2026/179

28.1.2026

DECISIÓN DE EJECUCIÓN (UE) 2026/179 DE LA COMISIÓN

de 26 de enero de 2026

relativa a la adecuación del nivel de protección de los datos personales conferido por Brasil con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

[notificada con el número C(2026) 373]

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) ([1]), y en particular su artículo 45, apartado 3,

Considerando lo siguiente:

1. INTRODUCCIÓN

(1) El Reglamento (UE) 2016/679 establece las normas que regulan la transferencia de datos personales de los responsables o encargados del tratamiento en la Unión a terceros países y organizaciones internacionales, en la medida en que tales transferencias se encuentren comprendidas dentro de su ámbito de aplicación. Las normas sobre las transferencias internacionales de datos se establecen en el capítulo V (artículos 44 a 50) de dicho Reglamento. Si bien la circulación de datos personales hacia y desde países no pertenecientes a la Unión Europea es esencial para la expansión del comercio transfronterizo y la cooperación internacional, el nivel de protección de los datos personales en la Unión no debe verse menoscabado por las transferencias a terceros países ([2]).

(2) De conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, la Comisión puede decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país o una organización internacional garantizan un nivel de protección adecuado. En tal caso, la transferencia de datos personales a un tercer país puede realizarse sin necesidad de obtener ninguna otra autorización, de conformidad con lo dispuesto en el artículo 45, apartado 1, y el considerando 103 de dicho Reglamento.

(3) Tal como se especifica en el artículo 45, apartado 2, del Reglamento (UE) 2016/679, la adopción de una decisión de adecuación ha de basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país, que contemple tanto las normas aplicables a los importadores de datos como las limitaciones y garantías en lo que respecta al acceso a los datos personales por parte de las autoridades públicas. En su evaluación, la Comisión debe determinar si el tercer país en cuestión garantiza un nivel de protección «equivalente en lo esencial» al ofrecido en la Unión ([3]). El criterio con el que se evalúa el nivel de protección «equivalente en lo esencial» es el que establece la legislación de la Unión Europea, en concreto el Reglamento (UE) 2016/679, así como la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) ([4]). Las «referencias sobre adecuación» del Comité Europeo de Protección de Datos (CEPD) también son importantes a este respecto para aclarar en mayor medida dicho criterio y proporcionar orientaciones ([5]).

([1]) DO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Considerando 101 del Reglamento (UE) 2016/679.
([3]) Considerando 104 del Reglamento (UE) 2016/679.
([4]) Asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximillian Schrems («Schrems II»), ECLI:EU:C:2020:559.
([5]) Referencias sobre adecuación, Comité Europeo de Protección de Datos, WP 254, rev. 01. Puede consultarse en el siguiente enlace: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Como ya aclaró el Tribunal de Justicia, no puede exigirse a un tercer país que garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la UE ([6]). En particular, los medios de que se sirve el tercer país en cuestión para la protección de los datos personales pueden ser diferentes de los aplicados en la Unión, siempre que, en la práctica, sean eficaces para garantizar un nivel de protección adecuado ([7]). Por consiguiente, el principio de adecuación no exige que se reproduzcan al pie de la letra las normas de la Unión. Se trata más bien de determinar si, a través de la esencia de los derechos de privacidad y las salvaguardias de protección de datos (especialmente su aplicación, fuerza ejecutiva y supervisión efectivas), así como atendiendo a las circunstancias que rodean a la transferencia de datos personales, el ordenamiento en cuestión ofrece, en su conjunto, el nivel de protección exigido ([8]).

(5) La Comisión ha analizado la legislación y la práctica de la República Federativa de Brasil («Brasil»). Basándose en las conclusiones expuestas en los considerandos 7 a 223, la Comisión concluye que Brasil garantiza un nivel adecuado de protección para los datos personales transferidos dentro del ámbito de aplicación del Reglamento (UE) 2016/679 de la Unión Europea a Brasil.

(6) La presente Decisión tiene como efecto que las transferencias de responsables y encargados del tratamiento en la Unión a responsables y encargados del tratamiento en Brasil puedan realizarse sin necesidad de obtener ninguna autorización adicional. No tiene ninguna incidencia en la aplicación directa del Reglamento (UE) 2016/679 a las entidades cuando se cumplan las condiciones relativas al ámbito territorial de dicho Reglamento, establecidas en su artículo 3.

2. NORMATIVA APLICABLE AL TRATAMIENTO DE DATOS PERSONALES

2.1. El marco constitucional de Brasil

(7) Brasil es una República Federativa compuesta por la unión de los 26 Estados y el Distrito Federal, tal como se establece en su Constitución federal (la «Constitución») ([9]). Los Estados brasileños también tienen sus propias constituciones, que no deben contravenir la Constitución federal ([10]). Brasil cuenta con un sistema presidencial según el cual el presidente y los miembros de las cámaras legislativas (es decir, la Cámara de Diputados y el Senado Federal) son elegidos directamente.

(8) La intimidad y la protección de datos están protegidas en la Constitución como derechos fundamentales. Más concretamente, el artículo 5, inciso X, de la Constitución protege la intimidad y la vida privada de las personas; el artículo 5, inciso XII, garantiza el secreto de las comunicaciones por correspondencia, incluidos los datos; y el artículo 5, inciso LXXIX establece el derecho a la protección de los datos personales en línea y fuera de línea ([11]).

(9) Todos los derechos que emanan de la Constitución se aplican a los brasileños y extranjeros residentes en Brasil de conformidad con su artículo 5. Las leyes federales aclaran que toda persona, residente o no, que se encuentre en el territorio de Brasil tiene derecho a la protección de los derechos fundamentales ([12]). El alcance de la protección de estos derechos ha sido ampliado por la jurisprudencia constitucional para incluir a los extranjeros que viven en el extranjero, como también destaca la doctrina jurídica pertinente ([13]). En consecuencia, cualquier extranjero, residente o no en Brasil, puede invocar estas protecciones constitucionales ([14]).

([6]) Asunto C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems I»), ECLI:EU:C:2015:650, apartado 73.
([7]) Schrems I, apartado 74.
([8]) Schrems I, apartado 75.
([9]) Constitución de la República Federativa de Brasil de 1988. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.
([10]) Artículo 25 de la Constitución de la República Federativa de Brasil de 1988.
([11]) Enmienda constitucional n.º 115 de 10 de febrero de 2022. Puede consultarse en el siguiente enlace: http://www.planalto.gov.br/ccivil_03/Constituicao/Emendas/Emc/emc115.htm#art1.
([12]) Véase, por ejemplo, el artículo 4, inciso XIII, de la Ley n.º 13.445, de 24 de mayo de 2017 (Ley sobre Migración). Disponible en https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o.&text=Art.,pol%C3%ADticas%20p%C3%BAblicas%20para%20o%20emigrante.
([13]) Véase, por ejemplo, Ferreira Filho Manoel Gonçalves, *Direitos humanos fundamentais* [«Derechos humanos fundamentales», disponible en portugués]. 6.ª ed., São Paulo: Saraiva, 2004.
([14]) Sentencia del Tribunal Superior de Justiça, 4a Turma, 2016. Puede consultarse en el siguiente enlace: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.

(10) Brasil ratificó la Convención Americana sobre Derechos Humanos, conocida como el «Pacto de San José», en 1992 ([15]) (la «Convención»). Entre otras cuestiones, el artículo 11 de la Convención garantiza el derecho a la intimidad y su artículo 8 protege el derecho a un juicio justo. En 1998, Brasil reconoció la autoridad vinculante de la Corte Interamericana de Derechos Humanos en lo que respecta a la interpretación y aplicación de la Convención ([16]). La Corte puede dictar decisiones relativas a la aplicación de los derechos en el contexto de las actividades llevadas a cabo por las autoridades públicas en Brasil, incluidas aquellas que llevan a cabo tareas con fines de seguridad pública y defensa ([17]).

2.2. **El marco de protección de datos de Brasil**

(11) Brasil promulgó en 2018 una ley general en el ámbito de la protección de datos que ofrece garantías a todas las personas, independientemente de su nacionalidad: la Ley General de Protección de Datos (Lei Geral de Proteção de Dados), en lo sucesivo, la «LGPD» ([18]).

(12) Desde su promulgación, la LGPD se ha reforzado y aclarado mediante legislación adicional. En particular, la Ley n.º 13.853 de 2019 creó la Autoridad Nacional de Protección de Datos de Brasil ([19]), denominada Agência Nacional de Proteção de Dados («ANPD»), que se convirtió en una autoridad independiente en virtud de una ley adoptada en 2022 ([20]). Otros decretos vinculantes completaron este marco legislativo para, entre otras cuestiones, mejorar el estatuto de la ANDP ([21]) y definir con mayor precisión su composición y el procedimiento para nombrar a sus directores ([22]).

(13) Como se describe más detalladamente en los considerandos 125 a 141 de la presente Decisión, la ANPD es la autoridad responsable de interpretar y hacer cumplir la LGPD. En este contexto, emite periódicamente reglamentos vinculantes para interpretar y aplicar la ley. La ANPD ha adoptado, por ejemplo, varios reglamentos para seguir desarrollando el régimen de sanciones y especificar las normas sobre notificación de violaciones de la seguridad de los datos ([23]). La ANPD proporciona más orientaciones sobre la aplicación e interpretación de la LGPD a través de documentos y guías, como los adoptados sobre la interpretación de la base jurídica (por ejemplo, el interés legítimo) y conceptos clave en el marco de la LGPD (como las sanciones o la figura del delegado de protección de datos).

([15]) Lista de signatarios y ratificación de la Convención Americana sobre Derechos Humanos. Puede consultarse en el siguiente enlace: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm.

([16]) Declaración de Brasil sobre la Convención. Puede consultarse en el siguiente enlace: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm#Brazil.

([17]) Véase, por ejemplo, asunto Escher *et al.*/Brasil, sentencia de 6 de julio de 2009. Puede consultarse en el siguiente enlace: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf.

([18]) Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos). Puede consultarse en el siguiente enlace: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm y en inglés: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf.

([19]) Ley n.º 13.853, de 8 de julio de 2019, por la que se modifica la LGPD para, entre otras cuestiones, crear la Autoridad de Protección de Datos - Autoridade Nacional de Proteção de Dados (ANPD). Puede consultarse en el siguiente enlace: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2.

([20]) Ley n.º 14.460, de 25 de octubre de 2022, por la que se transforma la ANPD en una autoridad de estatuto especial. Puede consultarse en el siguiente enlace: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7.

([21]) Decreto n.º 1.317, de 17 de septiembre de 2025, por el que se modifica la LGPD para transformar la Agência Nacional de Proteção de Dados. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

([22]) Decreto n.º 10.474, de 26 de agosto de 2020, por el que se establece la ANPD y su composición. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226 Decreto n.º 11.758, de 30 de octubre de 2023, por el que se modifica la composición de la ANPD. Puede consultarse en el siguiente enlace: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11758.htm Decreto de 5 de noviembre de 2020 sobre el nombramiento de los directores de la ANPD. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/decretos-de-5-de-novembro-de-2020-286734594.

([23]) Véase la lista de Reglamentos de la ANPD. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes y, en particular, el Reglamento n.º 4, de 24 de febrero de 2024, relativo a la aplicación de sanciones administrativas. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077 y el Reglamento n.º 15, de 24 de abril de 2024, sobre la notificación de la violación de la seguridad de los datos. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

(14) Como parte de su compromiso internacional para el fomento y la salvaguarda de la protección de datos, la ANPD de Brasil entró a formar parte de la Asamblea Global de Privacidad en 2023, junto con todas las autoridades de protección de datos de la Unión Europea ([24]). Brasil también se adhirió, en calidad de observador, al Convenio n.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ([25]). Brasil ha liderado además varios avances realizados en las Naciones Unidas (ONU) en relación con el derecho a la intimidad. Junto con Alemania, Brasil presentó las Resoluciones de las Naciones Unidas sobre el derecho a la privacidad en la era digital, adoptadas por la Asamblea General de las Naciones Unidas en 2013 y 2014 ([26]). Entre otras disposiciones, esta resolución señala que «la vigilancia y la interceptación ilícitas o arbitrarias de las comunicaciones, así como la recopilación ilícita o arbitraria de datos personales, al constituir actos de intrusión grave, violan los derechos a la privacidad y a la libertad de expresión y pueden ser contrarios a los preceptos de una sociedad democrática». Solicita a los Estados que revisen las normas sobre recogida de datos para adaptarlas al Derecho internacional en materia de derechos humanos y que «establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones, y la interceptación y recopilación de datos personales que realice el Estado» ([27]).

(15) En lo que respecta a su estructura y componentes principales, el marco jurídico de Brasil aplicable a los datos personales transferidos en virtud de la presente Decisión es similar al que se aplica en la Unión. Dicho marco no solo se basa en obligaciones establecidas en el Derecho interno y en derechos consagrados en su Constitución, sino también en las obligaciones que emanan del Derecho internacional, en particular mediante la adhesión de Brasil a la Convención Americana sobre Derechos Humanos y el reconocimiento de la competencia jurisdiccional de la Corte Interamericana de Derechos Humanos ([28]).

2.3. **Ámbito de aplicación material y territorial de la LGPD**

2.3.1. *Ámbito territorial*

(16) La LGPD se aplica a todo tratamiento de datos personales en Brasil, con independencia de los medios utilizados para llevar a cabo dicha actividad ([29]).

(17) El artículo 3 de la LGPD especifica el ámbito de aplicación territorial de la ley, indicando que se aplica a: 1) actividades de tratamiento realizadas en el territorio nacional de Brasil (que abarca la Federación, los Estados, el Distrito Federal y los municipios); 2) actividades de tratamiento que tengan por objeto ofrecer o suministrar bienes o servicios o el tratamiento de datos de personas situadas en el territorio nacional de Brasil; así como 3) casos en que los datos personales objeto de tratamiento se hayan recogido en el territorio nacional de Brasil. Se trata de un enfoque similar al adoptado en el artículo 3 del Reglamento (UE) 2016/679.

(18) Asimismo, de conformidad con el artículo 3, inciso II, de la LGPD, todo tratamiento de datos personales de personas físicas que se encuentren en el territorio nacional está incluido en el ámbito de aplicación de esta ley. Se incluye, pues, el tratamiento realizado para el control del comportamiento de las personas en el territorio, independientemente del lugar en el que se traten los datos.

([24]) La Asamblea Global de Privacidad (GPA) es un foro que conecta los esfuerzos de más de ciento treinta autoridades de protección de datos y privacidad de todo el mundo. Véase el anuncio de la ANPD sobre su incorporación a la GPA. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-aceita-como-membro-pleno-no-global-privacy-assembly.

([25]) Consejo de Europa, Observadores del Comité del Convenio 108. Puede consultarse en el siguiente enlace: https://rm.coe.int/list-of-observers-december-2022-bilingual-2781-7012-1734-1/1680a962eb.

([26]) Véase, por ejemplo, la Resolución sobre el derecho a la privacidad en la era digital de la Asamblea General de las Naciones Unidas, de 18 de diciembre de 2013. Puede consultarse en el siguiente enlace: https://digitallibrary.un.org/record/764407?ln=en&v=pdf.

([27]) Asamblea General de las Naciones Unidas, Resolución sobre el derecho a la privacidad en la era digital, 18 de diciembre de 2013, pp. 1-2.

([28]) Véase la información sobre la competencia jurisdiccional de la Corte en la sección de preguntas frecuentes del sitio web de la Corte Interamericana de Derechos Humanos. Puede consultarse en el siguiente enlace: https://www.corteidh.or.cr/que_es_la_corte.cfm?lang=en.

([29]) Artículo 3 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

(19) Por último, de la jurisprudencia del Tribunal Supremo Federal (Supremo Tribunal Federal) se desprende que las protecciones de los derechos fundamentales que ofrece la Constitución, como el derecho a la protección de datos, se aplican a cualquier persona, independientemente de la nacionalidad o lugar de residencia del interesado ([30]).

2.3.2. *Definición de «datos personales»*

(20) El artículo 5, inciso I, de la LGPD define los datos personales como «toda información sobre una persona física identificada o identificable». Esta ley especifica que un «interesado» es la «persona física a la que se refieren los datos personales tratados» ([31]).

(21) Además, la información seudonimizada, es decir, aquella que no permite identificar directa o indirectamente a una determinada persona ni asociarse a ella sin utilizar o combinar información adicional para restablecer el estado original de los datos, se considera datos personales en el marco de la LGPD ([32]).

(22) En cambio, la información totalmente «anonimizada» queda excluida del ámbito de aplicación de la LGPD ([33]). Con arreglo al artículo 5 de la LGPD, los datos anonimizados son aquellos que, mediante el uso de los medios razonables y técnicos disponibles en el momento del tratamiento, no puedan asociarse directa o indirectamente a una persona. El artículo 12 de la LGPD detalla además que los datos anonimizados no se consideran datos personales, salvo cuando se haya revertido el proceso de anonimización al que se sometieron o cuando pueda revertirse empleando «esfuerzos razonables». El artículo 12 de la LGPD subraya asimismo que para determinar qué se considera «razonable» se tendrán en cuenta factores objetivos como: 1) el coste y tiempo necesarios para la reversión; 2) la tecnología disponible; y 3) el uso exclusivo de los medios propios del responsable del tratamiento. El enfoque de anonimización y las salvaguardias introducidas en la LGPD para abordar la posibilidad de reidentificación son similares a los aplicados por la Unión.

(23) Esto corresponde al ámbito de aplicación material del Reglamento (UE) 2016/679 y a sus conceptos de «datos personales», «seudonimización» e «información anonimizada».

2.3.3. *La definición de tratamiento*

(24) Las definiciones de «tratamiento» de los sistemas brasileño y de la Unión se refieren ambas a «cualquier operación» realizada con datos personales ([34]). El artículo 5, inciso X, de la LGPD establece la siguiente lista no exhaustiva de actividades que constituyen tratamiento: «recogida, producción, recepción, clasificación, utilización, acceso, reproducción, transmisión, distribución, tratamiento, archivo, almacenamiento, supresión, evaluación o control de la información, modificación, comunicación, transferencia, difusión o extracción».

2.3.4. *Responsable del tratamiento y encargado del tratamiento*

(25) El concepto de «responsable del tratamiento» se define en la LGPD como «la persona física o jurídica, pública o privada, responsable de las decisiones relativas al tratamiento de datos personales» ([35]).

([30]) Decisión del Tribunal Superior de Justiça, 4a Turma, 2016. Puede consultarse en el siguiente enlace: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.
([31]) Artículo 5, inciso V, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([32]) Artículo 13 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([33]) Artículo 12 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([34]) Artículo 5, inciso X, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([35]) Artículo 5, inciso VI, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

(26) El concepto de «encargado del tratamiento» se define en la LGPD como «la persona física o jurídica, pública o privada, que lleva a cabo el tratamiento de datos personales por cuenta del responsable del tratamiento» ([36]). El encargado del tratamiento debe llevar a cabo el tratamiento con arreglo a las instrucciones facilitadas por el responsable del tratamiento, que es responsable de verificar el cumplimiento ([37]).

(27) El responsable y el encargado del tratamiento deben llevar un registro de las operaciones de tratamiento de datos personales que realizan, especialmente cuando se basen en un interés legítimo ([38]).

(28) En virtud de la LGPD, dos o más responsables del tratamiento que intervengan directamente en el tratamiento que ha dado lugar a daños y perjuicios al interesado son responsables solidarios ([39]). Un encargado del tratamiento es responsable solidario de los daños y perjuicios causados por dicho tratamiento cuando incumple las obligaciones impuestas por la LGPD, tal como se definen en su artículo 44, o cuando no ha seguido las instrucciones legales del responsable del tratamiento ([40]).

(29) Por lo tanto, las normas que regulan la relación entre los responsables y los encargados del tratamiento en el marco de la LGPD son similares a las recogidas en el capítulo IV del Reglamento (UE) 2016/679.

2.3.5. *Exención de determinadas disposiciones de la LGPD*

(30) Al igual que en el sistema de la Unión, la LGPD no se aplica a los datos anonimizados ([41]), al tratamiento de datos personales con fines exclusivamente domésticos ([42]) o cuando se lleve a cabo exclusivamente con fines de seguridad pública, defensa nacional, seguridad del Estado o investigación y enjuiciamiento de infracciones penales ([43]).

(31) No obstante, la exención en el ámbito de la seguridad pública, la defensa nacional, la seguridad del Estado y la investigación y el enjuiciamiento de las infracciones penales es parcial. El Tribunal Supremo Federal ha interpretado la aplicabilidad de la LGPD a la luz de la protección constitucional de los datos personales y ha establecido que los principios, derechos y objetivos fundamentales de la LGPD se aplican a todo tratamiento de datos personales por parte de las autoridades públicas, incluso cuando se realiza con fines de «inteligencia» ([44]). Además, en el artículo 4, apartados 2 a 4, de la LGPD, se establecen condiciones para el tratamiento de datos personales con fines de seguridad pública, defensa nacional, seguridad del Estado o investigación y enjuiciamiento de infracciones penales, en particular para impedir que las entidades privadas traten datos con tales fines, dar instrucciones a la ANPD para

([36]) Artículo 5, inciso VII, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([37]) Artículo 39 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([38]) Artículo 37 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([39]) Artículo 42, apartado 1, inciso II, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([40]) Artículo 42, apartado 1, inciso I, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([41]) Artículo 12 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([42]) Artículo 4, inciso I, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([43]) Artículo 4, inciso III, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([44]) Tribunal Supremo Federal. Decisión sobre la ADI 6649, septiembre de 2022. Puede consultarse en el siguiente enlace: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

que emita dictámenes técnicos y recomendaciones al respecto y facultar a la ANPD para solicitar una evaluación de los efectos de tales actividades en la protección de datos ([45]). Sobre esta base, la ANPD, por ejemplo, ha llevado a cabo investigaciones y ha publicado orientaciones, como una nota técnica dirigida al Ministerio de Justicia y Seguridad Pública sobre el uso de tecnologías, tales como el reconocimiento facial, en los espacios públicos ([46]). En esta nota, la ANPD recordó que el tratamiento para estos fines debe ajustarse a los principios y derechos generales previstos por la LGPD ([47]).

(32) El artículo 4, inciso II, de la LGPD introduce además una exención parcial de la ley en lo que respecta al tratamiento de datos personales con fines de investigación académica, periodísticos y artísticos.

(33) Por lo que se refiere a la investigación académica, la exención está limitada por varios elementos. En primer lugar, según el artículo 4, inciso II, de la LGPD, el tratamiento debe llevarse a cabo «exclusivamente» con fines de investigación académica. En segundo lugar, el artículo 4, inciso II, letra b), de la LGPD establece que los artículos 7 (requisito de base jurídica) y 11 (normas sobre el tratamiento de datos sensibles) se aplican a estos tipos de tratamiento ([48]). En tercer lugar, la ANPD ha elaborado una guía orientativa que especifica con mayor detalle las normas aplicables al tratamiento de datos con fines académicos y de investigación, para lo cual define estrictamente qué entidades pueden considerarse un «organismo de investigación», tal como se define en el artículo 5, inciso XVII, de la LGPD ([49]). En estas orientaciones, la ANPD confirma que el tratamiento de datos con fines de investigación académica solo está parcialmente exento de la LGPD y que se aplicarán los principios generales de la ley ([50]).

(34) En lo que respecta específicamente a los datos utilizados para la investigación sanitaria, la LGPD estipula limitaciones adicionales. Por una parte, el artículo 13 de la LGPD establece obligaciones de seguridad para las bases de datos utilizadas y fomenta el uso de técnicas de anonimización y seudonimización. Asimismo, dispone que las entidades de investigación serán consideradas responsables en caso de que no se apliquen medidas de seguridad para proteger los datos personales ([51]). Por otra parte, la transferencia de datos utilizados para la investigación sanitaria a terceras partes «está prohibida, bajo cualquier circunstancia» ([52]).

(35) Con respecto al tratamiento de datos personales con fines periodísticos y artísticos, la exención de la LGPD es similar a la prevista en el artículo 85, apartado 2, del Reglamento (UE) 2016/679. La exención contemplada en la LGPD incluye la situación en la que el tratamiento se realiza «exclusivamente» para estos fines ([53]). Por consiguiente, cuando la prensa, los medios de comunicación y las entidades artísticas traten datos personales para otros fines, tales como la gestión de recursos humanos o la administración interna, la LGPD es de aplicación en su totalidad.

([45]) Artículo 4, apartados 2 a 4, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([46]) Nota técnica n.º 175/2023 sobre el proyecto de Acuerdo de Cooperación entre el Ministerio de Justicia y Seguridad Pública y la Federación Brasileña de Fútbol para el intercambio de datos personales con vistas a mejorar el «Proyecto Estadio Seguro». Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

([47]) Nota técnica n.º 175/2023, apartado 5.1.

([48]) Artículo 4, inciso II, letra b), de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([49]) Guía de orientación de la ANPD sobre el tratamiento de datos personales con fines académicos y de realización de investigaciones, junio de 2023. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf.

([50]) Véanse, en particular, las páginas 18 a 43 de la Guía de orientación sobre el tratamiento de datos personales con fines académicos y de realización de investigaciones.

([51]) Artículo 13, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([52]) Artículo 13, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos). Véase también la «Guía de orientación sobre el tratamiento de datos personales con fines académicos y de realización de investigaciones» (disponible en portugués) de la ANPD, junio de 2023, p. 15.

([53]) Artículo 4, inciso II, letra a), de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

(36) La libertad de expresión artística y de los medios de comunicación forma parte de la libertad de expresión prevista en el artículo 5, inciso IX, de la Constitución, que garantiza la libertad de expresión para el discurso «intelectual, artístico, científico y de comunicación». En cuanto al ejercicio de ponderación entre la libertad de expresión y otros derechos (como los derechos a la intimidad y a la protección de datos), se rige por los criterios establecidos en la Constitución según la interpretación del Tribunal Supremo Federal. En particular, el ejercicio del derecho a la libertad de expresión no requiere autorización previa, pero sigue estando sujeto a los límites impuestos para la protección de otros derechos fundamentales. En concreto, una persona puede reclamar una indemnización en caso de daño o violación del derecho a la intimidad al amparo del artículo 5, inciso X, de la Constitución. Además, estas garantías se integraron en el Marco Civil para Internet, una ley adoptada en 2014 para proteger los derechos fundamentales en línea ([54]). En particular, el artículo 7, inciso I, del Marco Civil para Internet garantiza la «inviolabilidad de la intimidad» y establece el derecho a una indemnización por cualquier daño material o moral resultante de su contravención. Además, el Tribunal Supremo Federal menciona en su jurisprudencia la necesidad de «establecer un equilibrio entre los derechos, conciliando el derecho a la libertad de expresión con la inviolabilidad de la privacidad», destacando la importancia del derecho a la reparación y el acceso a vías de recurso en caso de violación de la privacidad ([55]). En otro asunto, el Tribunal Supremo Federal recordó que «las libertades de prensa y de comunicación social deben ejercerse en armonía con otros principios constitucionales», como la inviolabilidad de la intimidad y el derecho a la protección de datos ([56]).

(37) Por último, la LGPD exime del ámbito de aplicación de la ley el tratamiento de datos que tengan su origen fuera de Brasil y 1) no se compartan o comuniquen a los agentes de tratamiento en Brasil o, 2) procedan de un país considerado adecuado en virtud de la LGPD, siempre que no se transfieran a otro país ([57]). La ANPD ha proporcionado una interpretación vinculante para aclarar los dos escenarios de manera estricta en su Reglamento sobre la Transferencia de Datos ([58]).

(38) En el primer supuesto, el mero tránsito de datos personales a través de Brasil, sin que sean objeto de ningún tratamiento adicional en el país, quedaría excluido del ámbito de la ley ([59]). Sin embargo, la LGPD será de aplicación en el momento en que se acceda a los datos o estos se usen o traten de otro modo en Brasil. Las normas nacionales vigentes sobre ciberseguridad y sobre el acceso a los datos por parte de las autoridades públicas también seguirían aplicándose a este supuesto limitado, independientemente de que se produzca el tratamiento de los datos o estos se encuentren únicamente en tránsito.

(39) En el segundo supuesto, la ANPD ha aclarado que solo la transferencia retroactiva de datos transferidos originalmente desde un país que se beneficia de una decisión de adecuación en virtud de la LGPD queda excluida del ámbito de la ley, siempre que se aplique a dicho tratamiento la legislación nacional de este país adecuado. En este caso, también seguirían aplicándose las normas sobre ciberseguridad y acceso a los datos por parte de las autoridades públicas. En el contexto de la transferencia de datos personales entre la Unión y Brasil, cuando la Unión se beneficie de una decisión de adecuación de Brasil, la transferencia de datos de Brasil a la Unión no siempre entraría en el ámbito de aplicación del artículo 3 del Reglamento (UE) 2016/679. Por lo tanto, en los casos en que el tratamiento en cuestión se encontrase fuera del ámbito de aplicación del Reglamento (UE) 2016/679, del artículo 8, inciso II, letra b), del Reglamento sobre la Transferencia de Datos se desprende que la LGPD se aplicaría a la transferencia retroactiva de datos de Brasil a la Unión.

([54]) Ley n.º 12.965, de 23 de abril de 2014, Marco Civil da Internet («Marco Civil para Internet»). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([55]) Tribunal Supremo Federal, Decisión sobre la ADI 4815. Puede consultarse en el siguiente enlace: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057.

([56]) Tribunal Supremo Federal, Decisión sobre la ADI 5418. Puede consultarse en el siguiente enlace: https://www.jurisprudencia.stf.jus.br/pages/search/sjur446943/false.

([57]) Artículo 4, inciso IV, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([58]) Sección III, anexo I, del Reglamento sobre la transferencia internacional de datos personales («Reglamento sobre la Transferencia de Datos») de la ANPD. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([59]) Artículo 8, inciso I, del Reglamento sobre la transferencia internacional de datos personales de la ANPD.

2.4. **Garantías, derechos y obligaciones**

2.4.1. *Licitud y lealtad del tratamiento*

(40) Los datos personales deben tratarse de manera lícita y leal.

(41) Los principios de licitud, buena fe y transparencia y los fundamentos de la licitud del tratamiento están garantizados por los artículos 6 y 7 de la LGPD a través de condiciones similares a las de los artículos 5 y 6 del Reglamento (UE) 2016/679.

(42) De conformidad con los artículos 6 y 7 de la LGPD, los responsables y encargados del tratamiento tratarán la información personal de forma lícita y de buena fe en la medida mínima necesaria para la finalidad especificada, comprendiendo los datos que sean pertinentes, proporcionados y no excesivos en relación con la finalidad ([60]).

(43) Estos principios generales de tratamiento lícito se desarrollan en el artículo 7 de la LGPD, que establece las distintas bases jurídicas para el tratamiento, incluidas las circunstancias en las que esto pueda implicar un cambio de finalidad.

(44) De conformidad con el artículo 7 de la LGPD, el responsable y el encargado del tratamiento solo pueden tratar datos personales en base a un número limitado de fundamentos jurídicos. Estos fundamentos jurídicos previstos en la LGPD son los siguientes: 1) el consentimiento del interesado (inciso I); 2) la necesidad de ejecutar un contrato o llevar a cabo procedimientos preliminares relacionados con un contrato en el que el interesado sea parte, a petición del interesado (inciso V); 3) el cumplimiento de una obligación legal o reglamentaria por parte del responsable del tratamiento ([61]) (inciso II); 4) la protección de la vida o la seguridad física del interesado o de un tercero (inciso VII); 5) el tratamiento de datos por parte de una administración pública, necesario para la ejecución de las políticas públicas previstas en las leyes y reglamentos, o basado en contratos, acuerdos o instrumentos similares ([62]) (inciso III), y 6) cuando sea necesario para satisfacer los intereses legítimos del responsable del tratamiento o de un tercero, excepto en el caso de que prevalezcan los derechos y libertades fundamentales del interesado que requieran la protección de los datos personales (inciso IX).

(45) El artículo 7 de la LGPD establece cuatro bases jurídicas específicas adicionales para el tratamiento de datos, a saber: 1) la realización de estudios por parte de entidades de investigación, garantizando, siempre que sea posible, la anonimización de los datos personales (inciso IV); 2) el ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales ([63]) (inciso VI); 3) la protección de la salud, exclusivamente, en un procedimiento llevado a cabo por profesionales sanitarios, servicios sanitarios o autoridades sanitarias (inciso VIII); y 4) la cobertura del riesgo de crédito (inciso X) ([64]).

([60]) Véanse, en particular, el artículo 6, apartado principal, incisos III, I y V, y el artículo 7 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([61]) Toda obligación legal o reglamentaria se definirá por ley y será necesaria y proporcionada.

([62]) Se cumplirán las disposiciones específicas para el tratamiento de datos personales por parte de las autoridades públicas previstas en el capítulo IV de la Ley n.º 13.709, de 14 de agosto de 2018, (Ley General de Protección de Datos).

([63]) Los procedimientos se describen en la Ley n.º 9.307 de 23 de septiembre de 1996 (Ley de Arbitraje).

([64]) Por lo que se refiere a la cobertura del riesgo de crédito, la adición de estas bases jurídicas a la LGPD supone un mayor nivel de protección de los interesados, ya que, por ejemplo, garantiza que las entidades de crédito solo puedan tratar los datos personales necesarios para el análisis y la recuperación del crédito. Desde la adopción de la LGPD, los órganos jurisdiccionales de Brasil han promulgado varias decisiones para, por ejemplo, restringir el tratamiento de datos destinado a la cobertura del riesgo de crédito, excluyendo aquellos no considerados necesarios, como «el número de registro de votantes, el nombre de la madre, el estilo de vida, la clase social, la escolarización, la propensión marginal al consumo y la georeferenciación». Los órganos jurisdiccionales también han aclarado que un mayor acceso a los datos personales requeriría el consentimiento del interesado, limitando así el ámbito del tratamiento de datos a efectos de cobertura del riesgo de crédito. Véase Opice Blum Advogados, Informe Jurimetrics, 2022. Puede consultarse en el siguiente enlace: https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf.

2.4.2. *Criterios para el consentimiento*

(46) Los requisitos formales para obtener un consentimiento válido para el tratamiento de datos personales en virtud de la LGPD se establecen en el artículo 8, cuyo espíritu es similar al de los artículos 4, apartado 11, y 7 del Reglamento (UE) 2016/679. En primer lugar, el consentimiento debe darse por escrito o por otros medios que permitan demostrar la «manifestación de voluntad» del interesado ([65]). En sus directrices, la ANPD ha aclarado que «el consentimiento debe ser inequívoco, para lo que se requiere una manifestación de voluntad clara y positiva del interesado». Ello significa que no está permitido obtener el consentimiento «de manera tácita o por omisión del interesado» ([66]). En segundo lugar, el consentimiento se referirá a «fines particulares» y las «autorizaciones genéricas de tratamiento» de datos personales se considerarán nulas ([67]). En tercer lugar, el consentimiento se comunicará mediante información facilitada de manera «transparente, clara e inequívoca» ([68]). Cuando se incluya en un contrato más amplio, el consentimiento debe figurar en una cláusula diferenciada y específica que destaque claramente de las demás disposiciones contractuales ([69]). Además, el consentimiento se considerará nulo si la información facilitada al interesado contiene «contenido engañoso o abusivo» ([70]). El responsable del tratamiento también debe informar al interesado de cualquier cambio relativo a: 1) la finalidad específica del tratamiento; 2) el tipo o la duración del tratamiento; 3) la identidad del responsable del tratamiento; o 4) cualquier información relativa al tratamiento y posible intercambio de datos ([71]). En cuarto lugar, el consentimiento puede ser «revocado en cualquier momento» por el interesado mediante un «procedimiento gratuito» ([72]).

(47) La LGPD establece una prohibición estricta del tratamiento de datos personales cuando el consentimiento sea defectuoso o inválido ([73]). La LGPD aclara además que recae en el responsable del tratamiento la carga de la prueba de que el consentimiento se ha obtenido legalmente de conformidad con la LGPD ([74]).

(48) Por último, la LGPD establece que, en caso de que el consentimiento sea la base jurídica oportuna para el tratamiento, si los datos personales se han hecho «manifiestamente públicos por el interesado», se considerará que no se exige el consentimiento ([75]). El concepto de «datos manifiestamente públicos» también se encuentra recogido en el artículo 9 del Reglamento (UE) 2016/679. Sin embargo, incluso cuando se considere que se ha renunciado al consentimiento, los responsables y encargados del tratamiento no están exentos del cumplimiento de todos los demás derechos y obligaciones establecidos en la LGPD ([76]). En particular, los datos que el interesado haya hecho manifiestamente públicos podrán ser objeto de tratamiento ulterior siempre que se destinen a un fin «legítimo y específico» y se respeten los derechos de los interesados y los principios establecidos en la LGPD ([77]).

([65]) Artículo 8, parte introductoria, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([66]) ANPD, «Guía sobre cookies y protección de datos» (disponible en portugués), pp. 18-19. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.
([67]) Artículo 8, apartado 4, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos). Asimismo, cuando los datos personales deban compartirse entre responsables del tratamiento, se precisará un consentimiento específico e independiente para dicho intercambio, a menos que los datos se hayan hecho manifiestamente públicos, tal como se establece en el artículo 7, apartado 5, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([68]) Artículo 9, apartado 1, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([69]) Artículo 8, apartado 1, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([70]) Artículo 9, apartado 1, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([71]) Artículo 8, apartado 6, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([72]) Artículo 8, apartado 5, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([73]) Artículo 8, apartado 3, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([74]) Artículo 8, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([75]) Artículo 7, apartado 4, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos). El ámbito de aplicación de esta medida es limitado, ya que no abarca el tratamiento de datos sensibles autorizado en virtud del artículo 9, apartado 2, letra e), del Reglamento (UE) 2016/679.
([76]) Artículo 7, apartado 4, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([77]) Artículo 7, apartado 7, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

2.4.3. *Criterios de interés legítimo*

(49) El artículo 7, inciso IX, de la LGPD establece que el tratamiento de datos personales nunca podrá llevarse a cabo por motivos de interés legítimo cuando dicho tratamiento entre en conflicto con los derechos y libertades fundamentales de los interesados, destacando que prevalecerá la protección de los datos personales. Este enfoque es similar al seguido en la Unión, a tenor del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679.

(50) El artículo 10 de la LGPD establece las condiciones adicionales para que los responsables del tratamiento invoquen el «interés legítimo» como base jurídica para el tratamiento de datos personales. En primer lugar, cuando el tratamiento de datos personales se base en un interés legítimo, el responsable del tratamiento solo tratará los datos personales que sean «estrictamente necesarios» para la finalidad prevista ([78]). En segundo lugar, los responsables del tratamiento también deberán aplicar medidas para garantizar la transparencia de sus actividades de tratamiento ([79]). En tercer lugar, el interés legítimo solo podrá invocarse en «situaciones particulares» ([80]).

(51) Además, la ANPD ha publicado la «Guía sobre el interés legítimo», en la que se detallan las condiciones para la utilización del interés legítimo ([81]). Esta guía, por ejemplo, aclara que el interés legítimo no puede utilizarse como base jurídica para el tratamiento de datos sensibles ([82]) y también recoge en su anexo un modelo para la prueba de sopesamiento destinada a proteger los derechos y libertades fundamentales y que puede utilizar todo responsable del tratamiento que desee invocar un interés legítimo ([83]). Por otra parte, la ANPD puede exigir al responsable del tratamiento que lleve a cabo una evaluación de impacto relativa a la protección de datos ([84]).

(52) En esta guía, la ANPD aclara que, para que un interés se considere «legítimo», deben cumplirse tres condiciones: 1) compatibilidad con el ordenamiento jurídico de Brasil; 2) referencia a una situación específica; y 3) tratamiento vinculado a fines legítimos, específicos y explícitos ([85]). El primer requisito —compatibilidad con el ordenamiento jurídico— presupone que el interés legítimo invocado por el responsable del tratamiento debe ser compatible con los principios, normas jurídicas y derechos fundamentales garantizados en Brasil. Esto significa, por ejemplo, que el tratamiento previsto de datos personales no debe estar prohibido por la legislación de Brasil y no puede, directa o indirectamente, contravenir las disposiciones legales o los principios establecidos en la legislación de tal país. En segundo lugar, el interés legítimo invocado debe basarse en situaciones «concretas, claras y precisas», que tengan por objeto intereses específicos y bien definidos. El interés legítimo invocado no puede basarse en «situaciones abstractas o meramente especulativas» ([86]). La ANPD especifica además que los intereses que no estén relacionados con las «actividades actuales del responsable del tratamiento no se consideran legítimos» ([87]). El tercer requisito se refiere a la necesidad de demostrar una finalidad específica para el tratamiento. La ANPD señala que el interés legítimo del responsable del tratamiento (que justifica el tratamiento) no debe confundirse con la finalidad del

([78]) Artículo 10, apartado 1, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([79]) Artículo 10, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([80]) El artículo 10 de la LGPD ofrece algunos ejemplos de situaciones particulares en las que puede invocarse el interés legítimo: 1) apoyo y promoción de las actividades del responsable del tratamiento (inciso I); 2) protección del ejercicio de los derechos del interesado, o facilitación de la prestación de servicios que le beneficien, siempre que dicho tratamiento respete las expectativas legítimas, los derechos fundamentales y las libertades del interesado (inciso II). Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([81]) ANPD, «Bases jurídicas para el tratamiento de datos personales – Interés legítimo», febrero de 2024 («Guía sobre el interés legítimo»). Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf.
([82]) Guía de la ANPD sobre el interés legítimo, p. 8.
([83]) Guía de la ANPD sobre el interés legítimo, anexo 3.
([84]) Artículo 10, apartado 3, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([85]) Guía de la ANPD sobre el interés legítimo, p. 16-17.
([86]) Guía de la ANPD sobre el interés legítimo, p. 16, que interpreta el apartado principal del artículo 10 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([87]) Guía de la ANPD sobre el interés legítimo, p. 16.

tratamiento (el fin específico que se persigue al realizar el tratamiento). La existencia de un interés legítimo no exonera al responsable del tratamiento de la obligación de respetar el principio de limitación de la finalidad y todas las obligaciones derivadas de la LGPD. La finalidad debe describirse de manera clara y precisa, con la información necesaria para delimitar el alcance del tratamiento y permitir la ponderación de los intereses del responsable del tratamiento o de terceros con los derechos y expectativas legítimas de los interesados ([88]). Por consiguiente, cuando el responsable del tratamiento se base en un interés legítimo para respaldar o promover su actividad, deberá, entre otras cosas, definir claramente qué actividad pretende respaldar o apoyar y el vínculo con el tratamiento previsto.

2.4.4. *Tratamiento de categorías especiales de datos*

(53) Deben preverse salvaguardias específicas cuando se estén tratando «categorías especiales» de datos.

(54) El artículo 5, inciso II, de la LGPD define los datos personales sensibles como «datos personales relativos al origen étnico o racial, las convicciones religiosas, las opiniones políticas, la afiliación sindical, la organización religiosa, filosófica o política, la salud o la vida sexual, o datos de naturaleza genética o biométrica, cuando estén asociados a una persona física». Tal como se desprende de la jurisprudencia nacional, «vida sexual» debe interpretarse de manera que también comprenda la orientación o las preferencias sexuales de la persona. En particular, en su doctrina legal sobre el matrimonio entre personas del mismo sexo, el Tribunal Supremo Federal dictaminó que la discriminación por motivos de «sexo» abarca la «preferencia sexual» ([89]) y que la libertad de ejercer la «orientación sexual» es un «requisito previo para el desarrollo de la propia personalidad», que está protegido por la Constitución ([90]). Por lo tanto, las categorías de datos considerados sensibles con arreglo a la legislación brasileña son las mismas que en virtud del artículo 9, apartado 1, del Reglamento (UE) 2016/679.

(55) Los órganos jurisdiccionales de Brasil han ampliado aún más la definición de datos personales considerados sensibles en virtud de la LGPD para incluir otro tipo de información que podría utilizarse para discriminar a las personas ([91]). Esta interpretación se deriva del derecho a ser protegido contra la discriminación al amparo del Derecho brasileño, y se refleja asimismo en el artículo 6, inciso IX, de la LGPD. En particular, la doctrina legal de Brasil aclara que la información relativa a los registros de antecedentes penales se considerará datos sensibles ([92]).

(56) El tratamiento de datos sensibles en virtud de la LGPD solo se autoriza cuando el interesado o su representante legal hayan dado su consentimiento «específico y diferenciado» para fines específicos ([93]). Se aplicarán las condiciones para un consentimiento válido descritas en los considerandos 46 a 48 de la presente Decisión.

(57) De conformidad con el artículo 11, inciso II, de la LGPD, el tratamiento de datos sensibles puede llevarse a cabo sin el consentimiento explícito del interesado: 1) cuando dicho tratamiento sea necesario para el cumplimiento de una obligación legal o reglamentaria del responsable del tratamiento [letra a)]; 2) cuando sea necesario para el tratamiento por parte de la administración pública a los efectos de ejecutar políticas públicas previstas en leyes o reglamentos [letra b)]; 3) para proteger la vida o la seguridad física del interesado o de un tercero [letra e)]; 4) para el ejercicio de derechos, incluidos los contratos y los procedimientos judiciales administrativos y de arbitraje, de conformidad con la legislación de Brasil [letra d)]; 5) para proteger la salud de los interesados, exclusivamente en procedimientos llevados a cabo por profesionales sanitarios, servicios sanitarios o autoridades sanitarias [letra f)]; 6) para la realización de estudios por parte de entidades de investigación, con garantías de que los datos se anonimizan siempre que sea posible [letra c)]; y 7) para garantizar la prevención del fraude y la seguridad de los interesados, en los procesos de identificación y autenticación mediante el registro en sistemas electrónicos. Por lo tanto, los motivos para el tratamiento de datos sensibles con arreglo a la LGPD y el Reglamento (UE) 2016/679 son similares.

([88]) Guía de la ANPD sobre el interés legítimo, p. 17.

([89]) Véase la sentencia del Tribunal Supremo Federal de Brasil por la que se autoriza el matrimonio entre personas del mismo sexo, la cual se basa en la interpretación del artículo 3, sección IV, de la Constitución federal, que prohíbe toda discriminación por razón de sexo, raza y color. Tribunal Supremo Federal, Resolución sobre la ADI 4277 de 5 de mayo de 2011, puntos 2 y 6. Puede consultarse en el siguiente enlace: https://portal.stf.jus.br/peticaoInicial/verPeticaoInicial.asp?base=ADI&numProcesso=4277.

([90]) Véase la sentencia del Tribunal Supremo Federal de Brasil por la que se autoriza el matrimonio entre personas del mismo sexo, p. 14: «Como requisito ineludible para el desarrollo de la personalidad humana, el valor máximo protegido por la Constitución federal, es esencial eliminar cualquier obstáculo jurídico que constituya una limitación, incluso potencial, al pleno ejercicio de la libertad que todo ser humano tiene en el pleno ejercicio de su *orientación sexual*» *(cursiva de énfasis añadida)*.

([91]) Tribunal Superior de lo Laboral, Decisión TST-E-RR-933-49.2012.5.10.0001, de diciembre de 2021. Disponible en el siguiente enlace: https://www.jusbrasil.com.br/jurisprudencia/tst/713123452/inteiro-teor-713123472.

([92]) Tribunal Superior de lo Laboral, Decisión TST-E-RR-933-49.2012.5.10.0001, de diciembre de 2021.

([93]) Artículo 11, inciso I, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

2.4.5. *Limitación de los fines*

(58) Los datos personales deben recogerse para una finalidad específica y de manera que no sea incompatible con la finalidad del tratamiento.

(59) El artículo 6, inciso I), de la LGPD establece que los datos personales deben tratarse para una «finalidad legítima, específica y explícita de la que el interesado esté informado», sin posibilidad de tratamiento ulterior que sea «incompatible» con la finalidad original. Este principio, y su redacción, es casi idéntico al que recoge el artículo 5, apartado 1, letra c), del Reglamento (UE) 2016/679. Además, el artículo 6, inciso II, de la LGPD establece que toda actividad de tratamiento debe ser compatible con los fines comunicados al interesado.

(60) De las orientaciones publicadas por la ANPD se desprende que, para determinar si el tratamiento para otro fin es compatible con la finalidad para la que se recogieron inicialmente los datos, el responsable del tratamiento deberá demostrar la existencia de un vínculo entre los dos fines del tratamiento y tendrá en cuenta las «expectativas legítimas» de los interesados ([94]). Cuando el tratamiento obedezca a otros fines ulteriores compatibles, se aplicarán los principios y obligaciones recogidos en la LGPD, a saber, garantizar que la nueva finalidad sea específica y la protección de los derechos de los interesados. Esto también es aplicable al tratamiento ulterior de datos que el interesado haya puesto «manifiestamente a disposición» o que sean de dominio público ([95]).

2.4.6. *Exactitud y minimización de los datos*

(61) Los datos deben ser exactos y, si fuera necesario, estar actualizados. También deben ser adecuados, pertinentes y no excesivos en relación con los fines para los que se traten.

(62) Estos principios están garantizados por los principios de «calidad de los datos» y «necesidad» del artículo 6, incisos III y V, de la LGPD, respectivamente. De conformidad con el artículo 6, inciso V, de la LGPD, el responsable y los encargados del tratamiento velarán por que los datos personales sean exactos, claros, pertinentes y actualizados en lo que respecta a los fines de su tratamiento. El artículo 6, inciso III, de la LGPD establece la «limitación del tratamiento al mínimo necesario» para la consecución de una o varias finalidades específicas, «que abarque datos que sean pertinentes, proporcionales y no excesivos» en relación con dichas finalidades. Estos principios son similares a los establecidos en el artículo 5, apartado 1, letras c) y d), del Reglamento (UE) 2016/679.

2.4.7. *Limitación del almacenamiento*

(63) En principio, los datos no deben conservarse más tiempo del que sea necesario para las finalidades para las que se traten.

(64) Los principios de «finalidad», «necesidad» y «acceso» establecidos, respectivamente, en el artículo 6, incisos I, III y IV, de la LGPD prevén requisitos sobre la limitación del plazo de conservación. Limitan la posibilidad de conservar datos al mínimo necesario en relación con una finalidad «legítima, específica y explícita» y exigen que se informe a los interesados sobre la duración de la conservación.

([94]) Guía de la ANPD sobre el interés legítimo, p. 26 y anexo 2.

([95]) Artículo 7, apartado 7, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos). Véase también el considerando 48 de la presente Decisión. El concepto de datos «manifiestamente disponibles» también se encuentra en el Reglamento (UE) 2016/679, mientras que los datos «a disposición del público» se refieren a la información disponible en registros o bases de datos de carácter público con arreglo a la legislación brasileña en virtud de la Ley n.º 12.527, de 18 de noviembre de 2011 (Ley sobre el Acceso a la Información). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

(65) Además, el capítulo II, sección IV, de la LGPD se dedica a la «finalización del tratamiento de datos». En esta sección, el artículo 16 de la LGPD exige que todos los datos personales se supriman tras la finalización del tratamiento para un fin definido. Estos requisitos, leídos conjuntamente con los principios de «finalidad», «necesidad» y «acceso» de la LGPD son similares a las obligaciones derivadas del artículo 5, apartado 1, letra e), del Reglamento (UE) 2016/679.

(66) A tenor de las estrictas excepciones establecidas en el artículo 16 de la LGPD, los datos pueden conservarse y almacenarse más tiempo: 1) para el cumplimiento de obligaciones legales o reglamentarias; 2) con fines de investigación, garantizando, siempre que sea posible, la anonimización de los datos; 3) cuando se transfieran a terceros de conformidad con los requisitos de la LGPD; o 4) cuando sean utilizados exclusivamente por el responsable del tratamiento, siempre que los datos estén anonimizados y se prohíba el acceso a terceros.

(67) El requisito de seguridad de los datos estipulado en la LGPD y descrito en los considerandos 68 a 78 de la presente Decisión se aplica a los datos almacenados.

2.4.8. *Seguridad de los datos*

(68) Los datos personales deben ser tratados de tal manera que se garantice su seguridad, especialmente la protección contra su tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. A tal fin, los operadores económicos deben adoptar las medidas técnicas u organizativas apropiadas para proteger los datos personales frente a posibles amenazas. Estas medidas deben evaluarse teniendo en cuenta el estado de la técnica y los costes relacionados.

(69) Este principio está garantizado por el artículo 6, inciso VII, de la LGPD, que exige el uso de «medidas técnicas y administrativas» para proteger los datos personales frente a «accesos no autorizados y tratamientos accidentales o ilícitos», incluida la «destrucción, pérdida, alteración, comunicación o difusión de datos». Para reducir estos riesgos para la seguridad, el artículo 6, inciso VIII, de la LGPD exige la adopción de medidas para «evitar que se produzcan daños o perjuicios resultantes del tratamiento de datos personales».

(70) El artículo 44 de la LGPD establece que el tratamiento de datos personales es ilícito cuando no cumple las expectativas legítimas en cuanto a seguridad del interesado. Debe determinarse el nivel adecuado de seguridad, teniendo en cuenta, entre otros: 1) las circunstancias específicas que rodean el tratamiento efectuado; 2) el nivel razonable de riesgo esperado; y 3) las técnicas de tratamiento disponibles en el momento en que se efectuó dicho tratamiento ([96]).

(71) Para aplicar el principio de seguridad de los datos, la LGPD estableció una serie de requisitos en virtud del capítulo VII, sección I, sobre «Seguridad y confidencialidad de los datos». En esta sección de la LGPD, el artículo 46 obliga a los responsables y encargados del tratamiento a adoptar «medidas de seguridad, técnicas y administrativas capaces de proteger los datos personales frente a accesos no autorizados y tratamientos accidentales o ilícitos», como «destrucción, pérdida, alteración, comunicación o cualquier tipo de tratamiento indebido o ilícito». Estas medidas se cumplirán «desde la fase de concepción del producto o servicio hasta su ejecución» ([97]). El artículo 47 de la LGPD impone a todas las partes implicadas en cualquier fase del tratamiento la obligación general de cumplir los requisitos de seguridad. Estas obligaciones son similares a las que establece el artículo 32 del Reglamento (UE) 2016/679.

(72) El artículo 44 de la LGPD establece, además, que el responsable o encargado del tratamiento que no adopte medidas de seguridad será considerado responsable de los daños y perjuicios que se deriven de cualquier violación de la seguridad ([98]). La ANPD también podrá establecer normas técnicas mínimas de seguridad para garantizar el cumplimiento de las obligaciones en materia de seguridad de los datos ([99]).

([96]) Artículo 44, incisos I a III, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([97]) Artículo 46, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([98]) Artículo 44, párrafo independiente, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([99]) Artículo 46, apartado 1, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

(73) De conformidad con el artículo 48 de la LGPD, en caso de incidente de seguridad que pueda suponer un riesgo o causar un perjuicio significativo a los interesados, el responsable del tratamiento está obligado a notificarlo tanto a la ANPD como a los interesados. Dicha notificación deberá tener lugar en un plazo razonable, establecido por la ANPD, e incluir, como mínimo: 1) una descripción de la naturaleza de los datos personales afectados; 2) información que identifique a los interesados afectados; 3) una indicación de las medidas técnicas y de seguridad adoptadas para proteger los datos, sin perjuicio de la preservación de la confidencialidad comercial e industrial; 4) una evaluación de los riesgos asociados al incidente; 5) una explicación de cualquier retraso en la comunicación; y 6) una descripción de las medidas adoptadas o que vayan a adoptarse para mitigar o reparar los daños causados. El enfoque adoptado en la LGPD es en gran medida similar al establecido en los artículos 33 y 34 del Reglamento (UE) 2016/679.

(74) La ANPD ha adoptado normas adicionales sobre incidentes relativos a la seguridad de los datos para aclarar, por ejemplo, la definición de «incidente» y el calendario para la notificación de un incidente ([100]).

(75) El artículo 3, inciso XII, del Reglamento sobre Notificación de Incidentes de Seguridad define un incidente de seguridad como «cualquier acontecimiento adverso confirmado relacionado con la violación de la confidencialidad, integridad, disponibilidad y autenticidad de la seguridad de los datos personales». De conformidad con el artículo 48 de la LGPD, las violaciones de la seguridad de los datos y los incidentes de seguridad susceptibles de crear riesgos para los interesados deben comunicarse siempre a la autoridad de protección de datos (ANPD) y a los interesados. El artículo 5 del Reglamento sobre Notificación de Incidentes de Seguridad aclara que un incidente de seguridad puede suponer un riesgo para los interesados cuando pueda afectar a sus intereses y derechos fundamentales y cuando ataña al menos a uno de los siguientes tipos de datos: 1) datos personales sensibles; 2) datos de niños, adolescentes o personas mayores; 3) datos financieros; 4) datos de autenticación en sistemas; 5) datos protegidos por el secreto jurídico, judicial o profesional; o 6) bases de datos a gran escala. Además, se considerará que un incidente de seguridad afecta significativamente a los intereses y derechos fundamentales de los interesados cuando: 1) pueda impedir el ejercicio de derechos o el uso de un servicio; o 2) pueda causar daños materiales o morales a los interesados, como la discriminación, la violación de la integridad física, el derecho a la imagen y la reputación, el fraude financiero o la usurpación de identidad ([101]).

(76) La notificación de un incidente de seguridad a la ANPD y a los interesados tendrá lugar en un plazo de tres días hábiles a partir del momento en que el responsable del tratamiento tenga conocimiento de este ([102]). El Reglamento sobre Notificación de Incidentes de Seguridad, de carácter vinculante, aclara a los responsables del tratamiento la información que debe facilitarse a la ANPD y a los interesados. La notificación a los interesados incluirá, en particular: 1) una descripción de la naturaleza y categoría de los datos personales afectados; 2) las medidas técnicas y de seguridad utilizadas para proteger los datos; 3) los riesgos relacionados con el incidente, identificando las posibles repercusiones en los interesados; 4) los motivos del retraso, en caso de que la comunicación no se haya efectuado en el plazo de setenta y dos horas; 5) las medidas que se adoptaron o se adoptarán para invertir o mitigar los efectos del incidente, cuando proceda; 6) la fecha en que se descubrió el incidente de seguridad; y 7) los datos de contacto para obtener información y, en su caso, los datos de contacto de la persona responsable ([103]). Al comunicar el incidente a los interesados, los responsables del tratamiento utilizarán un «lenguaje sencillo y fácil de entender» ([104]). Si es posible identificar a los interesados afectados, la notificación se efectuará directa e individualmente ([105]).

(77) Además, cuando sea necesario para salvaguardar los derechos de los interesados, la ANPD podrá evaluar la gravedad del incidente y ordenar al responsable del tratamiento que adopte medidas específicas ([106]). Estas medidas pueden incluir la divulgación pública del incidente a través de los canales de comunicación adecuados, así como la aplicación de medidas correctoras o paliativas. El responsable del tratamiento llevará un registro de los incidentes de seguridad de los datos ([107]).

([100]) ANPD, Reglamento sobre Notificación de Incidentes de Seguridad, abril de 2024. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.
([101]) Artículo 5, apartado 1, del Reglamento sobre notificación de incidentes de seguridad de la ANPD, abril de 2024.
([102]) Artículos 6 y 9 del Reglamento sobre Notificación de Incidentes de Seguridad de la ANPD, abril de 2024.
([103]) Artículo 9, incisos I al VII, del Reglamento sobre Notificación de Incidentes de Seguridad de la ANPD, abril de 2024.
([104]) Artículo 9, apartado 1, inciso I, del Reglamento sobre Notificación de Incidentes de Seguridad de la ANPD, abril de 2024.
([105]) Artículo 9, apartado 1, inciso II, del Reglamento sobre Notificación de Incidentes de Seguridad de la ANPD, abril de 2024.
([106]) Artículo 48, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([107]) Artículo 10 del Reglamento sobre Notificación de Incidentes de Seguridad de la ANPD, abril de 2024.

(78) Por último, la LGPD vincula sus normas de «buenas prácticas y gobernanza (de datos)» con los requisitos en materia de seguridad de datos para, entre otras cuestiones, mitigar los riesgos relacionados con el tratamiento de datos ([108]). A tales efectos, promueve la adopción de programas internos de gobernanza de la privacidad para evaluar y mitigar los riesgos ([109]).

2.4.9. *Transparencia*

(79) Los interesados deben ser informados de las principales características del tratamiento de sus datos personales.

(80) Siguiendo un enfoque similar al del artículo 12 del Reglamento (UE) 2016/679, el artículo 6, inciso VI, de la LGPD establece que los interesados deben recibir información clara, precisa y fácilmente accesible tanto sobre el tratamiento de sus datos como sobre los agentes que efectúan dicho tratamiento, en observancia del «secreto comercial e industrial».

(81) El artículo 9 de la LGPD establece una lista de la información que se debe facilitar a los interesados en relación con el tratamiento de los datos, que comprende: 1) la finalidad específica del tratamiento; 2) el tipo y duración del tratamiento; 3) la identificación del responsable del tratamiento; 4) la información de contacto del responsable del tratamiento; 5) información sobre el tratamiento de los datos por parte del responsable del tratamiento y la finalidad; 6) las responsabilidades de las entidades que llevan a cabo el tratamiento y 7) los derechos de los interesados, incluida la información relativa al ejercicio de estos derechos.

(82) La limitación relacionada con el «secreto comercial e industrial» a que se refiere el artículo 6, inciso VI, y otras disposiciones de la LGPD debe interpretarse a la luz de la Ley sobre el Acceso a la Información de Brasil ([110]). La Ley sobre el Acceso a la Información establece, como norma general, la divulgación de la información contenida en los registros o documentos que obren en poder de organismos públicos ([111]). Cualquier excepción, esto es, la imposición de restricciones al acceso a documentos e información, debe estar justificada y prevista por ley ([112]). El secreto comercial e industrial es una de estas excepciones y está contemplado por una disposición legal específica que garantiza la protección de «la información relativa a las actividades empresariales de personas físicas o jurídicas de Derecho privado obtenida por otros organismos o entidades en el ejercicio de la actividad de control, regulación y supervisión de la actividad económica, cuya divulgación podría representar una ventaja competitiva para otros agentes económicos» ([113]). Por lo tanto, las disposiciones de la LGPD relativas al «secreto comercial e industrial» se interpretarán de manera que el tratamiento y la divulgación de otro modo de información no revelen ningún secreto comercial ni creen una ventaja competitiva para otros agentes, al tiempo que cumplen los objetivos de protección de los datos personales. Esto significa que, con respecto al principio de transparencia, y en todo el texto de la LGPD, la limitación del «secreto comercial e industrial» no se debe entender como un motivo general de denegación del cumplimiento de la ley, sino que se deben establecer salvaguardias específicas para garantizar la divulgación de la información de manera que se protejan estos intereses.

2.4.10. *Derechos individuales*

(83) Los interesados deben tener ciertos derechos que puedan hacer valer ante el responsable del tratamiento, en concreto los derechos de acceso a los datos, rectificación, supresión de datos, oposición al tratamiento y portabilidad, así como los derechos relacionados con el tratamiento automatizado de datos. Estos derechos pueden estar sujetos a limitaciones, en tanto en cuanto dichas limitaciones sean necesarias y proporcionadas para salvaguardar objetivos importantes de interés público general.

([108]) Artículos 49 y 50 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([109]) Artículo 50, parte introductoria y apartado 1, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([110]) Ley n.º 12.527, de 18 de noviembre de 2011 (Ley sobre el Acceso a la Información). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.
([111]) Artículos 6 y 9 de la Ley n.º 12.527, de 18 de noviembre de 2011 (Ley sobre el Acceso a la Información).
([112]) Artículo 22 de la Ley n.º 12.527, de 18 de noviembre de 2011 (Ley sobre el Acceso a la Información).
([113]) Artículo 5, apartado 2, del Decreto n.º 7.721, de 16 de mayo de 2012, relativo a la Ley n.º 12.527, de 18 de noviembre de 2011 (Ley sobre el Acceso a la Información).

(84) El capítulo III de la LGPD establece los derechos de los interesados de forma similar a los artículos 15 a 22 del Reglamento (UE) 2016/679. El ejercicio de todos los derechos es gratuito y los interesados deben ser informados de sus derechos ([114]). De conformidad con el artículo 21 de la LGPD, los datos relativos al ejercicio de derechos por parte de los interesados no pueden utilizarse en su perjuicio. Los interesados podrán recurrir ante los órganos jurisdiccionales, individual o colectivamente, en relación con sus intereses y derechos ([115]).

(85) Los responsables del tratamiento informarán «inmediatamente» a los encargados del tratamiento con los que puedan haberse compartido los datos de las solicitudes de rectificación, supresión, anonimización, limitación y oposición por parte de los interesados, a fin de garantizar que todas las partes implicadas puedan atender dichas solicitudes ([116]).

(86) De conformidad con el artículo 9 y el artículo 18, inciso II, de la LGPD, los interesados tienen derecho a la información y al acceso para obtener «en cualquier momento» información relativa al tratamiento de sus datos ([117]). Ello incluye: 1) la identidad del responsable del tratamiento (inciso III); 2) la información de contacto del responsable del tratamiento (inciso IV); 3) información sobre la finalidad específica del tratamiento (inciso I); 4) información sobre el posible intercambio de datos (inciso V); 5) el tipo y la duración del tratamiento (inciso II); 6) la existencia de derechos de los interesados, incluido el derecho a presentar una reclamación ante la autoridad de protección de datos; y 7) las responsabilidades de los encargados del tratamiento de datos. Asimismo, el artículo 10, apartado 2, de la LGPD exige que el responsable del tratamiento sea transparente en relación con el tratamiento basado en un interés legítimo. Del mismo modo, el artículo 9 del Reglamento relativo a las transferencias de datos especifica que se informará a los interesados en caso de transferencia de datos personales.

(87) El artículo 19 de la LGPD detalla el modo en que se debe facilitar a los interesados el acceso a su información personal. A petición del interesado, se facilitará el acceso a los datos personales: inmediatamente, «en un formato simplificado»; o en un plazo de quince días, mediante una declaración clara y completa ([118]). Además, el artículo 19, apartado 1, de la LGPD establece que los responsables del tratamiento almacenarán los datos personales en un formato que facilite el ejercicio del derecho de acceso. El interesado podrá decidir recibir su información en formato electrónico o en papel ([119]).

(88) Los interesados tienen derecho a solicitar la corrección de datos incompletos, inexactos u obsoletos, de conformidad con el artículo 18, inciso III, de la LGPD (derecho de rectificación).

(89) El artículo 18, incisos IV y VI, de la LGPD otorga a las personas el derecho a solicitar la supresión de sus datos cuando: 1) se trate de datos innecesarios o excesivos; 2) el tratamiento de cualquier dato se realice con el consentimiento del interesado; o 3) los datos sean objeto de un tratamiento ilícito. Además, la sección IV, capítulo II, de la LGPD sobre la «finalización del tratamiento de datos» indica que el tratamiento de datos debe cesar cuando un interesado se oponga al tratamiento o retire su consentimiento para el tratamiento ([120]). Posteriormente, los datos se suprimirán una vez finalizado el tratamiento ([121]). Así pues, estas disposiciones, entendidas conjuntamente, amplían indirectamente el alcance del derecho de supresión en virtud de la LGPD.

([114]) Artículo 18 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([115]) Artículo 22 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([116]) Artículo 18, apartado 6, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([117]) Artículo 6, inciso VI, artículo 18 y artículo 19 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([118]) Artículo 19, incisos I y II, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([119]) Artículo 19, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([120]) Véase el artículo 15, inciso III, de la Ley n.º 13.709, de 14 de agosto de 2018, (Ley General de Protección de Datos), donde la «comunicación por parte del interesado» se refiere, entre otras cosas, a la revocación del consentimiento (como se indica en el artículo). El significado de «comunicación» no se limita a este supuesto, y permite a los interesados solicitar que se detenga una actividad de tratamiento.
([121]) Artículo 16 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

(90) Las personas tienen derecho a oponerse al tratamiento de datos amparándose en una base jurídica distinta del consentimiento, en caso de incumplimiento de la LGPD (derecho de oposición) ([122]). Además, de conformidad con el artículo 15 y el artículo 18, inciso IV, de la LGPD, los interesados tienen derecho a restringir el tratamiento de datos («bloqueo»). Este derecho puede invocarse, en particular, cuando los datos objeto de tratamiento sean innecesarios o excesivos, o cuando se lleve a cabo su tratamiento de manera que vulnere la LGPD ([123]). El artículo 15, inciso II, de la LGPD estipula que los datos ya no se tratarán sobre la base de una «comunicación» del interesado al responsable del tratamiento. Aunque esta disposición está sujeta al «interés público», interpretado en sentido amplio, establece un amplio ámbito de aplicación para un derecho de oposición indirecto equivalente al previsto en el Reglamento (UE) 2016/679.

(91) Las personas tienen derecho a solicitar «una copia electrónica completa» de sus datos para que puedan utilizarla otras entidades (derecho a la portabilidad) ([124]). Del mismo modo, al igual que en la Unión, los interesados solo pueden solicitar esta copia cuando los datos hayan sido tratados sobre la base del consentimiento o de un contrato.

(92) Aunque cualquier decisión basada en el tratamiento automatizado de los datos recogidos en la Unión suele tomarla un responsable del tratamiento [que tiene una relación directa con el interesado de que se trate y, por tanto, entra directamente en el ámbito de aplicación del Reglamento (UE) 2016/679], cabe destacar que la LGPD regula este tipo de tratamiento de manera similar al artículo 22 del Reglamento (UE) 2016/679. En primer lugar, el artículo 6, inciso IX, de la LGPD reconoce el principio de no discriminación como un principio de protección de datos que prohíbe el tratamiento de datos con fines discriminatorios ilícitos o abusivos. Este principio es aplicable a toda actividad de tratamiento y es especialmente pertinente en el contexto del tratamiento automatizado. Además, de conformidad con el artículo 20 de la LGPD, los interesados tienen derecho a solicitar «la revisión de las decisiones adoptadas únicamente sobre la base del tratamiento automatizado de datos que afecten a sus intereses, incluidas las decisiones destinadas a definir su perfil personal, profesional, de consumidor y de crédito, o aspectos de su personalidad». Al responder a una solicitud de un interesado, el responsable del tratamiento deberá facilitar información clara sobre «los criterios y el procedimiento utilizados para la decisión automatizada» ([125]). En caso de que dicha información no pueda facilitarse al interesado por motivos de «secreto comercial e industrial», la ANPD tiene la facultad de llevar a cabo una auditoría para verificar aspectos discriminatorios en el tratamiento automatizado de datos personales ([126]). En consecuencia, el «secreto comercial e industrial» no puede esgrimirse como motivo para negarse a atender la solicitud del interesado.

(93) El artículo 23 de la LGPD establece que se aplicarán legislaciones específicas al procedimiento y al plazo para el ejercicio de los derechos de los interesados cuando sean tratados por las autoridades públicas ([127]). Por ejemplo, la Ley *Habeas Data* de Brasil regula el derecho de acceso de las personas a la información relativa a datos conservados en registros o bases de datos del Gobierno o de una entidad pública ([128]). Esta ley establece disposiciones específicas para el derecho de acceso, que se concederá en un plazo de diez días a partir de la solicitud de una persona, y para el derecho de rectificación, que se concederá en un plazo de quince días a partir de la solicitud ([129]). Del mismo modo, la Ley Federal de Procedimiento Administrativo de Brasil establece el derecho a la información y al acceso de las personas en el contexto de los procedimientos administrativos ([130]). La Ley sobre el Acceso a la Información de

([122]) Artículo 18, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([123]) Artículo 18, inciso IV, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([124]) Artículo 19, apartado 3, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([125]) Artículo 20, apartado 1, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([126]) Artículo 20, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([127]) Artículo 23, apartado 3, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([128]) Ley n.º 9.507, de 12 de noviembre de 1997 (Ley *Habeas Data* de Brasil). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm.
([129]) Artículos 7 y 8 de la Ley n.º 9.507, de 12 de noviembre de 1997 (Ley *Habeas Data* de Brasil). La ley prevé vías de reparación en caso de incumplimiento de la solicitud de una persona.
([130]) Véase, en particular, el artículo 6 de la Ley n.º 9.784, de 29 de enero de 1999 (Ley Federal de Procedimiento Administrativo). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm La ley establece procedimientos y plazos para las comunicaciones con las personas, así como vías de reparación en caso de incumplimiento.

Brasil también establece obligaciones de información y transparencia para las autoridades públicas, las empresas públicas y los tres poderes del gobierno (legislativo, ejecutivo y judicial) en Brasil ([131]). Las disposiciones de estas leyes refuerzan el derecho de acceso y a la información establecido en virtud de la LGPD para el tratamiento de datos por parte de las autoridades públicas. Cuando estas leyes no prevean derechos específicos establecidos en virtud de la LGPD (como los relacionados con la toma de decisiones automatizada), los interesados podrán ejercerlos amparándose en la LGPD.

(94) Toda violación de los derechos de los interesados será tratada por la ANPD como una infracción de la ley de importancia «moderada» o «grave», dependiendo del factor pertinente y, por tanto, podrá ser objeto del máximo nivel de sanciones y multas. Es importante señalar que, en virtud del Reglamento sobre sanciones de la ANPD, el mero hecho de que un derecho del interesado se haya visto afectado por una violación implica que dicha infracción no puede considerarse «leve» ([132]).

(95) Desde el inicio de la aplicación de la LGPD, la ANPD ha recibido un número constante de reclamaciones y peticiones de personas en relación con sus derechos de protección de datos ([133]). Estas cifras han aumentado significativamente desde julio de 2024, cuando la ANPD introdujo una plataforma modernizada y fácil de utilizar para la presentación de solicitudes y reclamaciones ([134]). Desde entonces, la ANPD recibe cada mes alrededor de cuatrocientas reclamaciones y un centenar de solicitudes de personas ([135]).

2.4.11. *Transferencias ulteriores*

(96) El nivel de protección de los datos personales que se transfieren desde la Unión a responsables y encargados del tratamiento en Brasil no debe verse comprometido por la transferencia ulterior de dichos datos a destinatarios que se encuentren en un tercer país.

(97) Estas «transferencias ulteriores» constituyen transferencias internacionales desde Brasil, desde la perspectiva del responsable del tratamiento brasileño.

(98) El capítulo V de la LGPD establece un marco para las transferencias internacionales de datos personales. Las disposiciones de este capítulo se complementan con un reglamento vinculante sobre las transferencias internacionales de datos (Reglamento sobre la Transferencia de Datos), que fue adoptado por la ANPD en agosto de 2024 ([136]).

(99) El Reglamento sobre la Transferencia de Datos define una «transferencia» como una «operación de tratamiento a través de la cual un agente de tratamiento transmite, comparte o facilita acceso a datos personales a otro agente de tratamiento» y una «transferencia internacional de datos» como una «transferencia de datos personales a un país extranjero o a una organización internacional de la que el país es miembro» ([137]).

([131]) Artículos 1, 6 y 9 de la Ley n.º 12.527, de 18 de noviembre de 2011 (Ley sobre el Acceso a la Información).

([132]) Artículo 8, apartado 2, de la ANPD, Reglamento sobre el cálculo y la aplicación de sanciones administrativas, febrero de 2023 («Reglamento sobre Sanciones»). Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077.

([133]) ANPD, «Informe sobre el cuarto año de la ANPD», noviembre de 2023, pp. 24-25 (disponible en portugués). Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([134]) ANPD, plataforma para ciudadanos. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados.

([135]) ANPD, «Informe sobre el cuarto año de la ANPD», noviembre de 2023, p. 25 (disponible en portugués).

([136]) ANPD, Reglamento sobre Transferencias Internacionales de Datos, agosto de 2024. Disponible en portugués en: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396 y en inglés en: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([137]) Artículo 3, incisos III y IV, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024, y artículo 5, inciso XV, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

(100) Las normas sobre transferencias internacionales establecidas en virtud de la LGPD y del Reglamento sobre la Transferencia de Datos se aplican a todos los tratamientos incluidos en el ámbito de aplicación de la LGPD. El artículo 7 del Reglamento sobre la Transferencia de Datos aclara expresamente que la aplicabilidad de la LGPD a una transferencia internacional de datos no depende de los medios técnicos utilizados para el tratamiento, la ubicación geográfica de los datos o la presencia física del responsable o del encargado del tratamiento ([138]). Lo que determina la aplicabilidad es la existencia de un vínculo material entre la actividad de tratamiento de datos y Brasil.

(101) Al igual que los artículos 44 a 49 del Reglamento (UE) 2016/679, el artículo 33 de la LGPD establece las circunstancias en las que «únicamente» puede permitirse una transferencia internacional de datos puede permitirse. Estas circunstancias se detallan en el artículo 9 del Reglamento sobre Transferencia de Datos.

(102) Una transferencia internacional de datos puede tener lugar si se cumplen, de forma acumulativa, las tres circunstancias siguientes: en primer lugar, una transferencia internacional de datos «únicamente puede llevarse a cabo con fines legítimos, específicos y explícitos comunicados al interesado, sin que exista la posibilidad de efectuar un tratamiento ulterior incompatible con dicha finalidad» ([139]). En segundo lugar, la transferencia internacional de datos debe basarse en una base jurídica válida establecida en el artículo 7 de la LGPD (o en su artículo 11 en el caso de los datos sensibles) ([140]). En tercer lugar, debe utilizarse un mecanismo de transferencia de datos «válido» ([141]).

(103) El artículo 33 de la LGPD prevé varios mecanismos de transferencia de datos.

(104) En primer lugar, puede adoptarse una decisión de adecuación con respecto a un tercer país o una organización internacional (artículo 33, inciso I). Para determinar si un tercer país o una organización internacional garantiza un nivel adecuado de protección de los datos personales, la ANPD tendrá en cuenta varios criterios establecidos en la LGPD y en el Reglamento sobre la Transferencia de Datos ([142]), similares a los consagrados en el Derecho de la Unión. Entre dichos criterios cabe citar los siguientes: 1) la legislación general y sectorial vigente en el país de destino o aplicable a la organización internacional, que tenga un impacto directo en la protección de los datos personales ([143]); 2) la naturaleza de los datos ([144]); 3) la garantía de que el tercer país o la organización internacional proporciona un nivel de protección de los datos personales y garantiza los derechos de los interesados en consonancia con la LGPD ([145]); 4) la adopción de medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos y mitigar los riesgos de efectos adversos para la privacidad y otros derechos fundamentales ([146]); 5) la existencia de mecanismos judiciales e institucionales para garantizar los derechos de protección de datos, en particular mediante la existencia de una autoridad de control independiente con competencias y recursos adecuados para supervisar y hacer cumplir las disposiciones en materia de protección de datos ([147]); y 6) cualquier otra circunstancia específica pertinente en el contexto de la transferencia internacional de datos ([148]).

([138]) Artículo 7 del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024.
([139]) Artículo 9 del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024.
([140]) Artículo 9, inciso I, del Reglamento sobre Transferencias Internacionales de Datos, de agosto de 2024, de la ANPD.
([141]) Artículo 9, inciso II, del Reglamento sobre Transferencias Internacionales de Datos, de agosto de 2024, de la ANPD.
([142]) Artículo 34 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos) y capítulo V del Reglamento sobre Transferencias Internacionales de Datos, de agosto de 2024, de la ANPD.
([143]) Artículo 34, inciso I, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos) y artículo 11, inciso I, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.
([144]) Artículo 34, inciso II, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos), y artículo 11, inciso II, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.
([145]) Artículo 34, inciso III, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos), y artículo 11, inciso III, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.
([146]) Artículo 34, inciso IV, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos), y artículo 11, inciso IV, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.
([147]) Artículo 11, apartado 3, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.
([148]) Artículo 34, inciso VI, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos), y artículo 11, inciso VI, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.

(105) Para evaluar el nivel de protección de los datos personales en el contexto de una decisión de adecuación, la ANPD también valorará: 1) los riesgos y beneficios proporcionados por una decisión de adecuación específica, teniendo en cuenta, entre otros aspectos, la garantía de los principios, los derechos del interesado y el régimen de protección de datos previsto en la LGPD; así como 2) las repercusiones de la decisión en el flujo internacional de datos, las relaciones diplomáticas, el comercio internacional y la cooperación internacional de Brasil con otros países y organizaciones internacionales ([149]). La evaluación y la emisión de una decisión de adecuación son responsabilidad de la ANPD ([150]). En la actualidad, la ANPD solo está trabajando en una decisión de adecuación con la Unión Europea.

(106) En segundo lugar, el artículo 33, inciso II, establece que las transferencias de datos pueden realizarse cuando los responsables del tratamiento aseguren que se dan «las garantías de cumplimiento de los principios y derechos de los interesados y del régimen de protección de datos» previstos por la LGPD. Para ello pueden recurrir a 1) cláusulas contractuales específicas [inciso II, letra a)]; 2) cláusulas contractuales tipo [apartado II, letra b)]; 3) normas corporativas vinculantes [apartado II, letra c)]; o 4) sellos, certificados y códigos de conducta aprobados [apartado II, letra d)].

(107) Los responsables del tratamiento pueden basarse en disposiciones contractuales específicas para las transferencias internacionales, así como en cláusulas contractuales tipo aprobadas por la ANPD ([151]). En virtud del Reglamento sobre la Transferencia de Datos, la ANPD ha adoptado un conjunto de cláusulas contractuales tipo que comprenden todos los requisitos pertinentes en materia de protección de datos (esto es, los derechos de los interesados, la supervisión y control independientes, las medidas de seguridad de los datos, las garantías aplicables a las transferencias ulteriores, etc.) ([152]). Estas cláusulas incluyen disposiciones que no pueden ser modificadas por las partes contratantes ([153]). Las cláusulas son de carácter modular, de manera que pueden adaptarse a diferentes supuestos de transferencia de datos (como, por ejemplo, transferencias del responsable del tratamiento al encargado del tratamiento, o entre encargados del tratamiento) ([154]).

(108) En cuanto a las normas corporativas vinculantes, la ANPD aclara en el capítulo VI del Reglamento sobre la Transferencia de Datos cómo puede utilizarse este mecanismo, así como los requisitos para su validez. La ANPD recuerda, en particular, el «carácter vinculante» del instrumento para todos los «miembros del grupo o conglomerado» que lo utilicen, los requisitos relativos a los derechos de los interesados y su ejercicio, las normas aplicables en materia de responsabilidad ([155]), así como toda la información obligatoria que deben incluir las normas corporativas vinculantes ([156]). Las normas corporativas vinculantes están sujetas a la aprobación previa de la ANPD con arreglo a un proceso definido en el capítulo VIII del Reglamento sobre la Transferencia de Datos, que obliga a las empresas a presentar documentación completa a la ANPD y dispone que la ANPD lleve a cabo un proceso de revisión ([157]). Las empresas también están obligadas a comunicar a la ANPD cualquier cuestión que pueda afectar al cumplimiento de la LGPD, también cuando los miembros del grupo estén sujetos a obligaciones internacionales ([158]). Todas las normas corporativas vinculantes aprobadas se publicarán en la página web de la ANPD, y las empresas tienen la obligación de informar de forma transparente sobre las transferencias internacionales realizadas ([159]).

([149]) Artículo 12 del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024.

([150]) El procedimiento para la adopción de una decisión de adecuación se describe en la sección III del Reglamento sobre Transferencias Internacionales de Datos, de agosto de 2024.

([151]) Artículo 35 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([152]) Anexo II del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.

([153]) Anexo II, sección II, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.

([154]) Anexo II, cláusula 4, del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024. Los responsables y encargados del tratamiento pueden elegir la «opción» adecuada que corresponda a sus circunstancias con arreglo a esta cláusula.

([155]) Artículo 3, inciso VIII, del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024. La definición de «entidad responsable» establece que «una empresa comercial con sede en Brasil es responsable de cualquier incumplimiento de una norma corporativa vinculante, incluso si este se deriva del acto de un miembro del grupo económico con sede en otro país», siguiendo un enfoque similar al del artículo 47, apartado 1, letra f), del Reglamento (UE) 2016/679.

([156]) Artículo 27 del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024.

([157]) Artículos 27 y 28 y capítulo VIII del Reglamento de la ANPD sobre Transferencias Internacionales de Datos, agosto de 2024.

([158]) Artículo 25, inciso VIII, del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024.

([159]) Artículo 32 del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024. Este artículo indica, además, que las empresas tienen la obligación de poner las normas corporativas vinculantes a disposición de los interesados que lo soliciten.

(109) La ANPD también puede designar entidades de certificación para desarrollar sellos, certificados o códigos de conducta para las transferencias de datos ([160]). La ANPD puede revisar las decisiones y actividades llevadas a cabo por las entidades de estas certificaciones, así como revisar y revocar dichas decisiones en caso de incumplimiento de la LGPD ([161]).

(110) Por último, la LGPD proporciona una lista de «situaciones específicas» en las que se puede llevar a cabo una transferencia internacional cuando: 1) sea necesario para la cooperación jurídica internacional entre organismos públicos, de conformidad con el Derecho internacional; 2) sea necesario para proteger la vida o la seguridad física del interesado o de un tercero; 3) lo autorice la ANPD; 4) guarde relación con un compromiso en el marco de la cooperación internacional; 5) sea necesario para el cumplimiento de una política pública o una obligación jurídica de una autoridad pública; 6) los interesados hayan prestado su consentimiento para una transferencia de datos específica tras haber sido previamente informados sobre la naturaleza del tratamiento; o 7) cuando sea necesario para el cumplimiento de una obligación legal o reglamentaria, en relación con la disposición de un contrato, o para el ejercicio de derechos en procedimientos judiciales, administrativos o de arbitraje ([162]). Como se indica en el Reglamento sobre Transferencia de Datos, las transferencias internacionales solo pueden llevarse a cabo en estos escenarios si «se cumplen las especificidades del caso concreto y los requisitos legales aplicables» ([163]).

(111) En cuanto a la situación específica en la que la transferencia de datos puede llevarse a cabo sobre la base del consentimiento de los interesados, se requiere que 1) se cumplan los criterios formales para obtener un consentimiento válido (es decir, que sea específico, libre, explícito e informado); 2) se informe a los interesados de la naturaleza de la transferencia *antes* de que se lleve a cabo (por ejemplo, información sobre la jurisdicción de la transferencia prevista y el nivel de protección que garantiza; información sobre la ausencia de una decisión de adecuación o de otros mecanismos de transferencia de datos; información sobre la duración de las transferencias); y 3) debe obtenerse el consentimiento para cada transferencia de forma específica y separada de cualquier otro tratamiento. Como se indica en el considerando 46, el acuerdo tácito no se puede considerar un consentimiento válido y los interesados tienen derecho a retirar el consentimiento en cualquier momento.

(112) El Reglamento sobre Transferencia de Datos regula estrictamente el recurso a todos estos mecanismos con arreglo a varias condiciones. Esto incluye, en particular, proporcionar «información clara, precisa y fácilmente accesible sobre la transferencia» al interesado, así como garantizar y poder demostrar que las transferencias internacionales se llevan a cabo de manera que se cumplan los principios y los derechos del interesado, sin menoscabo del nivel de protección que brinda la LGPD, «independientemente del país en el que se encuentren los datos personales objeto de la transferencia, incluso después de finalizar el tratamiento y en los casos de transferencias ulteriores» ([164]). Estos requisitos también se aplican cuando se realizan transferencias sobre la base de «situaciones específicas», a fin de garantizar la continuidad de la protección con independencia del instrumento utilizado para llevar a cabo una transferencia internacional.

(113) Las normas descritas en los considerandos 96 a 112 de la presente Decisión garantizan, por tanto, la continuidad de la protección cuando los datos personales se transfieren ulteriormente desde Brasil de una manera esencialmente equivalente a la prevista en el Reglamento (UE) 2016/679.

2.4.12. *Rendición de cuentas*

(114) En virtud del principio de responsabilidad, las entidades que traten datos están obligadas a adoptar las medidas técnicas y organizativas apropiadas para cumplir efectivamente sus obligaciones en materia de protección de datos y deben poder demostrar el respeto de estas obligaciones, en particular ante la autoridad de control competente.

([160]) Artículo 35, apartado 3, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([161]) Artículo 35, apartado 4, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([162]) Artículo 33, incisos III a IX, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([163]) Artículo 1 (párrafo único) del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024.
([164]) Artículo 2, incisos I y IV, y artículo 4, del Reglamento sobre Transferencias Internacionales de Datos de la ANPD, de agosto de 2024. Como es el caso con todas las transferencias internacionales, toda transferencia realizada en virtud de estos supuestos se realizará para «fines legítimos, específicos y explícitos comunicados al interesado, sin que exista la posibilidad de efectuar un tratamiento ulterior incompatible con dicha finalidad», tal como se establece en el artículo 9, apartado principal, del Reglamento relativo a las transferencias internacionales de datos, de agosto de 2024, de la ANPD.

(115) El artículo 6, inciso IX, de la LGPD establece el principio de responsabilidad proactiva según el cual el responsable y el encargado del tratamiento deben adoptar medidas que sean «eficaces y capaces» de demostrar el cumplimiento de la LGPD.

(116) Como medio para garantizar la rendición de cuentas, el artículo 50 de la LGPD establece que los responsables y encargados del tratamiento pueden adoptar normas internas y modelos de gobernanza, en particular para velar por la adopción de buenas prácticas en la tramitación de las reclamaciones y peticiones de los interesados, respetando las obligaciones en materia de seguridad y todas las demás obligaciones en virtud de la LGPD («Buenas prácticas y gobernanza»). Estos programas también deben incluir planes de actividades de formación, así como mecanismos de supervisión interna y mitigación de riesgos.

(117) La LGPD también establece el requisito de nombrar a un delegado de protección de datos que tenga una participación significativa en el diseño y la ejecución de estos programas internos. De conformidad con el artículo 5, inciso VIII, el delegado de protección de datos actuará como vínculo entre el responsable del tratamiento, los interesados y la ANPD. El artículo 41 de la LGPD obliga a todos los responsables del tratamiento a nombrar a un delegado de protección de datos y a que su identidad se haga pública.

(118) La LGPD ha facultado a la ANPD para introducir una exención de la obligación de los responsables y encargados del tratamiento de designar a un delegado de protección de datos ([165]). En su Reglamento sobre la Aplicación del LGPD a las Pequeñas y Medianas Empresas (pymes), la ANPD estableció que determinadas pequeñas empresas, pymes, empresas emergentes y organizaciones sin ánimo de lucro pueden acogerse a esta exención ([166]). En concreto, el ámbito de aplicación de la exención comprende las siguientes entidades: «microempresas, pequeñas empresas, empresas emergentes, entidades jurídicas de Derecho privado, incluidas las organizaciones sin ánimo de lucro, de conformidad con la legislación vigente, así como personas físicas y entidades privadas despersonalizadas que tratan datos personales» ([167]). Con arreglo a la legislación brasileña, las microempresas ([168]), las pequeñas empresas ([169]) o las empresas emergentes ([170]) se refieren a empresas con un único empleado o un número reducido de empleados ([171]) y que se sitúan por debajo de unos ingresos brutos anuales determinados ([172]).

(119) La exención de la obligación de nombrar a un delegado de protección de datos no se aplicaría a ninguna de estas empresas y entidades, independientemente de su tamaño o de sus ingresos, que lleven a cabo un tratamiento de datos personales «de alto riesgo» ([173]). Un tratamiento se considerará de alto riesgo si, con carácter acumulativo, posee al menos una de estas características generales: 1) tratamiento de datos personales a gran escala; y 2) tratamiento de datos que pueda afectar significativamente a los derechos e intereses fundamentales de los interesados; y al menos una de estas características específicas: 1) uso de tecnologías emergentes o innovadoras; 2) vigilancia o control de zonas accesibles al público; 3) procesos de toma de decisiones exclusivamente automatizados; y 4) tratamiento de datos sensibles o datos pertenecientes a niños o personas mayores ([174]). Un

([165]) Artículo 41, apartado 3, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([166]) ANPD, Reglamento sobre la Aplicación de la LGPD a las Pequeñas y Medianas Empresas («Reglamento sobre Pymes»), abril de 2024. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

([167]) Artículo 2, inciso I, del Reglamento sobre Pymes de la ANPD, abril de 2024.

([168]) Una «microempresa» se define como una empresa con unos ingresos brutos anuales iguales o inferiores a 360 000 BRL. Véase el artículo 3, inciso I, de la Ley complementaria n.º 123, de 14 de diciembre de 2006, relativa al estatuto nacional de las microempresas y las pequeñas y medianas empresas. 360 000 BRL equivalen a 56 500 EUR.

([169]) Una «pequeña empresa» o «pyme» se define como una empresa con unos ingresos brutos anuales de al menos 360 000 BRL e iguales o inferiores a 4 800 000 BRL. Véase el artículo 3, inciso II, de la Ley complementaria n.º 123, de 14 de diciembre de 2006 (Ley sobre el Estatuto Nacional de las Microempresas y las Pymes). 4 800 000 BRL equivalen a 753 000 EUR.

([170]) Una «empresa emergente» se define como una «organización empresarial o corporativa, incipiente o reciente, cuyas actividades se caracterizan por la innovación aplicada al modelo de negocio o a los productos o servicios ofrecidos». Véase el artículo 2, inciso III, del Reglamento sobre Pymes, de abril de 2024, de la ANPD.
Una empresa emergente solo puede registrarse como tal durante un máximo de 10 años y siempre que sus ingresos brutos anuales no superen los 16 000 000 BRL. Véase el artículo 4, inciso I, de la Ley n.º 182, de 1 de junio de 2021 (Ley sobre las Empresas Emergentes). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp182.htm. 16 000 000 BRL equivalen a 2 500 000 EUR.

([171]) Véase, en particular, el artículo 2, inciso II, del Reglamento sobre Pymes, de abril de 2024, de la ANPD, y el artículo 41 de la Ley n.º 14.195, de 26 de agosto de 2021, (Ley sobre la Creación de Empresas). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm.

([172]) Véase la Ley complementaria n.º 123, de 14 de diciembre de 2006 (Ley sobre el Estatuto Nacional de las Microempresas y las Pymes). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm.

([173]) Artículo 4 del Reglamento sobre Pymes, de abril de 2024, de la ANPD.

([174]) Artículo 4, incisos I y II, del Reglamento sobre Pymes, de abril de 2024, de la ANPD.

tratamiento de datos personales «a gran escala» se define como aquel que «implica a un número significativo de interesados, teniendo también en cuenta el volumen de datos afectados, así como la duración, la frecuencia y la extensión geográfica del tratamiento efectuado» ([175]). Un «tratamiento de datos que pueda afectar significativamente a los derechos e intereses fundamentales de los interesados» se define «entre otras situaciones, [como] aquellas en las que la actividad de tratamiento puede obstaculizar el ejercicio de los derechos o el uso de un servicio, así como causar daños materiales o morales a los interesados, como discriminación, violación de la integridad física, derecho a la imagen y la reputación, fraude financiero o usurpación de identidad» ([176]).

(120) La ANPD adoptó un Reglamento sobre la función del delegado de protección de datos, de carácter vinculante, que aclara sus obligaciones ([177]). En dicho Reglamento, la ANPD recuerda la obligación de las entidades privadas y las autoridades públicas de publicar información sobre la identidad de su delegado de protección de datos ([178]). El artículo 10 del Reglamento sobre el delegado de protección de datos (DPD) recuerda la obligación de los responsables y encargados del tratamiento de garantizar, entre otras cuestiones, que el delegado de protección de datos pueda desempeñar sus funciones con independencia, «sin injerencias indebidas, especialmente al proporcionar orientación sobre las prácticas que deben adoptarse en relación con la protección de los datos personales» y que se le proporcione acceso directo al más alto nivel de dirección y a todos los empleados que participen en decisiones estratégicas para el tratamiento de datos dentro de una entidad. Del mismo modo, el delegado de protección de datos desempeñará sus funciones y tareas con «ética, integridad e independencia técnica, evitando situaciones que puedan constituir un conflicto de intereses» ([179]).

(121) La función del delegado de protección de datos ha sido una prioridad en las medidas de ejecución de la ANPD. Por ejemplo, las primeras sanciones de la ANPD afectaron a una empresa que recibió una sanción y una advertencia específica por no poder demostrar que había nombrado a un delegado de protección de datos ([180]). La entidad decidió designar a un delegado de protección de datos durante el procedimiento administrativo para cumplir la orden de la ANPD. Desde entonces, la ANPD ha seguido imponiendo sanciones a entidades públicas y privadas en relación con las disposiciones con respecto al delegado de protección de datos establecidas en virtud de la LGPD ([181]).

(122) La evaluación de impacto relativa a la protección de datos (en lo sucesivo, la «EIPD») es otra herramienta importante para garantizar la rendición de cuentas. La EIPD permite evaluar y determinar el impacto de un tratamiento. De conformidad con el artículo 38 de la LGPD, la ANPD puede solicitar a un responsable o encargado del tratamiento que elabore una EIPD ([182]), la cual debe incluir una descripción del tipo de tratamiento de los datos personales, así como medidas, garantías y mecanismos para mitigar los riesgos. Además, la sección II de la LGPD establece disposiciones sobre rendición de cuentas que facultan a la ANPD para solicitar la publicación de una EIPD o recomendar la adopción de «buenas prácticas» para la protección de los datos personales por parte de las autoridades públicas ([183]).

(123) A la luz de los requisitos y prácticas de rendición de cuentas descritos en los considerandos 114 a 122 de la presente Decisión, el marco brasileño aplica el principio de rendición de cuentas de manera similar a las medidas previstas en las secciones 3 y 4 del capítulo 4 del Reglamento (UE) 2016/679, ya que establece diferentes mecanismos para garantizar y demostrar el cumplimiento de la LGPD.

2.5. **Supervisión y garantía del cumplimiento**

(124) Con el fin de garantizar un nivel adecuado de protección de los datos en la práctica, debe existir una autoridad de control independiente encargada de supervisar las normas en materia de protección de datos y hacerlas cumplir. Esta autoridad debe actuar con total independencia e imparcialidad en el desempeño de sus funciones y en el ejercicio de sus competencias.

([175]) Véase, por ejemplo, el artículo 4, apartado 1, del Reglamento sobre Pymes, de abril de 2024, de la ANPD.
([176]) Véase, por ejemplo, el artículo 4, apartado 2, del Reglamento sobre Pymes, de abril de 2024, de la ANPD.
([177]) Reglamento sobre la función del delegado de protección de datos en relación con el tratamiento de datos personales («Reglamento sobre el delegado de protección de datos»), de julio de 2024, de la ANPD. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074.
([178]) Artículos 5 y 9 del Reglamento sobre el delegado de protección de datos, de julio de 2024, de la ANPD.
([179]) Artículo 18 del Reglamento sobre el delegado de protección de datos, de julio de 2024, de la ANPD.
([180]) Véase ANPD, «Informe de la Instrucción n.º 1/2023 — Telekall Infoservice» (disponible en portugués). Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.
([181]) Véase, por ejemplo, ANPD, «Informe de la Instrucción n.º 5/2024 — Ministério da Saúde» (disponible en portugués). Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.
([182]) Artículo 38 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([183]) Sección II de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

2.5.1. *Supervisión independiente*

(125) En Brasil, la autoridad de control independiente encargada de supervisar y hacer cumplir la LGPD es la Agência Nacional de Proteção de Dados (ANPD).

(126) La ANPD fue creada en virtud del artículo 55-A de la LGPD como organismo independiente mediante un primer decreto provisional y, posteriormente, una ley en 2022 ([184]). La adopción de la ley por la que se transformaba la naturaleza de la ANPD incluía cambios en la LGPD para revocar disposiciones que subordinaban el funcionamiento y las operaciones financieras de la ANPD a autorizaciones que debía conceder el Ejecutivo en virtud de la Ley de Presupuestos de Brasil ([185]). La disposición modificada de la LGPD reconoce que la ANPD es una «autoridad especial, con autonomía técnica y decisoria, con su propio patrimonio y con sede en el Distrito Federal» ([186]).

(127) Como «autoridad de carácter especial», la ANPD posee autonomía para desempeñar plenamente sus funciones y competencias jurídicas establecidas en virtud de la LGPD, incluida la gestión administrativa de la agencia ([187]). Posee, pues, autonomía para gestionar su gasto y sus contrataciones ([188]). La ANPD se creó inicialmente como «autoridad» antes de convertirse en una «agencia» en septiembre de 2025, alineando su nombre con el de otras once entidades reguladoras que gozan de este alto grado de independencia en Brasil (por ejemplo, la Agencia Nacional de la Electricidad, la Agencia Nacional de Telecomunicaciones, etc.) ([189]).

(128) Los recursos de la ANPD proceden en gran medida del presupuesto general del Estado Federal de Brasil. Además, el presupuesto de la ANPD podrá incluir donaciones, subvenciones u otros créditos establecidos en el artículo 55-L de la LGPD. Desde su creación en 2021, la ANPD ha crecido exponencialmente. Los informes anuales de la ANPD indican que la autoridad contaba con 141 empleados y funcionarios a finales de 2023, tras solo 4 años de existencia ([190]). El presupuesto anual de 2025 de la ANPD es de 18 000 000 BRL ([191]). En septiembre de 2025, se anunció en Brasil la creación de una nueva carrera profesional de la función pública dedicada a la «protección de datos», con doscientos puestos, como parte de un aumento de la plantilla de la ANPD en los próximos años ([192]).

([184]) El artículo 55-A de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos), en su redacción original, ha sido modificado por la Ley n.º 14.460, de 25 de octubre de 2022, (Ley por la que se transforma la ANPD en una autoridad de régimen especial). En lo que respecta a la independencia, véase la Medida provisional n.º 1.124, de 13 de junio de 2022, por la que se transforma la ANPD en una autoridad de estatuto especial. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Mpv/mpv1124.htm y la Ley n.º 14.460, de 25 de octubre de 2022 (Ley por la que se transforma la ANPD en una autoridad de estatuto especial). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14460.htm. La posibilidad de que el Gobierno cambie el estatuto de la ANPD para aumentar su independencia se detallaba en el artículo 55-A, apartado 1 (ahora revocado) de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([185]) Véase el artículo 9 de la Ley n.º 14.460, de 25 de octubre de 2022 (Ley por la que se transforma la ANPD en una autoridad de régimen especial), por la que se revoca y sustituye el artículo 55-A de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([186]) Artículo 7 de la Ley n.º 14.460, de 25 de octubre de 2022 (Ley por la que se transforma la ANPD en una autoridad de estatuto especial).

([187]) Véase ANPD, «La ANPD se convierte en una autoridad de carácter especial», junio de 2022 (disponible en portugués). Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial.

([188]) Artículo 55-L de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([189]) Artículo 1 del Decreto n.º 1.317, de 17 de septiembre de 2025, por el que se modifica la LGPD para transformar la Agência Nacional de Proteção de Dados. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314 y el artículo 2, inciso XII, de la Ley n.º 13.848, de 25 de junio de 2019, sobre la organización de las agencias reguladoras. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm.

([190]) ANPD, «Informe sobre el cuarto año de la ANPD», noviembre de 2023, p. 8 (disponible en portugués). Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([191]) 18 225 566 BRL (2 857 768 EUR). Véase la Ley Presupuestaria Anual, p. 190. Puede consultarse en el siguiente enlace: LEI15121-VOLUME I.pdf.

([192]) Artículo 9, inciso I, del Decreto n.º 1.317, de 17 de septiembre de 2025, por el que se modifica la LGPD para transformar la Agência Nacional de Proteção de Dados. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

(129) La ANPD está compuesta por un Consejo de Administración (su máximo órgano de gobierno), un Consejo Nacional para la Protección de los Datos Personales y de la Privacidad (con competencias consultivas) y varias oficinas y unidades administrativas ([193]). Esta estructura se establece en el artículo 55-C de la LGPD y se detalla en dos decretos adoptados en 2020 y 2023, respectivamente ([194]).

(130) El Consejo de Administración está compuesto por cinco directores, incluido el presidente de la ANPD. Cada miembro del Consejo de Administración de la ANPD es nombrado por un período de cinco años por el presidente de la República de Brasil, previa aprobación del Senado Federal ([195]).

(131) Los directores deben ser de nacionalidad brasileña y poseer un nivel educativo elevado y adecuado para el puesto ([196]). Para garantizar su independencia, todos los directores deben abstenerse de cualquier actividad empresarial o política con ánimo de lucro, así como de ocupar puestos como directivos o asesores en cualquier empresa, entre otras restricciones ([197]). Además, la legislación brasileña que regula el ejercicio de altos cargos en la administración pública federal prohíbe a las personas que desempeñen funciones equivalentes a las de los directores de la ANPD ejercer actividades incompatibles con sus funciones, entre otras restricciones ([198]). No podrán, pues, ejercer como consultores o intermediarios de intereses privados (aun de manera informal) o prestar servicios a entidades sujetas a la supervisión o regulación de la ANPD, incluso de forma ocasional. Además, al término de su mandato o función en la ANPD y durante los seis meses siguientes, los directores no podrán ejercer determinadas funciones que puedan generar un riesgo de conflicto de intereses ([199]).

(132) Los administradores solo podrán ser destituidos en circunstancias específicas definidas en el artículo 55-E de la LGPD, a saber, «en caso de dimisión, condena judicial firme e inapelable o sanción de despido por procedimiento administrativo disciplinario». La Ley Federal de la Función Pública establece que dicha sanción debe estar justificada y solo puede proponerse en caso de infracciones específicas demostradas (faltas graves, corrupción, uso irregular de fondos públicos, etc.) ([200]). Estas normas y procedimientos proporcionan a los directores de la ANPD protección institucional en el ejercicio de sus funciones. Hasta la fecha, ningún director de la ANPD ha sido destituido ni sometido a procedimientos disciplinarios. El Consejo de Administración de la ANPD ha estado en funcionamiento y se ha mantenido inalterado debido a un cambio de administración que tuvo lugar en Brasil en 2023.

([193]) Artículo 55-C de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([194]) Decreto n.º 10.474, de 26 de agosto de 2020, sobre la estructura de la ANPD. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm, modificado por el Decreto n.º 11.758, de 30 de octubre de 2023, relativo a la estructura modificada de la ANPD. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11758.htm#art1.

([195]) Artículo 55-D, apartados 1 y 3, de la Ley n.º 13.709, de 14 de agosto de 2018, [Lei Geral de Proteção de Dados Pessoais (Ley General de Protección de Datos)] y artículo 12 del Decreto n.º 1.317, de 17 de septiembre de 2025, por el que se modifica la LGPD para transformar la Agência Nacional de Proteção de Dados. Puede consultarse en el siguiente enlace: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314. El artículo 12 de este Decreto amplía la duración del mandato de los directores de la ANPD de cuatro a cinco años para adaptarse a todas las demás agencias reguladoras independientes que existen en Brasil. Todos los directores de la ANPD nombrados con anterioridad a la adopción de este Decreto completarán un mandato de cuatro años, según lo previsto inicialmente por la ley en el momento de su nombramiento.

([196]) Artículo 55-D, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([197]) Artículo 11 del Decreto n.º 10.474, de 26 de agosto de 2020, sobre la estructura de la ANPD.

([198]) Artículo 5 de la Ley n.º 12.813, de 16 de mayo de 2013, sobre conflictos de intereses de los funcionarios públicos y otras funciones en las administraciones públicas. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm.

([199]) Artículo 6 de la Ley n.º 12.813, de 16 de mayo de 2013, sobre conflictos de intereses de los funcionarios públicos y otras funciones en las administraciones públicas.

([200]) La lista exhaustiva de delitos se encuentra recogida en el artículo 132 de la Ley n.º 8112, de 11 de diciembre de 1990 (Ley Federal de la Función Pública y el Funcionariado). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Véase también el capítulo V de esta Ley, relativo a las condiciones de aplicación de una sanción.

(133) Las funciones y competencias de la ANPD se detallan en el artículo 55-J de la LGPD. En particular, incluyen el desarrollo de políticas y directrices en materia de protección de datos, el fomento de la adopción de normas que faciliten a los interesados el control sobre sus datos personales, la investigación de las infracciones de los derechos individuales, la tramitación de reclamaciones, la garantía del cumplimiento de la LGPD y la imposición de sanciones, la garantía de la formación y la promoción en el ámbito de la protección de datos, así como el intercambio y la cooperación con las autoridades competentes en materia de protección de datos de terceros países, entre otros ([201]).

(134) La ANPD cuenta con un órgano consultivo formado por el Consejo Nacional para la Protección de los Datos Personales y de la Privacidad, establecido en virtud del artículo 58-A de la LGPD. Este órgano está compuesto por representantes del poder ejecutivo, legislativo y judicial, así como de la sociedad civil, los sindicatos y el sector empresarial ([202]). Tiene una función meramente consultiva que consiste en preparar estudios o informes anuales sobre la protección de datos, celebrar debates públicos y audiencias sobre la protección de datos personales y la privacidad, proponer recomendaciones no vinculantes a la ANPD y difundir conocimientos sobre la protección de los datos personales y la privacidad ([203]). La cooperación entre la ANPD y el Consejo Nacional se centra en la promoción de la protección de datos y la privacidad en Brasil. El Consejo Nacional no tiene competencias en relación con el seguimiento y la aplicación de la LGPD, ya que solo la ANPD tiene autoridad para supervisar la aplicación de la ley y hacerla cumplir, por ejemplo, mediante la publicación de reglamentaciones, la realización de investigaciones y la aplicación de sanciones. Por su condición de autoridad independiente, la ANPD no está obligada a aplicar ninguna sugerencia que pueda presentar el Consejo Nacional a través de sus informes o recomendaciones no vinculantes.

2.5.2. *Ejecución, en particular las sanciones*

(135) Con el fin de garantizar el cumplimiento, el legislador ha otorgado a la ANPD competencias tanto de investigación como de ejecución, que abarcan desde las advertencias hasta las sanciones administrativas.

(136) Por lo que se refiere a las competencias en materia de investigación, si se sospecha o notifica un incumplimiento de la LGPD, o cuando sea necesario para la protección de los derechos de los interesados que hayan sido o puedan ser vulnerados, la ANPD puede llevar a cabo en cualquier momento auditorías e inspecciones *in situ* a los responsables del tratamiento, tanto del sector público como privado, y solicitar cualquier información necesaria ([204]). En particular, el Reglamento sobre las Facultades Sancionadoras de la ANPD, de carácter vinculante, establece que los responsables y encargados del tratamiento deben permitir a la ANPD «acceder a oficinas/edificios, equipos, aplicaciones, instalaciones, sistemas, herramientas y recursos tecnológicos, documentos, datos e información de carácter técnico, operativo o de otro tipo que sean pertinentes para la evaluación de las actividades de tratamiento de datos personales, en su poder o en poder de terceros» ([205]).

([201]) Artículo 55-J, incisos I a XXIV, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([202]) Para obtener más información sobre los miembros y actividades del Consejo Nacional, véase ANPD, Consejo Nacional para la Protección de los Datos Personales y de la Privacidad. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/cnpd-2.

([203]) Artículo 58-B de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([204]) Artículo 55-J, inciso XVI, de la Ley n.º 13.709, de 14 de agosto de 2018, (Ley General de Protección de Datos), artículo 4, inciso I, del Decreto n.º 10.474, de 26 de agosto de 2020, sobre la estructura de la ANPD, y artículo 12 del Reglamento sobre Notificación de Incidentes de Seguridad, de abril de 2024, de la ANPD.

([205]) Artículo 5 del Reglamento de la ANPD sobre las Facultades Sancionadoras de la ANPD, de octubre de 2021. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021.

(137) Como parte de sus poderes correctivos, la ANPD puede imponer advertencias, multas u otras sanciones, como órdenes de interrupción temporal del tratamiento de datos o de supresión de datos personales ([206]). Estas sanciones pueden imponerse a entidades públicas o privadas, con la excepción de multas y multas diarias, que no pueden imponerse a entidades públicas ([207]). Pueden aplicarse varias sanciones acumulativas al objeto de lograr que una entidad cumpla sus obligaciones. La ANPD puede emitir una advertencia para conceder a un responsable del tratamiento un plazo específico para adoptar medidas correctoras con el fin de que el tratamiento se ajuste a la LGPD ([208]). De no hacerlo, se impondrían sanciones adicionales. La ANPD ha emitido, por ejemplo, varias advertencias al Ministerio de Sanidad por no proporcionar una EIPD ni notificar una violación de la seguridad de los datos, entre otras cosas ([209]). La ANPD puede imponer varias sanciones conjuntamente para proteger los derechos de los interesados o para hacer cumplir la LGPD. Así, la ANPD puede imponer una sanción administrativa por incumplimiento de la LGPD junto con una orden de supresión de los datos vinculados a dicha infracción ([210]). La ANPD también puede decidir, en caso de sanciones no pecuniarias, imponer «multas diarias» cuando «sea necesario para garantizar el cumplimiento [de la LGPD] dentro de un plazo» ([211]). La multa diaria se aplica de forma acumulativa, teniendo en cuenta el tiempo transcurrido entre la incidencia de la multa y el cumplimiento de la obligación, y puede alcanzar un importe máximo de 50 millones BRL ([212]).

(138) De conformidad con el artículo 52, inciso II, de la LGPD, la ANPD puede imponer sanciones administrativas, además de multas diarias, de hasta el 2 % de los ingresos de una entidad en Brasil y de una cuantía máxima de 50 millones BRL ([213]). Las multas pueden acumularse en caso de infracciones múltiples. Unos meses después de la adopción de su Reglamento sobre Sanciones, la ANPD impuso sus primeras multas pecuniarias a una empresa de telecomunicaciones que no identificó la base jurídica para un tratamiento ni nombró a un delegado de protección de datos. La empresa recibió una advertencia y dos multas por un total de 14 400 BRL ([214]). En el Reglamento sobre Sanciones, de carácter vinculante, la ANPD clasificó las sanciones según tres niveles de gravedad: leve, moderada y grave ([215]), en función de un factor establecido, como el tipo y el volumen de los datos objeto de tratamiento, el tipo de tratamiento o el impacto en los derechos del interesado. Por ejemplo, las infracciones relativas al tratamiento de datos personales sensibles se corresponden con el máximo nivel de sanciones que la ANPD puede imponer ([216]).

(139) El Reglamento sobre Sanciones establece una metodología para el cálculo de las multas a fin de tener en cuenta los factores agravantes o atenuantes ([217]). Por ejemplo, una multa puede incrementarse en un 10 % en caso de infracciones específicas reiteradas o incluso en un 90 % por cada medida correctora no cumplida en un plazo determinado ([218]). Del mismo modo, una multa puede reducirse en un 50 % si la infracción se subsana inmediatamente después del inicio del procedimiento administrativo por parte de la ANPD ([219]).

([206]) Artículos 55 y 55-J, inciso IV, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos), y Reglamento sobre Sanciones, de febrero de 2023, de la ANPD.
([207]) Artículo 52, apartado 3. Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([208]) Artículo 52, inciso I, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([209]) Véanse la Decisión n.º 4/2024 de la ANPD, disponible en https://www.gov.br/anpd/pt-br/centrais-de-conteudo/relatorio_de_instrucao_no_4_2024_fis_cgf_anpd_v-publica.pdf y la Decisión n.º 5/2024 de la ANPD, disponible en: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.
([210]) Artículo 52, inciso VI, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([211]) Artículo 16 del Reglamento sobre Sanciones, de febrero de 2023, de la ANPD.
([212]) Artículo 16, apartado 1, del Reglamento sobre Sanciones, de febrero de 2023, de la ANPD. 50 millones BRL equivalen a aproximadamente 7,8 millones EUR.
([213]) 50 millones BRL equivalen a aproximadamente 7,8 millones EUR.
([214]) ANPD, Decisión n.º 1/2023, disponible en: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.
([215]) Artículo 8 del Reglamento sobre Sanciones, de febrero de 2023, de la ANPD.
([216]) Artículo 8, apartado 3, inciso I, letra d), del Reglamento sobre Sanciones, de febrero de 2023, de la ANPD.
([217]) Anexo I, artículos 12-13 del Reglamento sobre Sanciones, de febrero de 2023, de la ANPD.
([218]) Artículo 12, incisos de I al IV, del Reglamento sobre Sanciones, de febrero de 2023, de la ANPD.
([219]) Artículo 13, inciso I, del Reglamento sobre Sanciones, de febrero de 2023, de la ANPD.

(140) Por lo tanto, el sistema de Brasil combina diversos tipos de sanciones, que pueden consistir en medidas correctoras o multas administrativas. Tan pronto como se hizo efectiva su competencia sancionadora, la ANPD empezó a hacer uso de sus facultades ([220]). Hasta la fecha, se han emitido sanciones y recomendaciones dirigidas tanto a las autoridades públicas, entre otras, del ámbito de la seguridad, como hacia operadores privados ([221]). Las sanciones impuestas hasta la fecha por la ANPD se refieren a una amplia variedad de irregularidades, como el hecho de no haber nombrado a un delegado de protección de datos, incidentes de seguridad como violaciones de la seguridad de los datos o la falta de cooperación con la ANPD. Además de imponer multas pecuniarias, la ANPD ha sido especialmente activa en el uso de sus distintos poderes correctivos para, por ejemplo, emitir órdenes a los responsables del tratamiento para que lleven a cabo una EIPD o detengan el tratamiento de datos personales. Por ejemplo, en julio de 2024, la ANPD emitió una orden dirigida a una gran plataforma de redes sociales que suspendiese el tratamiento de datos personales destinado al entrenamiento de sistemas de inteligencia artificial (IA) generativa en todos sus productos ([222]). Además de esta medida preventiva, destinada a proteger los derechos fundamentales de los interesados, la ANPD impuso una multa diaria de 50 000 BRL hasta que el tratamiento se ajustara a lo estipulado por la LGPD ([223]). Por último, la ANPD ha anunciado la incoación de investigaciones de varias grandes plataformas tecnológicas multinacionales, empresas de redes sociales y un banco, además de proseguir las investigaciones ya en curso de entidades del sector público ([224]). En sus pocos años de existencia, la ANPD ha mostrado un sólido historial de ejecución, haciendo uso de toda la gama de sus competencias de ejecución.

(141) Por último, las sanciones administrativas establecidas en virtud de la LGPD pueden concurrir con otras sanciones administrativas o civiles y penales, incluidas las establecidas en el Código de Protección de los Consumidores de Brasil ([225]) y en el Marco Civil para Internet ([226]). En particular, el Código de Protección de los Consumidores de Brasil exige a las empresas que faciliten a los consumidores información sobre sus negocios y actividades ([227]). El artículo 56 del Código de Protección de los Consumidores enumera además las sanciones a las que se enfrentan las empresas en caso de incumplimiento, que van desde multas hasta la prohibición de vender o producir un producto o la obligación de suspender un servicio. Además, los artículos 61 a 74 del Código de Protección de los Consumidores recogen las infracciones penales por las que las empresas pueden enfrentarse a entre seis meses y dos años de prisión; entre ellas, se encuentran las alegaciones falsas o engañosas en relación con un servicio o la promoción de un servicio susceptible de provocar un perjuicio al consumidor. Por ejemplo, en 2014, el Departamento de Defensa y Protección de los Consumidores de Brasil impuso una multa de 3,5 millones BRL a una empresa de telecomunicaciones por infringir el Código de Protección de los Consumidores y el Marco Civil para Internet al recurrir al seguimiento para la publicidad comportamental en línea y la venta de datos de navegación ([228]).

(142) De lo anterior se desprende que el sistema brasileño garantiza en la práctica una ejecución efectiva de sus normas de protección de datos.

2.5.3. *Reparación*

(143) Para que exista una protección adecuada y, en particular, que se puedan tutelar los derechos individuales por la vía coercitiva, el interesado debe poder obtener reparación judicial y administrativa efectiva, en particular la indemnización por daños y perjuicios.

([220]) ANPD, Registro de Sanciones. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/decisoes-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

([221]) Véase, por ejemplo, la Nota técnica n.º 175/2023 sobre el proyecto de Acuerdo de Cooperación entre el Ministerio de Justicia y Seguridad Pública y la Federación Brasileña de Fútbol para el intercambio de datos personales con vistas a mejorar el «Proyecto Estadio Seguro». Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

([222]) ANPD, Medida preventiva, Voto n.º 11/2024. Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf.

([223]) 50 000 BRL equivalen a 7 800 EUR.

([224]) La lista completa y actualizada de las investigaciones en curso y de los casos abiertos por la ANPD puede consultarse en la siguiente dirección: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao.

([225]) Ley n.º 8.079 de 11 de septiembre de 1990 (Ley de Protección de los Consumidores). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

([226]) Ley n.º 12.965, de 23 de abril de 2014, Marco Civil da Internet («Marco Civil para Internet»). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([227]) Artículo 6 de la Ley n.º 8.079 de 11 de septiembre de 1990 (Ley de Protección de los Consumidores).

([228]) 3,50 millones BRL equivalían a 1,5 millones EUR aproximadamente, según el tipo de cambio vigente en aquel momento.

(144) El sistema brasileño ofrece a las personas diversos mecanismos para hacer valer eficazmente sus derechos y obtener reparación.

(145) Como primer paso, aquellas personas que consideren que se han vulnerado sus derechos o intereses en el ámbito de la protección de datos pueden dirigirse al responsable del tratamiento correspondiente. De conformidad con el artículo 9 de la LGPD, el responsable del tratamiento facilitará, entre otras, la información de contacto oportuna para que los interesados puedan presentar la solicitud y los «escritos procesales» ([229]).

(146) Además, en virtud de la LGPD y del sistema jurídico brasileño, existen varias vías de reparación para las personas que consideren que el responsable o el encargado del tratamiento ha vulnerado sus derechos o intereses en materia de protección de datos.

(147) En primer lugar, cualquier persona que considere que el responsable o encargado del tratamiento ha vulnerado sus derechos o intereses en materia de protección de datos puede presentar una reclamación o denunciar dicha infracción ante la ANPD ([230]). La ANPD dispone de una sección específica en su sitio web desde la que los interesados pueden presentar una reclamación por incumplimiento de la LGPD o una petición en caso de problemas relacionados con una solicitud dirigida a un responsable del tratamiento en relación con sus derechos de protección de datos ([231]). Como se explica en el considerando 138 de la presente Decisión, en respuesta a una reclamación, la ANPD puede imponer una sanción tal como se detalla en el artículo 52 de la LGPD. El Reglamento sobre las Facultades Sancionadoras de la ANPD estableció el procedimiento administrativo para sus actuaciones, incluidos los plazos, los procesos por los que se rige el derecho a ser oído y la publicación de la resolución ([232]).

(148) Las decisiones de la ANPD pueden ser impugnadas por los interesados mediante la presentación de un recurso ante el Consejo de Administración de la ANPD en un plazo de diez días a partir de su recepción ([233]). Dentro de su derecho a un recurso efectivo, los interesados también pueden recurrir las decisiones del Consejo ante los órganos jurisdiccionales, así como presentar cualquier recurso contra la ANPD por incumplimiento de sus obligaciones en virtud de la LGPD (incluida la negativa a tramitar una reclamación o la desestimación en cuanto al fondo de una reclamación) ([234]).

(149) En segundo lugar, la ANPD puede fomentar la «conciliación directa» (mediación) entre los interesados y los responsables del tratamiento para dar prioridad a la resolución del problema y a la «indemnización por daños y perjuicios por parte del responsable del tratamiento» ([235]). Estos procesos no impiden a los interesados presentar reclamaciones o acceder a otras vías de reparación.

(150) En tercer lugar, por lo que respecta a los daños y perjuicios, el artículo 42 de la LGPD establece la obligación del responsable o encargado del tratamiento de subsanar «los daños materiales, morales, individuales o colectivos a terceros» derivados del tratamiento de datos personales. Los interesados pueden interponer una demanda, individual o colectiva, para solicitar reparación e indemnización por tales daños y perjuicios ([236]). La LGPD estipula que un juez posee la facultad discrecional de «invertir la carga de la prueba en favor del interesado», en particular en los casos en que «la presentación de pruebas por el interesado resulte excesivamente gravosa» ([237]).

(151) En cuarto lugar, cuando una violación de los derechos de los interesados entra en el ámbito de aplicación de la legislación en materia de protección de los consumidores y de las relaciones con los consumidores, será de aplicación dicha protección y podrá invocarse ante los órganos jurisdiccionales ([238]).

([229]) Artículo 9, leído en relación con el artículo 55-J, inciso V, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([230]) Artículo 55-J, inciso V, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([231]) Véase ANPD, «Servicios a los interesados, presentación de una reclamación o petición» (documento en portugués). Puede consultarse en el siguiente enlace: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular.
([232]) Secciones II y III del Reglamento de la ANPD sobre las Facultades Sancionadoras de la ANPD, octubre de 2021.
([233]) Artículo 59 del Reglamento de la ANPD sobre las Facultades Sancionadoras de la ANPD, de octubre de 2021.
([234]) Artículo 22 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([235]) Artículo 17, inciso VIII, del Reglamento de la ANPD sobre las Facultades Sancionadoras de la ANPD, octubre de 2021.
([236]) Artículo 42, apartado 3, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([237]) Artículo 42, apartado 2, de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([238]) Artículo 45 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

(152) En quinto lugar, el Tribunal Supremo Federal de Brasil ha reconocido que las personas tienen derecho a solicitar medidas cautelares por la vulneración de los derechos que les confiere la Constitución, entre los que se incluye el derecho a la protección de los datos personales ([239]). En este contexto, un órgano jurisdiccional puede, por ejemplo, ordenar a los responsables del tratamiento que suspendan cualquier actividad ilícita o que le pongan fin. Además, los derechos de protección de datos, también los protegidos por la LGPD, pueden ejercerse a través de acciones civiles. El artículo 22 de la LGPD permite explícitamente que la defensa de los derechos de los interesados se ejerza ante los órganos jurisdiccionales y, en términos más generales, que los interesados puedan presentar ante dichos órganos demandas relacionadas con la protección de datos, ya sea de forma individual o colectiva.

(153) Por lo tanto, el sistema brasileño ofrece diversas vías de reparación, desde opciones fácilmente accesibles y de bajo coste (como las reclamaciones ante la ANPD) hasta vías judiciales, que incluyen la posibilidad de obtener una indemnización por daños y perjuicios o de solicitar una reparación colectiva.

3. ACCESO A LOS DATOS PERSONALES TRANSFERIDOS DESDE LA UNIÓN EUROPEA Y USO DE ESTOS POR PARTE DE LAS AUTORIDADES PÚBLICAS BRASILEÑAS

(154) La Comisión ha evaluado asimismo las limitaciones y garantías previstas, incluidos los mecanismos de supervisión y las vías de impugnación para los particulares contemplados en el Derecho brasileño en lo que respecta a la recogida y la utilización ulterior por las autoridades públicas brasileñas de los datos personales transferidos a responsables y encargados del tratamiento en Brasil en aras del interés público, en particular con fines penales y de seguridad nacional (en lo sucesivo, «acceso de las autoridades públicas»).

(155) A la hora de evaluar si, con arreglo a la presente Decisión, las condiciones en las que el acceso de las autoridades públicas a los datos transferidos a Brasil supera la prueba de la equivalencia sustancial a efectos del artículo 45, apartado 1, del Reglamento (UE) 2016/679, según la interpretación del TJUE a la luz de la Carta de los Derechos Fundamentales, la Comisión tuvo en cuenta, en particular, los criterios siguientes.

(156) En primer lugar, cualquier limitación del ejercicio del derecho a la protección de los datos personales debe ser establecida por ley, y la base legal que permita la injerencia en dicho derecho debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate ([240]).

(157) En segundo lugar, para cumplir el requisito de proporcionalidad, según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario en una sociedad democrática para lograr objetivos específicos de interés general equivalentes a los reconocidos por la Unión, la normativa del tercer país en cuestión que permita la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de las medidas en cuestión e imponer unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso ([241]). En particular, esa normativa debe indicar en qué circunstancias y en qué condiciones puede adoptarse una medida que prevea el tratamiento de dichos datos ([242]), así como someter el cumplimiento de tales requisitos a una supervisión independiente ([243]).

([239]) El Tribunal Supremo Federal de Brasil dictó una sentencia en 2020 que suspendió un decreto presidencial que habría obligado a las empresas de telecomunicaciones a compartir datos de abonados con la oficina censal, reconociendo por vez primera la protección de datos como un derecho fundamental y allanando el camino para su inclusión en la Constitución de Brasil. Véase, Tribunal Supremo Federal, Decisión sobre la ADI 6387 de 7 de mayo de 2020. Puede consultarse en el siguiente enlace: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([240]) Schrems II, apartados 174 y 175, y jurisprudencia citada. Véanse también, por lo que se refiere al acceso por parte de las autoridades públicas de los Estados miembros, el asunto C-623/17 Privacy International, ECLI:EU:C:2020:790, apartado 65, y los asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, ECLI:EU:C:2020:791, apartado 175.

([241]) Véase Schrems II, apartados 176 y 181 y la jurisprudencia citada. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véanse también Privacy International, apartado 68, y La Quadrature du Net y otros, apartado 132.

([242]) Schrems II, apartado 176. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véanse también Privacy International, apartado 68, y La Quadrature du Net y otros, apartado 132.

([243]) Schrems II, apartado 179.

(158) En tercer lugar, dicha normativa y sus exigencias deben ser jurídicamente vinculantes según el Derecho interno. Esto afecta, en primer lugar, a las autoridades del tercer país en cuestión, pero también debe ser posible exigir judicialmente el cumplimiento de dichas obligaciones jurídicas por parte dichas autoridades ([244]). En concreto, los interesados han de tener la posibilidad de ejercer acciones en Derecho ante un tribunal independiente e imparcial para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión ([245]).

3.1. **Marco jurídico general**

(159) Las limitaciones y garantías que se aplican a la recogida y la utilización ulterior de los datos personales por parte de las autoridades públicas brasileñas se derivan del marco constitucional general, de leyes específicas que regulan sus actividades con fines penales y de seguridad nacional, así como de las normas que se aplican específicamente al tratamiento de datos personales.

(160) En primer lugar, el acceso a los datos personales por parte de las autoridades públicas brasileñas se rige por el principio general de legalidad consagrado en la Constitución brasileña y del que emanan los principios de razonabilidad, necesidad y proporcionalidad ([246]). En particular, de conformidad con el artículo 5 de la Constitución, los derechos y libertades fundamentales (incluido el derecho a la intimidad y a la protección de datos) solo pueden restringirse por ley y cuando sea imperativo por motivos de seguridad nacional, seguridad pública u otros fines específicos de interés público especificados por la ley. Dichas restricciones deben ser razonables y proporcionadas ([247]). En particular, la evaluación de la finalidad de interés público es esencial para apreciar la proporcionalidad de la injerencia, a la luz del principio de legalidad. El artículo 5, inciso LIV, de la Constitución establece que «nadie podrá ser privado de su libertad o de sus bienes sin las debidas garantías procesales».

(161) En segundo lugar, la orden brasileña garantiza el *habeas data* como vía de reparación constitucional concebida para proteger el derecho de acceso, rectificación y supresión de datos personales en poder de las autoridades públicas o en conjuntos de datos o registros públicos ([248]). Sirve de salvaguardia contra el uso indebido o la violación de la privacidad relacionada con el tratamiento de datos por parte de entidades públicas. Cualquier persona puede presentar una reclamación o solicitud sobre la base de *habeas data*, independientemente de su nacionalidad ([249]).

(162) En tercer lugar, los principios y derechos generales mencionados en los considerandos 155 a 158 también se reflejan en las leyes específicas que regulan las competencias de las autoridades garantes del cumplimiento del Derecho y de seguridad nacionales. Por ejemplo, el Marco Civil para Internet establece medidas que requieren una orden judicial previa para el acceso a los datos y la limitación del acceso a los datos en línea ([250]). Del mismo modo, la Ley de Interceptación Telefónica establece medidas y salvaguardias específicas para el tratamiento de datos de telecomunicaciones ([251]). En el ámbito de la seguridad nacional, la Ley por la que se crea el sistema de inteligencia brasileño establece medidas para el acceso lícito a los datos con fines de seguridad nacional ([252]).

([244]) Schrems II, apartados 181 y 182.

([245]) Schrems I, apartado 95, y Schrems II, apartado 194. En ese sentido, el TJUE ha destacado en particular que el cumplimiento del artículo 47 de la Carta de los Derechos Fundamentales, que garantiza el derecho a la tutela judicial efectiva ante un juez independiente e imparcial, «forma parte también del nivel de protección exigido dentro de la Unión cuyo respeto debe ser constatado por la Comisión antes de adoptar una decisión de adecuación en virtud del artículo 45, apartado 1, del RGPD» (Schrems II, apartado 186).

([246]) Artículo 5, inciso II, de la Constitución de la República Federativa de Brasil de 1988.

([247]) Brasil está sujeto a la jurisdicción de la Corte Interamericana de Derechos Humanos, que, entre otros, reconoció el principio de proporcionalidad como «esencial en una sociedad democrática» y que las limitaciones de los derechos fundamentales solo pueden producirse si se destinan a cumplir un objetivo público imperativo. Véase, por ejemplo, Mendes, Gilmar Ferreira. *Derechos fundamentales y control judicial* [no disponible en español]. Sao Paulo: Saraiva, 2012, p. 78.

([248]) Artículo 5, incisos LXXII y LXXVII, de la Constitución de la República Federativa de Brasil de 1988.

([249]) Véanse asimismo los considerandos 9 y 11 de la presente Decisión.

([250]) Ley n.º 12.965, de 23 de abril de 2014, Marco Civil da Internet («Marco Civil para Internet»). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([251]) Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

([252]) Ley n.º 9.883 de 7 de diciembre de 1999. Ley por la que se crea el sistema de inteligencia de Brasil.

(163) En cuarto lugar, el tratamiento de datos personales por parte de las autoridades públicas, incluso a efectos de control de la aplicación de la ley y de seguridad nacional, está sujeto a los requisitos de protección de datos en virtud de la LGPD. Como se describe en el considerando 31 de la presente Decisión, la exención relativa a la aplicación de la LGPD en el ámbito de la seguridad pública, la defensa nacional, la seguridad del Estado y la investigación y el enjuiciamiento penal establecida en el marco de la LGPD es parcial. El Tribunal Supremo Federal ha interpretado la aplicabilidad de la LGPD a la luz de la protección constitucional de los datos personales y ha establecido que los principios, derechos y objetivos fundamentales de la LGPD se aplican a todo tratamiento de datos personales por parte de las autoridades públicas, incluso cuando se realiza con fines de aplicación del Derecho penal o de seguridad nacional ([253]). Sobre esta base, por ejemplo, la ANPD ha llevado a cabo investigaciones y ha publicado orientaciones, como una nota técnica dirigida a las autoridades públicas sobre actividades relacionadas con la seguridad pública, en la que recordó que el tratamiento para estos fines de interés público debe cumplir los principios y derechos generales previstos por la LGPD ([254]).

(164) Por último, las personas pueden invocar sus derechos y libertades constitucionales ante el Tribunal Supremo Federal si consideran que han sido vulnerados por las autoridades públicas en el ejercicio de sus competencias. Pueden asimismo solicitar reparación, en relación con sus derechos de protección de datos, ante organismos de supervisión independientes (por ejemplo, la ANPD) y órganos jurisdiccionales, tal como se detalla en los considerandos 143 a 153 de la presente Decisión.

3.2. **Acceso y uso por parte de las autoridades públicas brasileñas con fines penales**

(165) El Derecho de Brasil impone una serie de limitaciones al acceso y la utilización de datos personales a efectos de control de la aplicación del Derecho penal y proporciona mecanismos de supervisión y reparación que se ajustan a los requisitos mencionados en los considerandos 155 a 158 de la presente Decisión. Las condiciones en las que se puede tener acceso y las garantías aplicables al ejercicio de estas competencias se precisan con detalle en las secciones siguientes.

3.2.1. *Base jurídica, limitación y garantías*

(166) Como norma general, el acceso por parte de las autoridades públicas a los datos personales a efectos de control de la aplicación del Derecho penal requiere una orden judicial previa dictada por una autoridad judicial competente ([255]). Como excepción a esta norma, la policía y la fiscalía, en los casos específicamente previstos por la ley, podrán tener acceso a los datos de las personas investigadas incluidos en un registro público, es decir, aquellos relativos a la cualificación personal, la afiliación y la dirección ([256]). La lista exhaustiva de registros accesibles, prevista por la ley, comprende la información de los ciudadanos brasileños o residentes en Brasil y no comprendería el acceso a los datos transferidos desde la UE, por lo que queda fuera del ámbito de aplicación de la presente Decisión ([257]). El acceso a estos registros se rige por el principio constitucional de legalidad, del que se derivan los principios de razonabilidad, necesidad y proporcionalidad, y puede estar sujeto a un control judicial *ex post*, como se explica en los considerandos 159 a 161.

(167) Las autoridades de Brasil que tienen derecho a acceder a datos personales con fines penales y a recogerlos mediante una orden judicial previa son: 1) la Policía Civil; 2) la Policía Federal; 3) el Ministerio Público Estatal; 4) Ministerio Público Federal; 5) Jueces y órganos jurisdiccionales; y 6) comisiones parlamentarias de investigación.

([253]) Tribunal Supremo Federal. Decisión sobre la ADI 6649, septiembre de 2022. Puede consultarse en el siguiente enlace: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([254]) Nota técnica n.º 175/2023, apartado 5.1.

([255]) Véase, por ejemplo, el artículo 5, inciso XII, de la Constitución de la República Federativa de Brasil de 1988.

([256]) Artículos 15 y 16 de la Ley n.º 12.850 de 2 de agosto de 2013 (Ley relativa a las organizaciones delictivas y a las investigaciones penales). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

([257]) Entre los registros accesibles se incluyen: registros de empleo, registros electorales, registros telefónicos, registros financieros, registros de proveedores de internet, registros de tarjetas de crédito. La información de estos registros incluye información sobre las personas que se suscriben a estos servicios o que utilizan estos servicios públicos. Artículos 15 y 16 de la Ley n.º 12.850 de 2 de agosto de 2013 (Ley relativa a las organizaciones delictivas y a las investigaciones penales). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

(168) De conformidad con el artículo 3-B del Código Penal, un magistrado «encargado del control de la legalidad de la investigación penal y de la salvaguardia de los derechos individuales» puede dictar una orden judicial por la que se autorice: 1) la interceptación telefónica de comunicaciones en sistemas informáticos y conectados u otras formas de comunicación; 2) la supresión del secreto fiscal, bancario, de datos y telefónico; 3) el registro e incautación domiciliarios; 4) el acceso a información secreta; y 5) «otras medidas para obtener pruebas que restrinjan los derechos fundamentales de la persona investigada» ([258]).

3.2.1.1. Interceptación de las comunicaciones

(169) La confidencialidad de la correspondencia de las comunicaciones electrónicas y telefónicas se considera un derecho fundamental en el marco jurídico brasileño ([259]).

(170) Las autoridades públicas solo pueden acceder a estos datos en casos excepcionales con fines de investigación o enjuiciamiento penal. La interceptación de las comunicaciones debe ser siempre una medida subsidiaria y excepcional, permitida únicamente cuando no existen otros medios para resolver un caso concreto, según lo establecido por el Tribunal Supremo Federal ([260]). Las modalidades de interceptación de las comunicaciones telefónicas y en línea se recogen en la Ley de Interceptación Telefónica ([261]).

(171) El artículo 2 de la Ley de Interceptación Telefónica establece condiciones estrictas para el acceso a la comunicación. Toda interceptación de comunicaciones requiere una autorización judicial previa. Las autoridades públicas autorizadas deberán presentar una solicitud válida de interceptación a un juez. Dichas autoridades podrán ser 1) la autoridad policial competente, en el contexto de una investigación penal; o 2) el representante del Ministerio Público, cuando se trate de una investigación penal y del ejercicio de acciones penales ([262]). No se autorizará la interceptación de comunicaciones telefónicas en ninguna de las circunstancias siguientes, en virtud de los requisitos de necesidad y proporcionalidad: 1) si no existen pruebas razonables de autoría o participación en una infracción penal; 2) si las pruebas pueden aportarse por otros medios disponibles; 3) si el hecho investigado constituye una infracción penal punible con privación de libertad ([263]).

(172) Además, la Ley de Interceptación Telefónica exige que la solicitud de interceptación aclare la necesidad de la medida ([264]). La autorización judicial previa deberá justificarse, teniendo en cuenta la proporcionalidad de los medios utilizados para llevar a cabo la interceptación ([265]). El juez podrá autorizar el acceso al contenido de las comunicaciones durante un máximo de quince días. Este período podrá ampliarse en virtud de una nueva resolución judicial una vez que se demuestre el carácter indispensable de la medida ([266]). Toda interceptación de comunicaciones, incluido el seguimiento medioambiental, realizada sin autorización judicial o con fines no autorizados por la ley constituye un delito punible con hasta cuatro años de prisión ([267]).

([258]) Decreto-ley n.º 3.689, de 3 de octubre de 1941, Código Penal. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([259]) Artículo 5, inciso XII, de la Constitución de la República Federativa de Brasil de 1988.
([260]) Tribunal Supremo Federal, HC 108147/PR, 2012. Puede consultarse en el siguiente enlace: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
([261]) Artículo 1 de la Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica).
([262]) Artículo 2, incisos I y II, de la Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica).
([263]) Artículo 2 de la Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica).
([264]) Artículo 4 de la Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica).
([265]) Artículo 5 de la Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica).
([266]) Artículo 5 de la Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica).
([267]) Artículo 10 de la Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica).

(173) Por regla general, los datos a los que se acceda y que se recojan con fines penales de conformidad con la Ley de Interceptación Telefónica se conservarán mientras dure el tratamiento y se suprimirán una vez dejen de ser necesarios para el procedimiento judicial, de conformidad con las directrices vinculantes del poder judicial ([268]). El artículo 9 de la Ley de Interceptación Telefónica establece además que, cuando el contenido recogido no guarde relación con el asunto investigado, los datos quedarán «inutilizables» ([269]).

(174) Por lo que se refiere a los metadatos de telecomunicaciones, el artículo 17 de la Ley relativa a las organizaciones delictivas y a las investigaciones penales exige a las empresas telefónicas que conserven la información sobre las cuentas de usuario de los ciudadanos residentes en Brasil y los registros de llamadas telefónicas (exclusivamente los números de teléfono) durante cinco años ([270]). El acceso a este registro gestionado por ANATEL (agencia reguladora de las telecomunicaciones de Brasil) está restringido a determinadas entidades públicas y, tal como se ha descrito anteriormente, requiere una autorización judicial.

(175) Por lo que respecta a la información disponible en línea, el artículo 7 del Marco Civil para Internet garantiza además «la inviolabilidad y confidencialidad del flujo de comunicaciones a través de internet», salvo resolución judicial, de conformidad con la ley; y «la inviolabilidad y confidencialidad de las comunicaciones privadas almacenadas, excepto por orden judicial» ([271]).

(176) De conformidad con el artículo 10 del Marco Civil para Internet, solo podrá accederse al contenido de las comunicaciones en línea y a los datos de conexión (incluidos los metadatos) mediante una orden judicial previa. De conformidad con el artículo 22 del Marco Civil para Internet, la solicitud de orden judicial debe incluir: I) pruebas fundadas de la comisión de la infracción; II) justificación motivada de la utilidad de los registros solicitados para la investigación o para fines probatorios; y III) determinación del período al que se refieren los registros. Asimismo, el artículo 13 exige a los proveedores de servicios de internet o de aplicaciones que conserven los registros de conexión durante un año «en un entorno controlado y seguro» ([272]). No existe una obligación similar de conservar datos en relación con el contenido de las comunicaciones en línea. El acceso a los registros almacenados de conexión solo puede concederse a una autoridad competente sobre la base de una autorización judicial, en las condiciones descritas en el presente considerando ([273]).

(177) El artículo 11 del Marco Civil para Internet recuerda que cualquier operación que implique la recogida, el almacenamiento, la retención o cualquier otro tratamiento de registros, datos personales o comunicaciones por proveedores de servicios de conexión y aplicaciones de internet en Brasil debe ser conforme a «la legislación brasileña y los derechos a la intimidad, la protección de los datos personales y la confidencialidad de las comunicaciones y registros privados». De las salvaguardias reflejadas en los considerandos 175 a 177 se desprende que, por lo general, Brasil no autoriza la recopilación y la conservación masiva de datos de comunicaciones por internet.

3.2.1.2. Supresión de la protección del secreto fiscal, bancario, de datos y de comunicaciones

(178) En Brasil existe protección constitucional de la confidencialidad de la correspondencia de las comunicaciones electrónicas (incluidos los datos) y telefónicas ([274]). La LGPD brinda además protección en cuanto al uso de los datos y la información de comunicación ([275]), mientras que la Ley sobre la Confidencialidad de las Entidades Financieras protege la confidencialidad de la información fiscal y bancaria ([276]).

([268]) Artículo 20, resolución n.º 324, de 20 de junio de 2020. Puede consultarse en el siguiente enlace: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/atos-do-poder-judiciario/resolucao-no-324-de-30-de-junho-de-2020.
([269]) Artículo 9 de la Ley n.º 9.296, de 24 de julio de 1996, (Ley de Interceptación Telefónica).
([270]) Artículo 17 de la Ley n.º 12.850 de 2 de agosto de 2013 (Ley relativa a las organizaciones delictivas y a las investigaciones penales). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.
([271]) Artículo 7 de la Ley n.º 12.965, de 23 de abril de 2014, Marco Civil da Internet («Marco Civil para Internet»).
([272]) Artículo 13, apartado principal, de la Ley n.º 12.965, de 23 de abril de 2014 (Marco Civil para Internet).
([273]) Artículo 13, apartado 5, de la Ley n.º 12.965, de 23 de abril de 2014 (Marco Civil para Internet).
([274]) Artículo 5, inciso XII, de la Constitución de la República Federativa de Brasil de 1988.
([275]) Véase el artículo 2 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).
([276]) Ley complementaria n.º 105, de 10 de enero de 2001 (Ley sobre la Confidencialidad de las Operaciones de las Entidades Financieras). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(179) Las autoridades públicas solo pueden acceder a esta información en casos excepcionales con fines de investigación o enjuiciamiento penal. La interceptación de las comunicaciones debe ser siempre una medida subsidiaria y excepcional, permitida únicamente cuando no existen otros medios para resolver un caso concreto, según lo establecido por el Tribunal Supremo Federal ([277]).

(180) Los criterios y garantías para el acceso a los datos y las comunicaciones se recogen en el Marco Civil para Internet y la Ley de Interceptación Telefónica y se detallan en los considerandos 169 a 177 de la presente Decisión.

(181) En cuanto a los datos fiscales y bancarios, el artículo 1 de la Ley sobre la Confidencialidad de las Entidades Financieras establece las condiciones para la supresión de las obligaciones generales de garantizar la confidencialidad de esta información. En primer lugar, la confidencialidad solo puede levantarse mediante una autorización judicial ([278]). En segundo lugar, las medidas solo pueden autorizarse cuando se trate de investigaciones penales o del enjuiciamiento de delitos o infracciones penales identificados como sigue: 1) terrorismo; 2) tráfico ilícito de estupefacientes o drogas similares; 3) contrabando o tráfico de armas, municiones o materiales destinados a su producción; 4) extorsión mediante secuestro; 5) delitos contra el sistema financiero nacional; 6) delitos contra la Administración pública; 7) delitos contra el sistema fiscal y de la seguridad social; 8) blanqueo de capitales u ocultación de bienes; y 9) asociación con una organización delictiva ([279]). El artículo 10 de la ley establece asimismo que la protección de la confidencialidad de los datos fiscales y bancarios no se levantará para ningún otro fin y que el incumplimiento de esta limitación constituye un delito punible con hasta cuatro años de prisión ([280]).

3.2.1.3. Registros e incautaciones

(182) Por regla general, la Constitución federal establece que los registros y las incautaciones solo pueden llevarse a cabo en circunstancias excepcionales estrictamente definidas o en las condiciones previstas por la ley y sobre la base de una orden judicial dictada por una autoridad judicial competente, y en observancia de las garantías procesales ([281]). Los registros e incautaciones deben respetar el principio de legalidad y llevarse a cabo en la medida en que sean necesarios.

(183) En las siguientes circunstancias excepcionales, podrán realizarse registros e incautaciones sin orden judicial: 1) en caso de delito flagrante (esto es, cuando la comisión del delito tiene lugar en presencia de las fuerzas y cuerpos de seguridad); 2) en caso de catástrofe natural (con el fin de salvar vidas o bienes materiales de las personas); o 3) prestar asistencia a una persona que no pueda dar su consentimiento y requiera ayuda ([282]). La jurisprudencia del Tribunal Supremo Federal de Brasil aclara que las autoridades garantes del cumplimiento del Derecho no pueden basarse en «avisos anónimos» y «conductas sospechosas» para llevar a cabo registros o incautaciones sin orden judicial, ya que ello incumple el requisito de legalidad y no otorga a las autoridades una justificación válida para vulnerar la inviolabilidad del domicilio ([283]).

(184) En cuanto a las garantías procesales, en consonancia con los principios constitucionales de Brasil, no puede efectuarse ninguna búsqueda en un dispositivo electrónico sin una sospecha razonable de que en dicho dispositivo se almacena alguna prueba de una infracción penal y, por regla general, sin una orden judicial ([284]). Además, no puede obligarse a una persona a proporcionar datos si ello es susceptible de vulnerar sus derechos constitucionales, como el derecho a no autoincriminarse ([285]). Al presentar una solicitud de orden de búsqueda ante los órganos

([277]) Tribunal Supremo Federal, HC 108147/PR, 2012. Puede consultarse en el siguiente enlace: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.

([278]) Artículo 3-B del Decreto-ley n.º 3.689, de 3 de octubre de 1941, Código Penal. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

([279]) Artículo 1, apartado 4, incisos del I al IX, de la Ley complementaria n.º 105, de 10 de enero de 2001 (Ley sobre la Confidencialidad de las Operaciones de las Entidades Financieras). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

([280]) Artículo 10 de la Ley complementaria n.º 105, de 10 de enero de 2001 (Ley sobre la Confidencialidad de las Operaciones de las Entidades Financieras). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

([281]) Artículo 5, inciso XI, de la Constitución de la República Federativa de Brasil de 1988.

([282]) Artículo 5, inciso XI, de la Constitución de la República Federativa de Brasil de 1988.

([283]) Tribunal Supremo Federal, 2020, asunto J.S. Recurso extraordinario n.º 603616.

([284]) Artículo 5, inciso XI, de la Constitución de la República Federativa de Brasil de 1988.

([285]) Artículo 5, inciso LXIII, de la Constitución de la República Federativa de Brasil de 1988. Véase también el Decreto-ley n.º 2.848, de 7 de diciembre de 1940, Código de Enjuiciamiento Penal. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

jurisdiccionales, la autoridad garante del cumplimiento del Derecho penal debe facilitar los hechos y pruebas pertinentes que respalden la necesidad de acceder al sistema informático y a los datos, utilizando credenciales de acceso adquiridas legalmente ([286]). En caso de que el órgano jurisdiccional conceda la orden de búsqueda de información, las autoridades utilizarán las credenciales de acceso para acceder al sistema informático y a sus datos, de conformidad con las condiciones especificadas en la orden. Una vez completada la búsqueda o el acceso, las autoridades competentes deberán presentar un informe al órgano jurisdiccional en el que se describan los resultados de la búsqueda o el acceso y que recoja una lista de los datos o la información obtenidos.

3.2.1.4. Acceso a información confidencial

(185) El artículo 4 de la Ley sobre el Acceso a la Información define la «información confidencial» como aquella que «está sujeta temporalmente a restricciones de acceso público debido a su carácter esencial para la seguridad de la sociedad y del Estado» ([287]). Los datos personales pueden formar parte del ámbito de la información confidencial, tal como se define en la frase anterior.

(186) El artículo 6 de la Ley sobre el Acceso a la Información exige a las entidades públicas que protejan la información confidencial y restrinjan el acceso a esta. En cuanto a las comunicaciones, los datos, la información bancaria y la información fiscal, el acceso a información confidencial con fines de investigación y enjuiciamiento penal requiere una autorización judicial y solo puede efectuarse en casos excepcionales, únicamente cuando no existan otros medios para resolver un caso concreto, según lo establecido por el Tribunal Supremo Federal y el marco legal ([288]).

3.2.1.5. Otras medidas para obtener pruebas que restrinjan los derechos fundamentales de la persona investigada.

(187) La expresión «otras medidas para obtener pruebas que restrinjan los derechos fundamentales de la persona investigada» se refiere, por ejemplo, a la posibilidad de ordenar la detención preventiva o de someter a una persona a vigilancia física. En principio, estas medidas no son pertinentes en el contexto de la transferencia de datos basada en una decisión de adecuación.

(188) En aras de la exhaustividad, tales medidas, propuestas por una autoridad pública, requieren una autorización judicial. Las medidas propuestas deben respetar el principio de legalidad establecido en la Constitución y solo pueden ordenarse en casos excepcionales y cuando no pueda utilizarse otra alternativa, tal como establece el Tribunal Supremo Federal.

3.2.2. *Utilización ulterior de la información*

(189) Por lo que se refiere a la utilización posterior de datos personales para otro fin por parte de una autoridad pública, el artículo 9 de la Ley de Interceptación Telefónica establece que, cuando el contenido recogido no guarde relación con el asunto investigado en una investigación específica, los datos resultarán «inutilizables». El artículo 13 del Marco Civil para Internet también limita la retención de los registros de datos de conexión a un año como máximo. El artículo 10 de la Ley sobre la Confidencialidad de las Entidades Financieras también limita la finalidad para la que puede levantarse el secreto de los datos fiscales y bancarios ([289]). En la práctica, estas medidas limitan los posibles usos ulteriores de la información.

([286]) Artículo 240 del Decreto-ley n.º 2.848, de 7 de diciembre de 1940, Código de Enjuiciamiento Penal.

([287]) Artículo 4, inciso III, de la Ley n.º 12.527, de 18 de noviembre de 2011 (Ley sobre el Acceso a la Información).

([288]) Tribunal Supremo Federal, HC 108147/PR, 2012. Puede consultarse en el siguiente enlace: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401 y el artículo 3-B del Decreto-ley n.º 3.689, de 3 de octubre de 1941, Código Penal. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

([289]) Artículo 10 de la Ley complementaria n.º 105, de 10 de enero de 2001 (Ley sobre la Confidencialidad de las Operaciones de las Entidades Financieras). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(190) Además, cabe destacar que el Tribunal Supremo Federal dictaminó que la LGPD se aplica al intercambio de datos personales entre organismos públicos, también cuando tal intercambio se produce entre las autoridades garantes del cumplimiento del Derecho y los servicios de inteligencia ([290]). En particular, el Tribunal recordó que «el intercambio de datos personales entre organismos y entidades de la administración pública presupone: 1) la definición de una finalidad legítima, específica y explícita para el tratamiento de datos; 2) la compatibilidad del tratamiento con los fines comunicados; 3) la limitación del intercambio de datos al mínimo necesario para alcanzar la finalidad declarada; así como el pleno cumplimiento de los requisitos, garantías y procedimientos establecidos en la LGPD, en la medida en que sea compatible con el sector público». El órgano jurisdiccional añadió que «el tratamiento de datos personales efectuado por organismos públicos en contravención de los parámetros jurídicos y constitucionales dará lugar a la responsabilidad civil del Estado por los daños sufridos por las personas», de conformidad con el artículo 42 de la LGPD.

(191) En cuanto al intercambio de datos personales entre las autoridades encargadas de garantizar el cumplimiento del Derecho penal de Brasil y autoridades similares de terceros países, estas actividades se rigen por instrumentos de Derecho internacional, en consonancia con la LGPD. En este sentido, el artículo 33, inciso III, de la LGPD dispone que las transferencias internacionales de datos podrán llevarse a cabo cuando sea «necesario para la cooperación internacional en el ámbito jurídico entre entidades públicas de inteligencia, investigación y enjuiciamiento, con arreglo a instrumentos del Derecho internacional». En Brasil, el Ministerio de Justicia y Seguridad Pública es la autoridad central encargada de la cooperación jurídica internacional penal. El Ministerio es responsable de la recepción, el análisis, la transmisión y el seguimiento de la ejecución de las solicitudes de cooperación internacional con autoridades extranjeras, de conformidad con las normas de Derecho internacional aplicables y la LGPD. El tratamiento de datos personales necesario para la cooperación jurídica internacional está sujeto a los principios de limitación de la finalidad (artículo 6, inciso I, de la LGPD), licitud y lealtad del tratamiento (artículos 6 y 7 de la LGPD), minimización y exactitud de los datos (artículo 6, incisos III y V, de la LGPD), transparencia (artículo 6, inciso VI, de la LGPD), seguridad de los datos (artículo 6, inciso VII, de la LGPD) y limitación del plazo de conservación (artículo 6, apartados I, III, IV y artículo 16 de la LGPD). La posible divulgación de datos personales a terceros (incluidos terceros países) solo podrá realizarse de conformidad con estos principios, tras haber evaluado el cumplimiento de los principios constitucionales de necesidad y proporcionalidad y garantizar la continuidad de la protección y el cumplimiento de los derechos de los interesados (artículo 2 del Reglamento sobre Transferencia de Datos).

(192) Por lo tanto, las competencias de las autoridades encargadas de garantizar el cumplimiento del Derecho penal de Brasil para recopilar datos y acceder a ellos están limitadas por normas claras y precisas previstas por la ley y sujetas a una serie de garantías. Estas garantías incluyen, en particular, la supervisión de la ejecución de dichas medidas, en particular mediante la aprobación judicial previa y garantías que limiten la duración del acceso y la retención de la información en consonancia con los principios de necesidad y proporcionalidad.

3.2.3. *Supervisión*

(193) En Brasil, las actividades de las autoridades encargadas de garantizar el cumplimiento del Derecho penal son supervisadas por distintos organismos.

(194) En primer lugar, como confirmó el Tribunal Supremo Federal, la ANPD está facultada para supervisar el tratamiento de datos personales efectuado por las autoridades encargadas de garantizar el cumplimiento del Derecho penal en virtud de determinados requisitos de la LGPD ([291]). En este contexto, la ANPD puede ejercer las competencias correctivas y de investigación que le confiere la LGPD. Por ejemplo, la ANPD ha investigado las actividades de la Policía Federal, el Ministerio de Justicia y Seguridad Pública y otros organismos públicos que llevan a cabo actividades de seguridad federal, estatal o local o que tienen responsabilidades policiales ([292]). Las investigaciones pueden llevarse a cabo por iniciativa propia de la ANPD o a raíz de solicitudes y reclamaciones, que pueden presentar, por ejemplo, particulares, organizaciones de la sociedad civil y autoridades públicas. Por ejemplo, la ANPD llevó a cabo varias investigaciones sobre el uso de cámaras de vídeo a petición de la sociedad civil ([293]).

([290]) Tribunal Supremo Federal. Decisión sobre la ADI 6649, septiembre de 2022. Puede consultarse en el siguiente enlace: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([291]) Véase el considerando 163 de la presente Decisión y la Decisión del Tribunal Supremo Federal sobre la ADI 6649, de 15 de septiembre de 2022. Puede consultarse en el siguiente enlace: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([292]) Véase ANPD, Inspecciones, incluidos los asuntos 00261.000836/2021-76 y 00261.001028/2021-26. Disponible en: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340.

([293]) Véase ANPD, Inspecciones, asunto 00261.002211/2022-20 relativo al uso de cámaras de seguridad por parte de las autoridades de la ciudad de Fortaleza. Solicitud presentada a la ANPD disponible en: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos/arquivos-processos-de-fiscalizacao-concluidos/processosesec_pblico00261-002211_2022-20.pdf.

(195) En segundo lugar, las actividades de las autoridades encargadas de garantizar el cumplimiento del Derecho penal son supervisadas por el poder judicial. Los órganos jurisdiccionales están facultados para autorizar la recogida de y el acceso a datos personales en las circunstancias mencionadas en los considerandos 165 a 187. Además, tienen la facultad de imponer sanciones civiles y penales en caso de abuso o incumplimiento de la legislación vigente, entre las que se incluyen la privación de libertad o la orden de cese de determinadas actividades.

(196) En tercer lugar, el Ministerio Público, institución independiente y permanente en Brasil encargada de defender el ordenamiento jurídico y el sistema democrático, está facultado para ejercer un control externo sobre las actividades policiales ([294]). Tal como se establece en la Resolución relativa al Ministerio Público, el control externo de las actividades policiales tiene por objeto mantener la «regularidad y adecuación de los procedimientos empleados en el ejercicio de las actividades policiales», con especial atención al «respeto de los derechos fundamentales garantizados por la Constitución y las leyes federales» ([295]). Como tal, el Ministerio Público puede, entre otras facultades, realizar visitas *in situ*, programadas o en cualquier momento, inspeccionar investigaciones, supervisar la incautación de mercancías y controlar el cumplimiento de las órdenes ([296]). Toda vulneración de la ley se denunciará ante los órganos jurisdiccionales. En el marco de sus funciones, el Ministerio Público ha participado en la investigación y el enjuiciamiento de casos de violencia policial, abuso de poder y violaciones de los derechos humanos. Además, la Fiscalía General del Estado desempeña un papel en la supervisión de la protección de datos, iniciando o participando en acciones legales sobre la base de protecciones constitucionales y promoviendo los derechos de protección de datos junto con la ANPD. La Fiscalía, por ejemplo, presentó ante el Tribunal Supremo Federal un argumento que respaldaba la decisión histórica de reconocer la protección de datos como un derecho fundamental en Brasil ([297]). En su página web también se puede consultar un registro de las actuaciones de la Fiscalía en relación con la LGPD ([298]).

3.2.4. *Reparación*

(197) El sistema brasileño ofrece distintas vías judiciales y administrativas para obtener reparación, entre ellas la indemnización por daños y perjuicios. Estos mecanismos ofrecen a los interesados soluciones administrativas y judiciales efectivas que les permiten, en particular, hacer valer sus derechos, en especial el derecho a acceder a sus datos personales o a obtener la rectificación o supresión de dichos datos.

(198) En primer lugar, las personas pueden acudir a la vía judicial para obtener reparación, entre otros, por daños y perjuicios. La Constitución federal y el Código Procesal Civil establecen las bases jurídicas para reclamar una indemnización por los daños morales o materiales causados por la autoridad pública que haya recopilado o utilizado ilegalmente datos con fines delictivos ([299]). En particular, la Constitución menciona expresamente que el derecho a la intimidad implica un «derecho a indemnización» por el daño material o moral resultante de su vulneración ([300]). Las resoluciones de los órganos jurisdiccionales pueden recurrirse ante el Tribunal Supremo Federal y también ante la Corte Interamericana de Derechos Humanos. En 2009, la Corte Interamericana de Derechos Humanos ordenó a Brasil indemnizar a los trabajadores de las cooperativas agrícolas debido a escuchas telefónicas indebidas llevadas a cabo en el Estado de Paraná en 1999, ya que incumplían la Ley de Intercepción Telefónica y la Convención Americana sobre Derechos Humanos ([301]).

([294]) Artículo 127 de la Constitución de la República Federativa de Brasil de 1988.

([295]) Artículo 20, resolución 20, de 28 de mayo de 2007, Control externo de las actividades policiales. Puede consultarse en el siguiente enlace: https://www.cnmp.mp.br/portal/images/Comissoes/CSP/Resolu%C3%A7%C3%B5es_/Resolu%C3%A7%C3%A3o_20.pdf.

([296]) Artículo 4, resolución 20, de 28 de mayo de 2007, Control externo de las actividades policiales.

([297]) Véase el considerando 199 de la presente Decisión y la Decisión del Tribunal Supremo Federal sobre la ADI 6.387, de mayo de 2020. Puede consultarse en el siguiente enlace: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([298]) Fiscalía General, «La LGPD en la Fiscalía General». Puede consultarse en el siguiente enlace: https://www.mpf.mp.br/servicos/lgpd/lgpd-no-mpf.

([299]) Véase, por ejemplo, el artículo 43 de la Ley n.º 10.408, de 10 de enero de 2002. Código Procesal Civil. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm.

([300]) Artículo 5, inciso X, de la Constitución de la República Federativa de Brasil de 1988.

([301]) Corte Interamericana de Derechos Humanos, asunto Escher y otros/Brasil, alegaciones preliminares, méritos, devoluciones y costas. Sentencia de 6 de julio de 2009. Disponible en http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

(199) En segundo lugar, cualquier persona, independientemente de su nacionalidad, puede invocar la protección que brinda el concepto de *habeas data* para obtener el acceso y la rectificación de sus datos que se encuentren en poder de las autoridades públicas ([302]). Sobre esta base, las personas también pueden iniciar procesos ante los órganos jurisdiccionales, tales como la acción directa de inconstitucionalidad (Ação Direta de Inconstitucionalidade o ADI) ante el Tribunal Supremo Federal. La resolución histórica de 2020 del Tribunal Supremo Federal, que allanó el camino para que Brasil reconociera la protección de datos como un derecho fundamental, tuvo su origen en las ADI presentadas al amparo del principio de *habeas data* ([303]). La Fiscalía también participó en el asunto, apoyando la posición de los ciudadanos y la sociedad civil que presentaron el caso. El proceso judicial fue iniciado para impugnar una orden ejecutiva que tenía por objeto compartir datos personales de más de doscientos millones de abonados a servicios de telecomunicaciones con el Instituto Brasileño de Geografía y Estadística durante la pandemia de COVID-19 ([304]). El Tribunal Supremo Federal estimó que la orden ejecutiva violaba los derechos fundamentales a la intimidad y a la confidencialidad de las comunicaciones protegidos por la Constitución ([305]). La orden ejecutiva se suspendió y el Tribunal Supremo Federal dictaminó que la protección de datos debe considerarse un derecho fundamental y protegerse como tal, al igual que el derecho a la intimidad ([306]). En el momento en que se emitió esta resolución, la LGPD aún no estaba en vigor. Por tanto, los jueces del órgano jurisdiccional utilizaron el Derecho comparado, en particular la jurisprudencia del Tribunal Constitucional Federal alemán y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, para respaldar su interpretación sobre la inconstitucionalidad de la orden ejecutiva, así como sobre los derechos fundamentales a la dignidad y a la intimidad consagrados en la Constitución y el reconocimiento del *habeas data* como instrumento para proteger el derecho a la autodeterminación en materia de información ([307]).

(200) En tercer lugar, las personas pueden solicitar reparación a la ANPD por infracciones de la LGPD conforme a lo dispuesto en su artículo 55-J, inciso V, y con arreglo a las condiciones detalladas en los considerandos 146 y 149 de la presente Decisión. También pueden ejercer ante las autoridades públicas sus derechos en materia de protección de datos establecidos en la LGPD ([308]).

(201) Los mecanismos de reparación descritos en los considerandos 197 a 200 de la presente Decisión proporcionan a los interesados recursos administrativos y judiciales eficaces que les permiten, en particular, hacer valer sus derechos, incluido el derecho a la protección de datos en relación con dichos datos.

3.3. **Acceso y uso por parte de las autoridades públicas brasileñas con fines de seguridad nacional**

(202) El Derecho de Brasil contiene una serie de limitaciones y garantías con respecto al acceso y la utilización de datos personales con fines de seguridad nacional, y proporciona mecanismos de supervisión y reparación que se ajustan a los requisitos mencionados en los considerandos (156) a (158) de la presente Decisión. Las condiciones en las que se puede tener acceso y las garantías aplicables al ejercicio de estas competencias se precisan con detalle en las secciones siguientes.

([302]) Véanse los considerandos 9 y 161 de la presente Decisión.

([303]) Tribunal Supremo Federal, Decisión sobre la ADI 6.387, de mayo de 2020. Puede consultarse en el siguiente enlace: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([304]) Orden ejecutiva suspendida n.º 954 de 17 de abril de 2020. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm.

([305]) Tribunal Supremo Federal, Decisión sobre la ADI 6.387 de mayo de 2020, p. 12.

([306]) Tribunal Supremo Federal, Decisión sobre la ADI 6.387 de mayo de 2020, p. 8.

([307]) Véase la Decisión del Tribunal Supremo Federal sobre la ADI 6.387, de mayo de 2020, p. 4, y Asociación Internacional de Abogados, *The impact of COVID-19 for data protection in Brasil: the perspective of Brazil's supreme court* [«El impacto de la COVID-19 en la protección de datos en Brasil: la perspectiva del Tribunal Supremo de Brasil», disponible en inglés]. Puede consultarse en el siguiente enlace: https://www.ibanet.org/article/82b25a81-7422-4f07-aaa8-9c2db19e22af#:~:text=On%206%20and%207%20May%202020%2C%20the,as%20an%20independent%20fundamental%20right%20in%20Brazil.&text=The%20processing%20of%20data%20is%20allowed%20only,legal%20principles%2C%20such%20as%20transparency%20and%20security.

([308]) Artículo 23 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

3.3.1. *Base jurídica, limitaciones y garantías*

(203) En Brasil, se puede acceder a los datos personales con fines de seguridad nacional en el marco de actividades de inteligencia sobre la base de la ley por la que se establece el sistema de inteligencia de Brasil (SISBIN) ([309]). Como regla general, el artículo 1 de esta ley estipula que el sistema de inteligencia de Brasil «debe respetar y preservar los derechos y garantías individuales y otras disposiciones de la Constitución federal, los tratados, convenios, acuerdos y compromisos internacionales de los que sea parte o signataria la República Federativa de Brasil» ([310]). Esto implica garantizar los principios de necesidad y proporcionalidad, así como el derecho a la protección de datos ([311]). Las actividades que puede llevar a cabo el sistema de inteligencia de Brasil se describen con más detalle en decretos vinculantes ([312]).

(204) De conformidad con el artículo 4 de la ley por la que se crea el SISBIN brasileño, las entidades que lo conforman pueden obtener y analizar datos específicos con fines de seguridad nacional («Segurança Pública»). El concepto de seguridad nacional se rige por una ley de 2021 que modificó el Código Penal ([313]) y que revocó la Ley de Seguridad Nacional de Brasil ([314]). La ley de 2021 recoge una lista exhaustiva de «delitos» contra la seguridad nacional para enmarcar este concepto. Estos delitos son 1) «delitos contra la soberanía nacional» (que abarcan los actos de guerra, la invasión de un condado, el intento de apropiarse de parte del territorio nacional para formar un nuevo país, el intercambio de información clasificada con gobiernos extranjeros u organizaciones delictivas extranjeras que puedan entrañar un peligro para el orden constitucional de la soberanía nacional, y los intentos de facilitar o falsificar credenciales para el acceso a los sistemas de información a personas no autorizadas) ([315]); 2) delitos contra las «instituciones democráticas» (se contempla todo intento violento de poner fin al Estado de Derecho mediante la prevención o la limitación de los poderes constitucionales y el golpe de Estado) ([316]); 3) delitos contra el «funcionamiento de las instituciones democráticas durante el proceso electoral» (que abarca la interrupción de un proceso electoral y restricción o imposición, mediante violencia, del ejercicio de los derechos políticos de las personas) ([317]); y 4) delitos contra el funcionamiento de los servicios esenciales (comprende el sabotaje de medios de comunicación pública o instalaciones de defensa con el objetivo de poner fin al Estado de Derecho) ([318]). El artículo 359-T de esta ley aclara que no puede considerarse delito el ejercicio de la libertad de expresión, los derechos y poderes constitucionales o el desarrollo de actividades periodísticas, en particular «a través de marchas, reuniones, huelgas, concentraciones o cualquier otra forma de manifestación política con fines sociales» ([319]). La política nacional de inteligencia (PIN) de Brasil establece una serie de objetivos clave para la inteligencia que las autoridades deben tener en cuenta, como la prevención del «sabotaje» o el «espionaje» ([320]). Sin embargo, como «documento de orientación de alto nivel», la política nacional de inteligencia no amplía la lista de delitos relacionados con el concepto de seguridad nacional ni modifica su definición ([321]).

([309]) Ley n.º 9.883 de 7 de diciembre de 1999. Ley por la que se crea el sistema de inteligencia de Brasil. Puede consultarse en el siguiente enlace: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

([310]) Artículo 1, apartado 1, de la Ley n.º 9.883 de 7 de diciembre de 1999. Ley por la que se crea el sistema de inteligencia de Brasil.

([311]) Véase el considerando 160 de la presente Decisión.

([312]) Decreto n.º 8.793/2016, de 29 de junio de 2016, sobre la política nacional de inteligencia. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm y Decreto n.º 4.376/2002, de 13 de septiembre de 2002, sobre la organización y el funcionamiento del sistema de inteligencia de Brasil. Puede consultarse en el siguiente enlace: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/decreto-no-4-376-de-13-de-setembro-de-2002-seopi_eng_rev-d.pdf.

([313]) Ley n.º 14.197, de 1 de septiembre de 2021, por la que se modifica el Código Penal y se deroga la Ley de Seguridad Nacional de 1983. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm.

([314]) Ley derogada n.º 7.170, de 14 de diciembre de 1983 (Ley de Seguridad Nacional). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/LEIS/L7170.htm.

([315]) Capítulo I de la Ley n.º 14.197, de 1 de septiembre de 2021, por la que se modifica el Código Penal y se deroga la Ley de Seguridad Nacional de 1983.

([316]) Capítulo II de la Ley n.º 14.197, de 1 de septiembre de 2021, por la que se modifica el Código Penal y se deroga la Ley de Seguridad Nacional de 1983.

([317]) Capítulo III de la Ley n.º 14.197, de 1 de septiembre de 2021, por la que se modifica el Código Penal y se deroga la Ley de Seguridad Nacional de 1983.

([318]) Capítulo IV de la Ley n.º 14.197, de 1 de septiembre de 2021, por la que se modifica el Código Penal y se deroga la Ley de Seguridad Nacional de 1983.

([319]) Artículo 359-T de la Ley n.º 14.197, de 1 de septiembre de 2021, por la que se modifica el Código Penal y se deroga la Ley de Seguridad Nacional de 1983.

([320]) Artículo 3 del Decreto n.º 8.793/2016, de 29 de junio de 2016, sobre la política nacional de inteligencia. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

([321]) Introducción, párrafo primero, del Decreto n.º 8.793/2016, de 29 de junio de 2016, sobre la política nacional de inteligencia. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

(205) Los datos a los que se puede acceder y que se pueden analizar para prevenir los delitos contra la seguridad nacional mencionados anteriormente incluyen información a la que las autoridades públicas que forman parte del SISBIN han accedido en el marco de sus operaciones y de conformidad con las condiciones descritas en los considerandos 165 a 187 de la presente Decisión (es decir, con una autorización judicial expedida para un fin claramente definido). Los datos compartidos con el SISBIN se tratan a través de un sistema electrónico cifrado seguro con registros de acceso para garantizar la trazabilidad y la auditabilidad de la información ([322]). Como ha aclarado el Tribunal Supremo Federal, el intercambio de datos con el SISBIN está sujeto a los principios de la LGPD, incluidos los de limitación de la finalidad (artículo 6, inciso I, de la LGPD), minimización y exactitud de los datos (artículo 6, incisos III y V, de la LGPD), transparencia (artículo 6, inciso VI, de la LGPD), seguridad de los datos (artículo 6, inciso VII, de la LGPD) y limitación del plazo de conservación (artículo 6, apartados I, III, IV y artículo 16 de la LGPD) ([323]).

(206) El artículo 2 de la ley por la que se crea el sistema de inteligencia brasileño indica que solo forman parte de este sistema las autoridades públicas. El SISBIN está compuesto por la Agencia Brasileña de Inteligencia (ABIN) y por representantes de los centros de inteligencia, ministerios, secretarías y agencias de la Administración Pública Federal. La lista de autoridades que son miembros del SISBIN se recoge en un decreto sobre la organización y el funcionamiento del sistema ([324]).

(207) La ABIN es el órgano central del sistema de inteligencia y es responsable de planificar, ejecutar, coordinar, supervisar y controlar las actividades de inteligencia. Estas actividades deberán llevarse a cabo utilizando medios y técnicas confidenciales basados en la información. Para el desempeño de sus funciones, la ABIN recibe información y datos específicos de las distintas autoridades públicas integrantes del SISBIN en el ámbito de la seguridad nacional. Las autoridades pertenecientes al SISBIN están obligadas a facilitar esta información ([325]), ya que la ley no autoriza a la ABIN a recopilar información por propia iniciativa. La legalidad de la obligación de compartir datos por parte de los integrantes del SISBIN fue impugnada ante el Tribunal Supremo Federal ([326]). En su sentencia de 2021, el Tribunal Supremo Federal aclaró que cualquier transmisión de datos de las autoridades públicas a la ABIN debe realizarse en observancia de los fines estrictos de interés público (por ejemplo, la defensa de las instituciones públicas y el interés nacional) y recordó que la finalidad específica y legítima de cada actividad de intercambio de datos se define mediante un procedimiento formal que se rige por una autorización judicial que lo define ([327]). Estas limitaciones también se aplican a cualquier otro intercambio de datos entre autoridades públicas ([328]).

(208) Por último, el tratamiento de datos realizado a través del SISBIN debe proteger la información del acceso de personas u organismos no autorizados. El artículo 5 del decreto sobre el funcionamiento del SISBIN exige explícitamente que la coordinación y el intercambio de datos entre los miembros de las autoridades del sistema cumplan «la legislación relativa al secreto profesional y la seguridad, la protección de los datos personales y la

([322]) Véase el folleto del SISBIN, 2024, p. 18. Puede consultarse en el siguiente enlace: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

([323]) Tribunal Supremo Federal. Decisión sobre la ADI 6649, septiembre de 2022. Puede consultarse en el siguiente enlace: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([324]) Artículo 7 del Decreto n.º 11.693, de 6 de septiembre de 2023, sobre la organización y el funcionamiento del SISBIN. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Entre las autoridades pertenecientes al SISBIN se encuentran: el Centro de Inteligencia del Ministerio de Defensa, la Dirección de Inteligencia Penitenciaria de la Secretaría Nacional del Ministerio de Justicia y Seguridad Pública, la Secretaría General de Relaciones Exteriores del Ministerio de Asuntos Exteriores y la Dirección de Inteligencia de la Policía Federal.

([325]) Artículo 4 de la Ley n.º 9.883 de 7 de diciembre de 1999. Ley por la que se crea el sistema de inteligencia de Brasil. Puede consultarse en el siguiente enlace: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

([326]) Tribunal Supremo Federal, Decisión sobre la ADI 6529 de 15 de octubre de 2021. Puede consultarse en el siguiente enlace: https://www.jusbrasil.com.br/jurisprudencia/stf/1303041724/inteiro-teor-1303041733.

([327]) Tribunal Supremo Federal, Decisión sobre la ADI 6529 de 15 de octubre de 2021, p. 22.

([328]) Tribunal Supremo Federal, Decisión sobre la ADI 6529 de 15 de octubre de 2021, p. 3.

seguridad de la información y el conocimiento», legislación esta que incluye a la LGPD, como principal instrumento jurídico de Brasil para la protección de los datos personales ([329]). El artículo 6 de este Decreto precisa además que la información intercambiada por las autoridades en el SISBIN deberá respetar «el principio de seguridad jurídica, necesidad e interés público» y obedecer a un objetivo legítimo ([330]). El SISBIN también reconoce la importancia de cumplir la LGPD en sus materiales públicos y procedimientos internos ([331]).

(209) Las competencias de las autoridades que efectúan el tratamiento de datos con fines de seguridad nacional en Brasil están, por tanto, limitadas por normas claras y precisas recogidas en la ley y sujetas a una serie de garantías. Estas garantías incluyen, en particular, la supervisión de la ejecución de dichas medidas, con medidas como la aprobación judicial previa o la limitación de la duración del acceso y la retención de la información en consonancia con los principios de necesidad y proporcionalidad.

3.3.2. *Utilización ulterior de la información*

(210) El tratamiento de datos personales recogidos por las autoridades brasileñas con fines de seguridad nacional está sujeto a los principios de limitación de la finalidad (artículo 6, inciso I, de la LGPD), licitud y lealtad del tratamiento (artículos 6 y 7 de la LGPD), minimización y exactitud de los datos (artículo 6, incisos III y V, de la LGPD), transparencia (artículo 6, inciso VI, de la LGPD), seguridad de los datos (artículo 6, inciso VII, de la LGPD) y limitación del plazo de conservación (artículo 6, incisos I, III, IV y artículo 16 de la LGPD).

(211) La posible divulgación de datos personales a terceros (incluidos terceros países y a través de acuerdos internacionales) solo podrá realizarse de conformidad con los principios de la LGPD, tras haber evaluado el cumplimiento de los principios constitucionales de necesidad y proporcionalidad y garantizar la continuidad de la protección y el cumplimiento de los derechos de los interesados (artículo 2 del Reglamento sobre Transferencia de Datos).

3.3.3. *Supervisión*

(212) Las actividades de las autoridades brasileñas de seguridad son supervisadas por distintos organismos. El decreto sobre la Estrategia Nacional de Inteligencia de Brasil señala la importancia de contar con varios niveles de mecanismos de supervisión para proteger el «Estado de Derecho democrático» ([332]). El Tribunal Supremo Federal recordó la importancia de esta supervisión en un asunto relativo al tratamiento de datos en el marco del SISBIN, afirmando que «la efectividad de las actividades de inteligencia está a menudo vinculada al secreto del proceso y de la información recopilada. En el Estado de Derecho democrático, esta función está sujeta al control externo de los poderes legislativo y judicial al objeto de determinar si el secreto impuesto es adecuado para los objetivos públicos estrictos a los que se dirige» ([333]).

(213) En primer lugar, existe un control por parte de la Rama Ejecutiva que garantiza que los objetivos que debe alcanzar el sistema de inteligencia, las políticas que deben aplicarse y los planes formulados responden adecuadamente a las demandas de la sociedad. El Ejecutivo también es responsable de garantizar que el gasto de los servicios de inteligencia se lleve a cabo de forma racional y se dedique exclusivamente a acciones legítimas, necesarias y útiles para el Estado. En Brasil este control lo ejerce la Cámara de Relaciones Exteriores y Defensa Nacional del Consejo de Gobierno, que es responsable de supervisar la ejecución de la Policía Nacional de Inteligencia, y por la Oficina de Seguridad Institucional, que se encarga de coordinar las actividades de inteligencia a escala federal ([334]).

([329]) Artículo 5 del Decreto n.º 11.693, de 6 de septiembre de 2023, sobre la organización y el funcionamiento del SISBIN.

([330]) Artículo 6 del Decreto n.º 11.693, de 6 de septiembre de 2023, sobre la organización y el funcionamiento del SISBIN.

([331]) Véase, por ejemplo, el folleto sobre el SISBIN, p. 9: «Uno de los objetivos de este reposicionamiento es aumentar los niveles de trazabilidad y transparencia de los procesos internos del SISBIN mediante la adopción de herramientas y plataformas digitales diseñadas específicamente para estos fines. Estas herramientas deben estar en consonancia con el marco jurídico establecido por la Ley sobre el Acceso a la Información y la Ley General de Protección de Datos (LGPD), ambas promulgadas en 2012». Puede consultarse en el siguiente enlace: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

([332]) Sección 2.4, apartado 4, del Decreto de 15 de diciembre de 2017 sobre una Estrategia Nacional de Inteligencia.

([333]) Tribunal Supremo Federal, Decisión de 15 de octubre de 2021, p. 2.

([334]) Sección 2.4 del Decreto de 15 de diciembre de 2017 sobre una Estrategia Nacional de Inteligencia. Puede consultarse en el siguiente enlace: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm.

(214) En segundo lugar, el poder legislativo ejerce un control en lo que respecta a las actividades de inteligencia. Dicho control tiene por objeto verificar tanto la legitimidad como la eficacia de la actividad de inteligencia. Los jefes de los partidos mayoritarios y minoritarios de la Cámara de Diputados y del Senado Federal, así como los presidentes de las Comisiones de Relaciones Exteriores y Defensa Nacional de la Cámara de Diputados y del Senado Federal, forman parte del órgano externo de supervisión de las actividades de inteligencia denominado Comisión Mixta para el Control de las Actividades de Inteligencia («Comissão mista de Controle da Atividade de Inteligência», en lo sucesivo, la «CCAI») ([335]). El control del poder legislativo sobre las actividades de inteligencia se estableció mediante la ley por la que se creó el sistema de inteligencia brasileño en 1999. La función de supervisión y las competencias de la CCAI se reforzaron considerablemente con la adopción en 2013 de una resolución vinculante del Congreso ([336]). Esta resolución trató las deficiencias que se habían detectado previamente para avanzar en el proceso de institucionalizar la CCAI y dotarla de una estructura y una secretaría permanentes, además de aclarar sus competencias y aumentar la transparencia de sus actividades. La función, las actividades y las competencias de la CCAI están estipuladas por ley y se detallan en dicha resolución. La CCAI supervisa y controla las actividades de inteligencia llevadas a cabo por los órganos de la administración pública federal, en particular los que integran el SISBIN, con el fin de garantizar que las actividades se lleven a cabo de conformidad con la Constitución y de proteger los derechos y garantías de las personas, de la sociedad y del Estado ([337]). La CCAI puede llevar a cabo revisiones *a posteriori*, así como auditorías y controles de las operaciones en curso ([338]). Los miembros de la CCAI tienen la máxima autorización para acceder a los documentos. La CCAI elabora informes anuales de sus actividades, sin incluir información que pueda poner en peligro la seguridad nacional ([339]). Como se detalla en el considerando 222 de la presente Decisión, la CCAI también puede recibir e investigar las denuncias de particulares.

(215) En tercer lugar, la ANPD supervisa el cumplimiento de los parámetros definidos por la LGPD por parte de las autoridades nacionales de seguridad en sus actividades de tratamiento de datos personales. La LGPD se aplica parcialmente al tratamiento de datos personales realizado con fines de seguridad pública, defensa nacional, seguridad del Estado o actividades de investigación y enjuiciamiento de infracciones penales ([340]). En este contexto, la ANPD puede ejercer las competencias correctivas y de investigación que le confiere la LGPD. Por ejemplo, la ANPD puede, en cualquier momento, llevar a cabo auditorías de todas las autoridades públicas, incluida la agencia de inteligencia ([341]).

(216) Por último, el Poder Judicial resolverá las demandas de los ciudadanos contra las autoridades públicas y, en este contexto, podrá supervisar las actividades realizadas con fines de seguridad nacional para garantizar el cumplimiento de todos los derechos constitucionales y del marco legislativo pertinente, incluida la LGPD. Las resoluciones de los órganos jurisdiccionales pueden recurrirse ante el Tribunal Supremo Federal y también ante la Corte Interamericana de Derechos Humanos.

3.3.4. *Reparación*

(217) El sistema brasileño ofrece distintas vías judiciales y administrativas para obtener reparación, entre ellas la indemnización por daños y perjuicios. Estos mecanismos ofrecen a los interesados soluciones administrativas y judiciales efectivas que les permiten, en particular, hacer valer sus derechos, en especial el derecho a acceder a sus datos personales o a obtener la rectificación o supresión de dichos datos.

([335]) Artículo 6, apartado 1, de la Ley n.º 9.883 de 7 de diciembre de 1999. Ley por la que se crea el sistema de inteligencia de Brasil.

([336]) Resolución n.º 2 de 2021-CN sobre la Comisión Mixta para el Control de las Actividades de Inteligencia (CCAI). Puede consultarse en el siguiente enlace: https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html.

([337]) Sección 2.4 del Decreto de 15 de diciembre de 2017 sobre una Estrategia Nacional de Inteligencia.

([338]) Véase, en particular, el artículo 3 de la Resolución n.º 2 de 2021-CN sobre la Comisión Mixta para el Control de las Actividades de Inteligencia (CCAI).

([339]) Artículo 13, resolución n.º 2 de 2021-CN sobre la Comisión Mixta para el Control de las Actividades de Inteligencia (CCAI). La información sobre las reuniones y los documentos elaborados por la CCAI están disponibles en línea y se actualizan periódicamente en: https://legis.senado.leg.br/atividade/comissoes/comissao/449/ and https://www.congressonacional.leg.br/legislacao-e-publicacoes/glossario-legislativo/-/legislativo/termo/comissao_mista_de_controle_das_atividades_de_inteligencia_ccai_cn.

([340]) Artículo 4 de la Ley n.º 13.709, de 14 de agosto de 2018 (Ley General de Protección de Datos).

([341]) Artículo 55-J, inciso XI, de la Ley n.º 13.709, de 14 de agosto de 2018 [*Lei Geral de Proteção de Dados Pessoais* (Ley General de Protección de Datos)].

(218) Como se detalla en el considerando 9 de la presente Decisión, el acceso a las vías de reparación está garantizado para los nacionales brasileños y de terceros países, independientemente de que se encuentren o no en el territorio nacional.

(219) En primer lugar, las personas tienen un derecho «absoluto» a interponer una demanda relativa a la protección de sus derechos. De conformidad con las normas generales establecidas en el Código Procesal Civil, para interponer una demanda ante los órganos jurisdiccionales, una persona no tiene que demostrar un perjuicio (es decir, no tiene que demostrar que está sometida a vigilancia o que sus datos han sido tratados con fines de seguridad nacional). Puede ejercer sus derechos en virtud del *habeas data* en lo que respecta a los datos objeto de tratamiento por parte de las autoridades de inteligencia ([342]).

(220) En el procedimiento de reparación ante los órganos jurisdiccionales, la persona podrá solicitar una indemnización por daños y perjuicios. Como ocurre con el tratamiento de datos con fines de garantía del cumplimiento del Derecho penal, la Constitución federal y el Código Procesal Civil establecen la base jurídica para reclamar una indemnización por los daños morales o materiales causados por la autoridad pública que haya recopilado o utilizado ilegalmente datos, también a través de acciones colectivas ([343]).

(221) En segundo lugar, el Tribunal Supremo Federal ha confirmado la aplicación parcial de la LGPD a los fines de seguridad nacional y, por extensión, las competencias de la ANPD para tramitar las reclamaciones relacionadas con el tratamiento de datos personales por parte de las autoridades públicas con dichos fines ([344]). En la misma sentencia, el órgano jurisdiccional señaló que «el tratamiento de datos personales efectuado por organismos públicos en contravención de los parámetros jurídicos y constitucionales dará lugar a la responsabilidad civil del Estado por los daños sufridos por las personas», de conformidad con el artículo 42 de la LGPD ([345]).

(222) En tercer lugar, la CCAI puede recibir e investigar denuncias de cualquier ciudadano, partido político o asociación relativas a violaciones de los derechos y garantías fundamentales cometidas por organismos y entidades públicos que lleven a cabo actividades de inteligencia y contrainteligencia ([346]). Sobre esta base, la CCAI puede llevar a cabo controles o investigaciones. Por lo tanto, la CCAI proporciona una vía administrativa adicional para la reparación en caso de violación de los derechos relacionados con el tratamiento de datos con fines de seguridad nacional. Las reclamaciones recibidas por la CCAI pueden remitirse posteriormente a los órganos jurisdiccionales.

(223) Los diferentes recursos judiciales disponibles con arreglo al régimen brasileño permiten a las personas obtener reparación, en particular, impugnar la legalidad de las acciones de las autoridades públicas y de inteligencia. Asimismo, pueden obtener una indemnización por daños y perjuicios.

4. **CONCLUSIÓN**

(224) La Comisión considera que la República Federativa de Brasil, a través de la LGPD, garantiza un nivel de protección de los datos personales transferidos desde la Unión Europea que es esencialmente equivalente al otorgado por el Reglamento (UE) 2016/679.

(225) Por otra parte, la Comisión estima que, en su conjunto, los mecanismos de supervisión y las vías de reparación contempladas en el Derecho brasileño permiten detectar y abordar en la práctica las infracciones de las normas de protección de datos cometidas por los responsables y encargados del tratamiento en Brasil y ofrecen al interesado soluciones jurídicas para obtener acceso a sus datos personales y, en su caso, su rectificación o supresión.

([342]) Véase el considerando 9 de la presente Decisión.

([343]) Véase, por ejemplo, el artículo 43 de la Ley n.º 10.408, de 10 de enero de 2002. Código Procesal Civil. Puede consultarse en el siguiente enlace: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm y el artículo 1 de la Ley n.º 7.397 de 24 de julio de 1985 (Ley de Responsabilidad Civil). Puede consultarse en el siguiente enlace: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm.

([344]) Véanse los considerandos 31 y 162 de la presente Decisión y la Decisión del Tribunal Supremo Federal sobre la ADI 6649, de 15 de septiembre de 2022. Puede consultarse en el siguiente enlace: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([345]) Tribunal Supremo Federal, Decisión sobre la ADI 6649 de 15 de septiembre de 2022, punto 8. Puede consultarse en el siguiente enlace: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([346]) Artículo 3, inciso XI, de la Resolución n.º 2 de 2021-CN sobre la Comisión Mixta para el Control de las Actividades de Inteligencia (CCAI).

(226) Por último, con arreglo a la información disponible acerca del ordenamiento jurídico de Brasil, la Comisión considera que toda injerencia en aras del interés público, en particular con fines de garantía del cumplimiento del Derecho penal y de seguridad nacional, por parte de las autoridades públicas de Brasil en relación con los derechos fundamentales de las personas cuyos datos personales son transferidos desde la Unión Europea a Brasil se limitará a lo estrictamente necesario para la consecución del objetivo legítimo perseguido, y estima además que existe una tutela judicial efectiva contra tales injerencias.

(227) Por consiguiente, en vista de las conclusiones de la presente Decisión procede estimar que Brasil garantiza un nivel de protección adecuado de los datos personales transferidos desde la Unión a responsable y en cargados del tratamiento con arreglo a la LGPD, en el sentido del artículo 45 del Reglamento (UE) 2016/679, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

5. EFECTOS DE LA PRESENTE DECISIÓN Y ACTUACIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

(228) Los Estados miembros y sus organismos están obligados a adoptar las medidas necesarias para dar cumplimiento a los actos de las instituciones de la Unión, ya que estos disfrutan de una presunción de legalidad y producen, por consiguiente, efectos jurídicos en tanto no hayan sido revocados, anulados en el marco de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad.

(229) Por lo tanto, toda decisión de adecuación de la Comisión adoptada en virtud del artículo 45, apartado 3, del Reglamento (UE) 2016/679 vincula a todos los organismos de los Estados miembros destinatarios, incluidas sus autoridades de control independientes. En particular, pueden producirse transferencias de un responsable o encargado del tratamiento en la Unión a responsables o encargados del tratamiento en Brasil sin que sea necesario obtener ninguna autorización adicional.

(230) Cabe recordar que, de conformidad con el artículo 58, apartado 5, del Reglamento (UE) 2016/679 y como explicó el Tribunal de Justicia en la sentencia Schrems, cuando una autoridad nacional de protección de datos cuestiona, en especial a raíz de una reclamación, la compatibilidad de una decisión de adecuación de la Comisión con los derechos fundamentales del particular a la privacidad y la protección de los datos, el Derecho nacional debe prever las vías de acción para exponer las alegaciones correspondientes ante los tribunales nacionales, a los que podrá pedirse que planteen una cuestión prejudicial al TJUE ([347]).

6. SUPERVISIÓN, SUSPENSIÓN, DEROGACIÓN O MODIFICACIÓN DE LA PRESENTE DECISIÓN

(231) De conformidad con la jurisprudencia del TJUE ([348]) y tal como se reconoce en el artículo 45, apartado 4, del Reglamento (UE) 2016/679, la Comisión debe supervisar de manera continuada los acontecimientos en el tercer país después de la adopción de la decisión de adecuación, para evaluar si el tercer país todavía garantiza un nivel de protección equivalente en lo esencial. Debe procederse obligatoriamente a tal control, en cualquier caso, cuando la Comisión sea informada de algún indicio que genere una duda razonable al respecto.

(232) Por consiguiente, la Comisión debe efectuar una supervisión continuada de la situación en Brasil en lo que respecta al marco jurídico y a la práctica real relacionada con el tratamiento de los datos personales evaluada en la presente Decisión. A este respecto, debe prestarse especial atención a la aplicación en la práctica de los requisitos para la evaluación de impacto relativa a la protección de datos; los requisitos de transparencia y su posible limitación en relación con los derechos a la información y al acceso; las normas sobre notificación de violaciones de la seguridad de los datos; el régimen de sanciones, así como el cumplimiento de las limitaciones y salvaguardias con respecto al acceso del Gobierno, teniendo en cuenta cualquier novedad pertinente al respecto.

([347]) Schrems I, apartado 65: «A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta».

([348]) Schrems I, apartado 76.

(233) Para facilitar el proceso de seguimiento, se invita a las autoridades brasileñas, incluida la ANPD, a informar a la Comisión de toda novedad pertinente para la presente Decisión, en lo que respecta al tratamiento de datos personales por parte de los operadores económicos y las autoridades públicas, así como a las limitaciones y garantías aplicables al acceso de las autoridades públicas a los datos personales.

(234) Además, a fin de que la Comisión pueda desempeñar eficazmente su función de supervisión, los Estados miembros deben informarle de toda medida pertinente tomada por las autoridades nacionales de protección de datos, en particular en lo que respecta a las consultas o las reclamaciones de los interesados de la UE en relación con la transferencia de datos personales desde la UE a los responsables y encargados del tratamiento en Brasil. También debe informarse a la Comisión de todo indicio de que las medidas de las autoridades públicas brasileñas responsables de la seguridad nacional o de la prevención, la investigación, la detección o la persecución de las infracciones penales no garantizan el nivel de protección necesario.

(235) En aplicación del artículo 45, apartado 3, del Reglamento (UE) 2016/679 ([349]) y teniendo en cuenta el hecho de que el nivel de protección que ofrece el ordenamiento jurídico de Brasil puede ser objeto de modificación, la Comisión, tras la adopción de la presente Decisión, debe revisar periódicamente si las conclusiones relativas a la adecuación del nivel de protección garantizado por Brasil siguen estando justificadas de hecho y de Derecho.

(236) A tal fin, la presente Decisión debe someterse a una primera revisión en un plazo de cuatro años después de su entrada en vigor. Las revisiones periódicas posteriores deben realizarse al menos cada cuatro años ([350]). Las revisiones deben abarcar todos los aspectos del funcionamiento de la presente Decisión, incluida la cooperación de la ANPD con las autoridades de protección de datos de la Unión en relación con las reclamaciones de particulares. Deben comprender asimismo la eficacia de la supervisión y la ejecución, en el ámbito de la garantía del cumplimiento del Derecho penal y la seguridad nacional.

(237) Al proceder a la revisión, la Comisión debe reunirse con la ANPD, acompañada en su caso de otras autoridades brasileñas responsables del acceso de las autoridades públicas, incluidos los correspondientes organismos de supervisión. La participación en esta reunión debe estar abierta a los representantes de los miembros del Comité Europeo de Protección de Datos. En el marco de la revisión, la Comisión debe solicitar a la ANPD que facilite información exhaustiva sobre todos los aspectos pertinentes a efectos de la constatación de adecuación, en particular sobre las limitaciones y garantías relativas al acceso de las autoridades públicas. La Comisión también debe pedir explicaciones sobre cualquier información pertinente para la presente Decisión que haya recibido, en particular los informes públicos elaborados por las autoridades brasileñas u otras partes interesadas de Brasil, el Comité Europeo de Protección de Datos, las distintas autoridades de protección de datos, los grupos de la sociedad civil, los informes de los medios de comunicación o cualquier otra fuente de información disponible.

(238) Sobre la base de la revisión, la Comisión debe elaborar un informe público que presentará al Parlamento Europeo y al Consejo.

(239) Cuando la información disponible, en particular la información resultante de la labor de supervisión respecto de la presente Decisión o proporcionada por las autoridades brasileñas o de los Estados miembros, muestre que el nivel de protección conferido por Brasil puede que ya no sea adecuado, la Comisión debe informar de ello a las autoridades competentes brasileñas y solicitar que se tomen medidas apropiadas dentro del plazo razonable que se fije.

(240) Si, al vencer dicho plazo, las autoridades brasileñas competentes no han tomado dichas medidas o no han demostrado satisfactoriamente de otro modo que se sigue garantizando un nivel de protección adecuado a efectos de la presente Decisión, la Comisión debe iniciar el procedimiento a que se refiere el artículo 93, apartado 2, del Reglamento (UE) 2016/679 con el fin de suspender o derogar, total o parcialmente, la presente Decisión.

(241) De manera alternativa, la Comisión iniciará este procedimiento con miras a modificar la Decisión, en particular mediante la imposición de condiciones adicionales para las transferencias de datos o limitando el alcance de la conclusión de adecuación solo a las transferencias de datos para las que se sigue garantizando un nivel adecuado de protección.

([349]) De conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, «[e]l acto de ejecución establecerá un mecanismo de revisión periódica, […] que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional».

([350]) El artículo 45, apartado 3, del Reglamento (UE) 2016/679 establece que debe procederse a una revisión periódica «al menos cada cuatro años». Véase también CEPD, Adequacy Referential, WP 254 rev. 01.

(242) La Comisión debe considerar asimismo la posibilidad de iniciar el procedimiento conducente a la modificación, suspensión o derogación de la presente Decisión, en el contexto de la revisión o si, por otro motivo, las autoridades competentes brasileñas no proporcionan la información o las aclaraciones necesarias para la evaluación del nivel de protección de los datos personales transferidos desde la UE a Brasil o en relación con el cumplimiento de la presente Decisión. A este respecto, la Comisión debe tener en cuenta en qué medida puede obtenerse la información pertinente de otras fuentes.

(243) Por razones imperiosas de urgencia debidamente justificadas, la Comisión debe hacer uso de la competencia de adoptar, de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3, del Reglamento (UE) 2016/679, actos de ejecución inmediatamente aplicables que suspendan, deroguen o modifiquen la presente Decisión.

7. **CONSIDERACIONES FINALES**

(244) El Comité Europeo de Protección de Datos publicó su correspondiente dictamen ([351]), que se ha tenido en cuenta en la elaboración de la presente Decisión.

(245) Las medidas previstas en la presente Decisión se ajustan al dictamen del comité creado en virtud del artículo 93, apartado 1, del Reglamento (UE) 2016/679.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

A efectos del artículo 45 del Reglamento (UE) 2016/679, Brasil garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a los responsables y encargados del tratamiento de Brasil sujetos a la Ley General de Protección de Datos.

Artículo 2

Cuando las autoridades competentes de los Estados miembros, a fin de proteger a los particulares en lo que respecta al tratamiento de sus datos personales, ejerzan los poderes otorgados por el artículo 58 del Reglamento (UE) 2016/679 en relación con las transferencias de datos a que se refiere el artículo 1, el Estado miembro en cuestión informará sin demora a la Comisión.

Artículo 3

1. La Comisión realizará un seguimiento continuo de la aplicación del marco jurídico en el que se sustenta la presente Decisión, a fin de evaluar si Brasil sigue garantizando un nivel de protección adecuado a efectos del artículo 1.

2. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que la Autoridad de Protección de Datos de Brasil (Agência Nacional de Proteção de Dados o ANPD) o cualquier otra autoridad brasileña competente no garantice el cumplimiento del marco jurídico en el que se sustenta la presente Decisión.

3. Los Estados miembros y la Comisión se informarán recíprocamente de cualquier indicio de que las injerencias de las autoridades públicas brasileñas en el derecho de las personas a la protección de sus datos personales van más allá de lo estrictamente necesario, o de que no existe una tutela judicial efectiva frente a tales injerencias.

4. Cuatro años después de la fecha de notificación de la presente Decisión a los Estados miembros y posteriormente al menos cada cuatro años, la Comisión evaluará la constatación mencionada en el artículo 1 sobre la base de toda la información disponible, incluida la información recibida como parte de la revisión realizada junto con las autoridades brasileñas pertinentes.

([351]) Comité Europeo de Protección de Datos, dictamen sobre una decisión de adecuación relativa a Brasil, noviembre de 2025. Puede consultarse en el siguiente enlace: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282025-regarding-european-commission-draft_es.

5. Siempre que la Comisión tenga indicios de que ya no se garantiza un nivel adecuado de protección, informará a las autoridades competentes de Brasil y podrá suspender, derogar o modificar la presente Decisión.

6. La Comisión podrá suspender, derogar o modificar la presente Decisión cuando la falta de cooperación del Gobierno de Brasil le impida determinar si la conclusión formulada en el artículo 1 de la presente Decisión se ve afectada.

Artículo 4

Los destinatarios de la presente Decisión son los Estados miembros.

Hecho en Bruselas, el 26 de enero de 2026.

Por la Comisión
Michael McGRATH
Miembro de la Comisión