IMPLICACIONES BIOÉTICAS DEL USO DE DATOS Y *APPS* DE SALUD EN LA PANDEMIA

Itziar DE LECUONA

SUMARIO: I. *Introducción*. II. *Las* Apps *de identificación de positivos y rastreo de contactos.* III. *Hacia un modelo de gestión de datos fiable, accesible e interoperable y que permita su reutilización.* IV. *El pasaporte inmunológico.* V. *La evaluación de la investigación e innovación en salud*. VI. *Conclusiones*. VII. *Fuentes de consulta*.

I. INTRODUCCIÓN

Desde el análisis bioético de la COVID-19, las medidas propuestas para el control de la epidemia han intensificado el debate sobre la protección de la intimidad y la confidencialidad de los datos personales.[1] En España y otros países europeos se han tomado decisiones que han conllevado determinadas restricciones de derechos por razones de interés colectivo, que en ningún caso deberían llegar a anularlos, y que plantean numerosas cuestiones sobre las que reflexionar desde la perspectiva de los principios éticos a aplicar, los derechos e intereses en juego y los mecanismos de garantía, así como el impacto social en personas y sociedades. El uso de datos personales en cualquier ámbito y la tendencia a su monetización en una sociedad de mercado es un signo de nuestro tiempo, situación que debe preocuparnos y ser objeto de análisis. La pandemia ha abierto nuevas oportunidades para la toma de decisiones fundamentada en la explotación intensiva de datos personales y en el contexto de la salud pública, en el que diversas medidas deberían ser temporales y reversibles. En una sociedad altamente digitalizada, las propuestas sobre *Apps*

[1] El trabajo recoge y actualiza las aportaciones efectuadas en la comparecencia de la autora ante la Comisión No Permanente para la Reconstrucción Social y Económica del Congreso de los Diputados en junio de 2020, disponible en: *http://www.congreso.es/portal/page/portal/Congreso/Congreso/Organos/Comision?_piref73_7498063_73_1339256_1339256.next_page=/wc/detalleInformComisiones?idOrgano=390&idLegislatura=14*.

de identificación de positivos y rastreo de contactos, algunas ya implementadas en varios países, o la desproporcionada medida del pasaporte serológico propuesta para la salida del confinamiento, son ejemplos de iniciativas que cuestionan el principio de proporcionalidad y el respeto por los derechos y libertades fundamentales de las personas. El trabajo analiza estas propuestas y también incluye el estudio del modelo de evaluación de los proyectos de investigación e innovación en salud que utilizan tecnologías emergentes como la inteligencia artificial, el *Big Data*, la biometría, entre otras, y para el desarrollo de aplicaciones de salud, y que necesitan tratar datos personales para programar algoritmos. Asimismo, la pandemia por COVID-19 ha evidenciado la falta de infraestructuras públicas para una adecuada gestión de los datos para mejorar la toma de decisiones y entre estas, las políticas.

Esta situación de crisis ha puesto en evidencia los efectos de los recortes sanitarios; la tendencia a la mercantilización y el adelgazamiento de los servicios públicos, acentuando las desigualdades existentes. Tendencia que también ocurre en el ámbito de la investigación en innovación en salud. Bajo el pretexto de la COVID-19 se abren mercados de datos personales disfrazados de investigación e innovación.[2] Se favorece así la participación de terceros, tradicionalmente ajenos a estos procesos de generación y transferencia de conocimiento, con interés en acceder a información personal de distinta índole y que requiere especial protección.

Los datos personales, los datos de salud entre otros, son el oro de nuestro tiempo a la vez que existe una tremenda desafección social por cuidarlos, y por proteger la intimidad propiciada por la falsa gratuidad digital. El valor de los datos personales debe ser objeto de análisis en la era post-COVID-19 en tanto que bien común. Determinados conjuntos de datos personales, y en particular los de salud, no pueden estar al alcance de cualquiera.[3]

El soporte que implica la tecnología digital para transitar hacia una "nueva normalidad" y hasta que lleguen las vacunas, nos puede conducir a un confinamiento digital encubierto sin fecha de caducidad, mediante la institucionalización de prácticas de vigilancia digital de las personas que suscitan cuestiones técnicas, éticas y legales, y con enorme impacto social.

---

[2] De Lecuona Itziar, "La tendencia a la mercantilización de partes del cuerpo humano y de la intimidad en investigación con muestras biológicas y datos (pequeños y masivos)" en Casado, María, (coord.) *De la solidaridad al mercado*, Editorial Fontamara, México, 2016, pp. 267-296, disponible en acceso abierto en *www.bioeticayderecho.ub.edu* (Universidad de Barcelona, 2017).

[3] De Lecuona, Itziar, Villalobos, María José, "El valor de los datos personales de salud en la sociedad digital", en García Manrique, Ricardo (coord.), *El cuerpo diseminado, Estatuto, uso y disposición de los biomateriales humanos,* Editorial Aranzadi, Cizur Menor, 2018, pp. 171-190.

Así el debate no sólo debería centrarse en la protección de la intimidad y la confidencialidad de los datos personales en un contexto de digitalización intensiva. También es preciso promover la autonomía de las personas para tomar decisiones libres e informadas, la equidad y la transparencia. No se puede caer en el error de entender el control de la epidemia como una dicotomía entre libertad o intimidad, porque ésta es falsa.

Las decisiones que se tomen en el marco de la salud pública deben ser proporcionales a los fines que se persiguen, respetuosas con los derechos de las personas, temporales y reversibles. Además, estas decisiones deben estar fundamentadas en la evidencia científica, y no en propuestas tecnológicas proclives a mercados de datos personales disfrazados de buenas intenciones con el pretexto de la COVID-19. Es necesario debatir con urgencia sobre la función del estado, y sobre las tecnológicas y la acumulación de poder, ante el despliegue de sistemas digitales basados en el acceso y correlación de conjuntos de datos personales, para extraer patrones de comportamiento, hacer predicciones y, así, mejorar la toma de decisiones también en el ámbito de la sanidad y la salud pública.

En la sociedad de los datos masivos, la inteligencia artificial y los algoritmos necesitamos nuevas estructuras de gobernanza. Co-crear valor a través de los datos y no extraer valor. El auge de las tecnológicas ha sido posible gracias a que los Estados han creado las infraestructuras necesarias mediante el pago de impuestos por parte de los contribuyentes. Internet y el GPS son ejemplos. Los gobiernos deben garantizar que un valor que se ha creado colectivamente esté al servicio del bien común.[4] Es necesario establecer un modelo de gobernanza que permita alinear los intereses de las personas y la salud pública con los distintos actores desde el diseño de la intervención, durante su desarrollo y en el acceso a los resultados, de acuerdo con la investigación e innovación responsable que Europa propugna.[5] El objetivo es evitar asimetrías y acumulación de poder por parte de los distintos actores, fundamentalmente el Estado y las tecnológicas.

Hace tiempo que Europa decidió crear un mercado único y una sociedad digital guiada por el dato. Se trata de una apuesta política, científica

---

[4] Mazzucato, Mariana, *El estado emprendedor*, Barcelona, RBA Economía, 2019 p. 400. Véase también, Mazzucato, Mariana, *Preventing digital feudalism*, Social Europe, 2019, disponible en: *https://www.socialeurope.eu/preventing-digital-feudalism*.

[5] European Union, *Responsible Research and Innovation - HORIZON 2020*, disponible en: *https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation*, y Casado, María *et al.*, *Declaración sobre integridad científica en investigación e innovación responsable*, Barcelona-Porto, Edicions de la Universitat de Barcelona, 2016, disponible en: *http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08489.pdf*.

y económica basada en la utilización de tecnologías emergentes y la explotación intensiva de conjuntos de datos, incluidos los datos personales, para mejorar la medicina personalizada, para tener sistemas sanitarios más eficientes y un envejecimiento activo y bienestar, entre otras prioridades.[6] Europa apuesta así por una inteligencia artificial confiable,[7] capaz de evitar los prejuicios raciales y de género; pero no depende de las máquinas que sea justa, depende de los datos con los que alimentemos a los algoritmos y de las decisiones resultantes que deben incorporar la corrección humana.

Los datos de salud, genéticos, biométricos, sociodemográficos, entre otros, son datos personales especialmente protegidos, porque lo dicen todo de nosotros y porque podrían ser utilizados con fines no deseados, y dar lugar a discriminaciones encubiertas, con profundas implicaciones para la libertad de las generaciones presentes y futuras. La posesión de conjuntos de datos personales por parte de terceros, sea la iniciativa pública y/o privada, afecta a nuestros derechos en función de los usos, confiriéndoles a estos actores un extraordinario poder sobre nosotros. Las decisiones que se tomen ahora marcarán los proyectos vitales de personas, de colectivos y sociedades.

II. Las *Apps* de identificación de positivos y rastreo de contactos

Las *Apps* de identificación de positivos y rastreo de contactos han cobrado protagonismo desde el inicio de la pandemia para ayudar a su gestión. Se reivindica aquí un modelo más analógico que digital haciendo énfasis en la necesidad de reforzar con carácter urgente la atención primaria y la intervención humana. En este sentido, es necesario no entusiasmarse con el modelo digital que invisibiliza las carencias del sistema analógico, que es tan necesario. Es preciso contar con rastreadores y ello implica contratar personal y recursos que puedan llevar a cabo esta crucial tarea.

Es sabido que el rastreo manual de contactos es una de las principales herramientas para el control de epidemias, pero requiere de una infraestructura y unas dotaciones de personal importantes, y, sobre todo, de una coordinación institucional den el ámbito de la salud pública. En un contexto de crisis económica y de pujante digitalización se han planteado estrate-

[6] European Union, *What can big data do for you?*, disponible en: *https://ec.europa.eu/digital-single-market/en/what-big-data-can-do-you*.

[7] High Level Expert Group on Artificial Intelligence, European Union, *Ethics Guidelines for Trustworthy AI*, 2019, disponible en: *https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai*.

gias para el control de la epidemia mediante la utilización de aplicaciones móviles con el objetivo de automatizar la identificación de positivos y el rastreo de contactos.

Las promesas de eficiencia y ahorro de costes se contraponen a las críticas que el uso de estas herramientas por cuestiones de seguridad y de falta de protección de los datos personales. Algunas de estas aplicaciones establecen el contacto a través de la geolocalización de los individuos y otras mediante tecnología *Bluetooth* que avisa en caso de haber estado en contacto con un positivo de una manera menos intrusiva. También hay diferencias entre las aplicaciones de tipo centralizado, en las que un servidor central procesa la información de los usuarios, o las de tipo descentralizado, donde este proceso se realiza en el móvil de cada usuario. En España, por ejemplo, se ha optado por este último.

Algunos países desarrollaron este tipo de herramientas al inicio de la pandemia, muchos de ellos influidos por previas experiencias de exposiciones a otros virus respiratorios y crisis de salud pública, como en el caso de Singapur y otros países de Asia con contagios por virus como el SARS o el MERS. Sin embargo, el desarrollo e implementación de estas aplicaciones ha sido desigual en los países europeos y no están claras su utilidad real, sus ventajas respecto a los rastreadores y no están exentas de implicaciones éticas, legales y sociales como se ha visto.

Así, las *Apps* de identificación de positivos y rastreo de contactos para controlar posibles rebrotes de la COVID-19, se deben enmarcar en el ámbito de la salud pública y como una herramienta de apoyo, pero no son la solución. La posible utilización de estas *Apps* obliga a reflexionar también sobre la dependencia europea de las tecnológicas estadounidenses y sobre nuestro entusiasmo tecnológico falsamente liberador del virus. Las *Apps* no devuelven la libertad ni aseguran el turismo, o el funcionamiento de la economía, pero sobre todo no pueden concebirse como un modelo de negocio. El Estado tiene que establecer las condiciones para proteger los derechos de los ciudadanos.

Conviene centrar la atención en el factor humano, porque la relación médico-paciente y el sistema sociosanitario son cruciales. Por ello, es necesario fortalecer, como se ha dicho, la atención primaria, la vigilancia epidemiológica y mejorar la gestión de los datos, y hacer las pruebas correspondientes —nunca de forma indiscriminada[8]—. Estas medidas son más adecuadas y menos invasivas que activar el GPS o el *Bluetooth* de nuestros

[8] AMaSaP-SESPAS, *Posicionamiento AMaSaP-SESPAS sobre la realización de test masivos a toda la población en relación con el SARS-CoV-2 (COVID-19)*, disponible en: *https://sespas.*

móviles. Además, se debería fomentar la investigación científica y la investigación sociológica, para conocer los datos de seroprevalencia en la población y diseñar estrategias acordes a los datos más actualizados. Un ejemplo de buenas prácticas es el estudio de seroprevalencia de Instituto de Salud Carlos III y el Instituto Nacional de Estadística, realizado en tres fases en abril, mayo y junio y cuyos resultados fueron presentados en julio de 2020.[9]

Para la identificación de positivos y rastreo de contactos, se debería priorizar la contratación de personal cualificado para realizar estas funciones; que parece más efectiva, fiable y segura que dejarlo en manos de la tecnología digital, por razones éticas, legales y fundamentalmente técnicas. Fomentar las llamadas de teléfono y el seguimiento al estilo tradicional, considerando que no toda la población tiene acceso a internet ni a dispositivos móviles, en particular aquellos más vulnerables. Conviene recordar aquí que el derecho de acceso universal a internet está reconocido en leyes europeas.[10]

Parece poco acertado copiar sistemas implantados en contextos que nada tienen que ver con el nuestro, ni cultural, ni social ni políticamente (Corea del Sur, Singapur o China). Se ha demostrado que para que estas *Apps* sean útiles, se las debe descargar, siempre de forma voluntaria, un porcentaje elevado de personas. La tecnología *Bluetooth*, elegida como la más adecuada para el rastreo no fue concebida para gestionar una pandemia, ni para garantizar la intimidad; puede dar lugar a falsos positivos y negativos, con la consecuente sobrecarga del sistema de salud, y plantea problemas de seguridad y hackeo nada despreciables.[11] Por ello, es mejor apostar por un modelo más analógico que digital, y que la red de rastreo mediante dispositivos digitales por la que se opte esté controlada por el sistema público de salud.[12]

---

es/2020/05/31/posicionamiento-amasap-sespas-sobre-la-realizacion-de-test-masivos-en-relacion-con-el-sars-cov-2-covid-19/.

[9] Instituto de Salud Carlos III, Estudio nacional de sero-epidemiología de la infección por SARS-CoV-2 en España, 2020, disponible en: *https://www.mscbs.gob.es/ciudadanos/ene-covid/docs/ESTUDIO_ENE-COVID19_INFORME_FINAL.pdf*.

[10] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, disponible en: *https://www.boe.es/eli/es/lo/2018/12/05/3*.

[11] González, Juan *et al*, *Abriendo la caja de Pandemia: por qué necesitamos repensar el rastreo digital de contactos*, CYPRIAN: Cibersecurity, Privacy and Anonymity Lab, Universidad de Vigo, 2020, disponible en: *https://www.gradiant.org/wp-content/uploads/2020/05/Informe-Cyprian-contact-tracing_v1-1.pdf*.

[12] Grupo de Trabajo Multidisciplinar sobre la COVID-19 del Ministerio de Ciencia e Innovación, *Análisis del informe de la Academia de las Ciencias de Alemania y su posible aplicabilidad a la situación actual de España*, 2020, disponible en: *https://www.ciencia.gob.es/stfls/MICINN/Ministerio/FICHEROS/Doc_GTM_InformeAcadLeopo ldina_Mayo2020_GTM.pdf*.

No deberíamos haber aceptado que los sistemas operativos de los teléfonos inteligentes incluyan por defecto este tipo de aplicaciones, como así ha ocurrido. En ajustes de su teléfono podrán comprobar que, con la última actualización de software, ya tienen disponible el servicio de Google y Apple "Notificaciones de exposición por COVID-19". La plataforma permite desplegar el sistema descentralizado, al que ya se ha hecho referencia en líneas anteriores. Estas medidas pueden implicar un gran hermano digital a las puertas potenciado por la COVID-19, y no parecen en absoluto temporales, sino que se instalan, nunca mejor dicho, por defecto en las vidas de las personas.

En el caso español, la decisión sobre qué modelo adoptar y cómo probarlo e implementarlo se ha caracterizado por la falta de transparencia. A finales de mayo de 2020 se anunció una prueba piloto en Canarias; pero todavía no hay información suficiente para poder valorar las medidas propuestas y tomar decisiones libres e informadas. Esta opacidad, propia de los negocios digitales[13] no puede aceptarse en una cuestión que afecta a la salud pública. Razones como la solidaridad o el miedo pueden dar lugar a que las personas se instalen la aplicación sin más. En octubre de 2020, tras un tiempo en el que varias comunidades autónomas han ido adaptándose a las directrices establecidas por la Aplicación (App) Radar Covid dependiente de la Secretaría de Estado para la Digitalización y la Inteligencia Artificial en el marco del Ministerio de Economía, la prensa ha dado cuenta de una serie de brechas de seguridad que permiten a terceros conocer la identidad de las personas declaradas como positivas. Entre esos terceros se encuentra Amazon. También se ha publicado que el Gobierno rechaza facilitar la documentación sobre la contratación de la citada aplicación.

En septiembre de 2020 más de 230 investigadores y académicos firmamos un manifiesto[14] en favor de la transparencia en lo relativo al software público y su aplicación en el rastreo mediante aplicaciones móviles.

El Reglamento General de Protección de Datos establece la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, que debe efectuar el responsable de este en determinados supuestos, como por ejemplo ante el uso de nuevas tecnologías; tratamientos de categorías especiales de datos (datos salud, genéticos y biométricos); tratamientos que impliquen la elaboración de perfiles de personas; y/o toma de decisiones automatizada. Ante cualquiera de estas iniciativas de recogida

13 Pasquale, Frank, *The Black Box Society*, Harvard University Press, 2016.

14 *Manifiesto en favor de la transparencia en desarrollos de software públicos* (septiembre de 2020), disponible en: *https://transparenciagov2020.github.io/*.

de datos de salud a partir de *Apps*, habría que efectuar una evaluación del impacto de los tratamientos de forma anticipada, para valorar los aspectos éticos, legales y sociales junto a las medidas técnicas y organizativas. Así sería posible evaluar la viabilidad de las propuestas, corregir las limitaciones y anticipar riesgos, así como su mitigación. Esta evaluación no se está llevando a cabo en la mayoría de los casos, y no debe entenderse como un proceso burocrático sino como una herramienta útil que va a permitir gestionar y mitigar los riesgos relacionados con los datos personales.[15]

III. Hacia un modelo de gestión de datos fiable, accesible e interoperable y que permita su reutilización

La pandemia por COVID-19 ha puesto de manifiesto los problemas sobre el acceso y la gestión de datos, incluidos los datos personales. Es urgente y necesario construir un modelo de datos fiable e interoperable, y que sea seguro y trazable.[16] La transferencia de competencias en materia de sanidad a las CCAA no debería suponer un obstáculo. La combinación de distintos conjuntos de datos personales almacenados en bases de datos es fundamental para extraer conclusiones y tomar decisiones. Por lo tanto, el quid de la cuestión radica en qué datos se van a solicitar, cómo se van a obtener, quién va a tener acceso —y durante cuánto tiempo—, y de qué forma se van a combinar esos datos con otros datos fiables de las personas (por ejemplo, aquellos almacenados en historias clínicas digitalizadas en bases de datos altamente protegidas), para llegar a conclusiones válidas. Las encuestas asociadas a las *Apps* y la conexión de esta información con la que está almacenada en bases de datos de salud altamente protegidas no es una cuestión baladí.

Debido al desarrollo de la tecnología y a la ingente cantidad de información almacenada en bases de datos, y la que emitimos constantemente a través de los dispositivos digitales, no es posible garantizar el anonimato. Sin embargo, es frecuente afirmar que los datos personales serán anonimizados, y no es cierto, aunque esta fuera la intención. Ante esta situación, es preciso articular las medidas técnicas y organizativas necesarias para garantizar la seudonimización de la información.

---

15 Agencia Española de Protección de Datos, *Listado de tipos de tratamientos de datos que requieren evaluación del impacto relativa a la protección de datos,* 2019, disponible en: *https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf*.

16 European Commission, *Guidelines on FAIR Data Management in HORIZON 2020*, 2016, disponible en: *https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf*.

Se entiende por seudonimización 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 atribuyen a una persona física identificada o identificable".[17] Los datos se codifican o se seudonimizan,[18] pero no es posible mantener que se anonimizan como regla general, por lo que la seudonimización debería exigirse por defecto.

En la sociedad digital guiada por el dato hemos dejado de ser anónimos para ser reidentificables. Nuestro código postal, la fecha de nacimiento y el sexo nos hacen identificables casi en un 100%.[19] Las primeras aplicaciones móviles propuestas para la detección y seguimiento de síntomas en Madrid (*CoronaMadrid*) y Cataluña (*STOP COVID-19 CAT*) fueron criticadas porque, por ejemplo, para iniciar la sesión solicitaban la tarjeta sanitaria, y la ubicación, y estaban desarrolladas por terceros ajenos al ámbito de la salud pública con acceso a datos personales. Así, se deben priorizar aquellas propuestas que aseguren que no es posible identificar a las personas.

La gestión de la pandemia por COVID-19 no puede suponer la institucionalización del poder de las grandes tecnológicas, tampoco puede implicar un control absoluto del Estado sobre nuestro comportamiento. Hay que asumir que el riesgo cero no existe y que las propuestas locales serán inútiles. No existe acuerdo sobre una *App* europea para la identificación de positivos y el rastreo de contactos y, sin embargo, la Unión Europea anuncia que aplicará la biometría facial para controlar las fronteras en Europa en menos de dos años.[20] Es necesario revisar la tendencia a aplicar estas tecnologías tan invasivas y también la tendencia a la elaboración de perfiles de personas. Hay que evitar la excesiva dependencia de las tecnológicas, y en particular, de Europa hacia EEUU. El Estado debería establecer las condiciones para garantizar la protección de las personas y cambiar las reglas de

17 Real Academia Española, *Diccionario de la lengua española*, 23a. ed., versión 23.3 en línea, *https://dle.rae.es*.

18 Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). R. (UE) 2016/679 (27 abril 2016).

19 Sweeney, Latanya, *Simple demographics often identify people uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3, Pittsburgh, 2000.

20 "La Unión Europea prepara una base de datos biométrica", *La Vanguardia*, 6 de mayo de 2020, disponible en: *https://www.lavanguardia.com/internacional/20200606/481629030064/la-ue-prepara-base- de-datos-biometrica-controlar-fronteras-schengen.html*.

juego imperantes centradas en la acumulación, explotación y monetización de datos personales.[21]

Fomentar la alfabetización digital debería ser una prioridad, y desde la escuela, para evitar asimetrías entre la información que acumulan terceros sobre nosotros, por la información de la que disponen y el conocimiento sobre sus datos y, por lo tanto, el control sobre los mismos por parte de su titular. De hecho, la Ley de Protección de Datos Personales y de Garantías Digitales, de España, de 2018 establece el derecho a la educación digital (art. 83). Además, hay que informar a los titulares de los datos personales acerca de quién, por qué, cómo y durante cuánto tiempo se accede a sus datos y los resultados por razones de salud pública de forma clara e inteligible, permitiendo el ejercicio de los derechos reconocidos en la normativa aplicable.

IV. El pasaporte inmunológico

El pasaporte inmunológico o serológico se ha propuesto como un documento digital acreditativo de haber pasado la COVID-19, y que, por tanto, otorgaría a quien lo poseyera la posibilidad de realizar actividades que en tiempo de restricciones y confinamiento no están permitidas para todos. Trabajar de manera presencial, acudir a locales de ocio o restauración, desplazamiento entre localidades con confinamientos en activo, etcétera. Los defensores de esta propuesta la plantean como una opción para aquellas personas que, por estar teóricamente inmunizadas, pueden circular de manera libre sin suponer un peligro para los demás.

El pasaporte inmunológico debería descartarse por falta de evidencia científica y por ser incompatible con la protección de los derechos y libertades en nuestro contexto. Actuar en favor del interés colectivo y por razones de salud pública no puede anular derechos y condicionar nuestra libertad. El pasaporte serológico, que se ha llegado a plantear como una medida que nos permitiría recuperar nuestra vida en sociedad, ha sido rechazado por la OMS por falta de evidencia científica. Este es incompatible con la normati-

[21] European Data Protection Board, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, 2020, disponible en: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf,* y European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, 2020, disponible en: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en*.

va europea de protección de datos, entre otras, y, en definitiva, es contrario a la protección de los derechos y libertades fundamentales. Es una medida discriminadora y estigmatizante que, a efectos prácticos, animaría a las personas a contagiarse para obtener el semáforo verde. Haber pasado la COVID-19 no garantiza la inmunidad,[22] y es contrario al principio de respeto por las personas, beneficencia y justicia.

El portavoz del Ministerio de Sanidad en el contexto de la epidemia por coronavirus en España, Fernando Simón, en una de sus habituales comparecencias se quedaba pasmado y con razón, ante la pregunta de un periodista sobre la posibilidad de incluir en el *currículum vitae* información sobre la inmunidad de las personas.[23] Una inmunidad que, como se ha dicho, no puede garantizarse. Lo más preocupante es que noticias en algunos medios, en particular en sección negocios, plantean una suerte de DNI sanitario con tecnología *blockchain* para la vuelta al trabajo,[24] dando por hecho que la COVID-19 habilita para tomar cualquier medida digital, aunque sea contraria a los derechos y libertades también en el ámbito laboral.

Parece que grandes consultoras y *Start-ups* apuestan por este tipo de certificados (códigos QR) para trabajadores, a los que podrían acceder empresarios y centros de salud y hospitalarios mediante una aplicación, que en estos momentos estaría en fase de validación por parte de las autoridades. Un modelo de negocio que podría ser de interés hasta para fondos de inversión —ahora que dejan de invertir en residencias de mayores—,[25] y que anularía cualquier libertad, trayendo consigo una vigilancia intensiva con medidas tan inmediatas como rentables, enmarcadas incluso en la prevención de riesgos laborales.

---

[22] Kofler, Natalie y Baylys, Françoise, "Ten reasons why immunity passports are a bad idea Restricting movement on the basis of biology threatens freedom, fairness and public health", *Nature comment*, 2020, disponible en: *https://www.nature.com/articles/d41586-020-01451-0*.

[23] Fernando Simón: No es moral incluir en el curriculum si estás inmunizado, *La Vanguardia*, 16 de mayo de 2020, disponible en: *https://www.lavanguardia.com/vida/20200516/481181834313/pandemia- inmunidad-curriculum-simon.html*.

[24] Un DNI sanitario con tecnología *blockchain* para la vuelta al trabajo, *La Vanguardia*, 10 de mayo de 2020, disponible en: *https://www.pressreader.com/spain/la-vanguardia- dinero/20200510/281822875974758*.

[25] Residencias de mayores: un negocio en cuestión que factura 4.500 millones. La mortalidad en los centros para ancianos ha puesto el foco en estas instituciones, que habían atraído al capital riesgo por su alta rentabilidad, *El País Negocios*, 2 de mayo de 2020, disponible en: *https://elpais.com/economia/2020-05-02/residencias-de-mayores-cuando-la-busqueda-de-beneficios-devalua-la-calidad-de-los-servicios.html*.

V. La evaluación de la investigación e innovación en salud

La investigación es el pilar del sistema de salud. Es necesario destinar más presupuesto para aumentar los recursos humanos y materiales; efectuar una revisión de la priorización de las líneas de investigación para que sean socialmente valiosas y, sobre todo, desarrollar pautas comunes para su adecuada evaluación por parte de los comités de ética de la investigación (CEI).

Mi experiencia en tanto que miembro de distintos CEI, permite explicar aquí las cuestiones no resueltas en la evaluación de proyectos de investigación e innovación en salud en los que se utilizan datos personales y ante la aplicación de inteligencia artificial, *Big Data*, biometría y el desarrollo de *Apps* y otros dispositivos digitales. Evaluación que recae fundamentalmente en estos órganos colegiados e interdisciplinares. La COVID-19 ha evidenciado que se trata de un modelo de evaluación ineficaz y obsoleto. El principal problema es que los CEI, en tanto que mecanismos de protección de los derechos de las personas, no se han adaptado al cambio de paradigma que supone la digitalización y que se asienta en la explotación de conjuntos datos personales.[26]

En situación de pandemia por COVID-19 los CEI trabajan bajo presión y se les exige una rápida evaluación de los numerosos proyectos de investigación e innovación que se presentan. En los centros hospitalarios y de investigación, la COVID-19 ha provocado un aluvión de propuestas, ensayos clínicos, otros tipos de investigaciones biomédicas, y especialmente, proyectos para el desarrollo de sistemas de predicción y gestión de la COVID-19. En tiempos de pandemia no se pueden relajar los estándares de protección, y se necesitan pautas para evaluar adecuadamente si los tratamientos de datos personales propuestos cumplen con los requisitos éticos y legales aplicables. La responsabilidad de los CEI es clara, los proyectos deben ser científicamente válidos y socialmente valiosos.

Ejemplos son sistemas de predicción de COVID-19 basados en la programación de algoritmos, que se alimentan de distintos conjuntos de datos personales almacenados en historias clínicas y en otras bases de datos, así como de aquella información remitida por los titulares de los datos en dis-

[26] De Lecuona, Itziar, "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (big data)", *Gaceta Sanitaria*, vol. 32, núm. 6, noviembre-diciembre de 2018) pp. 576-578, DOI: 10.1016/j.gaceta.2018.02.007, disponible en: *https://www.gacetasanitaria.org/es-evaluacion-los-aspectos-metodologicos-eticos-articulo-S0213911118300864.*

tintos formatos. También proliferan las *Hackatones* o retos para desarrollar algoritmos como parte de proyectos para, por ejemplo, predecir el riesgo a desarrollar determinada patología.

Son diversos los terceros interesados en realizar proyectos de investigación e innovación basados en la aplicación de la citada convergencia de tecnologías. El objetivo es aumentar el conocimiento disponible, desarrollar intervenciones personalizadas y mejorar la toma de decisiones. Así, en salud se plantean propuestas que pueden estar fundamentadas en protocolos de investigación, y otras, para innovar en el ámbito asistencial que comparten el reto de asegurar que protegen la intimidad de los titulares de los datos personales que necesitan tratar.

A dos años de la aplicación del Reglamento General de Protección de Datos, la pandemia por COVID-19 ha puesto a prueba la capacidad de los CEI para evaluar, y también ha puesto de manifiesto su incumplimiento. Los CEI necesitan un desarrollo normativo con carácter urgente sobre las competencias, funciones, constitución, acreditación, composición y funcionamiento, que está pendiente desde la Ley española de Investigación Biomédica del año 2007. Y se debería revisar el sistema de control por parte de la administración. Es también urgente desarrollar pautas y homogeneizar las cuestiones que los CEI deben evaluar, para evitar que oportunistas abran mercados de datos personales disfrazados de investigación e innovación en salud.

Es aconsejable crear comités de ética de la innovación,[27] y mientras no se priorice cubrir esta necesidad, los CEI seguirán al límite. A la falta de recursos humanos y materiales, se les suma una sobrecarga evidente: seguirán evaluando proyectos de investigación al uso, y además iniciativas provenientes de las áreas de innovación de hospitales y centros de investigación basadas en la citada convergencia de tecnologías, sin la comprensión ni las pautas adecuadas para evaluar los tratamientos de datos personales.

Es también urgente asegurar la independencia de los CEI, que no se crean para secundar intereses espurios, sino para proteger a las personas. El aval ético de estos proyectos viene determinado por el dictamen favorable de los CEI correspondientes, que no están preparados, fundamentalmente por su composición y por la falta de directrices comunes y procedimientos de trabajo para evaluar adecuadamente las propuestas. La necesidad de identificar y evitar los conflictos de intereses es también apremiante.

[27] Ossit, Alan, "Why health care organizations need technology ethics committees", *Bioethics Forum, The Hastings Center Blog*, 5 de febrero de 2020, disponible en: *https://www.thehastingscenter.org/why-health-care-organizations-need-technology-ethics-committees/*.

En determinados supuestos, como es el caso de los tratamientos de especiales categorías de datos como los de salud, genéticos, biométricos; tratamientos que impliquen elaboración de perfiles de personas; y/o toma de decisiones automatizada, entre otros, los CEI deben comprobar que el proyecto ha sido sometido a la evaluación del impacto de los tratamientos de datos personales propuestos en las personas afectadas, mediante el recurso a unas metodologías. Esta evaluación que compete al investigador principal y que los CEI deben revisar, no se está llevando a cabo en la mayoría de los casos. La figura del Delegado de Protección de Datos establecida por el Reglamento General de Protección de Datos ha sido incorporada en muchos casos sin respetar su espíritu independiente y sin exigir la correspondiente especialización.

Un error común detectado en las memorias de los proyectos, y en la información y el consentimiento informado para los potenciales participantes, es indicar que los datos se anonimizan, cuando del análisis de los tratamientos de datos personales se constata que se seudonimizan o codifican.[28] Los CEI deben comprobar las técnicas previstas para los tratamientos de datos personales para asegurar que no se reidentifica a las personas.

Todas estas cuestiones, eminentemente técnicas requieren contar con expertos o asesores en el CEI que, de forma independiente, permitan comprobar que las propuestas son adecuadas y pertinentes. Deberían incorporarse a los CEI especialistas en inteligencia artificial, ciencia de los datos, bioingeniería y otros perfiles capaces de completar la interdisciplinariedad que se requiere para una adecuada evaluación.

Una cuestión clave, en línea con la ciencia abierta que Europa también propugna, es evaluar cómo se obtienen, procesan y se generan nuevos datos en el marco de un proyecto; qué ocurrirá una vez acabado y si se van a compartir en abierto. Para conocer estas cuestiones y las fórmulas para que los datos se puedan encontrar, sean accesibles, interoperables y reutilizables debería exigirse un Plan de Gestión de Datos de cada uno de los proyectos.

VI. Conclusiones

Las medidas que se tomen en tiempos de pandemia deben ser proporcionales a los fines que se persiguen, respetuosas con los derechos de las personas y

[28] European Commission, *Ethics and Data Protection*, Horizon2020, 2018, disponible en: *https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf*.

temporales. La tendencia a la mercantilización de datos personales ha de ser contrarrestada con nuevas estructuras de gobernanza que alineen los intereses de los actores implicados. Es además necesario evitar la excesiva dependencia de las grandes tecnológicas, fundamentalmente estadounidenses. Por ello, es urgente que Europa invierta en el desarrollo de infraestructuras públicas para la gestión de datos, construyendo un modelo que permita su acceso y combinación en condiciones de seguridad, fiabilidad, trazabilidad y calidad; su interoperabilidad y reutilización.

La salud pública y la atención primaria han de ser reforzadas con personal capacitado para hacer el rastreo de contactos, utilizando la tecnología digital como apoyo a las tareas, no como solución. La implementación de las aplicaciones de identificación de positivos y rastreo de contactos plantea cuestiones técnicas, éticas, legales y sociales de calado, y en particular, un posible gran hermano digital si no se activan mecanismos para exigir transparencia y rendición de cuentas por parte del estado y de los distintos agentes que intervienen. Lamentablemente no puede afirmarse que España sea un ejemplo de buenas prácticas en digitalización para la gestión de la pandemia.

El modelo evaluador de la investigación e innovación en salud —gestado en la segunda mitad del siglo XX— debe ser objeto de revisión porque ha quedado obsoleto en la sociedad digital. Los CEIs, sobre los que recae el peso de la evaluación de los aspectos metodológicos, éticos, legales y sociales tienen que modificar su composición: incorporar nuevos perfiles para hacer frente a los retos de la sociedad digital así como desarrollar pautas y procedimientos para asegurar que se respetan los derechos de las personas ante la utilización de tecnologías emergentes y la explotación de conjuntos de datos personales.

Propuestas tan invasivas como el pasaporte inmunológico deben descartarse por ser desproporcionadas e incompatibles con la protección de los derechos y libertades, y además no tienen evidencia científica. Los Estados deben fomentar la alfabetización digital, de tal forma que sea posible evitar asimetrías entre los titulares de los datos personales y los terceros que interviene en estos procesos de explotación de datos personales, en especial, en investigación e innovación en salud.

VII. Fuentes de consulta

Agencia Española de Protección de Datos. *Listado de tipos de tratamientos de datos que requieren evaluación del impacto relativa a la protección de datos,*

2019 disponible en: *https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf.*

AMaSaP- SESPAS, *Posicionamiento AMaSaP- SESPAS sobre la realización de test masivos a toda la población en relación con el SARS-Cov-2 (Covid 19),* disponible en: *https://sespas.es/2020/05/31/posicionamiento-amasap-sespas-sobre-la-realizacion-de-test-masivos-en-relacion-con-el-sars-cov-2-covid-19/.*

CASADO, María *et al.*, *Declaración sobre integridad científica en investigación e innovación responsable*, Barcelona-Porto, Edicions de la Universitat de Barcelona, 2016, disponible en: *http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08489.pdf.*

Directiva (UE) 2019/1024 del Parlamento europeo y del consejo del 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público (versión refundida).

EUROPEAN COMMISSION, *Guidelines on FAIR Data Management*, 2016, disponible en: *https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.*

EUROPEAN COMMISSION, Ethics and Data Protection, Horizon. 2020, 2018, disponible en: *https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf.*

EUROPEAN DATA PROTECTION BOARD, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, 2020, disponible en: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.*

EUROPEAN DATA PROTECTION BOARD, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, 2020, disponible en: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en*.

EUROPEAN UNION, *Responsible Research and Innovation-HORIZON 2020,* disponible en: *https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation*.

EUROPEAN UNION, *What can big data do for you*, disponible en: *https://ec.europa.eu/digital-single-market/en/what-big-data-can-do-you.*

GONZÁLEZ, Juan *et al*, *Abriendo la caja de Pandemia: por qué necesitamos repensar el rastreo digital de contactos*, CYPRIAN: Cibersecurity, Privacy and Anonymity Lab, Universidad de Vigo, 2020, disponible en: *https://www.gradiant.org/wp-content/uploads/2020/05/Informe-Cyprian-contact-tracing_v1-1.pdf.*

GRUPO DE TRABAJO MULTIDISCIPLINAR SOBRE LA COVID19 DEL MINISTERIO DE CIENCIA E INNOVACIÓN, *Análisis del informe de la Academia de las*

Ciencias de Alemania y su posible aplicabilidad a la situación actual de España, 2020, disponible en: *https://www.ciencia.gob.es/stfls/MICINN/Ministerio/FICHEROS/Doc_GTM_InformeAcadLeopo ldina_Mayo2020_GTM.pdf.*

HIGH LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, European Union, *Ethics Guidelines for Trustworthy AI*, 2019 disponible en: *https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai*.

INSTITUTO DE SALUD CARLOS III, *Estudio nacional de sero-epidemiología de la infección por SARS-CoV-2 en España,* 2020, disponible en: *https://www.mscbs.gob.es/ciudadanos/ene-covid/docs/ESTUDIO_ENE-COVID19_INFORME_FINAL.pdf*.

KOFLER, Natalie y BAYLYS, Françoise, "Ten reasons why immunity passports are a bad idea Restricting movement on the basis of biology threatens freedom, fairness and public health", *Nature comment*, 2020, disponible en: *https://www.nature.com/articles/d41586-020-01451-0.*

LECUONA, Itziar de, "El valor de los datos personales de salud en la sociedad digital", en GARCÍA MANRIQUE, Ricardo (coord.), *El cuerpo diseminado, Estatuto, uso y disposición de los biomateriales humanos,* Editorial Aranzadi, Cizur Menor, 2018.

LECUONA, Itziar de, "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (big data)", *Gaceta Sanitaria*, vol. 32, núm. 6, noviembre-diciembre de 2018, DOI: 10.1016/j.gaceta.2018.02.007, disponible en: *https://www.gacetasanitaria.org/es-evaluacion-los-aspectos-metodologicos-eticos-articulo-S0213911118300864.*

LECUONA, Itziar de y VILLALOBOS, María José, "La tendencia a la mercantilización de partes del cuerpo humano y de la intimidad en investigación con muestras biológicas y datos (pequeños y masivos)", en CASADO, María (coord.), *De la solidaridad al mercado*, Editorial Fontamara, México, 2016, disponible en acceso abierto en *www.bioeticayderecho.ub.edu*.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, disponible en: *https://www.boe.es/eli/es/lo/2018/12/05/3*.

MAZZUCATO, Mariana, *El estado emprendedor*, Barcelona, RBA Economía, 2019.

MAZZUCATO, Mariana, Preventing digital feudalism, *Social Europe*, 2019, disponible en: *https://www.socialeurope.eu/preventing-digital-feudalism.*

OSSIT, Alan, "Why health care organizations need technology ethics committees", *Bioethics Forum, The Hastings Center Blog*, 5 de febrero de 2020, disponible en: *https://www.thehastingscenter.org/why-health-care-organizations-need-technology-ethics-committees/*.

PASQUALE, Frank, *The Black Box Society*, Harvard University Press, 2016.

WILKINSON, Mark *et al.*, "The FAIR Guiding Principles for scientific data management and stewardship", *Scientific Data* 3, 160018, 2016, DOI. org/10.1038/sdata.2016.18.

REAL ACADEMIA ESPAÑOLA, *Diccionario de la lengua española*, 23a. ed., versión 23.3 en línea, *ttps://dle.rae.es.*

Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). R. (UE) 2016/679 (27 abril 2016).

SWEENEY, Latanya, *Simple demographics often identify people uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3, Pittsburgh, 2000.