LA TECNOLOGÍA DE LOCALIZACIÓN APLICADA A LA INVESTIGACIÓN CIENTÍFICA: EL CUMPLIMIENTO NORMATIVO EN TORNO A LA PROTECCIÓN DE DATOS PERSONALES

LORENA PÉREZ CAMPILLO

SUMARIO

Fecha recepción: 03.10.2022
Fecha aceptación: 21.03.2023

LA TECNOLOGÍA DE LOCALIZACIÓN APLICADA A LA INVESTIGACIÓN CIENTÍFICA: EL CUMPLIMIENTO NORMATIVO EN TORNO A LA PROTECCIÓN DE DATOS PERSONALES

LORENA PÉREZ CAMPILLO[1]

Universidad Europea de Madrid

I. INTRODUCCIÓN

I.1. El uso de la tecnología de localización en el contexto pandémico y el impacto en el derecho fundamental de protección de datos.

Nunca antes en la historia de la humanidad se ha podido rastrear los movimientos humanos de una forma tan completa, y todo ello, es gracias a un dispositivo o a nuestro teléfono móvil. Los sistemas de monitorización de la salud han evolucionado rápidamente durante las dos últimas décadas y tienen el potencial de cambiar la forma en que se presta actualmente tanto la asistencia sanitaria[2] como la investigación científica .Un ejemplo de iniciativa de investigación en el marco del sector privado es Meta (*Facebook),* en *Data For Good*[3]*,* que pretendía apoyar la investigación en salud pública y utilizaba mapeos de calor con usuarios con síntomas de Covid-19, recopilando «información agregada» usando técnicas de ruido y mecanismos de «privacidad diferencial».

---

[1] Lorena Pérez Campillo, Profesora Dra. de la Universidad Europea de Madrid. Departamento de Ciencias Jurídicas y Políticas. Email: lorena.perez.campillo@gmail.com, Calle Cabo San Vicente, 14, esc.centro, 9b, Alcorcón (Madrid), España. CP 28924. ORCID 0000-0002-8047-0293

[2] Baig M.M., Gholamhosseini H. (2013). «Smart health monitoring systems: an overview of designand modeling». [Sistemas de vigilancia de salud inteligente: vision general del diseño y la creación]. *J Med Syst.* Apr; 37(2): 9898. doi: 10.1007/s10916-012-9898-z.

[3] Vid. https://dataforgood.facebook.com/. Última consulta: 30 agosto de 2022

Al inicio de la pandemia surgieron un aluvión de aplicaciones móviles «escalables» con tecnología de rastreo promovidos por Administraciones Públicas y gobiernos que alcanzaban a miles de millones de usuarios y fueron desarrollados en varios países[4]. Los *smartphones* se convirtieron en una herramienta de ayuda para la gestión y control de la pandemia al generar datos sobre el comportamiento humano. Los operadores de telecomunicaciones las pusieron en manos de las autoridades, organizaciones sociales y organismos epidemiológicos. Los datos recogidos por las soluciones tecnológicas resultaban «bastante necesarios (…) y sirvieron como caldo de cultivo para el desarrollo de la investigación científica sobre Covid-19 a corto y largo plazo»[5].

En España, en la aplicación «asistencia Covid-19», se informaba de que los datos personales eran conservados durante el tiempo que perduraba la crisis sanitaria y, una vez finalizada, eran agregados de forma anónima para tratarlos con fines estadísticos, de investigación o de planteamiento de políticas públicas, durante un período máximo de dos años. No obstante, la Agencia Española de Protección de Datos sancionó —con una resolución[6] de más de 200 páginas— al gobierno por la vulneración de algunas de las obligaciones normativas en la implantación de esta solución tecnológica con fines de control y vigilancia pandémica. Respecto a lo que nos incumbe en este trabajo, cabe destacar la falta de información —específica y clara— sobre los plazos de conservación de los datos para los fines de investigación científica en la política de datos.

Pero, además, en la pandemia se requirió encontrar una dirección que permitiese equilibrar la gestión de la salud pública y la gobernanza de datos acercándonos a una ponderación de los derechos y libertades con las obligaciones públicas. En este sentido, Farina & Lavazza[7] señalaron que «en el marco de una búsqueda biopolítica de la inmunidad perfecta frente al contagio, nuestras libertades básicas podrían verse considerablemente erosionadas si no introducimos un principio de proporcionalidad entre los distintos valores». Por ende, las decisiones políticas resultaron eminentemente determinantes para la gobernanza de datos, el respeto a los derechos fundamentales y la gestión de la salud pública. En este periodo, por su parte, 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 el Covid-19, dedicó

[4] O'Neill, et al. (2020). «A flood of coronavirus apps are tracking us. Now it's time to keep track of them».[Una avalancha de aplicaciones de coronavirus nos sigue la pista. Ahora es el momento de seguirles la pista.] *MIT Technonlogy Review*, disponible en https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

[5] Pérez, L., Batista, C. (2021). «Tecnología y apps en la lucha contra COVID-19 y la protección de datos personales en España y Brasil". Revista General de Derecho Administrativo, disponible en https://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=423834

[6] Vid. https://www.aepd.es/es/documento/ps-00222-2021.pdf. Última consulta: 29 de diciembre de 2022.

[7] Farina, M., Lavazza, A. (2021). «The meaning of Freedom after Covid-19». [El significado de la libertad después de Covid-19] HPLS 43, 3, disponible en https://doi.org/10.1007/s40656-020-00354-7

prácticamente un capítulo entero a la detección, control y vigilancia, imponiendo 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». La legitimidad del tratamiento se basaba en el interés público esencial en el ámbito de la salud pública para la protección de intereses vitales de los afectados y de otras personas, y no parecía existir previsión de reutilización ni siquiera con fines de investigación o previsiones específicas respecto a las garantías o medidas de seguridad[8], remitiendo en todo caso al Reglamento general de protección de datos y la normativa nacional de desarrollo.

I.2. Los datos de localización como «bien común y público»

También hubo oportunidad de plantearse de forma recurrente el siguiente interrogante: *«¿debería prevalecer el bien del derecho fundamental de protección de datos o el interés público de la salud pública?»* El derecho de protección de datos de las personas físicas viene recogido en el artículo 18.4 de la Constitución Española y, además, éste tiene consideración de «derecho humano» (art.12. Declaración Universal de los Derechos Humanos de 1948), y, es, por ende, que se debe observar el impacto de las soluciones tecnológicas de localización, también en la investigación científica, en los derechos fundamentales y libertades de los participantes. Ahora bien, en el escenario pandémico, la respuesta fue clara: los datos personales de carácter de salud no debieron ser tratados ya que eran datos de categoría especial, no obstante, existieron y existen excepciones, aplicables en escenarios de crisis sanitarias, como la provocada por el Covid-19, donde los tratamientos de datos de salud sí son permitidos y autorizados para la lucha y el control de la pandemia en pro de los intereses vitales de la comunidad. Los datos debieron entenderse como un «bien común» o «bien público»[9]. Martínez[10] señaló que «tratar datos de salud con la función de prevenir y luchar en un escenario epidémico o pandémico no persigue un fin discriminatorio, al contrario, se alinea con el valor constitucional fundamental de la garantía de la vida, la salud y la dignidad humana».

La necesidad de investigar sobre el Covid-19 y la utilización de los datos de carácter de salud como bien común era evidente sin poder desdeñar la importancia de los datos masivos como pilar de los sistemas sanitarios del mundo. Hay autores

[8] Cotino, L. (2020). «Inteligencia artificial, big data y aplicaciones contra la COVID-19. Privacidad y protección de datos». *Revista de Internet, Derecho y Política*.

[9] Calacci, D et al. (2020).»The tradeoff between the utility and risk of location data and implications for public good». [El compromiso entre la utilidad y el riesgo de los datos de localización y las implicaciones para el bien público]. *Computers and Society. Cornell University*, disponible en https://doi.org/10.48550/arXiv.1905.09350

[10] Vid. http://lopdyseguridad.es/a-la-muerte-por-proteccion-de-datos/. Última consulta: 7 de septiembre de 2022.

como Nanni[11] que contemplaron la posibilidad de un «almacén de datos personales» donde se otorgaba la oportunidad a los usuarios de contribuir al bien colectivo, lo que podría tratarse de que el enfoque descentralizado tomara la idea de «autogestión de datos personales» del autor Solove[12] y, además, se extendiera al servicio del «bien común» de una sociedad desarrollada y saludable. Otros autores como Parker[13] se cuestionaron la existencia de una argumentación suficiente para otorgar incentivos y promover la aceptación y uso de las aplicaciones móviles. En cualquier caso, tal y como señala de Montalvo[14], debemos dirigirnos a un «modelo responsable tanto desde la perspectiva de la comunidad investigadora y la industria, como de los propios ciudadanos», en el cual en vez de promover un «modelo de responsabilidad punitiva» se opte por un concepto de responsabilidad como «deber de ayuda a los demás».

El uso de los datos de localización con fines de investigación ha de contener las suficientes garantías para proteger los derechos de las personas, contando, además, con flexibilidad y racionalidad necesarias para no obstaculizar la labor de investigación en salud pública, que incluye también la investigación epidemiológica[15].

Las generaciones futuras se podrían beneficiar del recurso inestimable de la investigación, el desarrollo de métodos, modelos y evaluación de respuestas a la pandemia[16]. En este sentido, el Comité de Bioética de España[17] apostó por un «enfoque utilitarista» señalando la importancia del *deber de solidaridad* como miembros de una comunidad. Por su parte, ya la Declaración Universal de Derechos Humanos estableció los cimientos a esta idea señalando que «toda persona tiene deberes respecto a la comunidad, puesto que solo con ella puede desarrollarse libre y plenamente su personalidad». Para encajar todas las piezas y conseguir la convivencia del deber pú-

---

[11] Nanni M., et al. (2021). «Give more data, awareness and control to individual citizens, and they will help COVID-19 containment». [Dar más datos, conciencia y control a los ciudadanos individuales, y ellos ayudarán a la contención COVID-19]. *Ethics Inf Technol.* https://doi.org/10.1007/s10676-020-09572-w

[12] Solove, D J. (2012). «Privacy Self-Management and the Consent Dilemma» [Autogestión de la privacidad y el dilema del consentimiento]. *GWU Legal Studies Research Paper* No. 2012-141, GWU Law School Public Law Research Paper https://ssrn.com/abstract=2171018 .

[13] Parker MJ, et al (2020). «Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic». [Ética del rastreo instantáneo de contactos mediante aplicaciones de telefonía móvil en el control de la pandemia de COVID-19]. *Journal of Medical Ethics*; 46:427-431.

[14] De Montalvo, 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*, 1(106), 43–75. Disponible en https://doi.org/10.5944/rdp.106.2019.26147

[15] Serrano, M. (2020). «El marco jurídico de Los datos relativos a la salud en el ámbito de la Salud y de la investigación en salud tras la entrada en vigor del Reglamento general de protección de datos y de la ley de protección de datos personales y garantía de los derechos». *Estudios De Deusto* 68 (2), 257-92, disponible en https://doi.org/10.18543/ed-68(2), pp. 257-292.

[16] *Supra cit.*

[17] Comité de Bioética de España, Informe del comité de bioética de España sobre la financiación pública del medicamento profilaxis preexposición en la prevención del VIH, 24 de noviembre de 2016, http://assets.comitedebioetica.es/files/documentacion/es/Informe_PrEP.pdf

blico y el respeto de los derechos deberán existir suficientes garantías de protección para evitar que, precisamente, bajo este enfoque, los derechos puedan ser «fácilmente infringidos, debido a que sus beneficios individuales se agregan para constituir los beneficios colectivos».

Por ello, los gobiernos debieron, deberán plantearse ciertas cuestiones éticas imprescindibles para la implantación de aplicaciones móviles de rastreo de contacto a la ciudadanía; tales como evaluar si la herramienta es necesaria para salvar vidas; si hay soluciones alternativas a la misma; o si es eficaz, oportuna, popular y precisa, temporal, voluntaria; o si el consentimiento es necesario; los datos son reidentificables y se pueden borrar; está definida la finalidad de la recogida de datos, se utiliza únicamente para limitar la propagación; se utiliza para el cumplimiento de una ley; está disponible de forma equitativa o era igualmente accesible para todos los usuarios[18].

I.3. Escenario actual en el sector privado y la protección del derecho de protección de datos personales.

Existen gigantes tecnológicos que de forma aislada o con alianzas con farmacéuticas[19] tienen intereses en diferentes conjuntos de datos personales más allá de los intereses de la comunidad investigadora responsable de los proyectos. Leucona[20], en este sentido, ha destacado la falta de infraestructuras públicas europeas con fondos públicos e independientes y la excesiva dependencia europea de las grandes tecnológicas, fundamentalmente, europeas. Se sabe que los datos de localización[21] recogidos pasivamente de los teléfonos móviles por empresas de telecomunicaciones se comercializan en los mercados privados[22].

---

[18] Morley, J et al. (2020). «Ethical guidelines por Covid-19 tracing apps». [Directrices éticas para las aplicaciones de rastreo de Covid-19]. *Nature* 582, 29-31, disponible en doi:https://doi.org/10.1038/d41586-020-01578-0

[19] Martínez, J.M., Pérez, L. (2021). *La transformación del marketing sanitario. Cómo los datos son el petróleo del Siglo XXI*. Madrid. ESIC Editorial, p. 123.

[20] Vid. https://www.youtube.com/watch?v=YyMEMXiViSY. Última consulta: el 7 de septiembre de 2022.

[21] Los *«datos de localización»* por su parte, se definen como «todos los datos procesados en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indiquen la posición geográfica del equipo terminal de una persona que utiliza un servicio público de comunicaciones electrónicas, incluidos los datos relativos a: i) La latitud, longitud o altitud del equipo terminal; ii) la dirección del viaje del mismo; o iii) El momento en que se registró la información de localización». Ahora bien, los «datos de tráfico» son «cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma» y los *«datos de geolocalización»* para la ICO inglesa, son «los datos tomados del dispositivo de una persona que indican la ubicación geográfica de ese dispositivo, incluyendo datos de GPS o datos sobre la conexión con el equipo wi-fi local».

[22] Vid. https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile. Última consulta: 25 de agosto de 2022.

En España, las empresas de telecomunicación comercializan datos de geolocalización y «datos masivos» de manera «anonimizada y agregada» a empresas e instituciones, aunque no comparten información individual salvo mandato judicial. Por ello, es oportuno reflexionar sobre la legitimidad del tratamiento de esos datos, su nivel de «anonimato» y límites. Se ha comprobado que las personas se desplazan acudiendo a sitios aleatorios como son el lugar del trabajo u ocio, de forma repetida y esto les convierte en personas «predecibles», de hecho, el noventa y cinco por ciento de las personas se pueden identificar fácilmente desde solo cuatro puntos de ubicación diferentes[23], pero no existe regulación sectorial a nivel internacional que regule los datos de localización y eso conlleva al riesgo de que los reguladores podrían llenar un «vacío ético» con reglas que no están bien calibradas para las necesidades de las comunidades[24]. En cualquier caso, el sector privado tiene que promover la autonomía y la famosa «autogestión de la privacidad»[25] de las personas como usuarias, desde el nacimiento de cualquier proyecto tecnológico y de innovación.

Además de ello, la representatividad y el sesgo discriminatorio son excepcionalmente importantes para los conjuntos de datos de localización. Las prácticas injustas de tratamiento de datos que implican la geolocalización recaen desproporcionadamente en las «comunidades marginadas y vulnerables», por ello, es especialmente importante para estos grupos que se aumente la protección de la privacidad. Por ejemplo, los grupos de mayor riesgo de infección por el Covid-19 fueron los ancianos, personas sin hogar y personas indocumentadas[26]. El «derecho de acceso universal de Internet» está recogido en el artículo 81 de la Ley Orgánica del 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales («LOPDGDD»). Ésta es una cuestión clave a tener en cuenta para definir el marco ético-jurídico que deberán plantearse todos los *stakeholders* en el desarrollo de herramientas tecnológicas en el marco de una investigación en la lucha contra las pandemias u otras enfermedades.

El Comité Europeo de Protección de Datos[27], se ha pronunciado a raíz del escenario pandémico, señalando que tratar «metadatos» podría presentar problemas

[23] De Montjoye, Y.A., et al. (2013). «Unique in the Crowd: The privacy bounds of human mobility».[Único en la multitud: Los límites de la privacidad de la movilidad humana] *Sci Rep* 3, 1376. Disponible en https://doi.org/10.1038/srep01376.

[24] National Academies of Sciences, Engineering, and Medicine. Location Data in the Context of Public Health, Research, and Law Enforcement: An Exploration of Governance Frameworks: Proceedings of a Workshop in Brief». [Datos de ubicación en el contexto de la salud pública, la investigación y la aplicación de la ley: una exploración de los marcos de gobernanza: actas de un taller en resumen]. 2022, Washington, DC, disponible en https://doi.org/10.17226/26645.

[25] Solove, D J. (2012). «Privacy Self-Management and the Consent Dilemma» [Autogestión de la privacidad y el dilema del consentimiento]. *GWU Legal Studies Research Paper* No. 2012-141, GWU Law School Public Law Research Paper https://ssrn.com/abstract=2171018 .

[26] *Supra Cit.*

[27] Comité Europeo de Protección de Datos (2020). Nota de prensa. Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak. [Declaración del

de protección de datos a la ciudadanía. Según la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas se incluyen como metadatos a los datos utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del dispositivo generados en el contexto de la prestación de servicios de comunicaciones electrónicas, así como la fecha, la hora, la duración y el tipo de comunicación.

I.4. La adaptación del desarrollo tecnológico e investigación científica a la normativa de protección de datos.

Se sabe que el cumplimiento de la normativa de protección de datos en el ámbito de la investigación de salud, por ejemplo, no ha sido ni es nada sencillo por diferentes motivos. Se percibe como una «mera carga burocrática», la cual deben soportar la comunidad investigadora con escasa o nula formación ético-jurídica y con apenas un presupuesto viable que afronte su aplicación. La garantía de la privacidad es impensable que se pueda obtener «gratuitamente» ya que requiere de inminente inversión humana y técnica. Según Martínez[28] contamos con un «ecosistema normativo favorable a la investigación» que exige la adopción de políticas de gestión responsable de los procesos de investigación, optando por la integración de las normas, en el diseño de la investigación desde la génesis de la idea investigadora y esto requiere de un «modelo de gestión estructurado y protocolizado». Si hay algo indiscutible es que el cumplimiento normativo en protección de datos por parte de la comunidad investigadora y de centros de investigación —públicos o privados— se convierte en valor añadido y evita riesgos reputacionales institucionales e infracciones, por lo que instamos a la adopción de la «privacidad como valor»[29].

En las investigaciones se requiere prestar especial atención a los procedimientos correspondientes para obtener el «consentimiento amplio»[30], dado el caso, en otorgar la suficiente información comercial y de colaboración con partes comerciales (industria farmacéutica), procesos que permitan a los participantes mantenerse informados sobre las novedades de sus datos, las actividades de investigación. Además de ello, se

---

Presidente de la EDPB sobre el tratamiento de datos personales en el contexto del brote de COVID-19]. Disponible en https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

[28] Martínez, R. (2022). «Anonimització i seudonimització: Interessos legítims com a base legal per a l'activitat d'investigació». [Anonimización y pseudonimización: intereses legítimos como base legal para la actividad de investigación]. Disponible en https://www.uv.es/catedra-microsoft/ca/actualitat-1285992809455/Novetat.html?id=1286269909592. Recuperado el 19 de septiembre de 2022.

[29] Pérez, L. (2021). «La Ética de los datos en las organizaciones e instituciones públicas y la gobernanza en el sector de la salud digital». *Revista de Privacidad y Derecho Digital*, núm. 25, pp. 77-8.

[30] Comité Internacional de Bioética (15 de septiembre de 2017). *Informe del IBC sobre big data y salud.* Recuperado de http://unesdoc.unesco.org/images/0024/002487/248724e.pdf

necesita pensar en el diseño de procedimientos para la supervisión ética y comunicación con proveedores y en un «mecanismo de recompensa»[31] con los participantes. Por otro lado, la particularidad de este tipo de datos de localización (personales, pseudonimizados y anonimizados) nos obliga a tener el foco en tres normativas: el Reglamento (UE) 2016/679 (o denominado en ocasiones como «RGPD»)[32] y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (o denominada con las siglas «LOPDGDD»)[33], y el Reglamento sobre la privacidad y las comunicaciones electrónicas[34], que regula lo referente a los datos anonimizados, y no a los datos personales.

Por su parte, el papel protagonista que adoptan los principios del tratamiento de datos se acopla bastante bien al escenario de necesidad ante la crisis pandémica y a su «incertidumbre»[35], debido a que ya la legislación europea contempló la posibilidad de hipotéticos escenarios pensando, quizás, en otras epidemias pasadas como el ébola, la gripe aviar, la gripe A, el VIH, etc., donde el uso de los datos pudo ser determinante para su control, gestión e investigación, y de esta manera, se incluyó expresamente la base legitimadora a la que se podrían sujetar los gobiernos, administraciones públicas y demás entes. Pero, además de ello, «la norma también se podría encajar a escenarios de tecnología e innovación, sobre todo, porque uno de los principales motivos de su creación fue poder estar a la altura de regular el tratamiento de datos masivos recogidos por tecnología»[36]. De hecho, las autoridades de control nacionales y el mismo Grupo de Trabajo del Artículo 29 previeron y analizaron el impacto posible del tratamiento de datos a través de dispositivos móviles mucho antes de la publicación del RGPD.

Por último, y no menos importante, cabe hacer una aclaración previa en relación con el término «investigación científica». El RGPD señala que «el tratamiento de

---

[31] Vid. https://www.newmedicaleconomics.es/cuestion-de-justicia/y-despues-del-ensayo-clinico-que/ Recuperado el 7 de septiembre de 2022.

[32] Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de Protección de Datos. «RGPD»). Diario Oficial de la Unión Europea, L119, de 4 de mayo de 2016. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

[33] España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales («LOPDGDD»). *Boletín Oficial del Estado*, de 6 de diciembre de 2018. Disponible en https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

[34] Unión Europea. Propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010 .

[35] Bradford L. et. Al. (2020). «COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes» [COVID-19 aplicaciones de localización de contactos: una prueba de resistencia para la privacidad, el RGPD y los regímenes de protección de datos] *Journal of Law and the Biosciences*, Vol. 7,1, lsaa034, Disponible en https://doi.org/10.1093/jlb/lsaa034

[36] *Supra cit.*

datos personales con fines de investigación científica debe interpretarse, (…) de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la *investigación aplicada y la investigación financiada por el sector privado*. (…) Entre los fines de investigación científica también se deben incluir los estudios realizados en *interés público en el ámbito de la salud pública*». En este mismo sentido, el considerando 157 amplia el ámbito de la investigación, teniendo en cuenta la posible recogida de datos procedentes de registros. Así, recuerda que «combinando información procedente de registros, la comunidad investigadora puede obtener nuevos conocimientos de gran valor sobre *condiciones médicas extendidas*, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. (...) Los resultados de investigaciones obtenidos de registros (también, electrónicos) proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la *concepción y ejecución de políticas* basada en el conocimiento, *mejorar la calidad de vida de numerosas personas* y mejorar la eficiencia de los servicios sociales. *Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas* establecidas en el Derecho de la Unión o de los Estados miembros». Es por ello, que hemos preferido la referencia a este concepto, renunciando a otros como «investigación biomédica» o «investigación en salud» y así, perseguir un alcance mayor.

En este trabajo además de analizar el estado del arte referente a los proyectos de investigación científica con el uso de datos personales de localización analizaremos la normativa sectorial específica afecta y sus disposiciones (tanto con el «RGPD» como la «LOPDGDD»), sin pasar por alto, el Real Decreto-ley 21/2020 de 9 de junio, o la propuesta del Reglamento sobre la privacidad y las comunicaciones electrónicas, al igual que la normativa futura del Espacio Europeo de Datos [37] o del Reglamento de Gobernanza de los Datos[38], tomando como referencia diversas y completas guías de las autoridades de control e instituciones comunitarias.

II. LA EFICACIA, NECESIDAD Y MINIMIZACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES

En primer lugar, el tratamiento de datos personales debe ser «eficiente y útil»; el uso de los datos de localización recogidos debe servir para el desarrollo y propósitos del tratamiento de datos en el marco de una investigación. Por ejemplo, a partir de un período de inactividad nocturna puede deducirse el lugar donde duerme la

[37] Unión Europea. Propuesta sobre el Reglamento del Espacio Europeo de Protección de Datos Vid. https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en

[38] Unión Europea. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al la gobernanza de los datos (Ley de Gobernanza de Datos). Com/2020/767 final. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0767&from=ES

persona, y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa. El perfil puede incluir asimismo datos derivados de las pautas de movimientos de terceros sobre la base de lo que se conoce como «gráfica social».

En segundo lugar, la comunidad investigadora, gestora y la industria asumen un papel principal en dar a demostrar que el tratamiento es «objetivamente necesario» para el objetivo perseguido y que es «menos intrusivo» en comparación con otras opciones para lograr el mismo objetivo, y no que sea una parte necesaria de sus métodos elegidos. Es decir, si existen alternativas realistas y menos intrusivas, el tratamiento «no será necesario». En todo caso, se impulsará el garantizar una revisión periódica de la «necesidad» de seguir con tratamiento de datos personales para la investigación, y por ello, se tendrán que establecer unas «cláusulas de extinción adecuadas», a fin de asegurar que el tratamiento no se extienda más allá de lo estrictamente necesario para esos fines. Por ejemplo, los dispositivos móviles inteligentes están inextricablemente ligados a las personas físicas por lo que requieren de un identificador único. Este identificador único permite el seguimiento de usuarios de un dispositivo específico y, por tanto, permite individualizar a los mismos, incluso si su verdadero nombre no es conocido[39]. El 89 % de los usuarios considera importante saber cuándo las aplicaciones transmiten sus datos personales y poder activar o desactivar esa posibilidad[40]. Se ha relevado que muchas de ellas recogen datos de los *smartphones* sin que exista una relación clara con función aparente de la aplicación.

En tercer lugar, y en relación estrecha con lo anterior, debemos señalar la importancia del cumplimiento del «principio de minimización de datos» ya que esta tecnología puede llegar a ser demasiado invasiva en ocasiones. Por ello, habrá que saber identificar el nivel de intromisión o invasión en función de la exactitud y frecuencia de datos que dependerá del tipo de dispositivo de localización con sensores o del sistema operativo. Pensemos que, por ejemplo, los *smartphones* pueden captar permanentemente las señales procedentes de las estaciones de base y de puntos de acceso wi-fi. Técnicamente, el seguimiento puede hacerse de forma secreta, sin informar al propietario, o también de forma semisecreta, cuando la persona «olvida» o no está adecuadamente informada de que los servicios de localización están activados o cuando los parámetros de accesibilidad de los datos sobre localización son cambiados de «privada» a «pública».

Previamente a desarrollar de forma más profunda estos principios tan esenciales, aprovechemos a enmarcar la posición jurídica de los diferentes sujetos para facilitar la comprensión al lector sobre el rol de cada uno de ellos en proyectos de investigación científica con tecnología e innovación.

---

[39] Grupo de Trabajo del Art. 29 (2007). Dictamen 4/2007 sobre el concepto de datos personales (WP136). Disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

[40] Vid. http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf. Recuperado el 31 de octubre de 2022.

Los «responsables de tratamiento de datos» son las persona físicas o jurídicas, autoridades públicas, servicios u otros organismos que, solo o junto con otros, determinan los fines y medios del tratamiento. Éstos tomarán las decisiones sobre qué datos tratar, de quién, para qué finalidad, dónde conservarlos, qué medidas implementar para protegerlos, etc. En nuestro trabajo, por ejemplo, pueden ser aquellos centros de investigación cuando sean «promotores» y decidan sobre la finalidad y uso de los datos y los desarrolladores y de una aplicación móvil o fabricantes de sistemas operativos y de servicios de geolocalización cuando sean capaces de tratar datos de localización. La comunidad investigadora, también podría ser responsable del tratamiento si deciden los medios y finalidades de la recogida de datos personales de localización. Por ejemplo, en el contexto pandémico, el apartado 3, del artículo 27 del 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, señaló específicamente que; los responsables del tratamiento serían «las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, en el ámbito de sus respectivas competencias (…)».

Por otro lado, los «responsables respectivos» no están contemplados en la normativa y asumirán la responsabilidad de sus respectivos tratamientos o de sus diferentes finalidades diferentes, correspondiendo a cada uno de ellos las obligaciones derivadas de su actividad. Por ejemplo, el centro de investigación asumirá responsabilidad de todos los datos que figuren en la historia clínica y que puedan identificarle y el promotor de los que se recogen en el estudio de forma pseudonimizada. Piénsese, también, en que una fundación de investigación de un hospital puede ser responsable de tratamiento de datos del estudio, y el propio hospital puede ser responsable del tratamiento de datos asistenciales de los pacientes, por lo que las finalidades son distintas

Por su parte, los «encargados de tratamiento de datos» como son las personas físicas o jurídicas, autoridades públicas, servicios u otros organismos que traten datos personales *por cuenta* del responsable del tratamiento, tratarán datos bajo las instrucciones del responsable y no podrán utilizar los datos para otras finalidades ni para las suyas propias. Por ejemplo, las CRO u organizaciones de investigación por contrato, —en su función de gestión y desarrollo de proyectos y estudios clínicos, ayudando a los promotores a reducir su carga de trabajo o labores monitorización[41] o los proveedores cloud de Microsoft o AWS, los cuales almacenan los datos—, asumirán funciones de encargo de tratamiento de datos. Entre los que asuman la responsabilidad y el encargo de tratamiento de datos deberán firmar el correspondiente «contrato de encargo de tratamiento».

Dicho esto, podemos afirmar que serán los responsables del tratamiento, antes de poner en marcha la solución tecnológica, quienes identificarán las «categorías

[41] Farmaindustria. Código de Conducta regulador del tratamiento de datos personales en el ámbito de los ensayos clínicos y otras investigaciones clínicas y de la farmacovigilancia. Pp. 60. https://www.aepd.es/es/documento/codigo-conducta-farmaindustria-cc-0007-2019.pdf Recuperado de 28 de diciembre de 2022.

especiales de datos existentes», por ejemplo, las visitas a hospitales, la presencia en actos políticos o en otros lugares específicos que, verbigracia, revelen datos sobre la vida sexual, etc. Este «*profiling*» podría ser utilizado en alguna forma para tomar decisiones que afecten significativamente al interesado. Para la toma de decisiones automatizadas en el contexto de la investigación científica (art. 22.2.c RGPD) y para la transferencia de datos a un tercer país en ausencia de una decisión de adecuación (art. 49.1.a RGPD), el «consentimiento explícito» sería una posible base jurídica (Supervisor Europeo de Protección de Datos, 2020)[42], siempre teniendo en cuenta los requisitos normativos[43].

En definitiva, el sector tecnológico que desarrolle soluciones tecnológicas y la comunidad investigadora perseguirán buscar los medios menos invasivos, y «evitar un seguimiento continuo», eligiendo, por ejemplo, un sistema que envíe alertas o recordatorios informando acerca del tratamiento de sus datos. La solución tecnológica tiene que permitir al individuo que «pueda desactivar el modo GPS» de la actividad en cualquier momento. Las aplicaciones móviles no deben basarse en el rastreo de movimientos *individuales* de personas sino en la «información de proximidad relativa» a los usuarios. El objetivo principal, dentro de todo lo posible, será «*minimizar*» la exposición de datos de las personas, por ello, la comunidad investigadora, gestora, el sector tecnológico que desarrolla soluciones y la industria asumen un rol primordial en evitar recopilar más «detalles granulares» de los que realmente se necesita, ofreciendo «diferentes configuraciones» para diferentes niveles de servicio. Por ejemplo, una aplicación móvil creada por desarrolladores y un equipo de investigación permite analizar la adherencia a un tratamiento antirretroviral para participantes VIH en entornos de bajos recursos. Los servicios de geolocalización tendrán que estar «desactivados» y los usuarios podrían consentir gradualmente la activación de aplicaciones específicas.

Los responsables del control perseguirán en primer lugar, trabajar con «datos pseudonimizados» evitando el uso de otros datos personales. Cada responsable del tratamiento debe definir qué datos personales «se necesitan realmente» (y cuáles no) a los efectos del tratamiento, incluidos los períodos de retención de datos pertinentes[44]. Según la propuesta del Espacio Europeo de Datos Sanitarios (EEDS), cuando el solicitante necesite datos estadísticos anónimos, tendrá que presentar una solicitud de datos, exigiendo al organismo de acceso a los datos sanitarios que le proporcione directamente el resultado.

---

[42] Vid. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOC_2019_370_R_0007&from=ES. Recuperado el 31 de octubre de 2022.

[43] Grupo de Trabajo del Art. 29 (2018). Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/670 (WP251rev.01).Disponible en : https://ec.europa.eu/newsroom/article29/items/612053

[44] Troncoso, A. (2018). «Investigación, Salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales». *Revista Derecho y Genoma Humano*, 49, pp. 187-266.

En general, requiere que el tratamiento sea una forma específica y proporcionada de lograr una finalidad específica. No sería suficiente con sostener que el tratamiento es necesario porque los responsables han elegido operar su proyecto de investigación de una manera particular. Se debe poder demostrar que el tratamiento es necesario para el objetivo que se persigue y que es menos intrusivo que otras opciones para lograr el mismo objetivo; no que sea una parte necesaria de sus métodos elegidos. Si existen alternativas realistas y menos intrusivas, el tratamiento de los datos personales no se consideraría necesario. Una vez que se haya llegado a este punto, se tendrán que establecerse «procesos específicos para excluir los datos personales innecesarios» que se estén recopilando y/o transfiriendo, reducir los campos de datos y prever mecanismos de supresión automatizada. Para determinar con precisión el rango y la cantidad de datos personales necesarios, es extremadamente importante contar con una persona «experta» capaz de seleccionar las características relevantes.

III. LOS RIESGOS Y LA RESPONSABILIDAD PROACTIVA EN EL TRATAMIENTO DE DATOS DE LOCALIZACIÓN EN LA INVESTIGACIÓN

Un acceso general e ilimitado crea riesgos que van desde la sustracción de datos hasta los robos en domicilios o incluso agresiones físicas y acoso. Por un lado, los «riesgos de seguridad» deben ser tomados en cuenta desde antes de la puesta en funcionamiento del proyecto de investigación con el uso de sensores de localización, por lo que la comunidad investigadora, gestora, el sector tecnológico que desarrolla soluciones técnicas y la industria contraen un compromiso inexcusable en la adopción de salvaguardias apropiadas y *medidas técnicas* como son la pseudonimización, la anonimización, la agregación, la codificación y la *descentralización*[45].

Quienes sean *stakeholders* «optarán siempre por datos anonimizados»[46], es decir datos que gracias a un conjunto de técnicas suprimieran la capacidad de asociar los datos de una persona física identificada mediante un «esfuerzo razonable»[47]. Según Platzer[48], la anonimización no funciona en el caso de datos de gran dimensión y la «reidentificación»[49] de los datos personales anonimizados recogidos a través de estas

[45] Vid. https://github.com/DP-3T/documents. Última consulta: 7 de septiembre de 2022.

[46] Canetti, R et al. (2020). "Anonymous Collocation Discovery: Harnessing Privacy to Tame the Coronavirus». [Descubrimiento de colocaciones anónimas: Aprovechando la privacidad para domar el Coronavirus]. *Boston University*, disponible en https://arxiv.org/pdf/2003.13670.pdf

[47] Esta «prueba de razonabilidad» deberá tener en cuenta tanto los aspectos objetivos (tiempo, medios técnicos) como los elementos contextuales, que pueden variar de un caso a otro (carácter excepcional de un fenómeno teniendo en cuenta, por ejemplo, la densidad de la población y la naturaleza y volumen de los datos). Si los datos no superan esta prueba, no se han anonimizado y, por tanto, se mantienen dentro del ámbito de aplicación del RGPD.

[48] Vid. *National Academies of Sciences, Engineering, and Medicine*, 2022.

[49] En España, con la LOPDGDD, podemos evidenciar el esfuerzo por la legislación para proteger a los titulares de datos o interesados, de la *reidentificación* en el caso de los datos anonimizados o

herramientas no se puede evitar por completo (AEPD, 2016)[50], aunque sea lo exigido normativamente. En la propuesta del Espacio Europeo de Datos Sanitarios (EEDS), en el artículo 44, parece proponer un enfoque coherente con el art. 89 RGPD, ya que «prioriza como primera opción la anonimización de los datos sanitarios eléctricos siempre que sea posible conseguir la finalización del tratamiento solicitado por la persona que utiliza que dispositivos con tecnología. En defecto de ello, los organismos de acceso a las estadísticas sanitarias facilitan el acceso a las estadísticas sanitarias electrónicas en formato pseudónimo», además, al igual que la normativa española, se define un escenario de «separación funcional» entre los que poseen los identificadores y los que investigan con los datos y un compromiso de no reidentificación para éstos últimos[51].

En la propuesta del Espacio Europeo de Datos Sanitarios se puede percibir la preocupación de la legislación respecto a algunas categorías de datos sanitarios electrónicos, los cuales siguen siendo especialmente sensibles incluso si están en «formato anónimo», de hecho, destacan y reconocen la imposibilidad de una anonimización irreversible debido a que siempre habrá un «riesgo residual de identificación» como ocurre con las enfermedades raras (Considerando 60).

En el caso de que los responsables del tratamiento sean las Administraciones Públicas, y en el escenario pandémico, el apartado 3, del artículo 27 del Real Decreto-ley 21/2020, de 9 de junio, señalaba específicamente; «que garantizarán la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que los tratamientos afectan a categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad».

Además, la resistencia a los ataques debería ser un objetivo de todos los sistemas incluidos las aplicaciones con sensores de localización. Los datos personales recogidos deberán haber sido recogidos conforme a la legislación aplicable, y de forma específica, se tendrán que realizar «pruebas verificables del origen legítimo de los datos, el cumplimiento del derecho de transparencia de los pacientes y la necesidad de cumplir con las aprobaciones éticas y legales adecuadas para el tratamiento de

pseudonimizados donde se exige la evaluación de impacto, normas de calidad, directrices internacionales, medidas que eviten el acceso de identificación a la comunidad investigadora, la exigencia de nombrar a un representante en un ensayo clínico si quien asume función de promoción no es de la Unión Europea. Además, de proteger a las personas físicas, pretende «no entorpecer la investigación en salud».

[50] Vid. https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf. Última consulta: 31 de octubre de 2022.

[51] Martínez, R. (2022). «Anonimització i seudonimització: Interessos legítims com a base legal per a l'activitat d'investigació». [Anonimización y pseudonimización: intereses legítimos como base legal para la actividad de investigación]. Disponible en https://www.uv.es/catedra-microsoft/ca/actualitat-1285992809455/Novetat.html?id=1286269909592. Recuperado el 19 de septiembre de 2022.

los datos»[52]. Por ejemplo, en el escenario pandémico, algunos autores como Zhang y otros[53] afirmaron que la mejora de la legibilidad de las políticas de privacidad de las aplicaciones móviles podría ser potencialmente tranquilizadora para los usuarios y podría facilitar el aumento del uso de las mismas. En concreto, se puede decir que, «los proyectos de investigación suelen exigir que se acredite el origen legítimo de los datos; que se demuestre la propia obtención por parte del proyecto, ya sea mediante actos declarativos de quien provee los datos, ya sea mediante la acreditación de las condiciones de uso del entorno de datos abierto de la fuente, ya sea mediante un acuerdo de compartición de datos; y, finalmente, que se cumpla con una declaración de aprobación ética emitida por un comité de ética acreditado conforme a la legislación nacional»[54].

Por otro lado, destacamos el riesgo de la «desviación de uso», es decir, el hecho de que, sobre la base de la disponibilidad de un nuevo tipo de datos, se desarrollen nuevos fines no previstos en el momento de la recogida de los datos, algo bastante habitual en proyectos con *big data*, por ejemplo[55]. En nuestro contexto de investigación y en la reutilización de los datos de carácter de salud no se suele aconsejar que la comunidad investigadora y los responsables del tratamiento opten como base legitimadora el consentimiento del paciente» puesto que implicaría la «interpretación estricta» parcelando un «área concreta de investigación». Piénsese, por ejemplo, en enfermedades neurodegenerativas que tienen implicaciones en las enfermedades cardiovasculares. Los responsables del tratamiento deben tener en cuenta «cualquier vínculo entre los fines para los que se han recopilado los datos personales y los fines del tratamiento posterior previsto» (art.6.4.a RGPD) o el contexto en el que se han recopilado los datos personales (Art.6.4.b RGPD).

Los responsables de tratamiento tendrán que cumplir con la normativa, y, además, tendrán que demostrarlo. A esto se refiere el *principio de accountability* y se basa en que «cuanto mayor sea el riesgo del tratamiento de datos para los derechos y libertades fundamentales de los interesados, mayores serán las *medidas (técnicas y organizativas) necesarias para mitigar esos riesgos*». Viene a fundamentarse en varios deberes de cumplimiento de los responsables del tratamiento de datos. Entre algunas obligaciones de transparencia se encuentran (art. 12 a 14 RGPD); garantizar el ejercicio de los derechos de protección de datos (art. 15 a 22); llevar registros de las operaciones de tratamiento de datos (art. 30); notificar las posibles infracciones de los datos a una autoridad nacional de supervisión (artículos 33) y a los interesados

[52] Martínez, R. (2020). «Tratamiento de datos personales en la Crisis del Covid-19. Un enfoque desde la salud pública». *Diario La Ley,* N.º 9601, Sección Doctrina, Wolters Kluwer.

[53] Zhang M, Chow A, Smith H. (2020). «COVID-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies». [COVID-19 Aplicaciones de seguimiento de contactos: Análisis de la legibilidad de las políticas de privacidad]*J Med Internet Res.* Dec 3;22(12):e21572. doi: 10.2196/21572. PMID: 33170798; PMCID: PMC7717894

[54] *Supra cit.*

[55] Grupo de Trabajo del Art. 29 (2011), p.7.

(art. 34); y, en casos de mayor riesgo, llevar a cabo una EIPD (art.35). La comunidad investigadora, gestora, el sector tecnológico que desarrolla soluciones y la industria adoptan un papel esencial al identificar, evaluar, documentar y reducir al mínimo los posibles efectos negativos de la solución tecnológica de localización, es decir, tendrán que demostrar el cumplimiento normativo respecto a la recogida de datos y la consideración de *medidas de seguridad concretas.* La recogida de datos de localización compromete inevitablemente la libertad de circulación de las personas, de ahí la necesidad de *realizar la evaluación de impacto de protección de datos personales* o EIPD[56]. Es un proceso en el que quien asume el papel del responsable del tratamiento de datos evalúa la repercusión de las operaciones de tratamiento previstas en la protección de los datos personales. No llevarla a cabo es considerado como una infracción grave, y, por ejemplo, en España puede conllevar la imposición de una sanción entre 40.000 y 300.000 € en función de los interesados afectados y la duración en el tiempo, entre otros factores. También en la propuesta del Reglamento europeo de privacidad y comunicaciones electrónicas (considerando 17) se señala la obligatoriedad de este documento, remitiendo al art. 35 y 36 del RGPD.

Otras herramientas que pueden ayudar a demostrar el cumplimiento tienen que ver con lo exigido por el comité de ética de investigación de turno, al solicitar al equipo investigador el plan de gestión de datos donde se deberá señalar el proceso y metodologías que se van a aplicar o si los datos se van a compartir en acceso abierto o la posibilidad de que se lleve a cabo una «*auditoría independiente interna y externa*». Otra forma de demostrarlo es contar con la figura del delegado de protección de datos, no obstante, se ha detectado que su ausencia en el sistema público presenta una gran dificultad técnica en los procesos y los escenarios de mayor riesgo suelen coincidir debido a la coexistencia del doble perfil académico y sanitario de los propios investigadores.

Por otro lado, el *riesgo de opacidad en la información sobre la finalidad* del tratamiento es otro de los desafíos que los responsables deben resolver. La información tendrá que ser clara y comprensible, es decir, debe contar con un vocabulario sencillo (frases cortas, sin términos jurídicos complejos o técnicos y sin ambigüedades). Además, tendrá que estar adaptada al público destinatario haciendo especial hincapié en los menores, discapacitados, minorías u otros grupos vulnerables. La transparencia en la información puede materializarse en la información relativa a la temporalidad de la conservación de los datos o a las finalidades limitadas o a la limitación en el acceso de sus datos únicamente por personas autorizadas empleando las medidas técnicas y organizativas oportunas.

El gobierno español fue sancionado, precisamente por no hacer especificado de forma clara los plazos de conservación de los datos para fines de investigación científica en la política de privacidad, incumpliendo el art. 9.2.j y 89.1 del RGPD.

[56] Vid. https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf, pp.11. Recuperado de 28 de diciembre de 2022.

En definitiva, los participantes deben comprender de forma clara las finalidades del tratamiento y, además, deberán conocer si hay terceros del sector privado como empresas farmacéuticas que comercialicen con sus datos personales pseudonimizados. La investigación científica cumple una función valiosa en una sociedad democrática para exigir cuentas a los «actores poderosos», y esto ha aumentado su importancia con la concentración del control sobre los flujos de información en manos de unas pocas empresas globales privadas (Supervisor Europeo de Protección de Datos, 2020)[57].

IV. LA LEGITIMIDAD DE LA FINALIDAD DEL TRATAMIENTO DE DATOS CON FINES DE INVESTIGACIÓN CIENTÍFICA

La comunidad investigadora, gestora, el sector tecnológico que desarrolla soluciones técnicas y la industria como sujetos jurídicos adoptarán una posible base jurídica que les legitime para el uso de los datos personales en el marco de una investigación científica. La legalidad es un principio esencial en materia de protección de datos e implica que los responsables del tratamiento se asegurarán de tener una base legal para el tratamiento de los datos personales.

El «consentimiento» puede ser una base jurídica útil para el tratamiento de datos en una aplicación móvil que recoja datos de localización, especialmente si los responsables del control tienen una relación directa con quien proporciona los datos que serán utilizados en el proyecto de investigación. Por ejemplo, si una aplicación móvil tiene por objeto recoger datos de localización de un grupo limitado de participantes con el fin de investigar y analizar la repercusión de la contaminación atmosférica y su relación con el desarrollo de la enfermedad del alzhéimer, el consentimiento puede servir de forma suficiente como base jurídica para el tratamiento. El consentimiento debe ser «específico para cada uno de los distintos fines» para los que se trataron los datos. Los participantes elegirán activamente el «nivel de la geolocalización» (por ejemplo, una localidad, un barrio, código postal o con la mayor precisión posible). En cualquier caso, los responsables del tratamiento tendrán muy en cuenta las directrices sobre el consentimiento proporcionadas por el Comité Europeo de Protección de Datos (Comité Europeo de Protección de Datos, 2020)[58]. Además, deberán indicar claramente si su servicio se limita a responder a la pregunta voluntaria *«¿dónde me encuentro ahora mismo?»* o si su finalidad es responder a las preguntas *«¿dónde estás?, ¿dónde has estado* y *¿dónde estarás la próxima semana?».* Si la finalidad del tratamiento cambia sustancialmente, los responsables del tratamiento tienen que recabar la «renovación del consentimiento específico». Por ejemplo, si inicialmente, la comunidad investigadora, gestora, desarrolladora o los fabricantes consideran

[57] Vid. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, pp. 5-6. Recuperado de 29 de diciembre de 2022.

[58] Vid. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf Recuperado de 28 de diciembre de 2022.

como «no relevante» la comunicarían datos personales a ningún tercero, pero ahora desean compartirlos, tendrán que contar con el consentimiento previo y expreso de cada participante. Una falta de respuesta —o cualquier otro tipo de modalidad de desistimiento— no sería suficiente.

En el contexto pandémico, el apartado 2, del artículo 27, del Real Decreto-ley 21/2020, de 9 de junio, señaló concretamente que el tratamiento tendrá por finalidad el *seguimiento y vigilancia epidemiológica del COVID-19* para *prevenir y evitar situaciones excepcionales* de especial gravedad, atendiendo a razones de *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, además, añade para más énfasis que «los datos recabados serían utilizados exclusivamente con esta finalidad», por tanto en este caso la base jurídica no se limitó al consentimiento sino que se adoptó el mero interés público de la salud pública.

La LOPDGDD señala las finalidades para las que se puede otorgar el consentimiento al tratamiento, recoge la posibilidad de reutilizar la información sobre la que se ya se haya prestado consentimiento con anterioridad y recoge el uso de datos pseudonimizados como una opción para facilitar la investigación sanitaria incluyendo garantías para evitar la reidentificación de los afectados. Además, regula las garantías de este tratamiento, incluyendo la intervención de los Comités de Ética de la Investigación o, en su defecto, del DPO o de un experto en protección de datos personales. De hecho, en su Disposición 17, 5.ª , parece facilitar o habilitar, de alguna manera, la propia investigación del Covid-19, por parte del sector público y privado con legitimación «sin el consentimiento directo», así como las cesiones de datos de fuentes variadas para usos secundarios y la reutilización en «líneas» o «áreas» de investigación afines en lucha contra el Covid-19. Esto último, únicamente a autoridades e instituciones públicas sanitarias estudios de salud sin consentimiento «en situaciones de excepcional relevancia y gravedad para la salud pública», como se trataría del contexto pandémico vivido[59].

Por su parte, el RGPD prevé una derogación específica de los atributos de consentimiento, permitiendo a los responsables del tratamiento hacer uso de un «consentimiento amplio» como base jurídica del tratamiento. Éste debe entenderse en relación con el considerando 33, en el que se afirma que «a menudo no es posible identificar plenamente la finalidad del tratamiento de datos personales con fines de investigación científica en el momento de la recogida de los datos». Por lo tanto, se debe permitir a los interesados dar su consentimiento a *determinados ámbitos de la investigación científica* cuando se ajusten a las normas éticas reconocidas para la investigación científica. Se trata de una herramienta excepcional que sólo puede ser aceptable si se cumplen varias condiciones, y si se utiliza para categorías especiales de datos, los responsables del tratamiento tendrán que asegurarse de que su regulación nacional lo

[59] Vid. Informe Jurídico 073667/2018 de la AEPD. Recuperado de https://www.aepd.es/es/documento/2018-0046.pdf . Última consulta: de diciembre de 2022.

permita. También deberán ser conscientes de las salvaguardias que deben aplicarse y debe garantizarse la «proporcionalidad entre el objetivo de la investigación y el uso de categorías especiales de datos».

Por tanto, *¿qué garantías podríamos utilizar para evidenciar el cumplimiento normativo?* Algunas podrían ser: (a) *el voto positivo de un comité de ética de investigación*[60] antes de tratar los datos para fines de investigación posteriores; (b) el uso de la *web del centro de investigación* para informar a los participantes en el estudio*;* (c) *el empleo* de *medidas citadas ya* relativas a la minimización de datos, la codificación, la anonimización o la pseudonimización; (d) el uso de *guías* que ilustren de forma clara los procesos de trabajo previstos y las cuestiones que serán objeto del proyecto de investigación; (e) la evaluación de la posibilidad de trabajar con *consentimiento dinámico*; (f) la *justificación* de por qué en este proyecto de investigación no es posible una especificación más detallada de los propósitos de la investigación.

Ahora bien, volviendo al «interés público» ¿se podría optar por el como base jurídica? (art. 6.1.e RGPD). Si se opta por esta opción, deberá ser establecido por la legislación de la UE o de un Estado Miembro[61]. Además, esta base jurídica supondría una exención a la prohibición de tratamiento de categoría de datos especiales (art. 9.2.i RGPD). Tal y como señala la jurisprudencia europea[62], la necesidad y el interés público implican una «necesidad apremiante», en oposición a ventajas principalmente privadas o comerciales. No obstante, como sólo se pueden tratar datos de categoría especial sobre la base de la legislación de la UE o de los Estados Miembros, es difícil, sino imposible, considerar el «interés público sustancial» como base para el tratamiento de datos confidenciales con fines de investigación científica (Supervisor Europeo de Protección de Datos, 2020)[63]. El desarrollo normativo de la Unión Europea y de los Estados Miembros deberá incluir todos los motivos legitimación para el tratamiento con las condiciones ofreciendo las garantías adecuadas conforme al artículo 6, 9(2) j y el 89 del Reglamento (UE) 2016/679[64].

---

[60] Vid. Disposición Decimoséptima, aptdo 2, letra c) de la LOPDGDD.

[61] Ayuso (2021) señala acertadamente la necesidad de disponer de una «base normativa» que ampare estos tratamientos y que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado. El autor distingue dos supuestos; (i) por un lado, «el tratamiento de datos de salud de interesados cuando sea necesario comunicar a otras personas con los que dicha persona física ha estado en contacto la circunstancia del contagio, para salvaguardarlas del mismo e impedir que estas, por desconocimiento de su contacto con un contagiado, puedan expandir la enfermedad a otros terceros». Por otro lado, distingue el supuesto de «la realización de estudios científicos sin necesidad de contar con el consentimiento del titular de los datos, siempre que la excepcionalidad, relevancia y gravedad de la situación para la salud pública así lo aconseje, como sucederá con aquellas investigaciones científicas que podrán llevarse a cabo para corregir los efectos propios del COVID-19, toda vez que las especiales circunstancias derivadas de esta pandemia así lo justifican».

[62] Vid. Sentencia Handyside contra el Reino Unido aplicación no. 5493/72 (CEDH, 7 de diciembre de 1976); Leander c. Suecia aplicación no. 9248/81 (CEDH, 13526.03.1987).

[63] *Ibidem.*

[64] *Ibidem.*

En los últimos tiempos[65] se está estudiando la posibilidad de completar de alguna forma este vacío jurídico, a través de nuevas normativas (Propuesta de Ley de Datos, Ley de Gobernanza de Datos y Propuesta de Reglamento del Espacio Europeo de Datos Sanitarios, etc.) de hecho, debido a la digitalización y al valor de ese conocimiento en manos de unos pocos poderosos, algo que podría considerarse como «antidemocrático», donde a través de sus políticas de privacidad se permite un amplio margen para determinar cómo desean tratar los datos y con quién compartirlos. Lo que se pretende regular es el acceso en toda la UE a datos personales de propiedad privada con fines de investigación que sirvan a un interés público como mejorar la prestación de atención médica. Estoy de acuerdo con el Supervisor Europeo de Protección de Datos al indicar que una base jurídica de interés público para que las empresas dominantes divulguen los datos a los investigadores debería estar formulada, junto a la prueba de proporcionalidad rigurosa y garantías contra el uso indebido y acceso ilegal. Esta institución podría efectivamente ayudar a generar un debate con grupos de usuarios, comunidad investigadora y empresas tecnológicas.

Por otro lado, a mi modo de ver, cuando se habla del consentimiento como base legitimadora no siempre va «sola» sino acompañada de otras. En este sentido, Nicolás[66] señala que la normativa «RGPD y la LOPDGDD reconocen distintas bases jurídicas, junto con el consentimiento de las personas, para tratar los datos de carácter personal relativos a la salud y los datos genéticos, en particular cuando se trata de finalidad científica, pero es importante subrayar que estas otras bases jurídicas no podrán sustentar el tratamiento si suponen que las garantías para los derechos de los titulares quedan debilitadas». Además, añade que «esta condición exige que los derechos del titular sobre sus datos estén nítidamente definidos y protegidos, lo que puede incluso significar un mecanismo que otorgue un control más reforzado que la expresión de un consentimiento».

Por todo ello, sería interesante señalar de una forma, qué bases legitimadoras podrían acompañar al consentimiento explícito, coinvirtiéndose en «doble legitimación».

El Comité Europeo de Protección de Datos señaló la necesidad e importancia de «revisar» la legitimación, ya que pueden existir situaciones donde las personas —también en investigación científica o biomédica— pertenezcan a un «grupo desfavorecido» desde el punto de vista económico o social, o en casos de dependencia institucional o jerárquica la legitimación puede resultar dudosa. Por ello, se podría

[65] Ver recomendaciones 16-23 de la Comisión de Ética de Datos de Berlín, Opinión de la Comisión de Ética de Datos-Resumen Ejecutivo, 22 de octubre de 2019. Disponible en https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.html;jsessionid=1B71C1E6D363C833EC7F485C2AF205AD.1_cid297?nn=11678512. Recuperado de 7 de septiembre de 2022.

[66] Nicolás, P (2019). «Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos». Revista de Derecho y Genoma Humano. Núm. Extr. 29-167

recomendar optar por una «doble legitimación del *interés público*[67] o legitimación de *interés legítimo*»[68]. Por su parte, la Agencia Española de Protección de Datos[69] ya comenzó hace años a recordar que se podría hacer investigación sin consentimiento «siempre que fuera investigación de interés público» con el visto del Comité de Bioética.

IV.1. Reutilización de datos secundarios. Limitación de la finalidad y presunción de compatibilidad

La legislación europea siempre ha detectado la importancia estratégica de la reutilización de datos y, prueba de ello es que, en el RGPD se ha visto reflejado con el art. 5.1.b, el cual señala que el *tratamiento posterior* con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el art. 89, apartado 1, «*no se considera incompatible con los fines iniciales*». La presunción no es una autorización general para seguir procesando datos en todos los casos con fines históricos, estadísticos o científicos. Cada caso debe ser considerado en sus propios méritos y circunstancias. Pero, en principio, los datos personales recopilados en el contexto comercial o sanitario, por ejemplo, pueden ser utilizados con fines de investigación científica por los responsables de tratamiento original o por uno nuevo, si existen las garantías adecuadas (Supervisor Europeo de Protección de Datos, 2020)[70]. De forma específica, la Disposición Decimoséptima de la LOPDGDD, señala que: «(b) las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos *sin el consentimiento* de los afectados en *situaciones de excepcional relevancia y gravedad para la salud pública*; (c) se considerará lícita y compatible la *reutilización de datos personales* con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los *datos para finalidades o áreas de investigación relacionadas* con el área en la que se integrase científicamente el estudio inicial».

Existen cada vez más iniciativas de grupos de *stakeholders* (comunidad de pacientes, científica, sanitaria, reguladora, o de la industria, etc..) que aúnan esfuerzos para crear mapas de actuación en el uso de datos sanitarios estructurados en ensayos y estudios de investigación sanitaria que no dependa de enfermedades concretas y que

---

[67] Vid. Art. 6.1.e RGPD y LIB.

[68] Vid. D.A. 17.ª 2. d)

[69] También la Autoridad Catalana de Protección de Datos señaló que el tratamiento de datos pseudonimizados para fines de investigación biomédica puede encontrar suficiente habilitación en bases jurídicas diferentes a la del consentimiento y artículo 9.2. aptdo. J) en conexión con el art. 89 RGPD. Cuando concurran las circunstancias del Decimoséptima Adicional, apartado 2, letra d, de la LOPDGDD, no será imprescindible el consentimiento de los afectados para llevar a cabo el tratamiento de los datos pseudonomizados.

[70] *Ibidem.,* p. 22.

responda a las necesidades de las partes interesadas y del público en general, aumentando el valor de los datos recogidos regularmente para el bienestar de la sociedad en el futuro. Es el caso del marco de normas mínimas CORE-EHR de la Sociedad Europea de Cardiología y el consorcio *Big Data Heart*[71]. Algunas normas señaladas son (i) «la construcción y vinculación del conjunto de datos»: aclarar la fuente, la integridad y la vinculación de los datos sanitarios utilizados en el estudio; (ii) «la adecuación de los datos a su finalidad»; (iii) «proporcionar detalles» sobre los sistemas de codificación utilizados, cualquier manipulación de los datos y la evaluación de la calidad de los mismos; (iii) «resultados y definiciones de las enfermedades; (iv) «permitir a otras personas investigadoras reutilizar y mejorar» indicando claramente todos los códigos y algoritmos utilizados, incluidos los relativos a la identificación de los pacientes, la terapia, los procedimientos, las comorbilidades y los resultados; (v) «análisis»: describir cómo se analizaron los resultados para permitir su validación y reproducción; (vi) «ética y gobernanza»: comunicar los procesos de consentimiento, privacidad de los datos y participación de los pacientes y el público. De hecho, también podría elaborarse o adaptarse las reglas básicas citadas en el trabajo para proyectos de investigación con tecnología de localización.

En la propuesta de Reglamento del Espacio Europeo de Datos Sanitarios, se indica de forma específica que «el tratamiento de los datos sanitarios electrónicos personales está sujeto a las disposiciones del Reglamento (UE) 2016/679», —algo que el Comité y el Supervisor europeo de protección de datos[72] de forma conjunta, acogen favorablemente—, ya que de esta manera se protege al titular, no obstante, la legislación se lamenta de que las bases de datos europeas (por ej. Plataforma Europea para el Registro de Enfermedades Raras) para «*uso secundarios y reutilización de datos*» en algunos ámbitos no se facilitan para fines distintos a los que se recogieron, ya que se limita la capacidad de la comunidad investigadora, sanitaria, o gubernamental, medicina personalizada, etc. En cualquier caso, cabe hacer una precisión —que ya advertimos al inicio—, se debe evitar toda opacidad en la información de las finalidades. La transparencia en el deber de información debe cumplirse en todos los ámbitos que contempla esta nueva ley. Por otro lado, la legislación otorga ciertos «deberes» a los titulares; «todos los titulares de datos deben contribuir a establecer diferentes categorías en los datos sanitarios electrónicos que tengan disponibles para

[71] Koetcha, D. et al. BigData@Heart Consortium, European Society of Cardiology, CODE-EHR international consensus group, «CODE-EHR best practice framework for the use of structured electronic healthcare records in clinical research», [Marco de buenas prácticas CODE-EHR para el uso de historias clínicas electrónicas estructuradas en la investigación clínica]. *European Heart Journal*, 2022;, ehac426, disponible en https://doi.org/10.1093/eurheartj/ehac426.

[72] Comité Europeo de Protección de Datos y Supervisor Europeo de Protección de datos. (EDPB & EDPS, 2022). Joint Opinion EDPB-EDPS 03/2022 on the proposal for a Regulation on the European Data Space for Health Data [Opinión conjunta EDPB-EDPS 03/2022 sobre la propuesta de un Reglamento sobre el Espacio Europeo de Datos Sanitarios], 11, julio 2022. Disponible en https://edps.europa.eu/system/files/2022-07/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en_.pdf

su uso secundario». Puede parecer que se traslada la obligación al interesado del buen funcionamiento de una competencia que corresponde a la Administración Pública y a los entes públicos. Quizás podría ser más acertado incentivar los ecosistemas comunitarios donde pacientes, usuarios, personal sanitario, hospitales, gobierno y demás *stakeholders*[73] participan trabajando con *«data for good»* a través de diferentes políticas públicas.

También, respecto a datos secundarios, ha querido pronunciarse la legislación en la normativa denominada Ley Europea de Datos (considerando 68), señalando, sin entrar en detalles que, las actividades de investigación científica o actividades analíticas «deben ser compatibles con la finalidad para la que se solicitaron los datos y los titulares de datos deben ser informados del ulterior intercambio de los datos que había facilitado», algo que probablemente las instituciones como el EDPS y la EPDB revisarán de cerca, instando al principio de limitación de la finalidad (artículo 5.1.b) RGPD) y «prueba de compatibilidad» (artículo 6.4 RGPD), así como las salvaguardas y excepciones relativas al tratamiento con fines científicos (artículo 89.1 RGPD). La prueba debería seguir considerándose antes de la reutilización de los datos con fines de investigación científica en particular cuando los datos hayan sido recolectados originalmente para propósitos muy diferentes o fuera del área de investigación científica[74].

V. CONCLUSIONES

i. A lo largo del trabajo se ha señalado que los datos recogidos por las soluciones tecnológicas resultan bastante necesarios a corto y largo plazo (Pérez & Batista, 2020), y, además, de forma más específica, se ha determinado que los datos de localización en el entorno científico tendrán que entenderse como un «bien común» o «bien público» (Calacci, et. Al., 2020), protegiendo los derechos y libertades de las personas con las garantías normativas establecidas. Por ende, las decisiones políticas resultaron eminentemente determinantes para la gobernanza de datos, el respeto a los derechos fundamentales y la gestión de la salud pública.

ii. No podemos desdeñar el contexto de incertidumbre vivido en la pandemia y el papel protagonista que tuvieron que adoptar los principios del tratamiento de datos (Bradford et al, 2020) para intentar acoplarse a las necesidades de salud pública. Esto fue posible, mayormente, debido a que la legislación contemplaba hipotéticos escenarios pensando en el ébola o la gripe aviar,

[73] Vid. https://www.rri-tools.eu/-/salus-coop-a-framework-for-a-citizen-led-approach-to-the-collaborative-managing-amp-governance-of-health-data . Recuperado a 30 de diciembre de 2022.

[74] Supervisor Europeo de Protección de Datos (SEPD, 2020), p. 23. Un dictamen preliminar sobre la protección de datos y la investigación científica. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOC_2019_370_R_0007&from=ES

donde el uso de los datos son determinantes para su control, gestión e investigación, siendo precavida incluyó expresamente la base legitimadora a la que se podrían sujetar los gobiernos, administraciones públicas y demás entes. Y no sólo eso, sino que, además, «la norma también se podría encajar a escenarios de tecnología e innovación, sobre todo, porque uno de los principales motivos de su creación fue poder estar a la altura de regular el tratamiento de datos masivos recogidos por tecnología» (Pérez &Batista, 2021). Realizar una evaluación de impacto de protección de datos, contar con delegados de protección de datos, y ser transparentes otorgando información a los participantes de forma clara y concisa, son algunas de las obligaciones imprescindibles a tener en cuenta por el sector público y privado.

iii. También se han abordado algunos riesgos como son el alto impacto en los derechos de los miembros de comunidades o grupos vulnerables, el nivel de invasión de esta tecnología, la dificultad práctica de la irreversibilidad de los datos anónimos, o incluso, la desviación del uso de la información, proponiendo a la comunidad académica y científica una aproximación a posibles soluciones. Por ejemplo, adoptamos como medida posible el optar por la «doble legitimación» del interés público o legitimación de interés legítimo para reforzar la protección de los derechos fundamentales de estas personas.

iv. Respecto a la «anonimización», la preocupación es mayor debido a la temida y advertida «reidentificación» que no puede ser evitada por completo tal y como se viene señalando más aún en el caso de datos de gran dimensión. Desde las instituciones comunitarias se ha reconocido que siempre existirá el «riesgo residual de identificación» como ocurre con las enfermedades raras. Se debe tener presente que los datos anomizados no son datos personales y, por tanto, la aplicación de la normativa no será por cuenta del RGPD o LOPDGDD sino por cuenta del Reglamento sobre la privacidad y las comunicaciones electrónicas.

v. Además, se ha arribado a la deducción de que la «presunción de compatibilidad» para el uso de datos secundarios no supone una autorización general para seguir tratando datos en todos los casos con fines, por lo que cada caso debe ser considerado en sus propios méritos y circunstancias, pero, en principio, los datos personales recopilados en el contexto comercial o sanitario pueden ser utilizados con fines de investigación científica por los responsables del tratamiento original o por uno nuevo, siempre que existan las garantías adecuadas. En el contexto pandémico, 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 el Covid-19, preveía que la legitimidad del tratamiento se basaría en el interés público esencial en el ámbito de la salud pública para la protección de intereses vitales de los afectados y de otras personas, sin parecer existir previsión de «reutilización de datos» ni siquiera con fines de investigación o previsiones

específicas respecto a las garantías o medidas de seguridad (Cotino, 2020), remitiendo en todo caso al RPGD y a la LOPDGDD.

vi. Por su parte, la normativa futura del Espacio Europeo de Datos Sanitarios parece trasladar la obligación a la ciudadanía como titulares de los datos del buen funcionamiento y de la diversidad de categorías de datos disponibles para su uso secundario. Se trata de una competencia que quizás, correspondería más bien a la Administración Pública y a los entes públicos en el marco de las oportunas políticas públicas. En este sentido, podría ser más acertado incentivar los ecosistemas comunitarios donde pacientes, participantes, personal sanitario, hospitales, gobiernos y demás *stakeholders* participaran trabajando con *«data for good»* o datos para el bien.

vii. En definitiva, el uso de los datos de localización con fines de investigación han de contener las suficientes garantías para proteger los derechos de las personas, contando, además, con «flexibilidad y racionalidad necesarias para no obstaculizar la labor de investigación en salud pública, que incluye también la investigación epidemiológica» (Serrano, 2020).

Title:

Location Technology Applied to Scientific Research: Regulatory Compliance with Regard to the Protection of Personal Data.

Summary:

Resumen:

Al inicio de la pandemia surgieron múltiples aplicaciones móviles escalables con tecnología de rastreo promovidos por administraciones públicas

y gobiernos con el objeto de gestionar y controlar la pandemia, generando datos personales e individuales como agregados. Los operadores de telecomunicaciones las pusieron en manos de las autoridades y organismos epidemiológicos y aunque no se compartía información personal se pudo comprobar que a través de los metadatos y la combinación de los mismos se podía obtener información personal y vulnerar los derechos fundamentales de las personas e incluso su propia seguridad. El noventa y cinco por ciento de las personas se pueden identificar fácilmente desde solo cuatro puntos de ubicación diferentes. Además, con las alianzas entre empresas tecnológicas y organizaciones farmacéuticas nace un cierto riesgo a la «mercantilización» de los datos con fines más espurios que no tendría porque coincidir con el principal interés público de la salud pública, y esto nos sitúa a la comunidad investigadora en el momento oportuno para reflexionar sobre la legitimidad del tratamiento de esos datos, los riesgos y su nivel de «anonimización» (y la más temida y advertida) «reidentificación», la cual no puede ser evitada por completo.

Cuando se habla del consentimiento como base legitimadora no siempre tiene que ir «sola» sino acompañada de otras bases legitimadoras. Por ello, sería importante que se estableciera normativamente cuáles podrían componer una «base legítima doble», optando preferiblemente, por el interés público y el interés legítimo. En caso de elegir únicamente la base jurídica de interés público, debería estar formulada junto a la prueba de proporcionalidad rigurosa y garantías contra el uso indebido y acceso ilegal.

En definitiva, se deberá percibir a la privacidad como un valor institucional (acorde a las políticas públicas) desde el inicio identificando el nivel de invasión recogiendo la menor cantidad de datos, evitando cualquier tipo «opacidad en la información» e implementando medidas técnicas como la anonimización y pseudonimización sin perjudicar el fin propio de la investigación.

Abstract:

At the beginning of the pandemic, multiple scalable mobile applications with tracking technology emerged, promoted by public administrations and governments with the aim of managing and controlling the pandemic, generating personal and individual data as aggregates. Telecommunications operators put them in the hands of epidemiological authorities and agencies, and although no personal information was shared, it became clear that through metadata and the combination of metadata it was possible to obtain personal information and violate people's fundamental rights and even their own safety. Ninety-five percent of people can be easily identified from only four different locations). Moreover, with alliances between technology companies and pharmaceutical organisations comes a certain risk of 'commoditisation' of data for more spurious purposes that would not necessarily coincide with the overriding public interest of public health, and this places us in the research community at the right

moment to reflect on the lawfullness of the processing of these data, the risks and the level of «anonymisation» (and the most feared and warned against) «re-identification», which cannot be completely avoided.
When talking about consent as a legitimate basis, it does not always have to be «alone» but accompanied by others, so it would be important to establish normatively, which could make up the «double legitimate basis», opting for the public interest and the legitimate interest. In case only the public interest legal basis is chosen, for dominant companies to disclose data to researchers, it should be formulated together with the strict proportionality test and safeguards against misuse and illegal Access.
In short, privacy should be perceived as an institutional value (in line with public policy) from the outset, identifying the level of invasiveness by collecting the least amount of data, avoiding any kind of 'data opacity' and implementing technical measures such as anonymisation and pseudonymisation without harming the purpose of the research itself.

Palabras clave:

geolocalización, investigación científica, protección de datos personales, legitimación, COVID.

Key words*:*

geolocation, scientific research, personal data protection, lawfullness, covid.