DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

LA PROTECCIÓN DE DATOS PERSONALES EN TIEMPOS DE PANDEMIA: ASPECTOS CONTROVERTIDOS DESDE LA RELACIÓN PÚBLICO-PRIVADA

PROTECTION OF SENSITIVE DATA: LESSONS LEARNED FROM THE PUBLIC-PRIVATE RELATIONSHIP

Jorge Luis Ordelin Font*

The same technology that identifies coughs could also identify laughs

Noah Harari, 2020

RESUMEN. La pandemia provocada por el COVID-19 ha demostrado que las previsiones legislativas adoptadas en la gran mayoría de los países latinoamericanos para el tratamiento de los datos personales no son suficientes. El presente trabajo tiene como objetivo analizar los principales riesgos que se presentan en el tratamiento de datos personales a partir de la relación entre los sectores público y privado. Para ello, se analizan las inconsistencias que, en materia regulatoria y su aplicación, se observan en los términos y condiciones de algunas de las aplicaciones utilizadas para el enfrentamiento de la pandemia. Todo ello lleva a concluir que la configuración, interpretación y aplicación de las regulaciones del tratamiento de los datos relativos a la salud necesitan ser repensadas.

PALABRAS CLAVE. Datos relativos a la salud, anonimización, riesgos, relación público-privada, datos personales.

* Investigador Nacional Nivel 1. Investigador en el Centro Interamericano de Estudios en Seguridad Social (CIESS). Miembro de la Línea de Investigación de Inteligencia Artificial y Derecho. Email: *jlordelin@gmail.com*.

Revista Estudios en Derecho a la Información, núm. 14, julio-diciembre de 2022, pp. 29-56.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

ABSTRACT. *The pandemic caused by COVID-19 has shown that the legislative provisions adopted in the vast majority of Latin American countries for the treatment of sensitive data are not sufficient. The objective of this work is to analyze the main risks that arise in the treatment of sensitive data from the relationship between the public and private sectors. For this, are analyzed the regulatory inconsistencies and their application observed in the terms and conditions of some of the applications used to deal with the pandemic. All this leads to the conclusion that the configuration, interpretation, and application of the regulations for the treatment of sensitive data need to be rethought.*

KEYWORDS. *Data related to health, anonymization, risks, public-private relationship, personal data.*

I. INTRODUCCIÓN

El enfrentamiento de la pandemia de la enfermedad por COVID-19 ha permitido extraer un grupo de lecciones en relación con la regulación del tratamiento de los datos, en particular los relativos a la salud[1] y en las sinergias que se establecen entre el sector público y privado. Pese a lo que pudiera pensarse, las interrogantes no se encuentran en la legitimación para realizar el tratamiento de estos datos por parte de los Estados, sino de cómo este tiene lugar y sus implicaciones, a raíz de la colaboración entre los sectores público-privado para la resolución de una situación de emergencia como la que enfrentamos.

La revisión a los términos y condiciones de algunas de las aplicaciones en América Latina deja entrever la existencia de un grupo de vacíos y lagunas que potencialmente abren brechas para un tratamiento negativo de los datos, especialmente los relativos a la salud. Dichos usos no se corresponden con las regulaciones sobre el respeto de la privacidad de las personas y pueden tener

[1] También denominados en algunas legislaciones y en la doctrina sensibles o categorías especiales de datos personales. El artículo 9o. del Reglamento Europeo de Datos Personales (RGPD) hace referencia al término "tratamiento de categorías especiales de datos personales", *entre los que se encuentran los datos relativos a la salud, entendidos como los* "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" (artículo 4.15 RGPD). A los efectos de este trabajo se utilizarán indistintamente ambos términos.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

incidencia en la vulneración de otros derechos. En este sentido se impone una revisión de los marcos regulatorios vigentes para concretar disposiciones jurídicas que hasta este momento parecían muy claras y que hoy devienen insuficientes. Por otro lado, las normas que regulan el tratamiento no son claramente interpretadas y aplicadas, no sólo desde él ámbito privado sino también en el público. De hecho, inconsistencias que se presentan en el tratamiento de datos personales realizado por el sector público inciden en la forma que este se realiza en el ámbito privado.

Las normas de protección de datos personales están esencialmente enfocadas desde un ámbito individualista, de protección de la privacidad de las personas y el poder de estos frente a quienes utilizan sus datos personales, no obstante, es necesario replantear algunos aspectos de este modelo, especialmente en relación con una visión colectiva y proactiva del uso de estos datos personales. Ello no es solo una responsabilidad del titular del dato, sino también del Estado en cuanto a su deber de protección y regulación ante el uso de nuevas tecnologías. Al respecto surgen interrogantes sobre la legitimación del sector privado para tratar datos personales relativos a la salud y bajo cuáles condiciones, cuando existe colaboración entre el sector público y el privado. En correspondencia con ello surge la pregunta: ¿Cuáles son los principales riesgos que existen en el tratamiento de datos personales en la relación entre el sector público y privado para enfrentamiento de la pandemia provocada por la COVID-19?

El presente artículo tiene como objetivo analizar algunos de los riesgos que se presentan en el tratamiento de datos personales a partir de la relación entre el sector público y privado durante el enfrentamiento de la pandemia, con especial énfasis en la gestión de la anonimización. Como principal idea se plantea que en la relación público-privada para el desarrollo y aplicación de soluciones tecnológicas en el enfrentamiento de la pandemia de la COVID-19, existe un grupo de riesgos para la protección de los datos personales, lo que hace necesaria la adopción de un conjunto de garantías efectivas que minimicen el impacto del uso de estas tecnologías en la protección de este derecho, y al propio tiempo, permita maximizar la eficacia en el uso de estas tecnologías. Ante esta situación es necesario resaltar el papel de las entidades de protección de datos personales en la supervisión y control de este tipo de iniciativas y en particular el cumplimiento de las garantías relacionadas con la anonimización, y las exigencias de transparencia y privacidad en el diseño.

Para lograr el objetivo se divide en tres partes, la primera describe la relación entre el tratamiento de datos relativos a la salud y la pandemia, la segunda explica los riesgos que existen con el tratamiento de estos datos y su

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

anonimización, en particular las posibilidades de reidentificación y la cesión a terceros, y por la tercera hace especial referencia a la necesidad de reforzar el papel de las autoridades de protección de los datos personales en este contexto. El artículo utiliza una metodología esencialmente descriptiva, no persigue realizar un análisis comparado sobre estos riesgos y los ejemplos utilizados hacen referencia a prácticas encontradas durante la investigación en varios países. Un análisis pormenorizado requiere de un estudio de mayor envergadura que proponga soluciones para cada uno de los supuestos conforme a la tecnología utilizada.

II. La intervención del sector privado en la atención de la pandemia: ¿colaboración o lucha de contrarios?

Uno de los aspectos más controvertidos en el enfrentamiento a la pandemia ha sido la participación de la iniciativa privada en el desarrollo de soluciones tecnológicas y el papel de los entes reguladores. Este no es un tema baladí. Son innumerables los ejemplos que existen de esta colaboración.[2]

En el continente americano se ha reconocido el valor del sector privado en este contexto donde los problemas de los sistemas de salud públicos son agudos. Carissa F. Etienne, directora de la Organización Panamericana de la Salud, en la Reunión Virtual de la Plataforma de Acción COVID del Foro Económico Mundial para América Latina, reconoció la importancia de la colaboración pública-privada e hizo un llamado a potenciar este tipo de relaciones para poder enfrentar la pandemia, al respecto apuntó:

> El sector privado tiene un papel importante para garantizar la resiliencia de los sistemas de salud. Sus recursos, incluidos los servicios de atención médica, las instalaciones, los laboratorios, la capacidad de logística de transporte,

[2] Podemos citar, por ejemplo, la Alianza del Gobierno vasco con la empresa regional Sherpa.ai, experta en servicios de inteligencia artificial. A partir de esta alianza se desarrolló la tecnología de una plataforma que predice las necesidades futuras de las Unidades de Cuidados Intensivos (UCI), específicamente el número necesario en los siguientes siete días. La exactitud de esta tecnología permite reconocer patrones y tendencias de infectados y futuros focos (Redacción TICPymes, 2020). En Estados Unidos el gobierno estuvo particularmente interesado en comprender los patrones de los movimientos de las personas, que se pudieran derivar a través de los datos que gigantes tecnológicos como Facebook, y recopilación de los usuarios. La administración de Trump solicitó a las empresas utilizar su experiencia técnica para ayudar a quienes se ocupan de las consecuencias del coronavirus, incluyendo información relacionada con el rastreo y propagación del virus, así como la creación de bases de datos de empresas tecnológicas y el análisis de información utilizando inteligencia artificial (Overly, 2020).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

> la dotación de personal, los sistemas de información, la tecnología y los dispositivos, incluyendo equipos clave como los ventiladores, pueden ponerse a disposición de manera rápida para aumentar la capacidad del sistema de salud (OPS, 2020).

Sin embargo, lo cierto es que, desde el ámbito digital el tema es más complejo, desde una perspectiva social y digital esta colaboración no puede obviar las brechas que existen en la región. Según el Observatorio del Ecosistema Digital del Banco de Desarrollo de América Latina (CAF) la penetración de Internet en América Latina es sólo de un 68%, siendo su uso fundamental como herramienta de comunicación y redes sociales. El propio informe señala que el índice de resiliencia digital del hogar[3] muestra un promedio de 30,70 (en una escala de 1 a 100). En otras palabras, el 32% de la población se halla marginalizada en cuanto al acceso a Internet.[4]

Tampoco se puede dejar de tener en cuenta que los niveles de acceso son desiguales entre los distintos países, es una región muy heterogénea. Incluso en un mismo país la conectividad y el uso de Internet no se manifiesta de la misma forma en las regiones urbanas y en las rurales. Por ende, importantes sectores de la población quedarán sin acceso a estos aplicativos y, por ende, serán excluidos de los análisis estadísticos. Bajo estas circunstancias es necesario una mayor colaboración con el sector privado y establecer las sinergias que permitan subvertir estas brechas del ecosistema digital.[5]

La relación entre los sectores público y privado en el ámbito de desarrollo y aplicación de soluciones tecnológicas no es nueva. Como bien refiere el intelectual Noah Harari, tanto los gobiernos como las corporaciones han estado utilizando sofisticadas tecnologías para rastrear, monitorear y manipular a las personas, sin embargo, la situación de la pandemia provocó un importante hito de la historia de la vigilancia (Noah Harari, 2020). Esta relación entre

[3] Este índice se calcula a partir del uso de Internet para bajar aplicaciones, realizar operaciones de comercio electrónico y el uso de tecnología Fintech (Katz, Jung y Callorda, 2020: 17).

[4] A nivel mundial se estima que aproximadamente 3,600 millones de personas carecen de conexión a Internet. En los países de ingresos bajos sólo dos de cada diez habitantes están conectados a Internet (Katz, Jung, Callorda, 2020: 17).

[5] Un ejemplo de esta relación ha sido la iniciativa de la Organización Mundial de la Salud (OMS) y la Unión Internacional de Telecomunicaciones (UIT), con apoyo del UNICEF, para enviar mensajes de texto a teléfonos móviles con información sobre la COVID-19, a personas que no pueden conectarse a Internet. Estas organizaciones colaborarán con las empresas de telecomunicaciones para enviar directamente a los teléfonos móviles mensajes de texto con información vital de salud para ayudar a las personas a protegerse frente a la COVID-19. Estos mensajes llegarán a miles de millones de personas que no pueden conectarse a Internet para obtener información (OMS, 2020).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

sectores público y privado no ha estado exenta de contratiempos. En Estados Unidos, por ejemplo, las relaciones entre las empresas tecnológicas y el gobierno, como la Agencia de Seguridad Nacional, quedó evidenciada a partir de las declaraciones realizadas por el contratista de esta última agencia Edward Snowden (Romm et al., 2020).

En España un grupo de más de 60 expertos en privacidad solicitaron al gobierno actuar ante las "iniciativas privadas" que utilizaban las aplicaciones con ánimo de lucro. En una carta enviada al ejecutivo español señalaron: "cuando esta situación acabe, habrá en manos de varios actores una ingente cantidad de datos de salud, y geolocalización, entre otros, que podrán ser tratados y reutilizados con ánimo de lucro y discriminatorio" (Castillo, 2020).

La CIDH recomendó, de forma clara, que tanto las empresas, como los prestadores de la salud y demás actores económicos que participan en la contención de la pandemia, "tienen un rol clave que desempeñar en estos contextos y su conducta debe guiarse por los principios y reglas de derechos humanos aplicables" (CIDH, 2020). En consecuencia, con ello el Estado deberá rendir cuentas por su actuación durante esta situación excepcional, así como los actores privados, especialmente las empresas, quienes además podrán ser sometidas a procesos judiciales por violación de derechos humanos (recomendación 16).

Sin embargo, no podemos decir que sea clara la relación que se establece entre el sector privado y público para enfrentar la pandemia en relación con la protección de los datos personales y el respeto de los derechos de privacidad. El tratamiento de datos personales, tanto por agentes públicos como privados, es uno de los mayores desafíos de la privacidad y, en el enfrentamiento a la pandemia provocada por la COVID-19, ha quedado evidenciado. Con excepción de las normativas establecidas en las leyes de protección de datos personales, no existen normas claras sobre cómo proceder en casos de excepcionalidad como el que enfrentamos, siendo necesario un incremento en los estándares de protección cuando se realizan este tipo de colaboraciones.

Existe una necesidad de colaboración entre los diferentes actores para de forma colectiva subvertir los efectos de la crisis, y en particular para desarrollar soluciones tecnológicas confiables y seguras que coadyuven a este objetivo. La tecnología ha permitido, entre otras funciones, la geolocalización mediante la información recogida por los operadores de telecomunicaciones, la geolocalización en redes sociales, el uso de aplicaciones, webs y *chatbots* para auto-test o cita previa, las aplicaciones de recogida de información de contagiados, las aplicaciones de seguimiento de contactos, pasaportes digitales de inmunidad y cámaras infrarrojas.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

Algunas de estas soluciones han sido desarrolladas por el sector privado exclusivamente y administradas por éste, otras se desarrollan en colaboración entre el sector público y privado, y algunas han sido desarrolladas por el sector privado pero gestionadas y administradas por el sector público. A efectos de este artículo hablamos de relación público-privada en los dos últimos supuestos anteriormente referidos. Estas relaciones se pueden materializar bajo distintos supuestos no sólo de desarrollo y gestión de las aplicaciones, sino también con fines de investigación científica.[6] Sin embargo, el punto determinante de este tipo de relación es la participación de las autoridades sanitarias, como encargadas de salvaguardar los intereses de la ciudadanía en el ámbito de la salud pública.

Debido a que el tratamiento de los datos personales se realiza en el ejercicio de las funciones de las autoridades sanitarias, como parte de la administración pública,[7] estas no solo quedan obligadas a adoptar y emitir las instrucciones sanitarias correspondientes, sino también, a ser considerados responsables del tratamiento de datos personales y garantizar su correcta protección (Domínguez Álvarez, 2020: 616).

Si la colaboración no se realiza a partir de reglas jurídicas claras de respeto al derecho a la privacidad es posible que nos encontremos ante riesgo de violaciones. Para el Consejo Europeo, por ejemplo, uno de los motivos por los cuales fue cautelosa la respuesta de las empresas a la solicitud del gobierno estadounidense de acceder a datos agregados y anónimos fue precisamente el riesgo legal y los posibles daños. Según el órgano comunitario, la reglamentación de los datos hubiera "contribuido a enmarcar el diálogo entre los sectores público y privado y a determinar qué tipos de emergencias deberían estar sujetas al interés colectivo sobre los derechos individuales (así como las condiciones y garantías de ese mecanismo)" (Consejo Europeo, 2020).

---

[6] Por ejemplo, en Estados Unidos se creó un grupo de trabajo conformado por gigantes tecnológicos (como Apple y Google), empresarios e inversores, líderes de salud pública y empresas de telesalud (Romm *et al*., 2020).

[7] El concepto de autoridad sanitaria debe abordarse desde el más amplio sentido teniendo en cuenta las particularidades de cada país y la organización de su sistema de salud. En Argentina, por ejemplo, el responsable de la base de datos es la Subsecretaría de Gobierno Abierto y País Digital de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros de la Nación (la "Subsecretaría de Gobierno Abierto"), puede ceder la información personal del usuario recolectada por la aplicación únicamente a otras entidades estatales y/o establecimientos sanitarios nacionales, provinciales o municipales, para que estos puedan contener y/o mitigar la propagación del COVID-19, así como ayudar a prevenir la sobreocupación del sistema sanitario (Secretaría de Innovación Pública, 2020, art. 5.5). En este caso se debería reconocer a estos entes como parte de la administración pública.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

En España la Agencia de Protección de Datos personales procedió a investigar algunas aplicaciones privadas advirtiéndose riesgos de que los ciudadanos aportaran datos personales sensibles de buena voluntad, sin quedar determinada la finalidad para la que serían utilizados. En este país, el Informe núm. 17/2020 reconoció que, en el ámbito público, el responsable del tratamiento es el Ministerio de Sanidad y el resto de las entidades públicas o incluso privadas se constituyen como encargados del tratamiento o subencargados. Un ejemplo de este tipo de práctica tuvo lugar en la Comunidad de Madrid, la aplicación CORONAMADRID fue desarrollada de conjunto entre la Consejería de Sanidad de esta comunidad y otros actores como Telefónica, Google y otros. La aplicación permitía la recepción de resultados de la prueba, recomendaciones de actuación para la cuarentena, obtención de cita con el centro médico y el autodiagnóstico, asimismo en su política de privacidad se requería la autorización para el acceso de los datos suministrados a proveedores y colaboradores, así como a las empresas que estos subcontrataran para ayudar a las autoridades sanitarias de la comunidad en calidad de encargado del tratamiento. Este acceso de suministradores y colaboradores puede ser delicado si se tiene en cuenta que, además del nombre y apellidos, número de teléfono móvil, DNI / NIE para posterior cruce con la tarjeta sanitaria, fecha de nacimiento, dirección completa, código postal y comunidad autónoma, género, la aplicación permitía el acceso a la geolocalización (opcional) y datos de salud relacionados con la autoevaluación en función de los síntomas que se experimentan.

En Argentina se desarrolló la aplicación CUIDAR del Ministerio de Salud destinada a la prevención y al cuidado de la ciudadanía frente a la pandemia del nuevo Coronavirus SARS-CoV-2 que provoca la enfermedad por COVID-19, dicha aplicación es parte integral de las estrategias de prevención y cuidado de la salud pública ante la pandemia de COVID-19. Fue desarrollada a partir de la colaboración entre la Secretaría de Innovación Pública, el Ministerio de Ciencia y Tecnología de la Nación, la Fundación Sadosky, el Consejo Nacional de Investigaciones Científicas y Técnicas (Conicet) y la Cámara de la Industria Argentina del Software (empresas Hexacta, Globant, G&L Group, C&S, QServices, entre otras).

Empero, la colaboración público-privada que implica el tratamiento de datos personales no sólo tiene lugar en el ámbito de desarrollo de aplicaciones. En Ciudad de México a partir del 10 de junio de 2020 se implementó el Programa de Detección, Protección y Resguardo de Casos COVID-19 y sus contactos. Este programa procuraba identificar casos por medio del incremento en la capacidad para hacer pruebas, reducción de tiempo en la entrega de resultados y el aislamiento temprano de las personas y sus contactos. Para cumplimentar sus objetivos se utiliza un sistema de tamizaje automatizado

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

que utiliza diversas fuentes como SMS, la plataforma digital Locatel, la página *web* (*test.covid19.cdmx.gob.mx*), la aplicación móvil APP COVID-19 CDMX y *Facebook*. Para poder desarrollar este programa el gobierno solicitó los números de celular de las personas a las compañías telefónicas para el envío de mensajes y, a partir de ello, se realiza el contacto con las personas que tuvieron algún tipo de proximidad física con la persona confirmada para evaluar la exposición y síntomas, posteriormente los canaliza para realizar una prueba PCR.

III. El tratamiento de datos relativos a la salud en condiciones de pandemia

Existen bases jurídicas razonables para el tratamiento, la principal cuestión es cómo realizar estos (Martínez Martínez, 2020). El uso de estas aplicaciones debe ser entendido como parte de una estrategia de salud pública, y en consecuencia respetar dichos intereses. Cotino Hueso (2020a) llama a ser cautos en cuanto al hecho de que los datos sensibles y perfilados no fluyan al sector privado ni sirvan para el control de las personas, y en este sentido considera, que se debe analizar con cuidado el uso de los desarrollos tecnológicos privados, los cuales garantizarán mejor eficacia, pero muy dudosa privacidad y transparencia.

Ello significa que sólo podrá hacerse uso de las excepciones contempladas en las normas de protección de datos personales en aquellos supuestos en los cuales la colaboración sea necesaria para poder enfrentar la pandemia. En el contexto de la pandemia, y en otros de similar naturaleza el tratamiento debería ser realizado de forma transparente tras la adopción de medidas legales y tecnológicas adecuadas, y también ser realizado sin fines de lucro, sin posibilidad de intercambio de datos con terceros y bajo supervisión y control. Siendo altamente recomendable que el código fuente de las aplicaciones fueran públicos y ser susceptibles de ser sometidos a revisión. Las medidas de seguridad adoptadas deberían ser proporcionales con el volumen y sensibilidad de los datos personales tratados. Teniendo la excepción que fundamenta el tratamiento de los datos relativos a la salud, una naturaleza de carácter público no queda legitimada por la posibilidad de que los particulares puedan hacer uso de esta, si el tratamiento que hacen de este no tiene como finalidad la resolución de la situación que fundamenta dicho uso. Esto se encuentra estrechamente relacionado con la eliminación del fin de lucro tanto en el tratamiento como en la cesión de datos.

La cesión de datos por parte del sector privado sólo deber ser realizada a las autoridades competentes, teniendo en cuenta que es la colaboración

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

con estas lo que justifica dicho tratamiento. La cesión a terceros que no sean las autoridades sanitarias debe ser analizado de forma restrictiva, caso por caso y fundamentado bajo estrictos criterios tecnológicos, teniendo en cuenta las garantías brindadas por la tecnología utilizada y autorizada. No obstante, debe tenerse en cuenta que el ánimo de lucro es permitido en determinados supuestos, como es en el caso de Brasil donde el artículo 11.4 de la Ley núm. 13.709, del 14 de agosto de 2018,[8] dispone que, en principio, está vedada la comunicación o uso compartido de los datos sensibles referidos a la salud para la obtención de ventaja económica, sin embargo, la norma prevé excepciones entre las que se pueden citar la prestación de servicios de salud, de asistencia farmacéutica y de asistencia a la salud, incluidos los servicios auxiliares de diagnóstico y terapia, incluidas las transacciones financieras y administrativas resultantes de los servicios ya mencionados.

La importancia de restringir el tratamiento de datos relativos a la salud en condiciones como las que atravesamos se ve reforzada por otros elementos técnicos y jurídicos que deben ser tenidos en cuenta. Desde un punto de vista tecnológico la realidad de la pandemia demostró que el uso de estas aplicaciones para resolver este tipo de situaciones de carácter público, en particular, son esenciales en la investigación biomédica.

No sólo se recaban datos personales, sino también datos no personales los cuales en múltiples casos se hallan ligados (datos mixtos),[9] así como también datos de terceros.[10] Los datos proceden tanto de usos primarios de tratamientos médicos (como son análisis clínicos) como usos secundarios, dentro de los cuales se encuentran aquellos que son recabados a partir de la utiliza-

[8] La Medida Provisoria No. 959, de 29 de abril de 2020, modificó el artículo 65 y amplió la *vacatio legis* hasta el 3 de mayo de 2021. Sin embargo, la Ley No. 14.010, de 10 de junio de 2020, que dispuso lo concerniente al régimen jurídico emergente y transitorio de relación jurídica de Derecho Privado en el periodo de la pandemia del coronavirus (COVID-19), dispuso en su artículo 20 que la Ley No. 13.709 entraría en vigor el primero de agosto de 2020.

[9] Por ejemplo, la aplicación del Gobierno Abierto de Bogotá (GABO) reconoce que trata datos públicos, semiprivados, privados y sensibles (datos de salud y de georreferenciación). El sitio *web* locatel de Ciudad de México y su página web reconocen que solicitan, entre otros, los siguientes datos personales: género, nacionalidad, perfil en redes sociales, ubicación, descripción de sintomatologías, incapacidades médicas, discapacidades, consumo de fármacos y/o estupefacientes, estado físico o mental de la persona; enfermedades preexistentes, voz e imagen.

[10] En el Programa de Detección, Protección y Resguardo de Casos COVID-19 y sus contactos puesto que si la persona es confirmada de COVID-19 a través de una prueba, esta debe aportar cuáles son las zonas visitadas después de haber presentado síntomas de COVID-19, nombre, teléfono y domicilio de las personas con las que tuvo contacto antes y después de haber sido un caso confirmado y/o presentar síntomas.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

ción de aplicaciones tecnológicas. No es infrecuente que la separación de estos datos pueda ser imposible o inviable desde un punto de vista técnico y/o económico. Debido a que estos son datos, especialmente desestructurados, es necesaria la aplicación de inteligencia artificial para su ordenación, integración y extracción de información.

Tampoco es fácil corroborar que el tratamiento de los datos personales se realice conforme al respeto del principio mínimo, y que, en consecuencia, los datos recabados sean adecuados, relevantes y estrictamente necesarios, tampoco son claras las garantías para su tratamiento. La magnitud de los datos recabados es mayor si se tiene en cuenta que el uso de estas aplicaciones puede ser asociado no sólo a cuestiones relacionadas con la salud de los titulares, sino también, al propio sistema de protección que se ha establecido alrededor de la pandemia, como es el caso de Ciudad de México y Bogotá.[11] Lo cual como veremos más adelante incide en el periodo de conservación de estos datos.

Desde una perspectiva jurídica, el tratamiento de datos personales en el enfrentamiento de la pandemia no se materializó en la determinación de finalidades concretas en los Avisos de Privacidad, que estuvieran relacionados con la complejidad del tipo de datos que se tratan, así como tampoco en la aplicación del principio de conservación de estos datos. Es preciso la existencia de normas sencillas y claras de privacidad, que sean fácilmente accesibles y comprensibles para todo tipo de usuario, incluso para aquellas personas que tengan algún tipo de discapacidad. De manera transparente los términos y condiciones deberían permitir la comprensión de la finalidad específica de las aplicaciones, los derechos que detentan los usuarios, ante quien pueden ser estos ejercidos, las finalidades para su conservación y cuál sería el momento de supresión de los datos.

Es imprescindible tener claridad que el tratamiento de estos no puede ser realizado de forma permanente. En este sentido, la CIDH ha precisado que el almacenamiento de datos personales sólo puede ser realizado durante el periodo de duración de la emergencia, con el único fin de combatir la pandemia (apartado 36). Empero, como afirma Rodríguez (2020), es también necesario definir qué se entiende por normalidad, dado que siempre puede existir alguna razón para justificar el uso de este tipo de tecnologías. Por ejemplo, en la actualidad dos años después de la declaración de la situa-

[11] La aplicación GABO permite que los ciudadanos soliciten alguno de los programas de apoyo social y económico que brinda la Administración Distrital ("Necesito Apoyo"); ofrecer ayuda a otros ciudadanos ("Ofrezco Ayuda"), y reportar síntomas ("Reportar Estado de Salud").

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

ción de pandemia aún no existe precisión en relación con la posibilidad o no de determinar una fecha precisa de culminación de la pandemia, tras sucesivas olas de contagio y la aparición de diferentes cepas del virus.

Hace más complejo esta decisión el hecho de que el enfrentamiento a la pandemia, por parte de los Estados ha sido desigual. Mientras algunos países declararon estados de excepción conforme a lo establecido en sus textos constitucionales, otros adoptaron otro tipo de declaraciones o situaciones.[12] Aunque el común denominador fue, en todos los supuestos, la restricción de derechos tampoco puede interpretarse que una vez extinguidos estos estados excepción o situaciones declaradas se eliminará automáticamente la autorización para el tratamiento excepcional de estos datos.

La realidad ha demostrado que no coincide el fin de la pandemia con el fin del confinamiento. La práctica ha demostrado que el desescalamiento es complejo y puede ser largo aun cuando existen vacunas.[13] Cuestión distinta es la determinación del momento en que puede entenderse que la pandemia se encuentra controlada, téngase en cuenta además que esta situación puede considerarse así para un país y no para otro, motivado en gran medida por el acceso desigual a las vacunas. Cuando los países son vecinos existe riesgo de incremento de los casos positivos. Por ello, no existe claridad sobre el momento que deberá ser entendido como idóneo para la desactivación de este tipo de aplicaciones.

En México el sitio Web Locatel y su página web manifiestan que los datos especialmente protegidos (origen étnico o racial, características morales, emocionales, ideológicas, creencias, convicciones religiosas, preferencia sexual) tienen un ciclo de vida de cinco años. En Argentina los términos y condiciones de la aplicación CUIDAR establecen los datos sensibles y los relacionados a geolocalización se preservarán únicamente mientras sean necesarios y dure la emergencia

[12] En México el 23 de marzo de 2020 se adoptó por parte del Consejo de Salubridad General el Acuerdo por el que reconoce la epidemia de enfermedad por el virus SARS-CoV-2 (COVID-19) en México, como una enfermedad grave de atención prioritaria, así como se establecen las actividades de preparación y respuesta ante dicha epidemia; en España el Real Decreto 463/2020, del 14 de marzo, declaró el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19; en Argentina Decreto de Necesidad y Urgencia No. 297/2020 de 19 de marzo, adoptó el Aislamiento Social preventivo y obligatorio.

[13] Al 6 de enero de 2022 la declaración de la pandemia por parte de la Organización Mundial de la Salud continuaba vigente. Asimismo, se habían identificado al menos cinco cepas del virus (alfa, beta, delta, gamma y ómicron), los números de infectados continuaban en ascenso, se volvían a saturar los servicios sanitarios en muchos países y se imponían medidas de confinamiento parcial, entre otras restricciones, asimismo persiste inequidad en el acceso a las vacunas y en la atención sanitaria (OMS, 2022).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

sanitaria. Una vez finalizada esta, podrán preservarse versiones anonimizadas de los mismos con fines científicos y epidemiológicos (apartado 5.9).

Empero el cumplimiento del principio de conservación deviene más complejo si la aplicación es también utilizada para proporcionar apoyo o ayuda gubernamental. En el caso de la APP COVID-19 de Colombia si la persona recibe apoyo con recursos públicos utilizando estos mecanismos tecnológicos la información recabada en relación con estos datos será conservada, sin que queden claro los límites de tiempo, excepto los datos de ubicación del dispositivo móvil. La eliminación del resto de los datos se realizará "conforme a su ciclo de vida, atendiendo a las disposiciones aplicables en materias administrativa, contable, fiscal, jurídica e histórica de los datos personales para tratamientos ulteriores, que pueden ser disociación, minimización o supresión, entre otros".

1. *Los retos de la anonimización en la relación público-privada*

Como acertadamente refiere Martínez Martínez, durante la pandemia ha sido "imprescindible la generación de grandes lagos transnacionales de datos de salud anonimizados y de una intensa colaboración público-privada" (Martínez Martínez, 2020). Los datos anonimizados han adquirido un importante papel en la investigación, y en particular aquellos que implican una transferencia inmediata a los servicios de salud. El acceso a datos ha sido uno de los principales problemas durante la pandemia, unido a la falta de organización y planificación en la gestión, así como su opacidad (Sanz Larruga, 2020: 345 y ss.).

Es posible fomentar la relación pública-privada y el intercambio de datos si este se realiza de forma anonimizada, es decir, eliminar las posibilidades de identificación de las personas sin menoscabar el acceso a la información, el análisis técnico y científico sobre el conjunto de datos (AEPD, 2016: 1; Archivo General de la Nación, 2020: 11). El tratamiento de los datos en este contexto, especialmente para su uso por sistemas de inteligencia artificial, debe ser seguro, transparente, controlables y ajustados a las finalidades que se correspondan. Aun cuando el tratamiento de los datos sea realizado de forma anónima se debe considerar que la participación del sector privado en el tratamiento de datos relativos a la salud para el enfrentamiento de la pandemia debe partir de la excepcionalidad y del cumplimiento de estándares de garantías elevados. Los datos deberían ser utilizados esencialmente para investigar y controlar al coronavirus, no a las personas (Cotino Hueso, 2020)

La anonimización por sí misma entraña un conjunto de peligros y riesgos que no siempre son tenidos en cuenta al momento de establecer este

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

tipo de relación. Todo parte de aceptar que el tratamiento de datos de forma anónima queda excluido de las reglas de protección de datos personales. Las regulaciones jurídicas consideran que si existe anonimización no es preciso el consentimiento del titular, dado que no existe un dato personal. En Brasil, por ejemplo, el artículo 12 de la Ley de Protección de Datos no considera a estos datos como personales salvo que el proceso de anonimización fuera revertido, teniendo en cuenta tanto los medios utilizados como las tecnologías disponibles y medios utilizados para ello. De forma similar acontece en México donde el tratamiento de datos sensibles disociados no requiere del consentimiento del titular del dato, como ya se ha referido.

La anonimización ha adquirido una particular importancia en el uso de las aplicaciones para enfrentar el COVID-19 y el uso de la geolocalización.[14] No han sido pocos los debates en torno al uso de esta última tecnología para analizar y monitorear los indicadores epidemiológicos, y evaluar la eficacia de las medidas adoptadas y el control de la emergencia de forma particular, así como para mostrar las instalaciones sanitarias más cercanas al domicilio. En principio ello indica el cumplimiento del principio de plena funcionalidad, es decir, la utilidad de los datos anonimizados, especialmente si se tiene en cuenta la correspondencia con el objetivo perseguido con el uso de esta información, sin embargo, donde no existe claridad es en el diseño del proceso de anonimización. Como ya se ha referido la declaración de anonimización no es suficiente.

Pese a que no existe una anonimización absoluta lo cierto es que esta técnica no sólo protege contra el riesgo de que identifique de manera única a una persona en el conjunto de datos, sino que también dicho registro se vincule a otros conjuntos de datos de identificación personal, así como tampoco se pueda inferir información confidencial sobre un individuo a partir del conjunto de datos anonimizados (Castro, Cavoukian, 2014). En otras palabras, estos son los tres riesgos que permiten solventar la disociación cuando es irreversible y absoluta, la singularización, la vinculabilidad y el riesgo de inferencia.

[14] En España se declaró el estado de alarma para la gestión de la crisis sanitaria ocasionada por el COVID-19, en virtud del Real Decreto 463/2020, del 14 de marzo. La Orden SND/297/2020 del 27 de marzo, encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19. Esta orden previó la necesidad de permitir la geolocalización para verificar que cada persona se encuentra en la comunidad autónoma que dice declarar y realizar un estudio de movilidad a partir del cruce de datos de los operadores móviles (artículo 2o.). En Brasil, la Medida Provisoria No. 954/2020 permitía el compartimento de datos por parte de las empresas prestadoras de servicios telefónicos fijo y móvil con la finalidad de producir estadística oficial, así como realizar entrevistas con carácter no presencial en el ámbito de investigaciones domiciliares (apartado 1 del artículo 2o.).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

En este sentido, la Agencia Española de Protección de Datos ha hecho alusión de que estos riesgos ya existían antes de la pandemia, sin embargo, al existir un uso mayor de los datos anonimizados, existe un riesgo mayor, "aunque ello no significa necesariamente que sea exponencialmente mayor" (2020b: 3). Asimismo, el uso de información de geolocalización en redes sociales puede ser enriquecida con información personal derivada de la actividad en los perfiles, sin que sea posible considerar que las condiciones de uso y políticas de privacidad de dichas redes sociales puedan ser consideradas base jurídica para realizar estos tratamientos (2020b).

No puede obviarse que, dado el avance de la tecnología, las técnicas de anonimización pueden ser consideradas obsoletas en un breve espacio de tiempo, no sólo con técnicas que la superen, sino también con la aparición de técnicas que puedan vulnerar las utilizadas. Debido a que la anonimización es esencial, pero a su vez incompleta (Cotino Hueso, 2020), es necesario garantizar el respeto de la privacidad a partir del uso de tecnologías de protección de la intimidad (PET), así como la evaluación de su impacto.

La disociación como estrategia de ocultación para la protección de los datos desde el diseño debe ser desarrollada de conjunto con otras técnicas como la restricción en el acceso o el agrupamiento de la información utilizando técnicas de generalización, la desvinculación de datos y su interconexión, el uso de softwares de códigos abiertos, así como de cualquier otra solución tecnológica que sea más respetuosa con los principios de transparencia, auditabilidad y privacidad de las personas. Limitando las posibilidades de cruzamiento de datos, su utilización con propósitos distintos a los autorizados o el sufrimiento de ciberataques.

Empero, no sólo es necesario analizar las técnicas de anonimización utilizadas sino también aquellas que se podrían utilizar para realizar la reidentificación. La anonimización pasa también por el diseño de esta, si este es defectuoso puede dar lugar a la reidentificación de las personas. La reidentificación es un riesgo que necesita ser gestionado, al igual que la confidencialidad de la información anonimizada. Es necesario tener en cuenta el impacto del riesgo, y su cuantificación, especialmente el costo elevado en la relación esfuerzo-beneficio teniendo en cuenta requerimientos humanos, tecnológicos y económicos. A pesar de que la reidentificación no está necesariamente relacionada con el incumplimiento de las medidas de seguridad de protección de datos, si es importante que los riesgos sean clasificados en riesgos de reidentificación existentes, potenciales y no conocidos (AEPD, 2016: 9). Especialmente aquellas tecnologías que se centran en los identificadores indirectos o cuasi-identificadores que pudieran referirse a un individuo. Se ha reconocido la interconexión de fuentes de datos independientes brinda la posibilidad

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

de crear un registro electrónico de los individuos, aun cuando exista supresión de datos explícitos.

Empero, no se trata sólo de la posibilidad de reidentificación, sino también de los peligros que se encuentran asociados a ella, como la usurpación de identidad, la elaboración de perfiles discriminatorios, la vigilancia permanente o el fraude. Los datos anónimos recabados pueden ser utilizados en tratamiento automatizado. Conforme el artículo 2o., inciso c, del Convenio para la Protección de las Personas, el tratamiento automatizado de datos de carácter personal es entendido como cualquier operación que sea efectuada, en su totalidad o en parte, con ayuda de procedimientos automatizados, ya sea el registro de datos, la aplicación de estos a operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión. Según el grupo de trabajo sobre protección de datos del artículo 29 (2018), no es más que el tratamiento por medios tecnológicos y sin la participación del ser humano de datos de carácter personal.

En este supuesto hay que tener presente la posibilidad de que datos sesgados puedan ser utilizados en el entrenamiento de sistemas de inteligencia artificial, con posibles efectos discriminatorios, así como en la elaboración de perfiles (que no es más que el tratamiento automatizado de datos con el objetivo de evaluar aspectos personales sobre una persona física). Si el dato es inexacto existe un riesgo de estigmatización, especialmente si no se adoptan las garantías necesarias para su seudonimización, agregación, cifrado o descentralización.

El desarrollo de tecnologías como la inteligencia artificial permite que, aun cuando no exista una vulneración a los derechos de la persona de manera individual, puesto que, en principio, se cumplen determinados parámetros, como los establecidos en las leyes en relación con la anonimización, la persona sí pudiera ser objeto de vulneración de sus derechos a partir de la aplicación que se pudiera hacer de esta tecnología en ella. Tecnología que precisamente ha sido alimentada con datos personales anonimizados. Pudiéramos decir que entonces que estamos ante un uso indirecto de estos datos que puede incluso incidir sobre otros derechos de la persona cuando su utilización es realizada de forma sesgada.

Si bien el dato puede ser tratado automáticamente de forma anónima es posible que se puedan elaborar perfiles específicos que permitan la identificación de la persona. Cuando el dato tratado de forma anónima permite la elaboración de perfiles debe recibir tratamiento como dato personal. Como reconoce la AEPD aun cuando los protocolos de criptografía y anonimización sean robustos es posible que estos protocolos puedan ser rotos al asociarse con otros datos (2020b: 9).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

La elaboración de perfiles permite evaluar aspectos personales de la persona física como la predicción de sus movimientos, comportamientos y estados de salud. El cruce de datos de esta o diferentes fuentes que permitan la reidentificación de la persona. En este supuesto no es solo necesario el consentimiento de la persona titular del dato, sino también, que este reciba la información necesaria sobre este tratamiento, incluyendo la lógica aplicada y las consecuencias previstas con el mismo, tal como se prevé en el artículo 15 apartado H del Reglamento Europeo de Protección de Datos Personales (RGPD).

El dato puede identificar a una persona o convertir a esta en identificable, en el último supuesto si bien el dato no indica la identidad de la persona, tampoco aporta suficiente información sobre esta, pero sí nos permite averiguar la identidad mediante los medios adecuados. El dato no es personal en sí, pero por su combinación puede ofrecer información personal, dado que no está desprovisto de información. Hay que tener en cuenta que a suficiencia de los identificadores depende del contexto de la situación que se trate, y que los datos pueden ser cruzados, combinados o agregados respecto a los metadatos (Polo Roca, 2021: 217 y 218).

De hecho el propio Tribunal de Justicia de la Unión Europea en la sentencia del 8 de abril de 2014, en los asuntos acumulados C 293/12 y C 594/12, Digital Rights Ireland Ltd (asunto C-293/12) ha reconocido que algunos de estos datos (los datos necesarios para rastrear la fecha, hora y duración de una comunicación, el equipo de comunicación de los usuarios y para identificar la localización del equipo de comunicación móvil, como son la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet).

> Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones y los medios sociales que frecuentan.

En consecuencia, si se consideran un dato personal, deben cumplirse con los requisitos de protección de datos que se derivan y brindar las garantías suficientes para proteger estos datos de abuso o de cualquier acceso o utilización ilícita respecto de estos datos, como lo ha reconocido el propio tribunal, lo que a su vez es sumamente importante cuando dichos datos se someten "a un tratamiento automático y existe un riesgo elevado de acceso ilícito a dichos datos".

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

¿Cómo entonces se puede garantizar que se cumplan estos requerimientos cuando se tratan datos anónimos o se ceden estos a terceros? ¿Cómo corroborar que la entrega a terceros se realice bajo estrictos criterios de anonimidad y sin identificadores directos? Máxime cuando se trata de datos relativos a la salud que se encuentran en la escala más alta de sensibilidad de la información y dónde su titular no tiene noción del índice de riesgo de reidentificación que es asumido por el responsable del tratamiento desde el diseño del proceso de anonimización.

2. *Garantías legales en el proceso de anonimización*

Como bien refieren Castro y Cavoukian (2014) debe establecerse un equilibrio en no exacerbar el riesgo de reidentificación, y la oportuna valoración de sus beneficios en investigación, para la economía y la sociedad que supone la anonimización y la información que aporta. En este sentido, la AEPD ha recomendado que el tratamiento implemente una "estrategia global basada en evidencias científicas, evaluando su proporcionalidad en relación con su eficacia, eficiencia y teniendo en cuenta de forma objetiva los recursos organizativos y materiales necesarios" (2020b: 13).

En este contexto es de vital importancia que se adopten garantías legales y tecnológicas para prevenir la vulneración de los derechos de los titulares y evitar que estos puedan ser identificados o identificables. El análisis de la imposibilidad de asociación directa o indirecta con el titular solo es posible si se toman en cuenta los medios razonables y disponibles en el momento del tratamiento, si las medidas para revertir la anonimización se consideran desproporcionadas o inviables, entonces se puede afirmar que estamos ante un tratamiento responsable y ético.

El principio de responsabilidad proactiva, que toma como punto de partida la protección de datos desde el diseño y por defecto parece marcar la hora de ruta en este sentido (Piñar, 2020), y en particular, para el establecimiento de garantías cuando dichas aplicaciones se utilizan en el sector público.[15]

[15] Sobre el cumplimiento de garantías de protección a la privacidad en las tecnologías utilizadas por el sector público es imprescindible consultar la decisión del Tribunal de La Haya en el caso del Sistema de Indicación de Riesgo (SyRI). SyRI es una tecnología utilizada por el gobierno de los Paises Bajos para combatir el fraude, por ejemplo, beneficios, asignaciones e impuestos. Según el tribunal, esta tecnología no protege la privacidad de las personas, consagrada en el artículo 8o. del Convenio Europeo de Derechos Humanos (CEDH). A juicio del tribunal el Estado tiene una responsabilidad especial en la aplicación de nuevas tecnologías y debe encontrar un justo equilibrio entre los beneficios de la utilización de la tecnología y el respeto de la privacidad. En este supuesto no se cumple

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

El RGPD obliga al responsable del tratamiento de datos de aplicar medidas técnicas y organizativas apropiadas, tanto en el momento de determinar los medios como en el propio tratamiento. Las garantías necesarias deberán ser adoptadas teniendo en cuenta "el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas" (artículo 25.1).

Es necesario que queden establecidas, con claridad, cuáles son las acciones, actividades, controles o mecanismos técnicos y físicos que se han utilizado y que evitan el acceso, modificación, difusión o destrucción de forma no autorizada, así como el plan de contingencia para responder de forma directa, inmediata y efectiva cuando alguna de estas situaciones tenga lugar. Garantizar de forma efectiva una protección integral a los datos personales o anónimos desde los procesos de diseño, operación y gestión de los sistemas, que implica tanto un enfoque de riesgo como una responsabilidad proactiva.

La protección efectiva a la que nos hemos referido anteriormente está indisolublemente ligada a la existencia de sistemas lógicos transparentes desde su configuración, lo que es garantía del respeto de la privacidad que, a su vez, es la base de la confianza en el uso de estas aplicaciones por parte de los titulares, conforme se ha reconocido en la Recomendación (UE) 2020/518 de la Comisión del 8 de abril de 2020. Si las aplicaciones utilizadas no son transparentes no queda claro cómo y por qué se realiza el tratamiento, así como tampoco dónde se almacena esta información, con quién se comparte la información y su tratamiento. Empero, la transparencia no puede ser asociada sólo a la protección de datos de carácter personal, sino al propio diseño y uso de estos sistemas. Solo de esta forma es posible demostrar la diligencia y responsabilidad proactiva de los diseñadores y utilizadores de estas aplicaciones ante las autoridades, y que las partes puedan comprender y reproducir el uso de la información en cualquier momento del tratamiento.

Estas condiciones y garantías no siempre son tenidas en cuenta al momento de establecer el uso de estos aplicativos. Un ejemplo de la necesidad de que estos requerimientos técnicos y legales sean cumplidos se evidencia en la declaración de inconstitucionalidad de la Medida Provisoria núm. 954/2020 del Gobierno de Brasil. Entre los fundamentos esgrimidos por el Supremo Tribunal Federal, se consideró que la medida traspasó los límites trazados por la Constitución al disponer de estos datos personales (apartado 16). Aun cuando la medida provisoria estableció el carácter secreto de los da-

dicha prueba debido a que la aplicación no es suficientemente transparente (Tribunal de La Haya, 2020).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

tos compartidos, su uso sólo con la finalidad prevista, la prohibición de que estos pudieran ser utilizados como objeto de certificación o medio de prueba en proceso administrativo, fiscal o judicial (artículo 3o.) y la obligación de eliminar las bases de datos una vez superada la situación de emergencia de salud pública (artículo 4o.), la resolución judicial consideró que la finalidad declarada no delimitaba el objeto de la estadística que debía ser producida a partir de estos datos, así como su finalidad específica y amplitud.

A juicio de la magistrada ponente no se esclareció en dicha medida la necesidad de su disponibilidad ni cómo serían efectivamente autorizados estos datos (apartado 17). La relatora consideró que si bien por inferencia se podía asociar que la estadística debía tener relación con la pandemia, que es lo que justificaba la norma jurídica, lo cierto es que, esta conclusión, no se extraía claramente del texto, así como tampoco el interés público legítimo que podía justificar el compartimiento de los datos personales de los usuarios de los servicios de telefonía, considerando su necesidad, adecuación y proporcionalidad. Según la resolución judicial no se definían de manera clara cuál sería la utilidad de los datos recolectados y su limitación al mínimo necesario para alcanzar las finalidades previstas.

La protección de datos desde su diseño y por defecto además de la estrecha relación que guardan con la transparencia de datos personales y los sistemas de inteligencia artificial permiten que la toma de decisiones sea auditable, lo cual se traduce en la obligación de documentar el proceso y realizar una correcta evaluación del impacto que puede tener la aplicación en la protección de datos personales. La evaluación de la viabilidad de la herramienta, la posibilidad de control y mitigación de riesgos debe ser realizado en conjunto con el cumplimiento de los derechos de los titulares (acceso, rectificación, oposición y cancelación principalmente), así como de los deberes de los responsables y encargados, según lo previsto en la normativa aplicable de cada país. Además de los aspectos legales, también deben ser tenidos en cuenta el respeto de criterios éticos que van relacionados con el funcionamiento de la herramienta, entre los que cabe mencionar su nivel de precisión, calidad y pertinencia de los datos recogidos, correspondencia con la finalidad, seguridad y confidencialidad, así como la existencia de riesgos de reidentificación cuando exista correlación con otros datos. Además, es imprescindible empoderar al usuario para dotarlo del grado de información necesario que le permita determinar cuándo compartir los datos, así como solicitar su modificación y correspondiente eliminación cuando corresponda (Lozoya-de-Diego, Villalba-de-Benito y Arias-Pou, 2017: 300).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

IV. Control: validación y verificación

Ante la posibilidad de que el proceso de anonimización de los datos pueda ser revertido, o existir problemas en su gestión, es necesario garantizar el cumplimiento de las garantías y obligaciones de protección bajo criterios éticos, con exigencias de transparencia y el respeto a la privacidad y la ética desde el diseño. La pandemia también ha expuesto, en este sentido, que la autorregulación y la buena voluntad de los actores no es suficiente. Por ende, no puede desdeñarse el papel de las autoridades sanitarias como encargadas del tratamiento de estos datos, así como tampoco el de las autoridades independientes de protección de datos. De hecho, no es nuevo el llamado para que dichas autoridades (las de protección de datos) puedan exigir la incorporación y/o utilización de tecnologías de protección del derecho a la intimidad, tanto a proveedores y prestadores de servicios, como desarrolladores de productos y aplicaciones o fabricantes de dispositivos (Comisión Europea, 2007).

La configuración legal de la protección de datos personales se establece desde la perspectiva del control que realiza el titular, pero en una situación como la actual en la que es posible, bajo determinados supuestos, el uso de los datos un papel activo y de control por parte de las autoridades correspondientes. Todo ello con el fin de evaluar si el responsable del tratamiento está cumpliendo con los principios y obligaciones que establece la normativa.

No basta con la evaluación inicial de los riesgos, es preciso auditar el procesamiento de anonimización, sus resultados y el uso de esta información, la realización de pruebas de *hacking* ético, en virtud de las cuales se realizan ciberataques supervisados para poder detectar vulnerabilidades y debilidades de los protocolos y sistemas de ciberseguridad. Desde esta perspectiva existe la obligación no sólo de tener en cuenta medidas técnicas y organizativas conforme al riesgo, sino también el autoanálisis crítico, continuo y rastreable del responsable del tratamiento, en otras palabras, su capacidad de anticipación (*o accountability*).

El sistema de garantías previsto en la norma debe venir reforzado por un rol de control y gestión de las entidades regulatorias que deben velar por el cumplimiento de estos principios según cada supuesto específico y en dependencia del tipo de riesgo. El papel de estas autoridades no puede quedar limitado a la divulgación de las mejores prácticas. Debemos comprender que la intervención de la autoridad nacional de protección de datos es necesaria, no sólo de forma previa, sino también *a posteriori*, a los efectos de brindar una verdadera tutela. En particular en el contexto de la pandemia, donde no siempre ha sido posible realizar, con el tiempo que ello conlleva, un testeo

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

preventivo completo. Por ende, es necesario que las autoridades de datos monitoreen su implementación y funcionamiento, incluso el papel de las organizaciones de la sociedad civil y de los especialistas en el control del impacto de estas tecnologías.

Si no existen procesos de verificación y validación de la privacidad de forma clara cómo entonces se podrá tener en cuenta el respeto de la privacidad durante todo el periodo de vida útil de la aplicación, pasando por su diseño e implementación. No ha sido este el rol de las agencias de protección de datos en la región latinoamericana. En el caso de realizar algún tipo de verificación este tiene un impacto posterior y no de forma previa. Uno de los pocos ejemplos de supervisión de las aplicaciones ha tenido en lugar en Colombia donde la Superintendencia de Industria y Comercio (*sic*) requirió a las autoridades departamentales para comprobar si las aplicaciones y plataformas que utilizaban cumplían con lo establecido en la regulación colombiana en relación con la recolección y tratamiento de datos personales y la implementación del principio de responsabilidad demostrada.[16] Sin embargo, no son conocidos en la región el uso de sanciones por parte de las entidades de protección de datos por el incumplimiento de las normas de tratamiento de datos o de garantías de los procesos de anonimización.

Queda corroborada la necesidad de promover y utilizar mecanismos de certificación para la protección de datos personales, la evaluación de impacto de la tecnología y de la cadena de anonimización, vista como "el conjunto de medidas técnicas encaminadas a la ocultación, enmascaramiento o disociación de los datos personales" (AEPD, 2016: 1). Es imprescindible que a partir de las circunstancias específicas de cada caso se realice un análisis técnico sobre la robustez, debilidades y garantías de las técnicas de anonimización utilizadas. Debido a lo complejo de esta evaluación se puede analizar la posibilidad de que esta certificación pueda ser realizada por empresas u organizaciones independientes y privadas debidamente acreditadas por las autoridades nacionales de protección de datos.

Certificación que, a su vez, pueda ser sometida a supervisión por la autoridad de protección de datos personales en cualquier momento. La idea es que se establezca un mecanismo viable, sustentado en la colaboración público-privada de verificación y control que vigile, aun cuando se trate de datos anónimos por el cumplimiento de las normas de protección, así como que se

[16] Fueron requeridas las Gobernaciones de Caldas ("*EsperanzAPP*"), de Boyacá: ("*Aplicación Boyacá Covid-19*"), Risaralda ("*Plataforma EsperanzAPP*"), alcaldías de Medellín ("Medellín me Cuida-Familias") y Bogotá ("GABO"), Distrital de Cartagena ("*Plataforma Cuidémonos*") y la Gobernación del Valle del Cauca y Alcaldía de Santiago de Cali ("*CaliValleCorona*"). (*sic*, 2020).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

suprima o reduzca éste cuando es innecesario o indeseado, según las propias funcionalidades del sistema.

V. Conclusiones

Es importante precisar la participación del sector privado en la lucha contra la pandemia y la protección de datos personales. Al igual que acontece cuando el tratamiento lo realizan las autoridades sanitarias para este sector deberá quedar claro en qué momento procede la eliminación definitiva de los datos, cómo serán utilizados estos y el cumplimiento de los requerimientos de transparencia que deberán ser cumplimentados, en particular, el relacionado con el acceso abierto de la tecnología, lo que a su vez permitirá que esta sea sometida a control por las autoridades correspondientes que deben velar por el cumplimiento de los requerimientos que a estos efectos se establezcan. En ningún caso el tratamiento de estos datos podrá tener ánimo de lucro.

Es necesario que la excepcionalidad en el tratamiento sea interpretada de forma restrictiva. La utilización de técnicas de anonimización es una garantía válida para fortalecer la relación entre el sector público y privado, sin embargo deben tenerse en cuenta que la anonimización absoluta no existe, por ende, es necesaria la adopción de medidas jurídicas y tecnológicas para garantizar los principales riesgos que existen en relación al uso de esta tecnología, como es la reidentificación de los titulares, la elaboración de perfiles y su utilización en sistemas de inteligencia artificial que reproduzcan sesgos y patrones discriminatorios.

Es importante crear mecanismo de certificación y validación de las aplicaciones que utilicen estos datos personales o anonimizados. Estos mecanismos velarán por el cumplimiento de las medidas técnicas y organizativas necesarias, así como la evaluación de los procedimientos de anonimización utilizados según las circunstancias específicas de cada caso. La certificación puede ser realizada por instituciones y empresas independientes debidamente habilitadas por las autoridades nacionales de protección de datos personales que deberán garantizar el control y la gestión de estos sistemas.

VI. Referencias bibliográficas

Agencia Española de Protección de Datos Personales, 2016, Orientaciones y garantías en los procedimientos de Anonimización de datos personales, disponible en: *https://www.aepd.es/sites/default/files/2019-09/guia-orienta-*

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

ciones-procedimientos-anonimizacion.pdf (fecha de consulta: 14 de junio de 2020).

Agencia Española de Protección de Datos Personales, 2020a, La -ANONIMIDAD como medida de la privacidad, disponible en: *https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf* (fecha de consulta: 14 de junio de 2020).

Agencia Española de Protección de Datos Personales, 2020b, *El uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios*, disponible en: *https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf* (fecha de consulta: 27 de diciembre de 2021).

Agencia Española de Protección de Datos Personales, 2020c, Resumen de la Sesión Online Asociación Profesional Española de Privacidad y la Agencia Española de Protección de Datos, sobre criterios en protección de datos relacionados con COVID-19, Asociación Profesional Española de Privacidad, disponible en: *https://www.apep.es/resumen-de-la-sesion-apep-aepd-21m/?v=3b0903ff8db1,* acceso el 30 de abril de 2020.

Archivo General de la Nación de Colombia, 2020*, Guía de anonimización de datos estructurados. Conceptos generales y propuesta metodológica*, Bogotá, disponible en: *https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/Guia_de_Anonimizacion-min.pdf*, acceso el 7 de enero de 2022.

Castillo, C., 2020, "Mas de 60 expertos piden al gobierno que actúe ante «las iniciativas privadas» que usan las aplicaciones del coronavirus para lucrarse", *El Diario.es*, 21 de marzo de 2020.

Castro, D. y Cavoukian, A., 2014, *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*. Canadá: Information and Privacy Commissioner.

Comisión Europea, 2020, La IA y el control del coronavirus COVID-19, disponible en: *https://www.coe.int/en/web/artificial-intelligence/la-ia-y-el-control-del-coronavirus-covid-19* (fecha de consulta: 7 de enero de 2022).

Comisión Interamericana de los Derechos Humanos, CIDH, 2020, Resolución No. 1/2020 Pandemia y Derechos Humanos en las Américas, Costa Rica, OEA.

Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET), COM (2007) 228 final, Bru-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

selas (2007), disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52007DC0228*, acceso el 20 de abril de 2020.

Convenio No. 108 para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo de 28 de enero de 1981, disponible en: *https://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf*, acceso el 20 de abril de 2020.

Cotino Hueso, L., 2020, "Inteligencia artificial, *big data* y aplicaciones contra la COVID-19: privacidad y protección de datos", *IDP. Internet, Derecho y Política*, núm. 31, pp. 1-17, acceso el 21 de diciembre de 2021.

Cotino Hueso, L., 2020a, Inteligencia Artificial y vigilancia digital contra el Covid-19 y contra la privacidad. El diablo está en los detalles. Documento de opinión IEEE 36/2020, disponible en: *http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO36_2020LORCOT_CovidDigital.pdf* (fecha de consulta: 21 de diciembre de 2021).

Domínguez Álvarez, J. L., 2020, "La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19", *Revista de Comunicación y Salud,* vol. 10, núm. 2.

Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2018, Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, adoptadas el 3 de octubre de 2017, revisadas por última vez y adoptadas el 6 de febrero de 2018, Bruselas, Comisión Europea.

Katz, R. *et al.*, 2020, El estado de la digitalización de América Latina frente a la pandemia del COVID-19, Observatorio CAF del Ecosistema Digital.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación*, 5 de julio de 2010.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. *Diario Oficial de la Federación*, 26 de enero de 2017.

Ley No. 13.709, del 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei No. 13.853, de 2019), Brasília, DF., disponible en: *http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm* (fecha de consulta: 30 de mayo de 2020).

Lozoya-de-Diego, A. *et al*., 2017, "Taxonomía de información personal de salud para garantizar la privacidad de los individuos", *El profesional de la información*, vol. 26, núm. 2.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

Martínez Martínez, R., 2020, "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", *Diario La Ley*, disponible en: *https://diariolaley.laleynext.es/dll/2020/03/27/los-tratamientos-de-datos-personales-en-la-crisis-del-covid-19-un-enfoque-desde-la-salud-publica* (acceso el 7 de enero de 2022).

Medida Provisoria núm. 959, de 29 de abril de 2020, Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória núm. 936, de 1o. de abril de 2020, e prorroga a *vacatio legis* da Lei No. 13.709, del 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais-LGPD, disponible en: *http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv959.htm#art4* (fecha de consulta: 30 de mayo de 2020).

Noah Harari, Y., 2020, "The World after Coronavirus", *Financial Times* [online], disponible en: *https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75* (fecha de consulta: 7 de enero de 2022).

OMS, 2020, Declaración conjunta de la UIT y la OMS: Desencadenar el potencial de la tecnología de la información para derrotar la COVID-19, disponible en: *https://www.who.int/es/news/item/20-04-2020-itu-who-joint-statement-unleashing-information-technology-to-defeat-covid-19* (fecha de consulta: 25 de mayo de 2021).

OMS, 2022, Alocución de apertura del Director General de la OMS en la rueda de prensa sobre la COVID-19 del 6 de enero de 2022, disponible en: *https://www.who.int/es/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---6-january-2022* (fecha de consulta: 12 de enero de 2022).

OPS, 2020, Directora de la OPS llama al sector privado a cooperar en la respuesta a la COVID-19 en las Américas, disponible en: *https://www.paho.org/hq/index.php?option=com_content&view=article&id=15770:directora-de-la-ops-llama-al-sector-privado-a-cooperar-en-la-respuesta-a-la-covid-19-en-las-americas&catid=740:press-releases&lang=es&Itemid=1926* (fecha de consulta: 24 de abril de 2020).

Overly, Steven, 2020, "White House seeks Silicon Valley help Battling Coronavirus", *El Político* [online], disponible en: *https://www.politico.com/news/2020/03/11/white-house-seeks-silicon-valley-help-battling-coronavirus-125794* (fecha de consulta: 12 de enero de 2022).

Romm, T. *et al*., 2020, "U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus", *The Wash-*

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

ington Post [online], disponible en: *https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/* (fecha de consulta: 7 de enero de 2022).

Piñar, J. L., 2020, Privacidad en estado de alarma y normal aplicación de la Ley, disponible en: *https://www.hayderecho.com/2020/04/09/privacidad-en-estado-de-alarma-y-normal-aplicacion-de-la-ley/* (fecha de consulta: 21 de diciembre de 2021).

Polo Roca, A., 2021, "Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos", *Estudios de Deusto*, vol. 69/1, enero-junio de 2021.

Redacción TICPymes, 2020, *El Gobierno Vasco se apoya en la Inteligencia Artificial para combatir la COVID-19*. 13 de abril de 2020.

Recomendación (UE) 2020/518 de la Comisión de 8 de abril de 2020 relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados, *Diario Oficial de la Unión Europea*, 14 de abril de 2020.

Reglamento General 2016/679 de Protección de Datos Personales de 27 de abril de 2016, *Diario Oficial de la Unión Europea*, 4 de mayo de 2016.

Rodríguez, Andrea G., 2020, "Qué pasará si el gobierno sigue controlando nuestros móviles después del coronavirus", disponible en: *https://www.vice.com/amp/es/article/epgw37/espana-geolocalizacion-moviles-confinamiento-datacovid?utm_campaign=sharebutton&__twitter_impression=tr* (fecha de consulta: 20 de abril de 2020).

Sanz Larruga, F. J., 2020, "Derecho a una información sanitaria veraz y a una buena gestión de los datos epidemiológicos. Una asignatura pendiente en España con motivo del COVID-19", *Revista Galega de Administración Publica, EGAP.,* vol. 60.

Superintendencia de Industria y Comercio de Colombia, La Superintendencia de Industria y Comercio en su calidad de Autoridad Nacional de Protección de Datos, se permite informar lo siguiente, 2020, disponible en: *https://www.sic.gov.co/slider/la-superintendencia-de-industria-y-comercio-en-su-calidad-de-autoridad-nacional-de-protecci%C3%B3n-de-datos-se-permite-informar-lo-siguiente* (fecha de consulta: 14 de junio de 2020).

Superintendencia de Industria y Comercio de Colombia, 2020, *La Superintendencia de Industria y Comercio, en su calidad de Autoridad Nacional*

DOI: http://dx.doi.org/10.22201/iij.25940082e.2022.14.16892

de Protección de Datos, se permite informar lo siguiente, disponible en: *https://www.sic.gov.co/slider/la-superintendencia-de-industria-y-comercio-en-su-calidad-de-autoridad-nacional-de-protecci%C3%B3n-de-datos-se-permite-informar-lo-siguiente-0* (fecha de consulta: 14 de junio de 2020.

Supremo Tribunal Federal de Brasil. Medida Cautelar en la Acción Directa de Inconstitucionalidad. 6.387. 24 de abril de 2020, Brasília, D.F., disponible en: *https://www2.stf.jus.br/portalStfInternacional/cms/verConteudo.php?sigla=portalStfJurisprudencia_es_es&idConteudo=160170* (fecha de consulta: 30 de abril de 2020).

Sentencia del Tribunal de Justicia (Gran Sala), de 8 de abril de 2014, en los asuntos acumulados C 293/12 y C 594/12, Digital Rights Ireland Ltd (asunto C-293/12) y Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General y Kärntner Landesregierung (asunto C-594/12), Michael Seitlinger, Christof Tschohl y otros.

Tribunal de La Haya, 2020, Caso: C/09/550982 / HA ZA 18-388, 5 de febrero de 2020, disponible en: *https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865* (fecha de consulta: 7 de enero de 2022).