IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

Inteligencia artificial, *big data* y aplicaciones contra la COVID-19: privacidad y protección de datos

Lorenzo Cotino Hueso
Universidad de Valencia

Fecha de presentación: abril de 2020
Fecha de aceptación: julio de 2020
Fecha de publicación: julio de 2020

Resumen

El *big data* y la IA han fracasado en la prevención, pero pueden ser muy útiles frente a la COVID-19 e incluso para evitar confinamientos y otras restricciones de derechos que provoca. La IA puede ser extremadamente eficaz para integrar, estructurar y extraer información y conocimiento de ingente cantidad y variedad de *big data* para la investigación biomédica. También es útil para mejorar la atención e información ciudadana y de salud, la telemedicina y la mejor asignación de los recursos humanos y materiales. Más amenazante para la privacidad puede ser el desarrollo de *apps,* pasaportes biológicos electrónicos o sistemas de geolocalización, trazabilidad y monitoreo de personas implementados para hacer frente a la COVID-19, en especial si se sigue el caso asiático. No obstante, de momento no es el que parece seguirse en la UE. Se analiza el régimen jurídico aplicable, la legitimación legal de los diferentes tratamientos de datos, la necesidad de una base legal de calidad, especialmente para el caso de *apps* y rastreos. Y más allá de la base legal y legitimación se tienen en cuenta las necesarias garantías de estos tratamientos masivos, especialmente de las *apps*. El Consejo Constitucional francés y especialmente las instituciones europeas han marcado el camino a seguir, con una acción más discreta en España, que en junio ha regulado con fuerza de ley algunos aspectos del tratamiento de datos de manera muy insuficiente. Existen dos grandes modelos europeos (PEPP-PT y el DP-3T por el que se ha decantado España) más o menos centralizados y más o menos seguros, así como desarrollos propios. Y al parecer para su utilidad deben integrarse bajo las APIs y desarrollos conjuntos de Apple y Google, lo que genera suspicacias. Se sostiene que el Derecho impulsa que tecnológicamente sí sea posible maximizar tanto la eficacia de la lucha contra la COVID-19 como todos nuestros derechos. El tema, sin duda, exigirá un análisis continuo de expertos, sociedad civil y autoridades de datos.

Palabras clave

COVID-19, protección de datos, inteligencia artificial, geolocalización, privacidad

Artificial intelligence, big data and applications against Covid-19, and privacy and data protection

Abstract

Big data and AI did not succeed in preventing Covid-19, but they can be very useful in the fight against it and even for avoiding confinements and other restrictions on rights which it brings about. AI can be extremely useful for integrating, structuring and extracting an enormous quantity and variety of big data information and knowledge for biomedical research. It is also useful for improving civic and health assistance and information, telemedicine and the best assignment of human resources and materials. Even more threatening for privacy could be the development of apps, electronic biological passports, geolocation systems, and the traceability and monitoring of people in the fight against Covid-19, particularly if the Asian model is followed. However, it seems that this not being followed in the EU. There is an analysis of the applicable legal set of rules, the legal legitimation of the various data processing systems, and the need for a legal basis of quality, especially in the case of apps and searches. And besides the legal basis and legitimation, the necessary guarantees of these mass processing systems are considered, particularly of the apps. The impetus of law means that it is indeed technologically possible to maximise the efficiency of the fight against Covid-19 and to maximise all our rights.

Keywords

Covid-19, data protection, artificial intelligence, geolocation, privacy

1. Introducción. El virus de la amenaza

El coronavirus SARS-CoV-2 no se ve ni se aprecia en el momento, sino tarde y cuando se dan sus consecuencias, pudiendo estar atacando de modo silente los derechos COVID-19 y, en particular, la privacidad. El coronavirus se expandió de China a todo el mundo y esperemos que, en una segunda oleada, no exporte también el control social y la vigilancia totalitaria de la mano del *big data*, la IA, las *apps* covid y los pasaportes biológicos electrónicos. Entre los peligros de la IA (Cotino, 2019a), Han nos ha venido alertando desde hace años de la *psicopolítica digital data*; ahora lo hace con respecto a la *biopolítica digital*, en la que se controlan todos nuestros biodatos (Han, 2020). Al parecer, frente al coronavirus, la *d* de la *d*isciplina asiática ha sido mucho más eficaz que la *d*escoordinación europea o el *d*arwinismo norteamericano (Ferràs, 2020). Han nos recuerda que la mentalidad autoritaria asiática –procedente del confucionismo– conduce a la obediencia, donde impera el colectivismo y no hay conciencia crítica ante la vigilancia digital. La infraestructura de control social de la IA china parece ser sumamente eficaz contra la pandemia y ahora genera incluso admiración. Ello puede llevarnos a la *biopolítica*, o en términos de Harari (2020), a una «vigilancia hipodérmica». Hasta hace poco, imperaba una «vigilancia epidérmica»: «el Gobierno quería saber sobre qué clicaba exactamente nuestro dedo». Ahora quiere conocer nuestra temperatura, nuestra presión arterial y muchos otros datos relativos a nuestra salud para saber si estamos enfermos antes que nosotros, dónde hemos estado y con quién nos hemos reunido.

No solo los Gobiernos han fallado. La IA y el *big data*, las plataformas o redes sociales no han servido para predecir y alertar sobre la magnitud y propagación del coronavirus: ha habido un «fallo colosal del capitalismo de vigilancia» (Ortega, Balsa-Barreiro y Cebrián, 2020), que no lidia bien con las sorpresas, y tampoco la IA ha sabido integrar información de calidad de modo coherente. La competencia económica entre inteligencias artificiales parece que ha ido en contra de la inteligencia colectiva. Sin embargo, la IA y el *big data* pueden ser unas herramientas formidables contra la COVID-19, pero como toda herramienta dependerá del uso acertado de la misma.

Señala Harari (2020) que, «cuando a la gente se le da a elegir entre la intimidad y la salud, suele elegir la salud». También se ha afirmado que «anteponer el derecho a la privacidad al derecho a la vida o al de libertad de movimientos no tiene sentido, [y] es un dislate» (Pedreño, 2020). Plantear este tipo de debates en términos binarios es peligroso e incluso demagógico. El sistema constitucional política y jurídicamente tiene la virtud de saber deliberar, ponderar y armonizar derechos fundamentales entre sí y con otros bienes constitucionales. Como se verá, hay soluciones de carácter tecnológico que, guiadas por el Derecho, permiten una maximización de la eficacia contra el coronavirus minimizando los impactos en la privacidad, la libertad de circulación y otros derechos. Se trata de una cuestión cambiante, como lo ha sido desde el momento de entrega del presente estudio en abril hasta su revisión final dos meses después.

2. Usos esenciales de la IA y el big data frente a la COVID-19

2.1. IA y *big data* para estructurar y extraer información y conocimiento en la investigación biomédica

En el área de la sanidad, cada vez es más importante «el procesamiento de datos personales relacionados con la salud en los sectores público y privado mediante herramientas digitales» (apdo. 2.1)[1]. Y cada vez son más variadas las fuentes y su naturaleza. Se tratan datos estructurados, semiestructurados y, mayoritariamente, no estructurados[2] y brutos, procedentes de sensores, de grandes transacciones de datos, de registros médicos electrónicos y de datos biométricos (huellas dactilares, información genética, escáneres de retina, rayos X y otras imágenes médicas,

1. Recomendación CM / Rec (2019) 2 del Comité de Ministros a los Estados miembros sobre la protección de datos relacionados con la salud, de 27 de marzo de 2019.
2. Ortega, 2019, págs. 176-178; Alcalde y Alfonso, 2019, págs. 60 y sigs.

la presión arterial, el pulso y lecturas de oximetría de pulso y otros tipos similares de datos), pero también de historias clínicas, imágenes, pruebas, publicaciones, webs y redes sociales. Asimismo, también pueden ser de especial importancia los datos de tráfico, la geolocalización, los metadatos y la información procedente de aplicaciones COVID-19 y operadores de telecomunicación.

Algunos son datos primarios propiamente relativos a la salud, con un régimen jurídico relativamente nítido, pero cada vez se barajan más datos secundarios muy heterogéneos, en sus fuentes y tipología (German Ethics Council, 2017, núm. 99). Esta variedad de orígenes y usos primarios y secundarios genera cada vez más problemas e incertidumbres jurídicas (núm. 19). Estos datos se canalizan, integran o vierten en *datahubs* con fuente central, lagos de datos o de modo centralizado en *data warehouse*. La IA es esencial para que estos datos de usos secundarios y especialmente desestructurados puedan ser datos útiles para la investigación y los usos médicos (Montalvo, 2019, págs. 47-48).

En las acciones frente a la COVID-19 se ha de facilitar el flujo de estos datos entre los sectores público y privado de los distintos países –dentro y fuera de la UE– a fines de salud pública. Para extraer información y conocimiento se precisan tratamientos de ingentes cantidades de datos –principalmente secundarios y desestructurados– a los que aplicar esquemas de lectura y escritura y otros sistemas de IA. Esta se emplea asimismo para llevar a cabo un profundo análisis de datos clínicos de pacientes infectados, hospitalizados, en cuarentena o sospechosos (Martínez, 2020a). De especial interés con redes neuronales para el reconocimiento inteligente y la lectura natural de imágenes relativas o para el apoyo a la asignación selectiva e individualizada de fármacos.

2.2. IA para la atención e información ciudadana y de salud, la telemedicina y la asignación de recursos

La Comisión Europea (2020 c) ha subrayado los tres ejes o "funcionalidades" del tratamiento de datos frente al COVID-19: funcionalidad de información, de comprobación de síntomas y de telemedicina y de rastreo de contactos y de alerta. La IA puede jugar un papel importante a la hora de facilitar atención e información ciudadana y de salud. Puede canalizar las muchas consultas de la ciudadanía, generar datos y extraer conocimiento de las mismas. Es de interés gestionar el origen y localización de llamadas para la gestión de los riesgos granularizada por territorios y otros factores. Al respecto, hoy en día es posible gestionar datos de las conversaciones a través de la analítica de las emociones, una técnica habitualmente utilizada en el *neuromarketing*. La IA también es capaz de facilitar los mensajes perfilados e individualizados para cada tipología de consulta. Permite también el uso de *chatbots* que descongestionen las líneas de atención e incluso que proporcionen información de calidad y perfilada. Al respecto, el ICO (Information Commissioner's Office) ha señalado que es posible el envío de mensajes de salud pública, «ya que estos mensajes no son *marketing* directo» (ICO, 2020). Otra cuestión es, obviamente, cómo se efectúa el perfilado y selección de los destinatarios.

La IA y el *big data* también pueden ser muy útiles para proponer una farmacología adecuada y para implementar una asignación estratégica de recursos médicos humanos y materiales, así como para distribuir o derivar a los pacientes, según necesidades concretas derivadas de la COVID-19, maximizando así la eficiencia de los sistemas sanitarios. Esta trazabilidad, por supuesto, también podría potenciar la eficacia de nuestro hospitales y centros de salud.

Asimismo, la telemedicina (la seria) puede facilitar la prestación de servicios sanitarios, descongestionar la atención presencial y reutilizar al personal médico infectado y en cuarentena que siga estando operativo, pudiendo generar un estimable *big data* luego utilizable. El ICO (2020) ha recordado que la normativa «tampoco les impide utilizar la última tecnología para facilitar consultas y diagnósticos seguros y rápidos». Esencialmente, lo que hay que asegurar es la seguridad informática.

3. El régimen jurídico aplicable, legitimación legal y cumplimiento normativo en España y Europa. La constitucionalidad de la regulación francesa

La IA atrae casi por defecto la aplicación del régimen de protección de datos, el cual, en ocasiones, es casi el único régimen jurídico hoy día claramente aplicable. Y esto es así porque la IA implica el perfilado y activación de decisiones automatizadas que afectan a las personas (Grupo de trabajo del artículo 29, 2018, págs. 7-8). Para que el régimen de protección de datos pueda ser aplicado debe darse la premisa de que los variados macrodatos que *alimentan* la IA sean datos de personas identificadas, identificables o reidentificables. Como se ha recordado con ocasión de la crisis de la COVID-19, no se aplicará la normativa si existe una anonimización que garantice que los datos no vuelvan a ser personales[3]. Pero ello es realmente difícil puesto que, como ha recordado el Libro blanco de la IA (Comisión Europea, 2020, págs. 21 y sigs.), estas mismas tecnologías se utilizan para «rastrear y desanonimizar datos relativos a personas (...) con relación a conjuntos de datos que, en sí mismos, no contienen datos personales».

En cuanto a la legitimación del tratamiento de datos en razón de la pandemia, tanto las autoridades comunitarias[4] como españolas (AEPD y APDCAT) de protección de datos han señalado que «las reglas (...) actualmente vigentes en Europa son lo suficientemente flexibles» (SEPD, 2020a). En concreto, hay que seguir el considerando 46 y los artículos 6.2 párrafos c, d y e y el artículo 9.2, párrafos c, g, h e i) 6 y 9 del RGPD. Así, el EDPB (2020a) afirma que el RGPD «permite a las autoridades de salud pública competentes y a los empleadores procesar datos personales en el contexto de una epidemia, de conformidad con la legislación nacional y en las condiciones establecidas en ella por parte de las autoridades públicas competentes». Ello es aplicado «estrictamente a la duración de la emergencia» (EDPB, 2020a), pues las restricciones «no están aquí para quedarse después de la crisis» (SEPD, 2020a). La Comisión Europea ha ido en la misma línea (2020 b y c), pero con acierto señala que «cuanto mayor sea la repercusión de cara a las libertades de la persona, mayores deben ser las correspondientes salvaguardias previstas en la legislación pertinente». Es más, la Comisión concreta la necesaria previsión legal del detalle del tratamiento y la finalidad, excluyendo expresamente otros fines, determinación del responsable, así como las garantías específicas (2020 c 3.3). Algo que ni por asomo se da en la legislación española al momento de cerrar estas páginas.

En consecuencia, para el Derecho de la UE y en general es relativamente fácil legitimar legalmente los tratamientos de datos ordinarios y especialmente protegidos como los de salud, entre otros, con el fin de prevenir, atender y gestionar los servicios sanitarios, así como para la investigación médica. Hay que advertir que por lo general se requiere que haya una ley nacional, salvo en caso de la concreta excepción por la protección de intereses vitales del interesado u otras personas físicas (artículo 6.1.d) o por tratarse de datos sensibles (artículo 9, 2.º c, del RGDP).

Como ha recordado el EDPD, el papel del legislador nacional es muy importante, al punto que «las condiciones y el alcance de dicho tratamiento [de datos frente al COVID-19] varían en función de las disposiciones legislativas promulgadas en cada Estado miembro» (2020 b) 69. 2º). Pues bien, por cuanto a la regulación en España, la AEPD (2020b) y la APDCAT (2020) no han dudado en acudir al genérico artículo 3 de la Ley Orgánica 3/1986, de 14 de abril. Asimismo, los artículos 5, 9 y 84 de la Ley 33/2011, de 4 de octubre, General de Salud Pública contienen genéricas habilitaciones para el control de pacientes, la comunicación de datos y otras afectaciones de derechos que pueden valer también para la protección de datos. De modo más concreto, el artículo 16, 3.º de la Ley 41/2002 de autonomía del paciente regula el acceso concreto y motivado por profesional sanitario en caso de riesgos graves de salud. Asimismo, la legislación ordinaria excepcional de protección civil puede en su caso ser igualmente proyectable. En la última revisión cabe destacar, de un lado, la Orden SND/404/2020, de 11 de mayo, de medidas de

3. Alberto Sáiz, 2017, págs. 40 y sigs.; Grupo de trabajo del artículo 29, Dictamen 5/2014.
4. EDPB en un documento más informal al inicio y más concreto después, Supervisor Europeo de Protección de datos SEPD, Comisión Europea en sus dos documentos, posiblemente los más definidos y concretos. También en Reino Unido en primer lugar el ICO y luego sucesivas autoridades nacionales.

vigilancia epidemiológica dirigida a la adecuación de sistemas informáticos y los tratamientos y comunicaciones de datos, que se legitiman por «interés público esencial en el ámbito específico de la salud pública [...] y para la protección de intereses vitales» (art. 9). No parece que dicha norma infralegal fuera la más adecuada. En este sentido, y con mayor importancia a inicios de junio, destaca el Real Decreto-ley 21/2020, de 9 de junio de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por la COVID-19. Esta norma con fuerza de ley dedica un capítulo a la detección, control y vigilancia. Por lo que aquí interesa, se impone la obligación de facilitar al sector de salud información y datos de contacto para la trazabilidad a «establecimientos, medios de transporte o cualquier otro lugar, centro o entidad pública o privada en los que las autoridades sanitarias identifiquen la necesidad de realizar trazabilidad de contactos». Todo ello bajo la legitimación del «interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y de otras personas físicas». No hay delimitación concreta de datos, finalidades muy específicas, previsión de reutilización, ni siquiera para la investigación. Tampoco hay previsiones específicas respecto de las garantías o medidas de seguridad. No se da cobertura alguna a pasaportes biológicos y, especialmente, a aplicaciones de rastreo. Aunque se brinda cierta cobertura legal, ciertamente no es la respuesta legal que sería precisa en España y a buen seguro no pasaría el tamiz del Consejo Constitucional francés, por ejemplo, ni las especificaciones europeas. Más preocupante si cabe es para Cataluña su Decreto Ley 27/2020, de 13 de julio, que en su *escondido* Anexo III permite obligar a "registrar a los asistentes" a lugares de culto y "todas las reuniones tienen que registrar a los asistentes", para su posible cesión. Todo ello sin mayor concreción o garantía.

Además de la referida legitimación del RGPD y la base legal nacional, en el caso del uso de IA y *big data* para la investigación y lucha contra la COVID-19 hay que tener en cuenta el régimen claramente favorable a la investigación biomédica (artículos 5, 9 y 89 del RGPD) y prestar especial atención a la LO 3/2018 en el artículo 9 y especialmente su disposición adicional 17.ª[5]. Este régimen facilita la investigación de la COVID-19 por parte del sector público y privado con legitimación sin consentimiento directo, así como las cesiones de datos de fuentes variadas para usos secundarios y reutilización en «líneas» o «áreas» de investigación afines en lucha contra la COVID-19. Ello, no obstante, bajo garantías de minimización, seudonimización, confidencialidad, separación funcional e incluso de participación de comités de ética e informes particulares del DPD. Aunque no solo, hay que tener sobre todo en cuenta su apartado c 2.º, que permite únicamente a autoridades e instituciones públicas sanitarias estudios de salud sin consentimiento «en situaciones de excepcional relevancia y gravedad para la salud pública», como es el caso[6].

Más allá de la necesidad del consentimiento, hay que centrarse en el cumplimiento normativo y sus garantías. El EDPB recuerda que, «incluso en estos tiempos excepcionales, el responsable y el encargado de datos deben garantizar la protección de los datos personales de los interesados» con el cumplimiento de los principios de proporcionalidad, limitación al período de emergencia y a los fines específicos y explícitos e información transparente –incluyendo el tiempo de retención–, así como implementar las medidas de seguridad y políticas de confidencialidad adecuadas, que deben documentarse apropiadamente (EDPB, 2020). En la misma dirección, la AEPD (2020a) insiste en que hay que controlar solo aquellos datos que sean verdaderamente necesarios para la finalidad, «sin que pueda confundirse conveniencia con necesidad». Asimismo, hay que evitar innecesarias comunicaciones a terceros, «como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines» (considerando 54) (AEPD, 2020b, pág. 7). Sin perjuicio de la base legal y la no necesidad de consentimiento, se ha de seguir el régimen general de protección –principios, legitimación del tratamiento, transparencia, derechos, responsabilidad proactiva y privacidad– en el diseño o el régimen de las transferencias internacionales de datos. Igualmente, y por defecto, se exigirá el estudio de impacto. Será necesaria la articulación de un buen entramado jurídico entre responsables, corresponsables, encargados y todos aquellos sujetos que participan en la compleja cadena de valor de la IA que garantice el cumplimiento normativo y las distintas responsabilidades.

5. Sobre el tema cabe seguir los estudios de A. Troncoso o R. Martínez y, en especial, el ya citado monográfico de Revista de derecho y genoma humano, núm. extra 1, 2019.
6. Entre otros, Dictamen Autoridad Catalana de Protección de Datos CNS 15 y el 18/2019 y el «Informe 073667/2018», de la AEPD.

Además, el uso de la IA respecto de los humanos es el ámbito potencial de proyección del «derecho» a no ser sometido a decisiones automatizadas reconocido en el artículo 22 del RGPD de la UE con las garantías añadidas que implica (Cotino, 2019b). Tanto el Grupo de trabajo del artículo 29-UE (2018, págs. 35, 37-38) como la AEPD (2020a) van detallando las garantías del cumplimiento normativo respecto de la IA y las decisiones automatizadas, que no solo son relativas al derecho a expresar e impugnar decisión o las reforzadas garantías de transparencia (artículos 13. 2.º f, 14. 2.º g y 15. 1.º h del RGPD). En cuanto al ámbito de salud, este «derecho» emanado del artículo 22 también supone una prohibición más intensa de tratamientos automatizados si estos se basan en datos especialmente protegidos. No obstante, el consentimiento explícito o una legislación específica en razón de un «interés público fundamental» pueden levantar esta prohibición (artículo 9. 2 a y g del RGPD).

Igualmente, el empleo sanitario de la IA es sin duda un uso de alto riesgo para el Libro blanco de la IA de la Comisión Europea (2020, págs. 21 y sigs.). En estos casos se deben cumplir más severamente las garantías; y tanto es así que se prevé un sistema de control previo.

Además, si se trata del uso público de la IA por parte de los poderes públicos, habrá que modular y, por lo general, intensificar muchas garantías, tal y como hemos perfilado desde 2019 en la Red de Derecho Administrativo e IA (DAIA)[7] y en diferentes monografías[8], así como en otros estudios de Cerrillo (2019), Boix (2020) o Sierra (2020).

La reciente sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya (C / 09/550982 / HA ZA 18-388) es un buen recordatorio de que sí que se puede utilizar la IA para finalidades públicas, si bien bajo fuertes garantías de transparencia y caja blanca frente a la opacidad (Cotino, 2020b). De igual modo, deben darse garantías de separación funcional, control y auditorías independientes, seudonimización o confidencialidad.

En la revisión de este estudio, hay que destacar la regulación del tratamiento de datos frente a la COVID-19 en Francia de 9 de mayo[9] y su admisibilidad por el Consejo Constitucional (2020) el 11 de mayo. El extenso artículo 11 (1.500 palabras) regula los tratamientos de datos determinando claramente cuatro finalidades: identificación de personas infectadas y en riesgo de infección, orientación y apoyo, y vigilancia epidemiológica e investigación). Expresamente «Se excluye de estos propósitos el desarrollo o despliegue de una aplicación informática destinada al público y disponible en equipos móviles que permita informar a las personas que han estado cerca de personas diagnosticadas con COVID-19». Los tratamientos serán por el tiempo estrictamente necesario o como máximo seis meses para tratar y comunicar datos sin consentimiento por el sistema de información de salud y distintas entidades. Se señala un plazo de conservación de tres meses, hasta seis. Hay remisiones al desarrollo reglamentario, pero no en blanco, así como prescripciones de información y control parlamentario. El Consejo Constitucional da una amplia respuesta (núm. 59-82) a las diversas alegaciones de inconstitucionalidad y es prácticamente favorable a toda la regulación. Se pone de manifiesto del valor de la salud, señala que expresamente se excluye el desarrollo de *app* de este precepto (por lo que no hace valoración alguna sobre el tema), considera bien delimitados los datos a recabar, comunicar y utilizar y todos acordes a cada finalidad. Se admite igualmente como adecuado quiénes serán los cesionarios de los datos y se aceptan las remisiones reglamentarias. También se reputan como suficientes las garantías para la subcontratación y, especialmente de interés, se recuerda que esta regulación especial no exime del régimen jurídico general europeo y francés respecto de garantías, seguridad, derechos, transferencias, etc. Asimismo, se reafirman las competencias de la CNIL (autoridad francesa de datos), así como las atribuciones de las distintas autoridades, sin perjuicio del control parlamentario. Es más, para dicho control parlamentario no procede la remisión de datos personales sensibles. Se trata de un referente importante tanto la regulación legal, como la constitucionalidad de las diversas medidas a adoptar.

7. Ver las conclusiones de Toledo de 1 de abril (http://links.uv.es/PHAPt3l) y la declaración final de Valencia de 24 de octubre (http://links.uv.es/e2w7MCR).
8. Monográficos de la Revista general de Derecho Administrativo, núm. 50 (febrero de 2019) y de la Revista catalana de derecho público, núm. 58 (2019).
9. Ley que extiende el estado de emergencia de salud hasta el 10 de julio y complementa sus disposiciones, http://www.assemblee-nationale.fr/dyn/15/textes/l15t0418_texte-adopte-seance

4. *Apps*, pasaportes biológicos electrónicos, sistemas de geolocalización, trazabilidad y monitoreo de personas frente a la COVID-19

Preocupa sobre todo la captación y tratamiento masivo de datos especialmente protegidos (incluso *hipodérmicos*, en términos de Harari), así como de metadatos, datos de geolocalización y de tráfico a través de webs, plataformas y aplicaciones, principalmente aplicaciones creadas como medida frente al coronavirus. Siguiendo el caso de China, se especula con pasaportes biológicos electrónicos en razón de estas aplicaciones. Tales herramientas pueden resultar muy útiles para gestionar las relaciones, contactos y movilidad de los afectados o para controlar el cumplimiento de confinamientos generales y particulares, así como la ubicación de enfermos y contagiados. Además de para el control sanitario, y en su caso de seguridad, también puede ser esencial para la previsión y asignación de servicios de salud, sociales y de cualquier otro tipo. De igual modo, los sistemas y aplicaciones informáticas podrían posibilitar el autodiagnóstico a través de la introducción de datos o a partir de los datos captados directamente de los terminales y aplicaciones, implementar evaluaciones para saber si procede hacer test, aconsejar la permanencia en casa o acudir al ambulatorio o al hospital, entre muchos otros servicios. Estas herramientas también pueden servir para liberar servicios de atención.

Además de las finalidades anteriores, estos tratamientos y aplicaciones pueden ser una fuente de *big data* muy variada de la que extraer información y conocimiento para la investigación frente a las consecuencias de la COVID-19.

Como señalamos al inicio, según cómo estén configuradas, estas aplicaciones son capaces de extraer información *hipodérmica*, al tiempo que efectuar tratamientos profundos de datos. Es esencial fijar lo que se pretende de modo concreto, ya se trate de tratamientos informativos, asesoramiento, autodiagnóstico, diagnóstico médico y farmacológico, prestación de servicios sociales y médicos, o medidas de control (barreras de acceso a servicios de transporte, establecimientos o actividades económicas y laborales), incluidas posibles medidas de control administrativo, policial e incluso penal. Obviamente ello puede ser muy relevante para determinar el impacto y graduar las garantías, medidas de seguridad y deberes de transparencia.

Entre las *apps* vinculadas con la COVID-19 destacó Corea del Sur (*app* pública *self-quarantine safety protection*, o privadas: *Corona 100m, Corona map* o *Corona Alert*). Y, por supuesto, el control social chino previo y especialmente posterior a la pandemia. Además de aplicaciones, Google ha facilitado alguna información de movilidad comunitaria[10] y muy posiblemente las grandes plataformas cuenten con datos muy profundos que podrían ser de total interés para hacer frente a la presente pandemia. En España, desde los poderes públicos, también ha habido tempranas iniciativas autonómicas en cascada: *CoronaMadrid*; *Stop COVID-19 CAT* en Cataluña; *Salud Responde* en Andalucía; *Test COVID-19* en Castilla y León; *CoronaTest* en Navarra; *COVID-19.EUS* en Euskadi; web Coronavirus Sergas en Galicia, o *coronavirusautotest.san.gva.es* en la Comunidad Valenciana, entre otras. Aunque pueden haber implicado una captación de datos, se trata de iniciativas básicamente informativas. En todo caso, el Estado, a finales de marzo, inició sus pasos con la Orden SND/297/2020, de 27 de marzo, que encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SGAD) «el desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos». Sus finalidades parecen bastante limitadas a la «autoevaluación», «ofrecer información» y dar «consejos» y «recomendaciones», en ningún caso «diagnóstico» o «prescripción». Así, el Gobierno lanzó en abril *AsistenciaCOVID-19* para el autodiagnóstico, se encomendó una web informativa y el desarrollo de *chatbot* para ser utilizado por aplicaciones de mensajería tipo WhatsApp (apartado 1.º)[11] y se dispuso *Hispabot-Covid19*[12]. En cuanto al más sensible tema de la geolocalización se pretende «contar con información real sobre la movilidad de las personas en los días previos y durante el confinamiento» para «ver cómo de dimensionadas están las capacidades sanitarias en cada provincia» y «a los solos

10. https://www.google.com/Covid19/mobility/
11. https://asistencia.Covid19.gob.es/; https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2020/060420-asistencia-Covid19.aspx
12. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2020/080420-consulta.aspx

efectos de verificar que se encuentra en la comunidad autónoma en que declara estar» (apartado 1.º). También a través del INE se pretende, junto con los operadores, «el análisis de la movilidad de las personas en los días previos y durante el confinamiento» (apartado 2.º).

Está bien claro que con aquella orden no está «vaciándose de contenido» el derecho de protección de datos (Piñar, 2020) y que estábamos «muy lejos del apocalipsis orwelliano» (Martínez, 2020b). Era sólo un primer paso que debía haber venido acompañado de una cobertura legal. Y en la ley es donde han de recogerse usos y finalidades de esta u otras herramientas, incluso para el control de la salud, de la seguridad, laboral, etc. Además, y de especial importancia, hay que hacer un seguimiento de los datos que se están introduciendo y su posible comunicación y reutilización con las garantías oportunas.

En abril de 2020 el SEPD (2020b) abogó por un «European model *COVID-19 mobile application*». En la misma dirección y con mayor concreción, el 8 de abril la Comisión Europea (2020 b) recomendó la rápida adopción de tecnologías, la implicación de los estados y las autoridades europeas de protección de datos. Con una visión claramente garantista se insiste (núm. 10) en limitar estrictamente los tratamientos y datos empleados, revisar continuamente lo que se haga garantizando su terminación con la evolución de la pandemia y la destrucción irreversible de los datos salvo «su valor científico» a criterio de los consejos de ética y autoridades de datos. El núm. 16 concreta diversas garantías de la privacidad y opciones técnicas (*bluetooth*, cifrado, seguridad, ciberseguridad, finalización de las medidas cuando la pandemia esté bajo control, anonimato, transparencia). En esta línea ya destacaban iniciativas cooperativa y abiertas, como la *Pan-European Privacy-Preserving Proximity Tracing Project* (www.pepp-pt.org) centralizada, con sede en Alemania (aunque no empleada por ese país) y, en paralelo, iniciativa descentralizada y con sede en Suiza, el protocolo DP3T. Ambos protocolos confieren muchas garantías y normalización técnica interoperable. A la iniciativa PEPP-PT se sumó inicialmente la SGAD desde el 13 de abril[13], si bien finalmente parece haber apostado por el protocolo DP3T integrado con APIs Apple y Google. Esta línea es la seguida por Suiza, Austria, Estonia, Finlandia o Alemania. La mala experiencia de desarrollos propios no fácilmente integrables, como Reino Unido, pueden haber influido esta opción. Francia, aunque expresamente no ha regulado específicamente el desarrollo de una *covapp*, en mayo lanzó su app propia con el aval de su autoridad de datos (CNIL)[14]. Todo hay que decir que ya en julio, el desarrollo español parece ser un fiasco[15] (Radar Covid se puede descargar desde el 14 de julio) en contraste con aplicaciones masivamente descargadas como la alemana.

El 17 de abril de nuevo la Comisión (2020 c) concretó sus «orientaciones sobre las aplicaciones móviles» posiblemente en el documento más concreto desde las instituciones. Terminado este estudio, la AEPD (2020 d) en mayo de 2020 ha analizado el uso de apps, discerniendo entre las Apps para autotest o cita previa, las de información voluntaria de contagios (COVapps). Por lo general se aprecian positivamente si no se aprovechan para acumular y acceder a datos. Mayor atención implican las *apps* de seguimiento de contactos por *bluetooth* (*Contact trace apps*) por la realización de mapas de relaciones entre personas, reidentificación por localización implícita y la posible fragilidad de los protocolos que emplean. Se muestra escéptica sobre la eficacia de estos sistemas en general.

Finalizado este estudio, a fines de mayo, el Estado español anunció la puesta en marcha de app *Asistencia COVID-19* en junio[16]. Esta *app* (finalmente llamada Radar Covid) se integra bajo las APIs desarrolladas por Apple y Google y bajo el protocolo D3PT y no el inicialmente indicado PEPP-PT. Ello ha generado preocupación, al punto que la AEPD ha afirmado el inicio de «actuaciones de investigación su valor científico» de la *app*[17] y ha realizado actividades para conocer de cerca el protocolo D3PT[18].

13. https://twitter.com/SEDIAgob/status/1249610155408449537
14. https://www.cnil.fr/fr/lapplication-mobile-stopcovid-en-questions
15. De especial interés, MÉNDEZ, M. A. "El fiasco de España con la 'app' de rastreo del covid nos deja tres amargas lecciones" https://blogs.elconfidencial.com/tecnologia/homepage/2020-06-21/app-rastreo-contactos-covid-canarias-carme-artigas-sedia-sanidad-fernando-simon_2644739/
16. https://asistencia.covid19.gob.es/
17. https://twitter.com/AEPD_es/status/1263475663887044609
18. Así, cabe seguir la exposición del protocolo para la AEPD por Carmela Troncoso en mayo https://t.co/IKFON9jjfG?amp=1

Hay que esperar la coordinación y supervisión permanente de las autoridades de protección de datos y el EDPB. Sin perjuicio de las iniciativas públicas, el 10 de abril Google y Apple anunciaron que integrarán sus sistemas operativos con los dispositivos para que los usuarios no tengan que buscarlas, aunque sí consentir en su descarga y uso. Y lo que es mucho más importante, que van a «habilitar una plataforma más amplia de rastreo de contactos basada en Bluetooth», preferidas a las que usan GPS (Islandia, Canadá, China o Corea del Sur). No obstante, se prevé en todo caso su integración en «un ecosistema más amplio de aplicaciones y autoridades sanitarias gubernamentales», bajo «privacidad, la transparencia y el consentimiento»[19]. Pues bien, a fines de abril ya pusieron a disposición su tecnología. Como era previsible, no pocos países, incluido España desde inicio de mayo han confirmado la adopción e integración en las API de la *app* desarrollada.

5. Cuestiones específicas que suscitan legitimación, regulación legal de calidad y la dudosa voluntariedad de estas aplicaciones

Estas aplicaciones generan interrogantes jurídicos más allá de los generales, especialmente por los datos de geolocalización y la trazabilidad de los individuos. Además del RGDP converge la particular normativa de telecomunicaciones. El SEPD afirma que hay que «usar solo datos anónimos para mapear movimientos de personas». El EDPB (2020a) parte de que los datos de localización solo pueden ser utilizados por el operador cuando se hacen anónimos o con el consentimiento de las personas. No obstante, admite que, si no son útiles los datos anónimos o no se cuenta con el consentimiento, cabe aplicar la excepción de seguridad del artículo 15 de la Directiva 2002/58/CE de privacidad y comunicaciones, que permite a los Estados comunitarios adoptar disposiciones legales como «medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional». El EDPB (2020a, apartado 1.º) admite incluso medidas invasivas –como el «rastreo»– en circunstancias excepcionales y en función de las modalidades concretas del procesamiento. En todo caso, insiste en la obligación de «establecer las salvaguardias adecuadas»: minimización y proporcionalidad, el menor impacto posible con relación a la finalidad, garantías, recursos ante autoridades y recursos judiciales, medidas todas restringidas «estrictamente a la duración de la emergencia». En la misma línea el SEPD (2020b) insiste en que «la legalidad, la transparencia y la proporcionalidad son esenciales» y recuerda que «los grandes datos significan una gran responsabilidad».

Hay que tener en cuenta los límites y garantías de la excepción del artículo 15 de la Directiva 2002/58/CE y especialmente hay que seguir el análisis del Grupo de trabajo del artículo 29 (2016, págs. 7-12), en el que se destilaron las «garantías esenciales europeas» frente a medidas de vigilancia en transferencias electrónicas de datos, en síntesis: a) «que el procesamiento se base en normas claras, precisas y accesibles»; b) «demostración de la necesidad y la proporcionalidad con respecto a los objetivos legítimos que se persiguen»; c) «existencia de un mecanismo de supervisión independiente», así como d) «disponibilidad de recursos efectivos para el individuo». A ello hay que añadir que la excepción del artículo 15 no permite (en la lucha contra la delincuencia) «la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica» (STJUE, Gran Sala, de 21 de diciembre de 2016, asuntos C 203/15 y C 698/15).

Es preciso dotar de base legal de calidad y con garantías a estas futuras aplicaciones. El referido artículo 15 permite a los Estados «adoptar medidas legales» adecuadas. Según vimos más arriba, los artículos 6.2 c y 9 apartado 2.º del RGPD también abren la puerta a regulaciones legales. Así pues, hay que acudir de nuevo al muy genérico artículo 3 de la Ley Orgánica 3/1986 (que menciona expresamente la Orden SND/297/2020, de 27 de marzo) y a otra legislación relativa a salud y protección civil. Pero en este caso es mucho más problemático. Con ocasión de la crisis de la COVID-19, he tenido ocasión de analizar detenidamente el Derecho excepcional ordinario tanto de salud como de protección civil, que desarrolla el deber constitucional fundamental del artículo 30, apartado 4.º, de la CE y ha-

19. https://www.apple.com/es/newsroom/2020/04/apple-and-google-partner-on-Covid-19-contact-tracing-technology/

bilita para adoptar medidas restrictivas de derechos, en ocasiones muy indefinidas (Cotino, 2020a). Se dan insuficiencias constitucionales en esta legislación por cuanto pueden implicar severas restricciones de derechos muy genéricas. Hay que considerar que, para la adopción de medidas colectivas y generalizadas de impacto e intromisión en derechos –como es el lanzamiento de aplicaciones y herramientas para el tratamiento masivo de datos personales que afectan a las personas y que han de permanecer en el tiempo– es imprescindible una acción legislativa que legitime democráticamente la restricción, a ser posible con el correspondiente debate y deliberación social. No sería oportuna –ni bastaría– una legitimación con la intervención judicial inmediata *expost* que regula el artículo 8 apartado 6.º de la Ley 29/1998, de 13 de julio (Salamero, 2020), que se mantiene en general bajo el Decreto de alarma 463/2020, de 14 de marzo (disposición final 1.ª). No está pensada para ejecutar medidas no urgentes y de afectación de derechos no individualizados.

Para la regulación, valdrían las normas con valor de ley de derecho constitucional de excepción (artículo 116 de la CE: declaración de alarma, excepción y sitio (ATC 7/2012, FJ 9.º). Como no cabe suspensión del artículo 18 apartados 1.º y 4.º de la CE en ningún caso estas normas excepcionales podrían afectar al contenido esencial de estos derechos. Según el contenido a regular, puede dudarse si bastaría una ley ordinaria o un decreto ley. La excepcionalidad de la pandemia y la clara tolerancia por parte del TC (Cotino, 2020c) pueden justificar el uso del decreto ley. En todo caso, la ley (y no el reglamento) debe contener los elementos básicos, los requisitos de la restricción de derechos y, principalmente, las garantías. Además de las exigencias del artículo 23 del RGPD, precisamente respecto de restricciones en el ámbito de datos sensibles, la reciente STC 76/2019, de 22 de mayo (FJ apartado 8.º) sobre perfilado de datos por partidos políticos ha sido especialmente exigente en cuanto a las garantías y calidad de la ley limitadora de derechos fundamentales y las posibilidades de apoderar a un poder público para restringir derechos. El mandato de calidad «no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares». Asimismo, en el caso de ser aplicable, deben tenerse en cuenta los mínimos del artículo 41 apartado 2.º de la Ley 40/2015.

Pero, más allá de la base legal, hay que prestar atención a la voluntariedad y consentimiento del interesado en estos sistemas.

En España y en la UE desde el inicio se habla de aplicaciones voluntarias, por ejemplo, la Comisión Europea insiste en «garantizar que la persona siga teniendo el control», acompañado de garantías de transparencia y derechos (2020 c) 3.2). Se afirma que para la legitimación «el consentimiento [...] sería la justificación más adecuada». La eficacia de estas herramientas dependerá de su uso masivo y, si no lo hay voluntariamente, no hay que descartar su obligatoriedad sobre la base de una clara legalidad. Asimismo, hay que ser cautos respecto de esta «voluntariedad». En razón del artículo 7 apartado 4.º del RGPD y la doctrina continuada del Grupo de trabajo del artículo 29 –y como ha señalado la AGPD– salvo excepciones «la base jurídica del tratamiento en las relaciones con la Administración (...) no sería el consentimiento del interesado», siendo además que no cabe el interés legítimo (AEPD, 2018, I. Conclusión). No obstante, la voluntariedad real de los interesados en el uso de aplicaciones puede ser un elemento de importancia en cuanto al impacto y las garantías compensatorias precisas. Viendo el pasaporte biológico que utilizó China, en ningún caso sería válida la legitimación por consentimiento si la instalación de la aplicación, su uso y transmisión de datos es condición para la prestación de servicios sociales, de salud, transporte, acceso a actividades y establecimientos. La Comisión señala que «no debería haber ninguna consecuencia negativa para el usuario» (2020 c) 3.3). Para eludir el consentimiento sería precisa una legitimación legal especialmente intensa. Con respecto a las aplicaciones privadas, Google y Apple parten del consentimiento, que legitima tanto el tratamiento de datos sensibles (artículo 9 apartado 2.º a) del RGPD) como los perfilados y tratamientos automatizados (artículo 22 apartado 4.º del RGPD). No obstante, habrá que estar vigilantes. Si este tipo de *apps* privadas se consideran peligrosas cabría incluso una prohibición por ley (artículo 9 apartado 2.º de la LO 3/2018). Especialmente respecto de webs y *apps* privadas la AEPD (2020b) advirtió pronto de los riesgos de facilitar datos sensibles a estas plataformas y herramientas, «incluso en aquellos casos en los que aparentemente esos datos no se asocian a la identidad del usuario que utiliza la aplicación», pues podrían producirse importantes carencias de transparencia y delimitación de finalidades.

6. El diablo está en los detalles: garantías específicas exigibles en el diseño de estas aplicaciones

Según hemos visto, más allá de considerar si en principio se pueden utilizar aplicaciones y rastreos frente al COVID-19, hay que determinar exactamente *para qué* se quieren emplear. A partir de ello, la clave es *cómo* se hace. Desde la finalización y entrega de este estudio no han sido pocos los documentos que han ido concretando estos aspectos por instituciones y organizaciones, con más precisión por parte de la Comisión Europea (2020 b y c) o el SEPD (2020 c) y no tanto por la AEPD (2020 d).

La anonimización es esencial, pero, como esta no será completa, resultará ineludible el cumplimiento del régimen de protección de datos con sus principios y garantías, la privacidad y, por defecto, la evaluación de su impacto. Reforzar la transparencia de los perfilados y tratamientos automatizados es clave para la confianza social. Y lo mismo podría decirse para el sector público con respecto al inventario de actividades (artículo 31.2 de la LO 3/2018).

Anonimizar no es «simplemente eliminar identificadores obvios como números de teléfono y números IMEI». En este sentido, «el uso de identificadores temporales de radiodifusión y de la tecnología *Bluetooth* para el rastreo de contactos parece ser una vía útil para lograr la protección efectiva de la intimidad y de los datos personales» (SEPD, 2020a). No obstante, como veremos, sí que es muy posible la minimización, principalmente a través de la seudonimización y la separación de acceso a datos de los distintos sujetos participantes en la cadena de valor (responsables de las *apps*, sistemas operativos, terminales, operadores, etc.). La minimización es, sin duda, un elemento de garantía esencial como se ha subrayado desde el inicio y que ha especialmente en conexión para el rastreo de contactos y de alertas sobre la base de la distancia y duración de los contactos, señalando que la tecnología *Bluetooth* de baja energía (BLE) parece ser la más precisa y no permite el rastreo, a diferencia de la geolocalización, por lo que la recomienda, además de que no se almacene «ni el momento exacto ni el lugar del contacto», pero sí el día del contacto para determinar síntomas y medidas a adoptar (Comisión Europea 2020 c) 3.4).

Habrá que ser extremadamente cautos respecto de las cesiones de los datos que se *absorban* a través de estas *apps*. Para que estas aplicaciones o sistemas informáticos puedan nutrir de *big data* a la investigación biomédica contra la COVID-19, como prevé el sistema PEPP-PT, será de especial interés prever cesiones de datos para la investigación biomédica y los detalles de seudonimización. Así se complementaría o reforzaría la cobertura legal que para ello puede brindar la Disposición adicional 17.ª apartado 2.º de la LO 3/2018.

El SEPD (2020a) señala que incluso si se trata de datos anónimos hay obligaciones de seguridad relativas a la información y la confidencialidad que deben mantenerse si se acude a terceros encargados (operadores, desarrolladores, etc.). La Comisión Europea es más concreta si cabe (2020 c) 3.8) exigiendo «las técnicas criptográficas más avanzadas» y si hay un servidor central, el acceso al mismo bajo registro previo. El almacenamiento de los datos «cifrado y pseudonimizado» y que «todas las transmisiones desde el dispositivo personal a las autoridades sanitarias nacionales deberían cifrarse».

Si se trata de iniciativas del sector público será plenamente aplicable el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y su Anexo. A falta de definir y concretar la aplicación, finalidades, funcionamiento e impacto, es muy posible que haya que exigir un nivel de seguridad alto en las dimensiones de confidencialidad y trazabilidad y un nivel medio en las restantes (disponibilidad, autenticidad e integridad). Asimismo, es probable que haya que concretar la excepción de la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018 a fin de permitir la posibilidad de utilizar datos y metadatos para otras finalidades.

Apple y Google (2020) desde inicio de abril anunciaron las especificaciones técnicas de su propuesta, inicialmente inspirado en el protocolo DP-3T, al que finalmente se ha sumado el Gobierno español y no como inicialmente en abril a la también sólida iniciativa europea PEPP-PT. Estas iniciativas suponen un sistema de aplicaciones que detectan proximidad con otros posibles infectados con Bluetooth y calcula riesgos individuales de contagio por exposición a personas infectadas, pero manteniendo la información anónima. La diferencia de los protocolos es que PEPP-PT carga registros de los contactos en un servidor central de informes y con DP-3T el servidor central no accede a

los datos ni es quien los trata e informa a los usuarios del contacto. Hay debate sobre la eficacia de un sistema más o menos centralizado. Expertos han concluido que los ataques contra sistemas descentralizados son indetectables y, por el contrario, los sistemas centralizados permiten medidas de seguridad y auditoría más fuertes, aunque al parecer tampoco del todo seguros (Vaudenay, 2020).

Los detalles recogidos en el Libro blanco (AA.VV., 2020, págs. 2-3 y 29) no se pueden aquí más que abreviar en lo esencial: se certifica la seguridad y cumplimiento normativo bajo código abierto auditable y transparente. El sistema está preparado para implementarse en cada país y para su interoperabilidad. Se «insta firmemente» a adoptar un sistema descentralizado y a que se almacenen datos anonimizados con identificaciones efímeras y seudoaleatorias. Estos datos se utilizan para la investigación. Cuando hay una declaración de infección, entonces se recaban los datos almacenados para las alertas. En todo caso, los «datos siempre permanecen en los teléfonos de los usuarios y el cálculo del riesgo se realiza localmente». No hay un *backend* centralizado a la asiática, que facilitaría el control social: el servidor central solo tiene los identificadores anónimos de los no infectados. Además de eliminar datos en catorce días, el sistema se desmantelaría a sí mismo elegantemente (*graceful dismantling*) conforme se dejara de usar. Cabe apuntar que ante las dudas de seguridad y suspicacias que puedan generarse (como en Noruega), en Francia se acudió a una comunidad de *hackers* éticos (*Yeswehack*) que han examinado la *app* antes que su lanzamiento. El tema, sin duda, exigirá un análisis continuo de expertos, sociedad civil y autoridades de datos.

Referencias bibliográficas

AA.VV. (2020). *Decentralized Privacy-Preserving Proximity Tracing. White Paper* (versión del 25 de mayo de 2020), págs. 2-3 y 29. https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

AEPD (2018). «Informe 175/2018, noviembre, sobre investigación biomédica».

AEPD (2020a). «Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial» (febrero). https://www.aepd.es/media/guias/adecuacion-rgpd-ia.pdf

AEPD (2020b). «Informe 20/2020, de 12 de marzo, en relación con los tratamientos de datos resultantes de la actual situación derivada de la extensión del virus COVID-19» https://www.aepd.es/es/documento/2020-0017.pdf

AEPD (2020c). «Comunicado de la AEPD en relación con webs y apps que ofrecen autoevaluaciones y consejos sobre el coronavirus» (16 de febrero). https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-de-la-aepd-en-relacion-con-webs-y-apps-que-ofrecen

AEPD (2020 d). «El uso de las tecnologías en la lucha contra el Covid19. Un análisis de costes y beneficios». Mayo de 2020, https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf

ALBERTO SÁIZ, C. (coord.) (2017). *Código de buenas prácticas en protección de datos para proyectos de* Big Data. AEPD e ISMS Forum, págs. 40 y sigs. y especialmente Grupo de trabajo del artículo 29: *Dictamen 5/2014, de 10 de abril*, sobre anonimización.

ALCALDE BEZHOLD, G.; ALFONSO FARNÓS, I. (2019). «Utilización de tecnología *Big Data* en investigación clínica». *Revista de derecho y genoma humano*, núm. extra 1, págs. 55-83.

APDCAT (2020). «Nota en relación a los tratamientos de datos personales relacionados con las medidas para hacer frente al COVID-19» (15 de marzo). https://apdcat.gencat.cat/es/actualitat/noticies/noticia/Nota-en-relacio-amb-els-tractaments-de-dades-personals-relacionats-amb-les-mesures-per-fer-front-al-COVID-19

APPLE-GOOGLE (2020). «Privacy-Preserving Contact Tracing» (abril). https://www.apple.com/Covid19/contacttracing/

BOIX, A. (2020). «Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones». *Revista de Derecho Público: Teoría y Método*, vol. 1, págs. 223-270. https://doi.org/10.37417/RPD/vol_1_2020_33

CERRILLO I MARTÍNEZ, A. (2019). «El impacto de la inteligencia artificial en el derecho administrativo, ¿nuevos conceptos para nuevas realidades técnicas?». *Revista general de Derecho Administrativo*, núm. 50.

COMISIÓN EUROPEA (2020a). *Libro blanco sobre la inteligencia artificial* (19 de febrero). Bruselas: UE, págs. 21 y sigs. https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1

COMISIÓN EUROPEA (2020b). Recomendación (UE) 2020/518 de la Comisión de 8 de abril de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2020.114.01.0007.01.SPA&toc=OJ:L:2020:114:TOC

COMISIÓN EUROPEA (2020c). Comunicación Comisión UE, de 17 de abril (2020/C 124 I/01) orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo

referente a la protección de datos (2020/C 124 I/01). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020XC0417%2808%29

CONSEJO CONSTITUCIONAL (2020). Decisión núm. 2020-800 DC del 11 de mayo de 2020, https://www.conseil-constitutionnel.fr/decision/2020/2020800DC.htm

COTINO HUESO, L. (2019a). «Riesgos e impactos del *big data*, la inteligencia artificial y la robótica y enfoques, modelos y principios de la respuesta del Derecho». *Revista General de Derecho Administrativo*, núm. 50. https://bit.ly/37RifyJ

COTINO HUESO, L. (2019b). «Derecho y garantías ante el uso público y privado de inteligencia artificial, robótica y *big data*». En: BAUZÁ, M. (dir.). *El Derecho de las TIC en Iberoamérica*. Montevideo: FIADI-Thompson-Reuters, págs. 917-952, http://links.uv.es/BmO8AU7

COTINO HUESO, L. (2020a). «Los derechos fundamentales en tiempos del coronavirus. Régimen general y garantías y especial atención a las restricciones de excepcionalidad ordinaria». *IUSTEL* (monográfico «Coronavirus... y otros problemas»), págs. 88-101. www.elcronista.es

COTINO HUESO, L. (2020b). «SyRI, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020». *La Ley Privacidad, Wolters Kluwer,* núm. 2. www.academia.edu.

COTINO HUESO, L. (2020c). «La (in)constitucionalidad de la "intervención", "mordaza" o "apagón" de las telecomunicaciones e internet por el Gobierno en virtud del Real Decreto-Ley 14/2019», de próxima publicación.

EDPB (2020a). «Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak» (20 de marzo). https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-Covid-19-outbreak_en

EDPB (2020 b). Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19 (Abril) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_es

FERRÀS, X. (2020). «Las tres D». *La Vanguardia* (4 de abril). https://www.lavanguardia.com/economia/20200404/48311997448/las-tres-d.html

GERMAN ETHICS COUNCIL (2017). «Big Data and Health: Data Sovereignty as the Shaping of Informational Freedom. Opinion». Berlín: Deutscher Ethikrat. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/opinion-big-data-and-health-summary.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2016). «Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)». WP 237, págs. 7-12. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2018). «Directrices sobre decisiones automatizadas» (6 de febrero), págs. 7-8. https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

HAN, B. CHUL (2020). «La emergencia viral y el mundo de mañana». *El País* (22 de marzo). https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html

HARARI, Y. (2020). «El mundo después del coronavirus». *La Vanguardia* (6 de abril). https://www.lavanguardia.com/internacional/20200405/48285133216/yuval-harari-mundo-despues-coronavirus.html

ICO (2020). «Data protection and coronavirus» (12 de marzo). https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus

MARTÍNEZ, R. (2020a). «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública». *Diario La Ley*, núm. 9.604 (30 de marzo). Wolters Kluwer. https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAmMDc2NjM7Wy1KLizPw8WyMDI6CYoSVIIDOt0iU_OaSyINU2LTGnOBUAZxgvATUAAAA=WKE

MARTÍNEZ, R. (2020b). «Protección de datos y geolocalización en la Orden SND/297/2020». *Expansión* (blog Hay Derecho) (31 de marzo). https://hayderecho.expansion.com/2020/03/31/proteccion-de-datos-y-localizacion-en-la-orden-snd-297-2020/

MONTALVO JÄÄSKELÄINEN, F. (2019). «Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del *Big Data*». *Revista de Derecho Político*, núm. 106, págs. 43-75. https://doi.org/10.5944/rdp.106.2019.26147

ORTEGA GIMÉNEZ, A. (2019). «Implicaciones jurídicas de la internalización de la tecnología del *Big Data* y Derecho Internacional Privado». *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, núm. extra 1, págs. 169-204.

ORTEGA, A.; BALSA-BARREIRO, J.; CEBRIÁN, M. (2020). «Los límites del capitalismo de vigilancia». *El País* (8 de abril). https://elpais.com/elpais/2020/04/07/opinion/1586252351_094192.html

PEDREÑO, A. (2020). «La pandemia constata la hegemonía de Asia frente a Europa en Inteligencia Artificial». *El Independiente* (6 de abril). https://www.elindependiente.com/opinion/2020/04/06/la-pandemia-constata-la-hegemonia-de-asia-frente-a-europa-en-inteligencia-artificial/

PIÑAR MAÑAS, J. L. (2020). «Privacidad en estado de alarma y normal aplicación de la Ley». *Expansión* (blog Hay Derecho) (9 de abril). https://hayderecho.expansion.com/2020/04/09/privacidad-en-estado-de-alarma-y-normal-aplicacion-de-la-ley/

SALAMERO, L. (2020). «COVID-19 y jurisdicción contencioso-administrativa». www.academia.edu.

SEPD (2020a). «Comments to DG CONNECT of the European Commission on monitoring of COVID-19 spread» (25 de marzo). https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_Covid-19_monitoring_of_spread_en.pdf

SEPD (2020b). «EU Digital Solidarity: a call for a pan-European approach against the pandemic» (6 de abril). https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_Covid19_en.pdf

SEPD (2020c). TechDispatch on Contact Tracing with Mobile Applications, 7 de mayo, https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en

SIERRA, S. (2020). «Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la Administración Pública». *Revista General de Derecho Administrativo*, núm. 53.

VAUDENAY, S. (2020). «Centralized or Decentralized? The Contact Tracing Dilemma». *IACR*, mayo https://eprint.iacr.org/2020/531.

Cita recomendada

COTINO HUESO, Lorenzo (2020). «Inteligencia artificial, *big data* y aplicaciones contra la COVID-19: privacidad y protección de datos», *IDP. Internet, Derecho y Política*, núm. 31, págs. 1-17. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3244

Sobre el autor

Lorenzo Cotino Hueso
cotino@uv.es
Catedrático de la Universidad de Valencia

Lorenzo Cotino Hueso (www.cotino.es) es Catedrático de la Universidad de Valencia, Investigador de la Universidad Católica de Colombia (Proyecto "Derecho y Big Data", Grupo de Investigación en Derecho Público y TIC). IP Proyecto I+D+i Retos MICINN "Derechos y garantías frente a las decisiones automatizadas en entornos de inteligencia artificial, IoT, big data y robótica" (PID2019-108710RB-I00, 2020-2022). Ha sido magistrado suplente del TSJ Comunidad Valenciana desde el año 2000 hasta 2019. Doctor y licenciado en Derecho (UVEG), máster en la especialidad de derechos fundamentales en Barcelona (ESADE), licenciado y diplomado de Estudios Avanzados de Ciencias políticas (UNED). Premio Extraordinario de Doctorado, Ministerio Defensa, Ejército, INAP, CAC. Profesor invitado en Konstanz (Alemania) desde 2004 honorario en la Universidad Nacional de Colombia y en la Universidad Católica Cuenca, en Ecuador; con estancias de investigación en Utrech (Países Bajos) y Virginia (Estados Unidos). Investigador principal de quince proyectos de investigación, miembro de otros veintiuno, autor de diez libros y coordinador de catorce, así como de ciento cuarenta artículos o capítulos científicos. Ha impartido más de trescientas ponencias y conferencias. Dirige la red www.derechotics.com desde 2004 y desde 2019 es cofundador de la Red DAIA (Derecho Administrativo de la Inteligencia artificial). Profesor en la Universidad de Alcalá (2005-), en la UOC (2012-) y en la UNIR (2014-). ORCID 0000-0003-2661-0010. http://www.researcherid.com/rid/H-3256-2015.

Universitat Oberta de Catalunya