# Dictamen sobre la protección de datos personales en el contexto de la pandemia

## I. Introducción

El Estado argentino, al igual que otros Estados extranjeros, adoptó diversas medidas que involucran la recolección, el tratamiento y el almacenamiento de datos personales a fin de prevenir, controlar y mitigar los efectos de la pandemia. En la actualidad, el Estado dispone herramientas tecnológicas que son eficientes para prevenir los contagios de covid-19, detectar casos sospechosos, brindar asistencia médica, coordinar la atención médica entre las distintas instituciones, controlar el cumplimiento del aislamiento, entre otros propósitos públicos importantes.

Sin embargo, el uso de los datos personales puede avasallar los derechos constitucionales a la privacidad y a la autodeterminación informativa. Esos derechos otorgan al individuo el derecho de decidir, en forma libre e informada, "qué" información comparten con el Estado y con otros individuos, "para qué", "cuándo" y "cómo". Esos derechos son un valladar para que el Estado no abuse del tratamiento de datos personales, menos aún, los que involucran cuestiones de salud y de geolocalización, en el contexto de pandemia y en la posteridad.

La Sección de Derecho Constitucional del Instituto de Estudios Legislativos analiza si el tratamiento de datos personales realizado por el Estado argentino es congruente con la protección constitucional de esos derechos. En especial, el análisis se centra en el tratamiento de datos a través de la aplicación Cuidar y de los certificados de circulación. En ese marco, dictamina:

## II. El derecho a la privacidad y a la autodeterminación informativa

El derecho a la privacidad, que tiene una estrecha vinculación con la libertad personal, se encuentra consagrado en la Constitución Nacional y en instrumentos internacionales que tienen jerarquía constitucional (art. 19, Constitución Nacional). En relación con ambos derechos, el artículo 18 de la Constitución Nacional dispone la inviolabilidad de, en cuanto aquí interesa, la correspondencia y los papeles privados. El artículo 11 de la Convención Americana sobre Derechos Humanos dispone que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada y su correspondencia (en sentido similar, art. 17, Pacto Internacional de Derechos Civiles y Políticos).

En relación con el derecho a la privacidad, la Corte Suprema puntualizó en el precedente "Ponzetti de Balbín" que "[el] art. 19 CN (…) protege jurídicamente un ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro

real o potencial para la intimidad" (Fallos: 306:1892, considerando 8°; en igual sentido, Fallos: 335:799, "Albarracini").

En el caso registrado en Fallos: 338:556, "D., M. A.", la Corte enfatizó que "en innumerables precedentes ha resaltado el valor de la autodeterminación de la persona humana con fundamento en el artículo 19 de la Constitución Nacional, no solo como límite a la injerencia del Estado en las decisiones del individuo concernientes a su plan de vida, sino también como ámbito soberano de este para la toma de decisiones libres vinculadas a sí mismo (Fallos: 332:1963; 335:799)."

Tal como ha entendido la Corte Interamericana de Derechos Humanos, el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública y comprende, entre otras dimensiones, tomar decisiones relacionadas con diversas áreas de la propia vida libremente, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y "**controlar la difusión de información personal hacia el público**" ("Fontevecchia y D'Amico vs. Argentina", sentencia 29 de noviembre de 2011, párr. 48).

El derecho a la privacidad no solo supone una libertad frente a las intromisiones de terceros en áreas reservadas a la autonomía individual, **sino que otorga el derecho a controlar la difusión de esa información que integra su zona de reserva, esto es, a determinar cómo, en qué medida y para qué se puede comunicar a otros información sobre uno mismo.**

Este último aspecto de la privacidad, esto es, **la autodeterminación informativa es receptada expresamente en el artículo 43, tercer párrafo, de la Constitución Nacional**. Ese derecho tiene especial relevancia en la actualidad frente a los avances tecnológicos que han incrementado exponencialmente el flujo y el procesamiento de información de toda índole.

En el caso registrado en Fallos: 321:2767, "Urteaga", los doctores Carlos Fayt y Enrique Petracchi se refirieron expresamente a la autodeterminación informativa.

Por su parte, Fayt destacó que "el núcleo del tema es la libertad del individuo frente al procesamiento de datos, es decir, la protección del individuo contra la evolución técnica de la informática." Afirmó que el artículo 43 de la Constitución Nacional "protege la identidad personal y garantiza que el interesado -él y sólo él- tome conocimiento de los datos a él referidos y de su finalidad, que consten en registros o bancos públicos o los privados destinados a proveer informes. Constituye, por tanto, una garantía frente a informes falsos o discriminatorios que pudieran contener y autoriza a obtener su supresión, rectificación, confidencialidad o actualización. Se trata, pues, de una dimensión del derecho a la intimidad, en conexión de sentido con el art. 19 de la Constitución Nacional; constituye la acción que garantiza el derecho que toda persona tiene a decidir por sí misma en qué medida compartirá con los demás sus sentimientos, pensamiento y los hechos de su vida personal (caso "Ponzetti de Balbín", Fallos: 306:1893)."

Por su lado, el doctor Petracchi afirmó que "el instituto del hábeas data está entrañablemente vinculado al derecho a la intimidad, como un instrumento destinado a evitar injerencias extrañas en la vida privada, pero también a fin de

proteger el honor, el derecho a la identidad y a la propia imagen (…). Sin lugar a dudas, la difusión de herramientas de características similares al hábeas data, destinadas a proteger frente al registro indiscriminado de datos personales, se debió fundamentalmente a los avances tecnológicos, especialmente en materia de almacenamiento de datos informáticos (…). Es este fenómeno el que desencadena el temor frente a las posibilidades de "invasión" del individuo no sólo por parte del Estado, sino también por los particulares (confr. Hassemer, Winfried; Chirino Sánchez, Alfredo, op. cit., págs. 13 y sgtes.)."[1]

De este modo, el fundamento del habeas data es la "autodeterminación informativa" o libertad informática, que adquiere cada vez más relevancia frente al avance tecnológico que se nutre del tratamiento de datos personales.[2] De acuerdo con ese concepto, es el ciudadano quien debe decidir sobre el uso y la cesión de sus datos personales. Este derecho, como el resto de los derechos fundamentales, puede ser restringido por medio de una ley por razones de utilidad social pero respetando el principio de proporcionalidad y garantizando que no se produzca la vulneración del derecho a la personalidad.

## III. La ley de protección de datos personales: ley 25.326

En la actualidad, los derechos constitucionales a la privacidad y a la autodeterminación informativa están reglamentados, principalmente, en la ley 25.326 de Protección de Datos Personales ("LPDP").[3] Esa ley fue aprobada en octubre de 2000 y está basada en la ley española, esto es, la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Luego, la ley fue reglamentada en 2001 a través del decreto 1558/2001, que creó la Dirección Nacional de Protección de Datos Personales (DNPDP), autoridad de aplicación de la ley 25.326.

En la actualidad, hay modelos normativos superadores sobre protección de datos personales, que, por ejemplo, receptan el fenómeno de las nuevas tecnologías

---

[1] Petracchi cita: "(confr., entre otros, Hassemer, Winfried; Chirino Sánchez, Alfredo, "El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales", Buenos Aires, 1997, págs. 32 y sgtes.; Pérez Luño, op. cit.; Espinar Vicente, José María, "La primacía del derecho a la información sobre la intimidad y el honor", en "Estudios sobre el derecho a la intimidad", cit., págs. 36 y sgtes., 46 y sgtes.; Bidart Campos, Germán, "El derecho de petición, de acceso a la información y el recurso de insistencia en el derecho colombiano", E.D. 166-41)."
Además, cita: "confr. acerca de las diversas vías en el derecho comparado, Abad Yupanqui, Samuel B., "La jurisdicción constitucional en el Perú: Antecedentes, balance y perspectivas", en Anuario de Derecho Constitucional Latinoamericano, publicado por la Fundación Konrad Adenauer, Medellín, 1996, págs. 107 y sgtes.)."

[2] Además, el ministro de la Corte Suprema cita "Pérez Luño, op. cit., pág. 39; Bidart Campos, loc. cit.; Vanossi, Jorge R. "El 'hábeas data': no puede ni debe contraponerse a la libertad de los medios de prensa", E.D. 159-948, esp. pág. 949; respecto de regímenes legislativos en particular, Chirino Sánchez, op. cit., pág. 181, con referencia a la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de Carácter personal (LORTAD) de España; Hassemer, op. cit., págs. 36 y sgtes., sobre la Ley Federal de Protección de Datos de la República Federal de Alemania (BDSG) y del Land Hesse (HDSG); Bianchi, Alberto, "Hábeas data y derecho a la privacidad", E.D. 161-866, esp. pág. 874, con relación a la Data Protection Act inglesa, de 1984, y a la Privacy Act norteamericana, de 1974)."

[3] Otras normas que incluyen regulaciones de privacidad son el art. 52 del CCyC y las leyes 20.216, 27.078, 23.798, 26.529 y 26.951.

de la información y la comunicación (TIC). En particular, en el año 2018 entró en vigencia en la Unión Europea, el Reglamento General de Protección de Datos Personales (RGPD; 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea).[4] A raíz de ello, en nuestro país, la Agencia de Acceso a la Información Pública presentó un proyecto de reforma, que se encuentra a estudio del Congreso de la Nación.

A continuación, repasamos los ejes centrales de la actual LPDP que rige en nuestro país.

### (i) Objeto de la ley

La ley protege en forma integral los datos personales asentados en archivos, registros, bancos o bases de datos. No es condición necesaria para la aplicación de la ley que los datos se hallen en una base de datos, lo importante es que exista un "tratamiento de datos".

La ley regula bases de datos públicas y privadas. Más allá de que el artículo 1 de la ley solo menciona a las bases datos privadas "destinadas a dar informes", una interpretación respetuosa de los derechos fundamentales de los ciudadanos lleva a concluir que todas las bases de datos privadas que posean datos personales que puedan afectar los derechos de las personas están sujetas a las disposiciones de la ley.

### (ii) Estándares de protección: datos personales y datos sensibles

La ley contiene dos estándares de protección.

Por un lado, los **datos personales**, esto es, "la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables" (art. 2).

Por otro lado, **los datos sensibles**, "aquellos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e **información referente a la salud** o a la vida sexual". De este modo, la LPDP protege con mayor intensidad a los datos que pueden ser utilizados para discriminar a una persona. En ese aspecto, los derechos a la privacidad y a la autodeterminación informativa se interrelacionan con el derecho de igualdad y el principio de no discriminación. El Reglamento europeo incorpora entre los datos sensibles a los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física y los datos relativos a la orientación sexual de una persona.

La protección reforzada de los datos sensibles implica un tratamiento diferenciado para la recolección, el tratamiento y la cesión de esos datos, como explicaremos a continuación.

### (iii) El principio de licitud: consentimiento y sus excepciones

[4] Ferreyra, Eduardo, "Comparación entre la ley argentina de protección de datos personales y el nuevo Reglamento General de Protección de Datos de la Unión Europea", publicado por la Asociación por los Derechos Civiles (ADC).

Un principio que estructura la LDPD es el de **la licitud en la obtención y el tratamiento de los datos**. De acuerdo con este principio, la recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley.

En primer lugar, la ley establece que la única base legal para el procesamiento de datos personales es el **consentimiento** de los titulares de los datos. Ello es coherente con la idea de **autodeterminación** que surge del texto constitucional. A la vez, el consentimiento está revestido de ciertas garantías para ser válido. Debe ser "**expreso**", "**libre**", e "**informado**". De acuerdo con este último aspecto, el titular debe conocer la finalidad del tratamiento del dato, quiénes son los responsables del tratamiento de los datos, si los datos serán cedidos o archivados, la posibilidad de acceder a los datos, rectificarlos y suprimirlos, entre otras cuestiones (art. 6). La ley exige que el titular del dato tenga la certeza de qué es lo que van a hacer con sus datos. El consentimiento siempre es revocable. En el caso de los datos sensibles, la ley aclara que ninguna persona puede ser obligada a proporcionarlos (art. 7).

En segundo lugar, la ley establece en qué casos excepcionales el consentimiento no es necesario y ello depende del tipo de dato en cuestión: personal (art. 5) o sensible (art. 7).

Por un lado, en el caso de los datos personales, no es necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) **Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal**; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

Por otro, si se trata de datos sensibles, sólo pueden ser recolectados y objeto de tratamiento cuando medien **razones de interés general autorizadas por ley**. También podrán ser tratados con finalidades estadísticas o científicas **cuando no puedan ser identificados sus titulares** (art. 7).[5] Además, la ley prohíbe la formación de archivos que almacenen información que directa o indirectamente revelen datos sensibles.

Finalmente, con relación a los datos de salud, la ley prevé que los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del **secreto profesional** (art. 8).

Además, la ley no solo regula la recolección del dato, sino también su **cesión**. El principio general es que la cesión solo puede ser realizada con el consentimiento del

[5] La "disociación de datos" es todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

titular de los datos y a fin de alcanzar la finalidad perseguida por la recolección de los datos. Como excepción, el consentimiento no es exigido cuando lo disponga una ley; cuando no es necesario para su recolección, cuando se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; **cuando se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados**; o cuando se utiliza un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables (art. 11).

**(iv) El principio de la calidad (o exactitud) de los datos**

De acuerdo con ese principio, los datos que sean objeto de tratamiento deben ser "exactos y, cuando sea necesario, actualizados, debiendo tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados".

Este principio explica los derechos otorgados por la LPDP al titular de los datos: **derecho de información, derecho de acceso, derecho de rectificación, actualización o supresión** (arts. 13 a 16).

La Corte Suprema se refirió a la calidad de los datos en un recurso de hecho sobre la información difundida por una empresa de informes crediticios (CSJN, 5/4/2005, "Martínez, Matilde Susana c. Organización Veraz S.A", LA LEY, 2005-B, 743). En dicha ocasión el Máximo Tribunal sostuvo que "[d]e conformidad con los arts. 4°, incs. 4° y 5°, 26 y 33 de la LPDPA, los datos registrados por las empresas que prestan servicios de información crediticia deben ser exactos y completos; vale decir, no es suficiente con que la información haya sido registrada y transmitida sin "arbitrariedad manifiesta", sino que tiene que ser precisa…". Poco después, la Corte Suprema volvió a referirse a la exactitud de los datos en el caso "Di Nunzio, Daniel F. c. The First National Bank of Boston y otros s/hábeas data" (LA LEY, 2007-C, 131, 21/11/2006).

**(v) El principio de la finalidad y el principio de la adecuación:**

Otro principio que estructura la LPDT es el de la **finalidad**. Esto es, los datos son obtenidos para alcanzar un fin y su tratamiento no puede apartarse de ese fin. La ley dispone expresamente que "los datos objeto de tratamiento **no pueden ser utilizados para finalidades distintas** o incompatibles con aquellas que motivaron su obtención" (art. 4, inc. 3). En efecto, si se permitiera un cambio en la finalidad del tratamiento, el consentimiento otorgado por el titular sería burlado. Más claramente, el Reglamento europeo consagra que los datos pueden ser "recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines."

Además, la ley también exige que haya una relación adecuada entre los datos recolectados y la finalidad perseguida. En palabras de la LPDP, los datos deben ser "**adecuados, pertinentes y no excesivos** con relación al ámbito y finalidad para los que se hubieren obtenido" (art. 4º, inc. 1º). El Reglamento europeo consagra

explícitamente el principio de **minimización de los datos**, que ordena que los datos serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". De esta manera, la normativa europea dispone como principio general la obligación de recolectar, almacenar y procesar la menor cantidad de información posible.

En relación con esos principios, la ley prevé que los datos deben ser **destruidos cuando hayan dejado de ser necesarios** o pertinentes a los fines para los cuales fueron recolectados (art. 4 inc.7). Ello es una consecuencia lógica del hecho de que si la finalidad de recolección se ha cumplido ya no tiene sentido conservar el dato, este principio busca evitar la utilización de datos para fines cuyo consentimiento no ha sido dado por el titular. La limitación de la conservación también está definida de manera precisa por el Reglamento europeo, que establece que los datos sean "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales".

### (vi) El principio de la seguridad de los datos

El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Por ello, la ley prohíbe el registro de datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

En sintonía, la normativa europea consagra el principio de integridad y confidencialidad, ordenando que los datos sean "tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas". Finalmente, el Reglamento agrega el principio de responsabilidad proactiva, por el cual los responsables de tratamiento de datos serán responsables del cumplimiento de todos los principios y además, deberán ser capaces de demostrar tal cumplimiento.

## IV. Aplicación de la ley 25.326 en el contexto de pandemia: principios generales

En diciembre de 2019, el Congreso de la Nación declaró, a través de la ley 27.541, la emergencia en materia sanitaria. En marzo del presente año, la Organización Mundial de la Salud declaró pandemia al brote de coronavirus covid-19, que afecta al mundo entero y que genera una crisis sanitaria, socioeconómica, y cultural de dimensiones aún desconocidas. A raíz de ello, el Poder Ejecutivo de la

Nación dictó el decreto 260/2020, ampliando la emergencia sanitaria y dictando medidas drásticas para prevenir y controlar la crisis sanitaria.[6]

Algunas de esas medidas, como la aplicación Cuidar -que será analizada en profundidad en el capítulo siguiente- requiere la obtención y el tratamiento de datos personales y sensibles. Ello genera un conflicto entre la protección del derecho a la vida y a la salud amenazados por la pandemia, y la protección del derecho a la privacidad y a la autodeterminación informativa. En ese marco, ¿es aplicable la Ley de Protección de Datos Personales? En ese caso, ¿de qué modo? En otras palabras, ¿la ley 25.326 trata adecuadamente ese conflicto de derechos en la pandemia?

Esa cuestión ha suscitado respuestas disímiles en el derecho comparado. En ese sentido, puede diferenciarse tres tipos de posturas.[7] Algunos países, como Francia, Bélgica y México, aplican en forma directa las leyes de protección de datos personales a las diversas situaciones relacionadas con la pandemia, como ser tratamiento en el ámbito laboral o por parte del Estado, exigiendo siempre el consentimiento del titular del dato personal. Se trata de un enfoque restrictivo. Otros países, como Alemania, adoptan una postura intermedia, que tiene en cuenta los principios de datos personales pero que permite recopilar datos con la finalidad de evitar contagio o amparar el lugar de trabajo del empleado. Por último, otros países, como China, España y Reino Unido, dan prioridad al derecho a la salud y a la emergencia sanitaria por sobre las normas de protección de datos; entre otras cosas, permiten compartir datos e incluso publicarlos cuando ello ayude a frenar el contagio.[8] De este modo, aún países europeos, regidos por el mismo reglamento general, han adoptado interpretaciones diversas.

Esta Sección de Derecho Constitucional entiende que **la LDPD es aplicable en nuestro país, aún en el contexto de pandemia** puesto que en la emergencia no se suspenden los derechos constitucionales, y la LDPD ampara la privacidad y la autodeterminación informativa previstas en la Constitución Nacional. Sin embargo, la emergencia requiere que esa norma sea aplicada con cierta **flexibilidad** a fin de no impedir que el Estado argentino combata en forma eficiente la pandemia, que pone en juego otros derechos tan fundamentales, como la vida y el disfrute del más alto nivel posible de la salud (arts. 33 y 75, inc. 22, Constitución Nacional; 4 y 5, Convención Americana sobre Derechos Humanos; arts. 11 y 12, Pacto Internacional de Derechos Económicos, Sociales y Culturales).

En efecto, la relevancia de los fines perseguidos por el Estado puede justificar una mayor restricción a los derechos a la privacidad y a la autodeterminación informativa. En el ámbito de los derechos económicos, la Corte Suprema ha desarrollado la **doctrina de la emergencia** para justificar restricciones adicionales a esos derechos en situaciones excepcionales. Sin embargo, ha señalado límites, esto

[6] Decretos 260, 274, 287, 297, 298, 313, 325, 327, 331, 355, 365, 372, 408, 409, 410, 425 y 426. Todos del 2020.

[7] Palazzi, Pablo y Elaskar, Mercedes, "Pandemia (COVID-19) y protección de datos personales. Primeras aproximaciones"**,** LA LEY 13/05/2020, 13; AR/DOC/1068/2020.

[8] Tal como surge del artículo citado, la fuente de la información de esta sección sobre el derecho comparado fueron tomadas de la página web de la IAPP en https://iapp.org/resources/article/dpa-guidance-on-covid-19/, y la de /los estudios juridicos Hogan Lovells y Bird & Bird donde se publicó un cuadro con las opiniones de las distintas agencias de protección de datos europeas.

es, la "restricción debe ser razonable, limitada en el tiempo, un remedio y no una mutación en la substancia o esencia del derecho adquirido por sentencia o contrato".[9]

En relación a la restricción de derechos civiles y políticos, como la privacidad, la Comisión de Derechos Humanos de las Naciones Unidas dictó los "Principios de Siracusa sobre las Disposiciones de Limitación y Derogación del Pacto Internacional de Derechos Civiles y Políticos". Ellos establecen que "la salud pública puede invocarse como motivo para limitar ciertos derechos a fin de permitir a un Estado adoptar medidas para hacer frente a una grave amenaza a la salud de la población o de alguno de sus miembros. Estas medidas deberán estar encaminadas específicamente a impedir enfermedades o lesiones o a proporcionar cuidados a los enfermos y lesionados."[10] De este modo, esta norma avala una restricción adicional de derechos. Sin embargo, ello no es una carta en blanco para que los Estados limiten derechos, sino que los citados principios exigen que **las medidas adoptadas sean razonables y proporcionales, considerando la mejor evidencia científica disponible** al momento en que son adoptadas las medidas, teniendo especialmente en cuenta las consideraciones de la Organización Mundial de la Salud.

Esas pautas guían la restricción del derecho a la privacidad y a la autodeterminación informativa a través de la recolección y tratamiento de datos en la pandemia. Es importante no perder de vista que se trata de una respuesta frente a la emergencia, por lo que desaparecida esa situación excepcional, vuelve a regir con todo su vigor la LPDP y los derechos constitucionales subyacentes.

En el **análisis de razonabilidad y proporcionalidad**, deben ponderarse, en particular, los principios que estructuran la LPDP y aseguran la protección de la privacidad y la autodeterminación informativa: la licitud en la obtención y en el tratamiento de los datos, la calidad de los datos, la finalidad del procesamiento, la adecuación y necesidad de los datos (la proporcionalidad), lo que comprende su eliminación cuando se vuelven innecesarios, la seguridad y confidencialidad. Esos principios pueden sufrir alguna limitación en la emergencia a fin de que el Estado alcance algún fin imperativo, pero no desaparecen.

En primer lugar, con relación a la **licitud**, la ley prevé, tal como desarrollamos en el capítulo anterior, que el **consentimiento** es la base legal para obtener y procesar datos personales. Es importante destacar que, en el caso de los datos referidos a la salud, rige el principio de que nadie puede ser obligado a proporcionarlos puesto que son datos sensibles. En la pandemia, ese principio puede sufrir alguna limitación; por ejemplo, cuando no relevar datos de mi salud compromete la salud de otros individuos. Ello puede justificar la **obligación de**

[9] CSJN, Fallos, 313:1513 (1991), cons. 43. En igual sentido, CSJN, Fallos, 318:1887 (1995); CSJN, Fallos, 321:1984 (1998); CSJN, Fallos, 325:28 (2002); CSJN, Fallos, 330:3002; entre muchos otros.

[10] Los principios disponen a esos efectos de deben tenerse debidamente en cuenta las normas sanitarias internacionales de la Organización Mundial de la Salud.

**proporcionar datos sobre nuestra temperatura corporal para utilizar un transporte público**.[11]

La Corte Suprema se expidió en el caso "N.N. o D., c. s/protección y guarda de personas" (Fallos: 335:888) en favor de la protección de la salud pública por sobre el derecho a la privacidad. Con argumentos similares, sostuvo la constitucionalidad de pruebas de HIV realizadas a agentes de la Policía Federal, aun sin su consentimiento, en el caso "B. R. E. c. Policía Federal Argentina". Sin embargo, la cuestión es controvertida, como muestra la enfática disidencia emitida por el Dr. Fayt en ese caso.[12]

La LPDP admite la obtención y el tratamiento de datos sin el consentimiento del titular en ciertos supuestos.

En el caso de los **datos personales**, no se requiere el consentimiento cuando la obtención y el tratamiento del dato están relacionados con el ejercicio de una función propia del Estado. Durante la pandemia el Estado puede recolectar datos personales sin la autorización del titular, siempre que **efectivamente persiga una finalidad pública y que esté enmarcado en las excepciones al consentimiento previstas por la LPDP**.

A la vez, debe existir una **relación adecuada entre la recolección y el tratamiento del dato y la función del Estado**. Ningún dato puede ser recabado en forma **innecesaria o despoporcianada o excesiva a la finalidad perseguida**. Ello demanda precisar qué datos son necesarios para alcanzar el fin público. Además, el Estado debe garantizar la **seguridad** de los datos.

En el caso de los **datos sensibles**, no se requiere el consentimiento cuando "medien **razones de interés general autorizadas por ley**" o cuando sean tratados con finalidades estadísticas o científicas **cuando no puedan ser identificados sus titulares**. Por un lado, la ley exige que el propósito sea establecido por una ley, y ello genera la discusión sobre si, en la emergencia y ante el reciente y escaso funcionamiento del Congreso de la Nación, basta con un decreto de necesidad y urgencia. Entendemos que si hay una imposibilidad cierta para que se siga el trámite ordinario de sanción de leyes y hay urgencia en la recolección de los datos, el Poder Ejecutivo puede dictar un decreto de necesidad y urgencia con esos fines, siempre que el Congreso se avoque al control en los términos establecidos por la ley en forma inmediata. En caso de no darse las circunstancias referidas, no puede admitirse válidamente que un decreto de necesidad y urgencia reemplace a una ley.

De todos modos, **la finalidad de la recolección debe estar claramente fijada en esa norma** para cumplir con uno de los principios fundamentales en

[11] https://www.buenosaires.gob.ar/jefedegobierno/noticias/ya-funciona-el-primer-sistema-de-camaras-para-tomar-la-temperatura-de-los

[12] CS, 17/12/1996, "B. R. E. c. Policía Federal Argentina", AR/JUR/1112/1996. Fayt afirmó que "aceptar que la relación de sujeción especial que mantienen los agentes con la Policía Federal, supone algunas limitaciones al derecho a la intimidad en beneficio de los fines propios de la institución, no autoriza a cohonestar la pulverización de ese derecho (...). A lo que cabe agregar —lamentablemente— que gran parte de la sociedad, con base solo emocional, suele estigmatizar y segregar a quienes se encuentran infectados por el virus del HIV".

torno a la protección de los datos personales, como es, el principio de adecuación o pertinecia del dato (art. 4.1, LPDP). Por este principio, no sólo debe informarse al titular la finalidad para la que se recopila el dato, sino que el mismo debe ser destruído una vez finalizado el motivo que originó la recopilación y tratamiento de esos datos (art. 4.7, LPDP).

Por otro, algunos sectores de la doctrina exigen, además, que se use algún mecanismo de disociación del dato a fin de preservar la privacidad.[13] En el caso de ser posible, esos recaudos codyuvan a la protección tuitiva de los derechos constitucionales en juego. En caso de no ser posible, se debe exigir que la finalidad perseguida por el Estado sea legítima, y se fundamente en razones de interés general, como la defensa nacional, la protección a la seguridad pública, a la salud pública o en la represión de delitos. Además, en ese supuesto, debe haber una **relación de necesidad** entre la recolección del dato sensible y la finalidad perseguida, esto es, no debe haber otros medios disponibles que sean menos restrictivos de los derechos constitucionales en juego.

Asimismo, en la pandemia rige el principio de la **calidad del dato** (art. 4), o sea, los datos deben sea exactos y actualizados, y los titulares de los datos tienen **derechos de información, de acceso, de rectificación, actualización o supresión** (arts. 13 a 16).

**En ningún caso, los datos recolectados durante la pandemia pueden ser conservados una vez finalizada la situación excepcional**, a no ser que se obtenga un nuevo consentimiento de los titulares. Este límite es trascendental a fin de evitar los **abusos y opresiones** que podría conllevar la utilización y manipulación de datos por parte de los Estados. La realidad ha mostrado abusos en el tratamiento de datos a fin de ganar elecciones, por ejemplo.[14] La eficacia demostrada por los mecanismos digitales durante la pandemia no puede dar lugar la tan temida "**vigilancia estatal**", **"OJO PÚBLICO" o "inteligencia estatal"**, que amenaza las libertades fundamentales. Frente al avance de la tecnología, el desafío del Derecho es lograr un equilibrio, lo que requiere levantar las banderas infranqueables de los derechos constitucionales a la privacidad y a la autodeterminación informativa.

## V. La aplicación CUIDAR

La Nación, algunas jurisdicciones provinciales (Santa Fe, La Rioja, Tierra del Fuego, Misiones, Río Negro, Buenos Aires, Mendoza, Jujuy) y municipales (Ciudad de Córdoba y General Pueyrredón)[15] han recurrido a herramientas digitales para superar la pandemia.[16] La aplicación desarrollada por el gobierno nacional es

[13] Esa es la postura de la Asociación por los Derechos Civiles (ADC).

[14] https://es.wikipedia.org/wiki/Cambridge_Analytica.

[15] Para un análisis de esas aplicaciones locales, consultar: https://adc.org.ar/2020/05/21/en-caso-de-emergencia-descargue-una-app/.

[16] Para tener un panorama sobre las aplicaciones utilizadas en otros países, ver "Creating the coronopticon", The Economist, 26/03/2020, https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic?fsrc=newsletter.

*"Cuidar"* y está *"destinada a la prevención y al cuidado de la ciudadanía frente a la pandemia del nuevo coronavirus covid-19*".[17]

En la actualidad, el gobierno nacional no exige en forma obligatoria la utilización de la aplicación CUIDAR, aunque la recomienda enfáticamente, especialmente para las personas que tramitan certificados de circulación durante el aislamiento obligatorio. Las jurisdicciones locales podrían decidir que la aplicación es obligatoria en su ámbito, lo que no ha sucedido. La Provincia y la Ciudad de Buenos Aires recientemente afirmaron en forma contundente que no es obligatoria.[18] El carácter optativo de la aplicación es consistente con las recomendaciones de la Unión Europea.[19]

Si el individuo decide usar la aplicación, debe responder un cuestionario sobre su estado de salud y síntomas compatibles con el virus, para luego recibir un diagnóstico, además de instrucciones en caso de ser necesarias. Además, el usuario provee su nombre completo, DNI (a través de su escaneo), CUIT/CUIL, fecha de nacimiento, domicilio, género, correo electrónico, datos sobre el dispositivo y de manera automática la app registra los datos de geolocalización, aunque esto último puede ser desactivado por el usuario. Es importante aclarar que la aplicación no informa que está diseñada para realizar *contact tracing* (el rastreo de contactos de las personas contagiadas), una función más controvertida que tienen algunas aplicaciones extranjeras.

Mientras la utilización de la aplicación sea optativa en nuestro país, la base legal para recolectar y tratar los datos personales y sensibles es el consentimiento. Ello requiere analizar si se trata de un consentimiento "libre", "expreso" e "informado", tal como lo exige la LPDP. La política de privacidad de la aplicación figura en un ícono "términos y condiciones" y no hay una constancia cierta de que sean leídos y comprendidos por el titular de los datos. De todos modos, para el usuario que decide leer esos términos, **la información, en general, cumple las pautas previstas por la LPDP, aunque es recomendable que las finalidades de la obtención y la cesión de los datos sean precisadas**.

En este sentido, la aplicación informa que su finalidad "genérica" es "ayudar a prevenir la propagación del virus, como también erigirse en una fuente de información fidedigna para los usuarios." Con relación a los datos de salud, afirma que son utilizados para orientar o dar instrucciones al usuario para ser atendido en la unidad más cercana. Luego, especifica que se utilizarán los datos de geolocalización con fines específicos: "i) recomendar medidas preventivas o de evaluación sanitaria; ii) activar los sistemas de emergencia para la prestación de asistencia sanitaria, iii) conectar al usuario o usuaria con un sistema de atención sanitario cercano, iv)

[17] En la Argentina, el primer precedente fue la Decisión Administrativa 432/2020 del Gobierno nacional que reconoció la necesidad de "hacer uso de la tecnología con el fin de facilitar a las autoridades argentinas el cuidado de la población en su totalidad". En esa decisión, instó a la Dirección Nacional de Migraciones (DNM) a requerir la utilización de la aplicación "COVID 19-Ministerio de Salud" a los viajeros que regresen al país desde el exterior. Esto fue efectivizado 2 días después por la DNM, que dispuso su obligatoriedad para los repatriados.

[18] https://argentina.as.com/argentina/2020/05/30/tikitakas/1590843726_568649.html.

[19] https://www.europarl.europa.eu/news/es/headlines/society/20200429STO78174/covid-19-garantizar-privacidad-y-proteccion-de-datos-en-aplicaciones-moviles

realizar comparaciones y predicciones. Todo ello, con el objetivo específico de dar intervención a las autoridades sanitarias o bien llevar **adelante políticas públicas de prevención y mitigación relacionadas con el COVID-19 y con la emergencia declarada,** así como para contribuir a investigaciones científicas que permitan desarrollar y/o mejorar técnicas sanitarias y preventivas relacionadas con la pandemia".

Si bien estas declaraciones le permiten al usuario tener una idea sobre las finalidades del tratamiento de datos y sus limitaciones, la **suma de propósitos y la amplitud de algunos de ellos dificultan su comprensión, a la vez que amplía la discreción estatal** en el procesamiento de datos en desmedro de la privacidad y la autodeterminación informativa.

Con relación a la cesión de datos, informa que pueden ser cedidos "únicamente a otras entidades estatales y/o establecimientos sanitarios nacionales, provinciales y municipales, para que estos puedan contener y/o mitigar la propagación del virus COVID-19. El usuario podrá requerir a la Subsecretaría de Gobierno Abierto y País Digital que informe las cesiones que se hubieran realizado en forma no disociada sobre los datos recabados por la aplicación". En este sentido, las **finalidades informadas con relación a la cesión de datos son demasiado amplias y ambiguas**, lo que puede comprometer la privacidad de los usuarios, más aún cuando **la disociación de datos no está garantizada.**

La aplicación también informa: (i) quién es el responsable de los datos (Subsecretaría de Gobierno Abierto y País Digital de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros de la Nación), (ii) los derechos de acceso, supresión y rectificación de los usuarios, (iii) la posibilidad de revocar el consentimiento, (iv) la seguridad y confidencialidad de los datos, (v) la prohibición de utilizar los datos para fines diversos a los informados, (vi) el almacenamiento de los datos, entre otros. **Ello es congruente con la información exigida por la LPDP.**

Finalmente, la aplicación afirma que "los datos sensibles y los relacionados con la geolocalización se preservarán únicamente mientras sean necesarios y dure la emergencia sanitaria. Una vez finalizada esta, podrán preservarse versiones anonimizadas de los mismos con fines científicos y epidemiológicos". **La declaración es relevante; y es esencial que se lleve a la práctica.** Una vez finalizada la pandemia, habrá en manos de varios actores una gran cantidad de datos de salud y geolocalización, entre otros, que podrían potencialmente ser tratados y reutilizados con ánimo de lucro y/o discriminatorio.[20] Es esencial que los responsables estatales de la recolección y procesamiento de los datos personales aseguren una gestión legal, ética y transparente de los datos personales recolectados, y su eliminación, una vez superada la pandemia.

En el caso de que el **Estado decidiera imponer el uso de la aplicación Cuidar,** debería justificar la licitud de la obtención y el tratamiento de esos datos a partir de su vinculación con fines estatales en el marco de la pandemia. Ello requiere un escrutinio del cumplimiento de los principios de adecuación, finalidad y

[20] Palazzi y Elsakar, ob. cit.

proporcionalidad en el marco de una emergencia sanitaria. Ese análisis depende del tipo de dato en cuestión.

En el caso de los datos sensibles, como los vinculados a la salud, la finalidad del procesamiento debe ser establecida por **"ley"** y es recomendable que sean utilizados a través de algún **mecanismo de disociación**. Si la disociación no es posible, el Estado debe mostrar el carácter imperativo del fin perseguido y la necesidad del medio empleado.

En relación con la función de "autodiagnóstico", cabe destacar que: (i) **la calidad y precisión que pueden tener esos datos es limitada;** (ii) cuando estas funciones son vinculadas al ejercicio de otros derechos, como los que habilita el permiso/certificado de circulación, los incentivos para que las personas envíen datos falsos sobre sus síntomas son muy altos y (iii) **puede generarse una falsa sensación de seguridad**, sobre todo si las personas reportan sus síntomas y no tienen una respuesta rápida desde el sistema de salud. De hecho, la propia aplicación afirma que "no sustituye la opinión médica" y que las sugerencias y guías que pueden encontrarse en la aplicación "no constituyen opinión médica ni deben utilizarse para realizar un diagnóstico ni iniciar un tratamiento médico sin consulta de un profesional de la salud".

De este modo, la eficacia de las aplicaciones como método de diagnóstico es incierta. Por ello, entendemos que **esa finalidad no justifica la obtención de datos tan sensibles, como los vinculados a la salud, menos aún cuando no está demostrada la inexistencia de otros medios menos intrusivos** a esos efectos, como la utilización de una página web donde el titular no sea identificado ni se acceda a sus datos de geolocalización. A la vez, **tampoco se requiere el registro de los datos personales y sensibles de los individuos a fin de informarlos sobre los centros de atención** a los que deben recurrir, aun cuando ello sea eficiente para organizar y coordinar la atención médica. Ello se puede hacer a través de servicios digitales que no requieren la identificación del usuario.

Sin embargo, **hay otra finalidad que puede justificar la recolección de esos datos, esto es, evitar la proliferación del virus.** Se trata de una finalidad **imperativa**, teniendo en cuenta la altísima tasa de contagiosidad del coronavirus, el carácter potencialmente letal de la enfermedad que genera, la falta de métodos adecuados para el tratamiento de la infección y la situación de posible saturación de los servicios públicos de salud permitiría. Es importante que el Estado demuestre **la eficacia** de utilizar los datos de salud y de geolocalización para adoptar medidas preventivas, por ejemplo, a través de la identificación de los casos "sospechosos" y de contagios, y del estudio de la cadena de contagios. Ello no surge con claridad de la información proporcionada por la aplicación Cuidar y tampoco hay consenso en la doctrina sobre ese aspecto.[21] La eficacia debe sea analizada considerando la información científica disponible. Si la eficacia es demostrada, la utilización de los

[21] Agustina Del Campo, directora del Centro de Estudios de Libertad de Expresión (CELE) de la Universidad de Palermo, afirma que no está del todo claro que la geolocalización sea un mecanismo eficaz para los fines para los que suele utilizarse. Hay opiniones que cuestionan este tipo de tecnología tanto desde el sector privado como desde la sociedad civil. En este sentido, las medidas excepcionales que se adopten en el contexto de la COVID-19 deberían ser evaluadas periódicamente en cuanto a eficacia, resultados, riesgos e impacto.

datos podría superaría el test de necesidad en el actual contexto excepcional de una pandemia de dimensiones desconocidas. Una vez transcurrida la emergencia sanitaria, o modificadas esas circunstancias particulares, deja de ser lícito obligar a los individuos a dar al Estado sus datos de salud y geolocalización.

## VI. **Los permisos de circulación**

El Poder Ejecutivo Nacional decretó, a través de los decretos 260/2020 y 297/2020, el aislamiento social obligatorio y lo prorrogó hasta la actualidad. A la vez, exceptuó de esa medida y de la consecuente prohibición de circular a las personas afectadas a las actividades y servicios declarados esenciales en la emergencia. La excepción comprende solamente los desplazamientos que se realicen para cumplir esas actividades y servicios.

A los efectos de controlar el cumplimiento del aislamiento obligatorio, el gobierno nacional dispuso que las personas exceptuadas deben tramitar un certificado de circulación. El Certificado Único Habilitante de Circulación vigente requiere que el individuo informe el motivo de la circulación (trabajo y, en ese caso, qué actividad esencial realiza; o permiso especial, y, en ese caso, cuál: trámites, tratamiento prolongado, traslado de hijos o hijas, asistencia a familiar), nombre y apellido, DNI, domicilio, género, CUIL, correo electrónico, teléfono, domicilio de residencia, domicilio laboral, CUIT del empleador, nombre de la empresa, teléfono de la empresa, medio de transporte utilizado para la circulación (nro. de tarjeta sube, si ese el medio utilizado). En el caso de los permisos especiales, el certificado exige una descripción del motivo, bajo el título "Datos del tratamiento médico/nombre hijos/nombre familiar/descripción de la emergencia".

A fin de analizar la validez de la obtención y el tratamiento de esos datos, debe tenerse especialmente en cuenta los **principios que estructuran la LDPD: la licitud, la calidad de los datos, la finalidad y la adecuación, la seguridad y la transparencia**. Aun cuando esos principios puedan sufrir alguna restricción en la emergencia, esa limitación debe superar el test de razonabilidad y proporcionalidad.

En primer lugar, cabe destacar que para las personas exceptuadas del aislamiento, la prestación de esos datos personales es obligatoria, y no optativa. En ese caso, la base legal del Estado para obtener y tratar los datos no es el consentimiento, sino su vinculación con el ejercicio de una **función del Estado,** esto es, controlar el cumplimiento de la medida de aislamiento obligatorio adoptada a fin de hacer frente a la pandemia (art. 5, inc. 2.b y 2.c; art. 7, inc. 2, LPDP).

Los datos peticionados por el certificado actual son, en su gran mayoría, **personales**, y no sensibles, lo que facilita su obtención y tratamiento por parte del Estado (art. 5, inc. 2.b). Únicamente, en el caso del permiso especial para asistir a un tratamiento médico o para el cuidado de una persona discapacitada, hay que proporcionar datos que involucren cuestiones de salud, y que, por ende, tienen mayor protección legal (art. 7, inc. 2). De todos modos, en ese caso, el usuario debe hacer una breve descripción del motivo de la circulación y el sistema digital no le exige una precisión desmedida que lo exponga más allá de lo decida el usuario. Con

relación al tratamiento de esos datos, sería importante que el Estado utilice algún mecanismo de disociación que preserve la identidad de la persona.

En segundo lugar, ha generado cierta controversia si los datos recabados en los certificados de circulación cumplen los requisitos de **adecuación y necesidad**.

Por un lado, algunas voces sostienen que los datos peticionados no son desmedidos puesto que le permiten al Estado cumplir una función estatal en los términos del artículo 5, inc. 2.b, de la LPDP; esto es, controlar el cumplimiento del aislamiento obligatorio en forma eficiente. En este sentido, se puede afirmar que, por ejemplo, los datos vinculados con el empleo (el CUIT del empleador, el nombre de la empresa, el domicilio y el teléfono laboral) permiten controlar la legalidad de ese supuesto excepcional de circulación. Más cuestionable son los datos vinculados al transporte, que llegan a exigir el número de patente del auto o el número de la tarjeta Sube. Esos datos pueden exceder el fin estatal.

Por otro lado, otras opiniones plantean que los datos solicitados por el Estado son excesivos e innecesarios y no cumplen el principio de minimización de la información. En este sentido, puede afirmarse que el Estado puede controlar el cumplimiento del aislamiento obligatorio requiriendo menos información; más concretamente, supliendo el certificado de circulación con una declaración jurada en la cual el individuo afirme que se encuentra exceptuado de esa medida. Algunas provincias han adoptado ese sistema.[22]

En cualquier caso, la razonabilidad de los datos peticionados debe ser analizada diferenciado las circunstancias concretas que se presentan en las distintas provincias; esto es, en las jurisdicciones que presentan situaciones más comprometidas de covid-19, el Estado podría recurrir a medidas más estrictas; mientras que en jurisdicciones con menos casos de covid-19, esas medidas son innecesarias. Además, la razonabilidad debe ser analizada sobre la base de las circunstancias actuales, por lo que ese juicio debe ser actualizado en forma permanente.

Además, el Estado debe asegurar una **gestión transparente y confiable de los datos, y su eliminación** una vez culminado el aislamiento obligatorio. Con relación a los datos de salud, la LPDP prohíbe su almacenamiento (art. 7, inc. 3), por lo que esos datos deben ser destruidos a fin de evitar que puedan ser utilizados con fines discriminatorios o estigmatizantes, o para cualquier otra finalidad que no sea la que justificó su recolección durante la emergencia.

## VII. **Conclusiones**

La Sección de Derecho Constitucional del Instituto de Estudios Legislativos concluye:

(i) Frente a los avances tecnológicos, que se nutren de la utilización de datos personales, adquieren cada vez más relevancia **los derechos constitucionales a la privacidad y a la autodeterminación**

[22] Por ejemplo, Santa Fe. https://www.santafe.gob.ar/ms/covid19/wp-content/uploads/sites/36/2020/04/Permiso-de-circulaci%C3%B3n-DDJJ-COVID19.pdf.

**informativa.** Son los individuos los que tienen derecho a decidir sobre el uso y la cesión de sus datos personales.

(ii) En la situación excepcional de **pandemia** que atraviesa nuestro país, **la Ley de Protección de Datos Personales es aplicable**. Sin embargo, debe ser aplicada con cierta **flexibilidad** a fin de no impedir que el Estado argentino combata en forma eficiente el coronavirus, que pone en riesgo el derecho a la vida y a la salud.

(iii) A fin de analizar la validez de las restricciones a la privacidad y a la autodeterminación informativa durante la emergencia, las medidas adoptadas deber ser **razonables y proporcionales**, considerando la mejor evidencia científica disponible, teniendo especialmente en cuenta las consideraciones de la Organización Mundial de la Salud. Deben tenerse en cuenta los principios que estructuran la protección de los datos personales: **la licitud en la obtención y en el tratamiento de los datos, la calidad de los datos, la finalidad del procesamiento, la adecuación y necesidad de los datos.**

(iv) En la emergencia, el Estado puede obtener y tratar los datos personales y sensibles, si obtiene el consentimiento del titular. Ello es lo que sucede con la aplicación **Cuidar**, que, en la actualidad, no es obligatoria en nuestro país. Además, el Estado puede obtener y tratar datos personales y sensibles sin el consentimiento del titular, si ello está vinculado a una función del Estado, como evitar la propagación del covid-19. En el caso de los datos sensibles, esa finalidad debería ser establecida por una "**ley**" del Congreso de la Nación y esos datos deberían ser utilizados a través de **mecanismos de disociación**, de ser posible. Además, es necesario que el Estado demuestre la **eficacia** de las aplicaciones tecnológicas que utilizan datos sensibles.

(v) En el caso de los **permisos de circulación**, la base legal para la obtención y tratamiento de los datos es su vinculación con una función del Estado, esto es, controlar el cumplimiento del aislamiento obligatorio. Los datos peticionados **no deben exceder** los necesarios para el cumplimiento de esa finalidad. Ese análisis debe realizarse diferenciado las circunstancias concretas que se presentan en cada provincia, y reevaluado sobre la base del progreso en la contención de la pandemia.

(vi) En el tratamiento de los datos, son relevantes la protección del secreto profesional y el deber de confidencialidad. Las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Además, los permisos de circulación no pueden comprometer el secreto profesional de, entre otros, los abogados.

**(vii)** Es dirimente que una vez finalizada la emergencia sanitaria, los datos personales y sensibles recolectados por el Estado sean eliminados. La eventual eficacia demostrada por los mecanismos digitales durante la pandemia no puede dar lugar la tan temida "**vigilancia estatal**", **"OJO PÚBLICO" o "inteligencia estatal"**, que amenaza las libertades fundamentales.

**FIRMANTES**

**Basterra,** Marcela

**Esain,** José

**Ibañez Rosaz,** Víctor

**Medizza,** Fabián

**Recalde,** María Cecilia

**Toricelli,** Maximiliano

**Vásquez,** Guadalupe

**Vigier,** Miguel