemos definir como inaugural y de salto cualitativo en lo que se refiere a las posibilidades que abren la tecnología, el *big data,* el algoritmo y la inteligencia artificial para luchar contra la pandemia. Y por ello es también el momento de la alianza entre la técnica y el derecho, pues las formas a través de las cuales se tomen ahora las decisiones, y la manera en la que queden plasmadas, determinarán la suerte de los derechos a la salud y a la intimidad de las generaciones futuras.

6 Referencias bibliográficas

Bergonzini, Chiara. (2020). Non solo privacy. Pandemia, contact tracing e diritti fondamentali. *Dirittifondamentali.it*, *2*.

Colapietro, Carlo, y Iannuzzi, Antonio. (2020). App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali. *Dirittifondamentali.it*, *2*.

Cotino, Lorenzo. (2020). Inteligencia artificial, *big data* y aplicaciones contra la COVID-19: privacidad y protección de datos. *Revista de Internet, Derecho y Política*, *31*.

Eiermann, Martin. (31 de marzo de 2020). Privacidad, salud pública y pandemia de la Covid-19. [Entrada de blog]. *Open Democracy*.

Floridi, Luciano. (2020). Mind the App. Considerations on the Ethical Risks of COVID-19 Apps. *Philosophy & Technology*, *33*, 167-172.

Foessel, Michaël. (2010). *Estado de vigilancia. Crítica de la razón securitaria*. Madrid: Lengua de Trapo.

Foucault, Michel. (2002). *Vigilar y castigar: nacimiento de la prisión*. Buenos Aires: Siglo XXI Editores.

Martínez, Ricard. (2020). Los tratamientos de datos personales en la crisis del COVID-19: un enfoque desde la salud pública. *Diario La Ley*, *1*(38).

Martínez, Ricard. (30 de marzo de 2020b). Protección de datos y geolocalización en la Orden SND/297/2020. [Entrada de blog]. *Hay Derecho - Expansión*.

22 "La 'app' Radar COVID libera su código fuente mostrando sus fortalezas y debilidades", *Confilegal,* 11 de septiembre de 2020.

Martínez, Ricard. (27 de julio de 2020c). Apps coronavirus y desconfianza ciudadana. *La Ley*.

McGregor, Lorna. (30 de abril de 2020). Contact-tracing Apps and Human Rights. [Entrada de blog]. *EJIL: Talk! Blog of the European Journal of International Law*.

Petkova, Bilyana. (2019). Privacy as Europe's First Amendment. *European Law Journal*, *25*, 140-154.

Piñar, José Luis. (9 de abril de 2020). Privacidad en estado de alarma y normal aplicación de la Ley. [Entrada de blog]. *Hay Derecho - Expansión*.

Revenga, Miguel. (2016). El derecho a la intimidad: un derecho en demolición (y necesitado de reconstrucción). En Asociación de Letrados del Tribunal Constitucional (España) (coord.), *El derecho a la privacidad en un nuevo entorno tecnológico. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional* (p. 71-98). Madrid: Tribunal Constitucional - CEPC.

Saetta, Bruno. (16 de abril de 2020). Pandemia, app e tecnologia: un test per le democrazie. [Entrada de blog]. *Valigia Blu*.

Snowden, Edward. (2019). *Vigilancia permanente*. Barcelona: Planeta.

Taddeo, Mariarosaria. (2020). The Ethical Governance of the Digital During and After the COVID-19 Pandemic. *Minds and Machines*, *30*, 171-176.

Timón Herrero, Marta. (7 de agosto de 2020). Protección de datos de carácter personal y crisis sanitaria (Covid-19). [Entrada de blog]. *ElDerecho.com*.