Dictamen 28/2025, sobre el proyecto de Decisión de Ejecución de la Comisión Europea relativa a la adecuación del nivel de protección de los datos personales conferido por Brasil con arreglo al Reglamento (UE) 2016/679

Versión 1.0

Adoptado el 04 de noviembre de 2025

Translations proofread by EDPB Members.

This language version has not yet been proofread.

ADOPTADO

Resumen

El 5 de septiembre de 2025, la Comisión Europea inició el proceso de adopción de su proyecto de Decisión de Ejecución (en lo sucesivo, «proyecto de Decisión») relativa a la adecuación del nivel de protección de los datos personales conferido por la República Federativa de Brasil (en lo sucesivo, «Brasil»).

El 5 de septiembre de 2025, la Comisión Europea solicitó el dictamen del Comité Europeo de Protección de Datos (en lo sucesivo, «CEPD»). La evaluación del CEPD relativa a la adecuación del nivel de protección de los datos personales conferido por Brasil se ha realizado sobre la base del examen del propio proyecto de Decisión, así como sobre la base de un análisis de la documentación que está a disposición del público en los sitios web oficiales de las autoridades brasileñas.

El CEPD se centró en la evaluación tanto de los aspectos generales del Reglamento General de Protección de Datos (en lo sucesivo, «RGPD») del proyecto de Decisión como del acceso por parte de las autoridades públicas a los datos personales transferidos desde el EEE a efectos de aplicación de la ley y seguridad nacional, incluidas las vías de recurso disponibles para los particulares en el EEE. El CEPD también evaluó si las garantías previstas en el marco jurídico de Brasil están en vigor y son eficaces.

El CEPD ha utilizado como referencia principal para este trabajo el documento Referencias sobre adecuación adoptado el 28 de noviembre de 2017 por el Grupo de Trabajo[2] del Artículo 29, revisado por última vez y adoptado el 6 de febrero de 2018 por el CEPD (en lo sucesivo, «Referencias sobre adecuación») y las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia.

El CEPD observa positivamente que el marco de protección de datos, en particular la Ley General de Protección de Datos de Brasil (en lo sucesivo, «LGPD»), junto con los decretos presidenciales y los reglamentos vinculantes promulgados por la Agencia Nacional de Protección de Datos de Brasil (en lo sucesivo, «ANPD»), establecen requisitos (también en relación con los principios, los derechos de los interesados, las transferencias, la supervisión y las reparaciones) que se ajustan estrechamente al RGPD y a la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «TJUE»).

El CEPD también concluyó que la Comisión Europea debería aclarar en el proyecto de Decisión determinados aspectos del marco jurídico de Brasil y seguir de cerca su evolución.

En relación con el principio de rendición de cuentas y los requisitos para la evaluación de impacto relativa a la protección de datos (en lo sucesivo, «EIPD»), el CEPD considera importante la obligación de llevarla a cabo en los casos en que el tratamiento pueda dar lugar a un alto riesgo para los derechos y libertades de las personas físicas y que la EIPD abarque la evaluación de la necesidad y la proporcionalidad del tratamiento. Por lo tanto, el CEPD invita a la Comisión Europea a supervisar la aplicación práctica de estos requisitos.

La LGPD prevé una limitación del suministro de información a los interesados o a la autoridad de control sobre la base del «secreto comercial e industrial» en determinados

[1] 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.

[2] Grupo de Trabajo del Artículo 29, WP 254 rev. 01, adoptado el 28 de noviembre de 2017 y revisado y adoptado por última vez el 6 de febrero de 2018, refrendado por el CEPD.

casos. Teniendo en cuenta la importancia de los requisitos de transparencia para la posibilidad de los interesados de controlar cómo se tratan sus datos, así como la importancia de las obligaciones de cooperar con la autoridad de control, en particular para proporcionar la información necesaria para sus tareas de control, el CEPD invita a la Comisión Europea a supervisar la aplicación de estas limitaciones en la práctica para comprender mejor su repercusión en los derechos de información y acceso, así como en los poderes de la ANPD, en su caso.

En relación con las normas sobre transferencias ulteriores, el CEPD invita a la Comisión Europea a aclarar en el proyecto de Decisión si las transferencias pueden llevarse a cabo de conformidad con condiciones, equivalentes a las del artículo 49 del RGPD, únicamente en las circunstancias excepcionales en las que no puedan utilizarse otros instrumentos para la transferencia. También se invita a la Comisión a que aclare si se informa a los interesados acerca de: los posibles riesgos de la transferencia cuando ello se base en su consentimiento y en las circunstancias de la transferencia (duración y finalidad de la transferencia, países de destino, responsabilidades de las partes implicadas, derechos de los interesados y medios para ejercerlos), independientemente de la herramienta de transferencia utilizada.

Además, el CEPD invita a la Comisión Europea a profundizar en las tareas del Consejo Nacional para la Protección de los Datos Personales y de la Privacidad y su interacción con la ANPD.

En relación con el acceso y el uso por parte de las autoridades públicas brasileñas de los datos personales transferidos a los responsables y encargados del tratamiento en Brasil con fines de control de la aplicación del Derecho penal y de seguridad nacional (en lo sucesivo, «acceso gubernamental»), el CEPD señala que la LGPD no se aplica al tratamiento de datos realizado con fines *exclusivos* de seguridad pública, defensa nacional, seguridad del Estado o investigación y enjuiciamiento de delitos. Al mismo tiempo, el CEPD observa positivamente que el Tribunal Supremo Federal de Brasil, en su jurisprudencia, ha interpretado la LGPD de una manera que amplía su aplicabilidad parcial al tratamiento de datos personales para las investigaciones penales y el mantenimiento del orden público.

En vista de ello, invita a la Comisión a que siga evaluando y aclarando en el proyecto de Decisión la aplicabilidad de la LGPD en caso de tratamiento de datos personales a efectos de la aplicación del Derecho penal, incluidos los poderes en materia de investigación y correctivos de la ANPD con respecto a las autoridades encargadas de garantizar el cumplimiento de la ley, y a que tenga muy en cuenta cualquier novedad pertinente a este respecto como parte de su obligación de supervisión.

Teniendo presente el hecho de que se concede a los Estados un amplio margen de apreciación a la hora de definir las cuestiones de seguridad nacional, lo que permite entonces exenciones de seguridad nacional en el tratamiento de datos personales, el CEPD invita a la Comisión a describir y explicar con mayor precisión en el proyecto de Decisión el esbozo del concepto de seguridad nacional con arreglo a la legislación brasileña. En relación con esto, el CEPD invita a la Comisión a que aclare en mayor medida cómo se relacionan las exenciones de la LGPD con fines de seguridad nacional con la recogida y el intercambio de datos entre las entidades públicas dentro del Sistema Brasileño de Inteligencia (en lo sucesivo, «SISBIN»).

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra s), del 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 (en lo sucesivo, «RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, «EEE»), y en particular su anexo XI y su Protocolo n.º 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[3],

Vistos los artículos 12 y 22 de su Reglamento interno,

HA APROBADO EL SIGUIENTE DICTAMEN:

[3] Las referencias a los «Estados miembros» en el presente dictamen deben entenderse como referencias a los «Estados miembros del EEE».

1. INTRODUCCIÓN

(1) El capítulo V del RGPD establece condiciones para transferencias de datos personales a terceros países u organizaciones internacionales. Las transferencias de datos personales pueden tener lugar sobre la base de una decisión de adecuación de la Comisión Europea (artículo 45 del RGPD) o, en ausencia de dicha decisión de adecuación, cuando el responsable o el encargado del tratamiento ofrezcan garantías adecuadas, incluidos derechos exigibles y acciones legales para el interesado (artículo 46 del RGPD). En ausencia de una decisión de adecuación o de garantías adecuadas, una transferencia o un conjunto de transferencias a un tercer país o a una organización internacional solo tendrá lugar en determinadas condiciones (artículo 49 del RGPD).

(2) El CEPD recuerda que las decisiones de adecuación reconocen la protección continua de los datos personales transferidos desde el EEE a terceros países u organizaciones internacionales y son una herramienta sólida de transferencia para garantizar la protección de los derechos del interesado cuando los datos se transfieren fuera del EEE. Según las Referencias sobre adecuación[4] y la jurisprudencia pertinente del TJUE[5], si bien el tercer país no tiene que proporcionar un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión, la expresión «nivel de protección adecuado» que figura en el artículo 45, apartado 1, del RGPD debe entenderse en el sentido de que exige que ese tercer país garantice efectivamente, con arreglo a su legislación nacional o a sus compromisos internacionales, un nivel de protección de los derechos y libertades fundamentales esencialmente equivalente al garantizado en la Unión, interpretado a la luz de la Carta de los Derechos Fundamentales.

(3) Brasil es una República Federativa compuesta por la unión de los veintiséis Estados y el Distrito Federal, tal como se establece en su Constitución federal (en lo sucesivo, «la Constitución»)[6]. Los Estados brasileños también tienen sus propias constituciones, que no deben contravenir la Constitución federal. La privacidad y la protección de datos están protegidas por la Constitución como derechos fundamentales (artículo 5, puntos X, XII y LXXIX, de la Constitución)[7] y reconocidas por el Tribunal Constitucional a cualquier persona, incluida una persona extranjera, independientemente de que dicha persona resida o no en Brasil[8].

(4) El principal acto legislativo que regula la protección de datos es la Ley General de Protección de Datos (n.º 13.709, de 14 de agosto de 2018, modificada en último lugar por la Ley n.º 14.460, de 25 de octubre de 2022). La LGPD se complementa con los decretos vinculantes (Decreto presidencial n.º 10.474, de 26 de agosto de 2020, y Decreto presidencial n.º 11.758, de 30 de octubre de 2023), que son jurídicamente vinculantes y ejecutables[9].

[4] Grupo de Trabajo del Artículo 29, WP 254 rev. 01, adoptado el 28 de noviembre de 2017 y revisado y adoptado por última vez el 6 de febrero de 2018, refrendado por el CEPD, capítulo 3, letra C.
[5] TJUE, 6 de octubre de 2015, sentencia en el asunto C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems») y Tribunal General, 3 de septiembre de 2025, sentencia en el asunto T-553/23, Philippe Latombe/Comisión Europea («Latombe»).
[6] Véase el considerando 7 del proyecto de Decisión.
[7] Véase el considerando 8 del proyecto de Decisión.
[8] Véase el considerando 9 del proyecto de Decisión.
[9] Véanse los considerandos 11 y 12 del proyecto de Decisión.

(5) Además de la LGPD, el marco brasileño de protección de datos incluye reglamentos vinculantes promulgados por la Agencia Nacional de Protección de Datos [10]. Estos reglamentos establecen normas adicionales sobre la interpretación y aplicación de la LGPD[11]. Por ejemplo, el Reglamento n.º 4, de 24 de febrero de 2024, relativo a la aplicación de sanciones administrativas, el Reglamento n.º 15, de 24 de abril de 2024, relativo a la notificación de incidentes de seguridad (en lo sucesivo, «Reglamento sobre notificaciones de incidentes de seguridad»), el Reglamento n.º 19, de 23 de agosto de 2024, relativo a la transferencia internacional de datos personales (en lo sucesivo, «Reglamento sobre transferencia de datos»), el Reglamento n.º 2, de 27 de enero de 2022, relativo a la aplicación de la LGPD a las pequeñas y medianas empresas, el Reglamento n.º 18, de 15 de julio de 2024, relativo al papel del delegado de protección de datos (en lo sucesivo, «Reglamento sobre el DPD»).

(6) El CEPD acoge con satisfacción el reconocimiento constitucional de los derechos a la privacidad y a la protección de datos como derechos fundamentales, aplicados en mayor medida a través del Derecho nacional. Además, el CEPD toma nota positivamente de los compromisos internacionales contraídos por Brasil[12].

(7) El CEPD señala que, de conformidad con los artículos 47 y 94 del Reglamento (UE) 2018/1725, las instituciones[13], órganos y organismos de la Unión Europea pueden transferir datos personales a un tercer país, territorio, sector u organización internacional que, a juicio de la Comisión Europea en virtud del artículo 45, apartado 3, del Reglamento (UE) 2016/679, garantice un nivel de protección adecuado, siempre que la transferencia sirva únicamente a tareas que sean competencia del responsable del tratamiento, sin necesidad de autorización adicional. El CEPD invita a la Comisión Europea a recordar esta posibilidad jurídica en los considerandos del proyecto de Decisión.

2. ASPECTOS GENERALES RELATIVOS A LA PROTECCIÓN DE DATOS

2.1 Rendición de cuentas y gobernanza de los datos

(8) La LGPD establece el principio de rendición de cuentas como uno de los principios generales aplicables al tratamiento de datos personales. Según esta, los responsables y encargados del tratamiento[14] adoptarán las medidas técnicas y organizativas adecuadas para cumplir eficazmente sus obligaciones en materia de protección de datos y deben poder demostrar dicho cumplimiento, entre otras cosas, a la autoridad de control competente (artículo 46 de la LGPD). El CEPD señala que dichas medidas incluyen la designación de un delegado de protección de datos (artículo 41 de la LGPD), tal como se detalla en el Reglamento sobre el DPD de la ANPD; la evaluación de impacto relativa a la protección de datos (artículo 38 de la LGPD), así como el mantenimiento de registros de las actividades de tratamiento de datos

[10] Todos los reglamentos vinculantes promulgados por la ANPD pueden consultarse en la siguiente dirección: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd.
[11] Véase el considerando 13 del proyecto de Decisión.
[12] Véanse los considerandos 8 a 10 del proyecto de Decisión.
[13] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).
[14] Agentes de tratamiento, de conformidad con el artículo 5, punto IX, de la LGPD.

(artículo 37 de la LGPD). Además, la LGPD establece que los responsables y encargados del tratamiento pueden formular normas internas para modelos de buenas prácticas y gobernanza, incluidos planes de actividades educativas, mecanismos de supervisión interna y reducción de riesgos (artículo 50 de la LGPD). El CEPD observa positivamente que estos instrumentos son similares a los previstos en el RGPD para aplicar el principio de rendición de cuentas y acoge con satisfacción esta estrecha armonización.

(9) El CEPD señala que, en lo que respecta a la EIPD, la LGPD no incluye una obligación clara de llevar a cabo la EIPD en los casos en que el tratamiento pueda dar lugar a un alto riesgo para los derechos y libertades de las personas físicas, en los que solo se refiere a la posible solicitud de la ANPD. A este respecto, el CEPD señala que la ANPD recomienda llevar a cabo una EIPD cuando la operación de tratamiento pueda dar lugar a un alto riesgo en las «preguntas frecuentes»[15] relacionadas con la EIPD (en lo sucesivo, «preguntas frecuentes sobre la EIPD»). Además, la LGPD no incluye explícitamente la evaluación de la necesidad y la proporcionalidad en el ámbito de aplicación de la EIPD. Sin embargo, las preguntas frecuentes sobre la EIPD recomiendan a los responsables y encargados del tratamiento que evalúen en sus EIPD la necesidad y proporcionalidad del tratamiento.

(10) En este contexto, el CEPD invita a la Comisión Europea a supervisar la aplicación práctica de estos requisitos para verificar que la EIPD se lleve a cabo cuando la operación de tratamiento pueda dar lugar a un alto riesgo para los derechos y libertades de las personas físicas y que la evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en relación con los fines también se incluya en las EIPD.

2.2 Ámbito de aplicación y definiciones

(11) El capítulo 3 de las Referencias sobre adecuación se dedica a los «Principios relativos al contenido» y hace referencia a conceptos y principios básicos sobre protección de datos. Un sistema de un tercer país o de una organización internacional debe contener tales conceptos y principios básicos para garantizar un nivel de protección de los datos personales esencialmente equivalente al garantizado por el Derecho de la Unión. Estos no deben imitar la terminología del RGPD, pero deben reflejar los conceptos consagrados en la legislación de la UE en materia de protección de datos y ser coherentes con ellos. Las Referencias sobre adecuación se refieren a los siguientes conceptos importantes: «datos personales», «tratamiento de datos personales», «responsables del tratamiento», «encargado del tratamiento», «destinatario» y «datos sensibles». Este aspecto de la legislación brasileña se comentará en los apartados siguientes.

2.2.1 Ámbito de aplicación material y territorial de la LGPD

(12) El CEPD acoge con satisfacción que el ámbito de aplicación de la LGPD, tanto material como territorial, sea muy similar al previsto en el marco de protección de datos de la UE.

(13) El artículo 4 de la LGPD excluye de su ámbito de aplicación el tratamiento con fines puramente personales y no económicos, y tales excepciones también están previstas en el RGPD [artículo 2, apartado 2, letra c), del RGPD]. Además, algunas otras operaciones de tratamiento quedan parcialmente fuera del ámbito de aplicación de la LGPD, en particular el tratamiento para: la seguridad pública, la defensa nacional, la legislación estatal o la

[15] https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

investigación y el enjuiciamiento de delitos; fines periodísticos y artísticos; investigación académica; investigación sanitaria (artículo 3, punto III, de la LGPD). Esta cuestión se detalla con más profundidad en el anexo 3.1 del presente Dictamen.

(14) Por lo que se refiere específicamente a la aplicación parcial de la LGPD al tratamiento de datos personales realizado con fines periodísticos y artísticos, el CEPD señala que el ámbito de aplicación de la excepción es equivalente al establecido en el artículo 85, apartado 2, del RGPD[16], es decir, que dicha excepción se aplica únicamente cuando los datos personales se tratan exclusivamente para tales fines, y todo otro tratamiento por parte de la prensa, los medios de comunicación y los organismos artísticos entra en el ámbito de aplicación de la LGPD. Asimismo, siguen siendo aplicables algunas excepciones previstas para el tratamiento de los datos personales con fines exclusivamente académicos, a saber, los artículos 7 (requisitos de la base jurídica) y 11 (normas sobre el tratamiento de datos sensibles) de la LGPD[17]. El ámbito de aplicación de estas excepciones también está en consonancia con el establecido en el artículo 85, apartado 2, del RGPD.

2.2.2 Definiciones

(15) El CEPD acoge favorablemente la armonización con el marco de protección de datos de la UE en relación con las definiciones utilizadas en la LGPD, que son coherentes con las previstas en el RGPD. En particular, la LGPD define los «datos personales», «información seudónima», «datos anónimos»[18], «tratamiento de datos», «responsable del tratamiento», «encargado del tratamiento» y «datos sensibles» (artículo 5 de la LGPD) de manera similar a como se definen en el RGPD, a saber, el considerando 26, el artículo 4 y el artículo 9, apartado 1. Otras definiciones, como «interesado», «delegado de protección de datos», «consentimiento», «evaluación de impacto relativa a la protección de datos» y un concepto de «corresponsabilidad del tratamiento»[19], también son esencialmente equivalentes a los conceptos previstos en el RGPD.

2.3 Principios y bases jurídicas de la protección de datos

2.3.1 Principios del tratamiento

(16) La Referencias sobre adecuación, de conformidad con el RGPD, establecen que el tratamiento de los datos debe ser lícito, leal y legítimo. De conformidad con el artículo 6 de la LGDP, las actividades de tratamiento de datos personales se llevarán a cabo de buena fe y estarán sujetas a los siguientes principios: finalidad, adecuación, necesidad, libre acceso[20], calidad de los datos, transparencia, seguridad, prevención, no discriminación, responsabilidad y rendición de cuentas.

[16] Véase igualmente el considerando 35 del proyecto de Decisión.
[17] Véanse igualmente los considerandos 32 y 33 del proyecto de Decisión.
[18] El artículo 12 de la LGPD detalla además que los datos anonimizados no se consideran datos personales, salvo cuando la anonimización se haya revertido o pueda revertirse empleando esfuerzos razonables. Según este artículo, la determinación de lo que se considera «razonable» debe basarse en 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.
[19] Véase el artículo 42, apartado 1, punto I, de la LGPD.
[20] «Libre acceso: garantía a los interesados de una consulta facilitada y gratuita sobre la forma y la duración del tratamiento, así como sobre la integridad de sus datos personales» (artículo 6, punto IV, de la LGPD).

(17) Teniendo en cuenta los conceptos de estos principios, el sistema jurídico brasileño consagra los mismos principios relativos al tratamiento de datos establecidos en el artículo 5 del RGPD. Por ejemplo, en relación con la limitación de la finalidad, la LGPD establece en su artículo 7, apartado 7, que «el tratamiento posterior de los datos personales a que se refieren los apartados 3 (datos personales de acceso público) y 4 (datos hechos manifiestamente públicos por el interesado) del presente artículo podrá llevarse a cabo con nuevos fines, siempre que se respeten los fines legítimos y específicos para el nuevo tratamiento y la preservación de los derechos del interesado, así como los motivos y principios establecidos en la presente Ley».

(18) El RGPD exige claramente que tal tratamiento posterior solo se lleve a cabo si esa nueva finalidad es compatible con la finalidad inicial. El requisito de garantizar la compatibilidad de los fines (así como el cumplimiento de las normas éticas aplicables y las garantías técnicas y jurídicas) se destaca en la Guía para el tratamiento de datos personales con fines académicos y para la realización de estudios e investigaciones publicada por la ANPD, así como en las Directrices sobre el interés legítimo. La ANPD, en las Directrices sobre el interés legítimo, explica cómo el responsable del tratamiento debe demostrar un vínculo efectivo entre los dos fines del tratamiento y tener en cuenta la «confianza legítima» del interesado. Estas Directrices aclaran además que «El análisis de la confianza legítima puede basarse en varios factores, entre los que cabe destacar los siguientes: d) la finalidad prevista de la recogida de datos y su compatibilidad con el tratamiento basado en un interés legítimo». El CEPD acoge con satisfacción esta aclaración de la ANPD, que contribuye a armonizar mejor los requisitos de la limitación de la finalidad.

(19) El principio de limitación del plazo de conservación previsto en el RGPD establece que los datos solo se almacenarán durante no más tiempo del necesario para los fines del tratamiento [artículo 5, apartado 1, letra e), del RGPD]. Aunque el artículo 6 de la LGPD no incluye explícitamente el principio de limitación del plazo de conservación, este artículo debe leerse en relación con el artículo 15 de la LGPD, que especifica el requisito en caso de finalización del tratamiento de datos. En este artículo, el principio de limitación del plazo de conservación está claramente vinculado a los principios de «adecuación» y «necesidad» que forman parte de los principios generales que figuran en el artículo 6 de la LGPD. En aras de una mayor claridad, el CEPD anima a la Comisión Europea a aclarar en el proyecto de Decisión la interacción de los artículos 6 y 15 de la LGPD en relación con el principio de limitación del plazo de conservación.

(20) Además, en lo que respecta a los requisitos de limitación del plazo de conservación, el artículo 16 de la LGPD establece las condiciones para la conservación y la supresión de los datos personales una vez finalizado el tratamiento. Este artículo también prevé cuatro fines para los que los datos pueden conservarse una vez finalizado el tratamiento de datos: 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. El CEPD señala que estas situaciones de tratamiento están en consonancia con el principio de limitación del plazo de conservación consagrado en el RGPD.

(21) El principio de transparencia y lealtad tiene por objeto garantizar que los interesados tengan control sobre sus datos personales y, a tal fin, la información se facilitará al interesado de

manera proactiva por regla general[21]. Mientras tanto, la LGPD establece una limitación a este principio en lo que respecta al «secreto comercial e industrial» que puede afectar a los interesados a la hora de recibir información sobre su tratamiento de datos para poder ejercer su control sobre él (por ejemplo, mediante la presentación de la reclamación ante la ANPD). Sin embargo, la Comisión Europea explica en el proyecto de Decisión que esta limitación debe interpretarse a la luz de la Ley de acceso a la información de Brasil y del Decreto presidencial n.º 7.721, de 16 de mayo de 2012, y que, por lo tanto, debe interpretarse de manera que el tratamiento y la divulgación de información no revelen secretos comerciales ni generen una ventaja competitiva para otros agentes, cumpliendo al mismo tiempo 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[22].

(22) A la luz de la importancia del principio de transparencia, el CEPD invita a la Comisión Europea a supervisar la aplicación de esta disposición en la práctica para comprender mejor su repercusión en el derecho de información y acceso.

2.3.2 Medidas de seguridad e infracciones

(23) La LGPD incluye los principios de seguridad y prevención que exigen la aplicación de medidas para la protección de los datos personales y la prevención de daños y perjuicios relacionados con dicho tratamiento (artículo 6, puntos VII y VIII, de la LGPD). Además, la LGPD indica explícitamente que, cuando no se aplican adecuadamente las medidas de seguridad, el tratamiento de datos se considera ilícito. La ley exige aplicar las medidas necesarias para demostrar el cumplimiento de este principio mediante el enfoque basado en el riesgo (artículos 44, 46 y 47 de la LGPD) y cumplir los requisitos para la evaluación y notificación de infracciones (artículos 48 y 49 de la LGPD). El CEPD observa con satisfacción que dichos principios y obligaciones están estrechamente alineados con los establecidos en el RGPD.

(24) El CEPD acoge con satisfacción la adopción de un Reglamento sobre notificaciones de incidentes de seguridad adicional vinculante por parte de la ANPD que prevé el concepto del incidente y detalles para la evaluación de su gravedad (por ejemplo, cuando se considere que el incidente crea riesgos para los interesados o afecta significativamente a los intereses y derechos fundamentales de los interesados y, por tanto, se comunicará a la ANPD y al interesado), así como sobre los requisitos de notificación de incidentes[23]. A este respecto, el CEPD señala que, de conformidad con el Reglamento sobre notificaciones de incidentes de seguridad, como norma general, «el responsable del tratamiento debe llevar a cabo la comunicación de un incidente de seguridad a la ANPD en un plazo de tres días hábiles»[24], e invita a la Comisión Europea a adaptar en consecuencia su proyecto de Decisión (considerando 75)[25].

(25) En relación con la notificación de violaciones de la seguridad de los datos, el CEPD señala que la LGPD establece que dicha notificación (tanto a la ANPD como al interesado) incluirá,

[21] Esto también se destaca en las Referencias sobre adecuación, véase el capítulo 3, letra A, apartado 7.
[22] Véase el considerando 81 del proyecto de Decisión.
[23] Véanse los considerandos 73 a 77 del proyecto de Decisión.
[24] Véanse los artículos 6 y 9 del Reglamento sobre notificaciones de incidentes de seguridad.
[25] Véase el considerando 75 del proyecto de Decisión según el cual «La notificación de un incidente de seguridad a la ANPD y a los interesados tendrá lugar en un plazo de tres días (setenta y dos horas) a partir del momento en que el responsable del tratamiento tenga conocimiento de este».

entre otras cosas, información sobre las medidas técnicas y de seguridad utilizadas para la protección de los datos personales, adoptadas antes y después del incidente, respetando secretos comerciales e industriales (artículo 6, punto III, y artículo 9, punto II, de la LGPD). El CEPD entiende la necesidad de garantizar eficazmente que el derecho a la privacidad y a la protección de datos no afecte negativamente a la protección de otros derechos e invita a la Comisión a supervisar la aplicación de dicha limitación cuando se haya facilitado parcialmente información sobre el incidente (teniendo en cuenta los secretos comerciales e industriales), y su repercusión en los poderes de la ANPD, en su caso.

2.3.3 Licitud del tratamiento

(26) El CEPD señala que el principio de licitud y su aplicación, tal como se prevé en la LGPD (artículo 5, punto XII, y artículos 7, 8 y 10), está estrechamente alineado con el consagrado en el RGPD (artículo 4, punto 11, y artículos 6, 7 y 9) y acoge con satisfacción esta armonización.

2.3.3.1 Interés legítimo

(27) Los requisitos del interés legítimo que debe utilizarse como base jurídica para el tratamiento en la LGPD (artículo 7, punto IX) se ajustan al RGPD [artículo 6, apartado 1, letra f)]. La LGPD también subraya que, por lo general, deben prevalecer los derechos y libertades fundamentales (que incluyen el derecho a la protección de datos[26]).

(28) El CEPD señala que el artículo 10 de la LGPD enumera los fines legítimos para los que podría utilizarse dicha base jurídica. Uno de estos fines legítimos es apoyar y promover la actividad del responsable del tratamiento (artículo 10, punto I, de la LGPD).

(29) Aunque esta expresión parece ser amplia, el CEPD señala que las condiciones para que se utilice el «interés legítimo» se describen con más detalle en la Guía «Bases jurídicas para el tratamiento de datos personales: Interés legítimo» (en lo sucesivo, «Guía sobre interés legítimo») adoptada por la ANPD. En esta guía se 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[27]. Estas condiciones son similares a los tres requisitos acumulativos definidos y explicados por el TJUE[28] para que el tratamiento de datos personales sea lícito con arreglo a esta base jurídica. Además, las condiciones para el «interés legítimo» especificadas en la Guía sobre interés legítimo son similares a las de las Directrices adoptadas por el CEPD[29]. El CEPD acoge con satisfacción el enfoque adoptado por la ANPD en relación con el interés legítimo y su uso para el tratamiento.

2.4 Derechos individuales

(30) El CEPD acoge con satisfacción que la LGPD otorgue a las personas derechos similares a los establecidos en el RGPD (ambos en el capítulo III). En particular, la LGPD contempla el derecho de acceso, el derecho de rectificación, el derecho a la portabilidad de los datos, el

[26] Véase la sección 3 del presente Dictamen.
[27] Véase el considerando 52 del proyecto de Decisión.
[28] Por ejemplo, TJUE, 7 de diciembre de 2023, sentencia en los asuntos acumulados C-26/22 y C-64/22, SCHUFA Holding AG, apartados 75 a 80.
[29] *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Version 1.0)* [«Directrices 1/2024 sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD (versión 1.0)», documento en inglés], adoptadas el 8 de octubre de 2024.

derecho a la limitación del tratamiento, el derecho de supresión, el derecho a la información, el derecho a denegar o retirar el consentimiento, y el derecho a oponerse al tratamiento y el derecho de petición (artículos 9 y 18 de la LGPD).

(31) La LGPD también otorga a los interesados el derecho a solicitar la revisión de las decisiones adoptadas únicamente sobre la base del tratamiento automatizado de datos personales que afecten a sus intereses (artículo 20 de la LGPD). El contenido del artículo 20 de la LGPD refleja, en esencia, el artículo 22 del RGPD.

(32) El CEPD señala que, en relación con los derechos de los interesados, la Ley brasileña de datos *habeas data* establece disposiciones específicas para conceder el derecho de acceso y el derecho de rectificación en un breve plazo (diez y quince días, respectivamente) de la solicitud de una persona, y acoge con satisfacción este aspecto.

(33) El EDPD considera que la LGPD establece requisitos esencialmente equivalentes para los derechos de los interesados a los garantizados en el RGPD.

2.5 Restricciones a transferencias ulteriores

(34) Las Referencias sobre adecuación aclaran que el nivel de protección de las personas físicas cuyos datos personales se transfieren en virtud de una decisión de adecuación no debe verse menoscabado por la transferencia ulterior y, por tanto, las transferencias ulteriores «solo se permitirán cuando otro destinatario (el destinatario de la transferencia ulterior) también esté sujeto a normas (incluidas normas contractuales) que otorguen un nivel de protección adecuado y cumplan las instrucciones pertinentes al tratar los datos en nombre del responsable del tratamiento».

(35) En relación con la evaluación de la adecuación del marco jurídico y la práctica de Brasil, por «transferencia ulterior» se entiende la transferencia de datos personales de la entidad, que actúa como responsable del tratamiento, dentro del ámbito de aplicación territorial de la LGPD de Brasil, a la entidad no incluida en este ámbito.

(36) Los requisitos relativos a la transferencia ulterior se establecen en el capítulo V de la LGPD y se complementan con la ANPD mediante la adopción del «Reglamento sobre transferencia de datos», que establece las definiciones de «transferencia», «transferencia internacional de datos», «importador» y «exportador» e incluye requisitos detallados para las transferencias

(37) El CEPD observa positivamente que la definición de «transferencia» y de «transferencia internacional de datos» está en consonancia con las de las Directrices 05/2021 del CEPD[30].

(38) De conformidad con la LGPD y el Reglamento sobre transferencia de datos, las transferencias ulteriores solo pueden tener lugar con fines legítimos, específicos y explícitos y cuando existan instrumentos o condiciones específicos (artículo 33 de la LGPD y artículos de 9 a 33 del Reglamento sobre transferencia de datos)[31]. El CEPD estima que estos instrumentos se aproximan a las herramientas de transferencia previstas en el capítulo V del RGPD. Sin embargo, el CEPD invita a la Comisión Europea a aclarar en el proyecto de Decisión si las transferencias pueden llevarse a cabo de conformidad con el artículo 33, puntos III a IX, de

[30] *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* [«Directrices 05/2021 sobre la interacción entre la aplicación del artículo 3 y las disposiciones sobre transferencias internacionales de conformidad con el capítulo V del RGPD», documento en inglés], apartado 9, adoptadas el 14 de febrero de 2023.
[31] Véanse igualmente los considerandos 101 a 109 del proyecto de Decisión.

la LGPD únicamente en las circunstancias excepcionales, cuando no se cumplan las condiciones establecidas en el artículo 33, puntos I a II, de la LGPD[32].

(39) Sin embargo, el Reglamento sobre transferencia de datos especifica que las transferencias internacionales de datos personales están permitidas «cuando el interesado haya dado un consentimiento específico y distinguible para dicha transferencia, con información previa sobre el carácter internacional de la operación prevista, distinguiéndola claramente de otros fines». No queda claro si este requisito implica la obligación de informar a los interesados sobre los posibles riesgos de las transferencias internacionales derivados de la ausencia de una protección adecuada en el tercer país y la ausencia de garantías adecuadas (por ejemplo, información de que podría no haber una autoridad de control o principios de tratamiento de datos o derechos de los interesados en el tercer país), lo que constituye un requisito en virtud del artículo 49, apartado 1, letra a), del RGPD. Para el CEPD, y en virtud del RGPD, el suministro de esta información es fundamental para que el interesado pueda dar su consentimiento informado con pleno conocimiento de causa de estos hechos específicos de la transferencia. Así pues, el CEPD invita a la Comisión Europea a aclarar en el proyecto de Decisión si el interesado está informado de los posibles riesgos de dicha transferencia derivados de la ausencia de una protección adecuada en el tercer país y de garantías adecuadas.

(40) Además, el Reglamento sobre la transferencia de datos incluye que «tanto el responsable como el encargado del tratamiento adoptarán medidas eficaces que puedan demostrar el cumplimiento y la observancia de las normas de protección de datos personales y la eficacia de dichas medidas, de manera compatible con el nivel de riesgo del tratamiento y con la modalidad de transferencia internacional utilizada» (artículo 4, apartado 2, del Reglamento sobre transferencia de datos). El CEPD acoge con satisfacción la inclusión de esta obligación. Al mismo tiempo, sería beneficioso aclarar que la eficacia de estas medidas debe evaluarse para garantizar también que la legislación local del tercer país de que se trate no menoscabe la continuidad de la protección de los interesados cuyos datos se transfieren[33]. El CEPD invita a la Comisión Europea a aclarar que este elemento también se tendrá en cuenta en los escenarios de transferencia.

(41) El CEPD acoge con satisfacción la inclusión de un requisito explícito de transparencia en relación con el interesado, es decir, los interesados tienen derecho a recibir el instrumento contractual utilizado para la transferencia ulterior, así como la descripción de dicha transferencia, por ejemplo, la duración y la finalidad de la transferencia, los países de destino, las responsabilidades de las partes implicadas, los derechos de los interesados y los medios para ejercerlos (artículo 16 del Reglamento sobre transferencia de datos).

(42) Sin embargo, parece que este alcance de la obligación de transparencia solo es pertinente cuando las transferencias se realizan sobre la base de cláusulas contractuales tipo y no cuando se utilizan otras herramientas[34]. Por lo tanto, el CEPD invita a la Comisión Europea a

[32] El artículo 49 del RGPD especifica que las excepciones previstas en este artículo solo pueden utilizarse en ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46 del RGPD.

[33] Véase la sentencia Latombe. Véase también TJUE, 16 de julio de 2020, sentencia en el asunto C-311/18 («Schrems II»).

[34] Por ejemplo, el Reglamento sobre transferencia de datos incluye requisitos generales de transparencia cuando se pretende utilizar las NCV, en particular «el establecimiento y la aplicación de un programa de gobernanza de la privacidad que tenga por objeto establecer una relación de confianza con el interesado, mediante acciones transparentes que garanticen mecanismos para la participación del interesado» (artículo 25, punto V, del Reglamento sobre transferencia de datos) y transparencia en relación con el ejercicio de los derechos y el derecho de reclamación del interesado (artículo 26, punto VI, del Reglamento sobre transferencia de datos).

aclarar que se aplican las mismas obligaciones de transparencia independientemente de la herramienta de transferencia utilizada.

(43) El CEPD también señala que los requisitos relativos al contenido de las normas corporativas vinculantes (en lo sucesivo, «NCV») no están plenamente en consonancia con los del RGPD, en particular el artículo 47, apartado 2, letras f) y l), del RGPD. Con el fin de garantizar que el nivel de protección ofrecido por el RGPD no se vea menoscabado, el CEPD invita a la Comisión Europea a aclarar en el proyecto de Decisión que también se tendrán en cuenta estos elementos [35] cuando esta herramienta de transferencia deba utilizarse para las transferencias ulteriores de datos personales transferidos a Brasil en virtud de la decisión de adecuación.

2.6 Mecanismos relativos al procedimiento y la ejecución

(44) Según las Referencias sobre adecuación[36] y la jurisprudencia pertinente del TJUE[37], un sistema de protección de datos esencialmente equivalente al modelo de la Unión Europea debe prever: i) una autoridad independiente, que debe supervisar y hacer cumplir la legislación en materia de protección de datos, con el poder de investigar y actuar sin influencia externa. Los sistemas de protección de datos deben garantizar que: ii) los responsables y encargados del tratamiento de datos rindan cuentas y sean conscientes de sus responsabilidades, al tiempo que se informa a los interesados de sus derechos. Deben establecerse sanciones y procesos de verificación eficaces para garantizar el cumplimiento de las normas; iii) los responsables y encargados del tratamiento demuestren el cumplimiento, a través de medidas como las evaluaciones de impacto relativas a la protección de datos, los registros de las actividades de tratamiento y el nombramiento de delegados de protección de datos; y iv) el sistema de protección de datos ofrezca apoyo y ayuda a los interesados individuales en el ejercicio de sus derechos y mecanismos de reparación adecuados.

(45) En esta sección, el CEPD ha centrado su evaluación en la existencia de una autoridad independiente, de un mecanismo de reparación adecuado y de sanciones efectivas.

2.6.1 Supervisión independiente

(46) La LGPD establece la Agencia Nacional de Protección de Datos (ANPD) como la autoridad de control nacional responsable del seguimiento y la ejecución de sus disposiciones.

(47) El CEPD acoge con satisfacción el hecho de que se haya concedido a la ANPD el estatuto de «autoridad de carácter especial», una designación destinada a garantizar la autonomía necesaria para ejercer plenamente las funciones y los poderes jurídicos que le confiere la LGPD, en particular mediante la revocación de disposiciones que subordinaban el funcionamiento y las operaciones financieras de la ANPD a las autorizaciones que debía conceder el Ejecutivo.

(48) Del mismo modo, el CEPD acoge con satisfacción los cambios introducidos el 15 de septiembre de 2025 en el marco jurídico brasileño, según el cual la ANPD se reconoce ahora

[35] Responsabilidad y cooperación con la autoridad de control [artículo 47, apartado 2, letras f) y l), del RGPD].
[36] Véase el capítulo 3, letra C, de las Referencias sobre adecuación.
[37] TJUE, 6 de octubre de 2015, sentencia en el asunto C-362/14, Schrems.

como **agencia reguladora**[38]. El CEPD entiende que, por lo tanto, uno de los principales cambios es que la ANPD presentará su presupuesto directamente al Ministerio de Planificación y Presupuesto en lugar de tener que presentarlo a través del Ministerio de Justicia. El presupuesto de la ANPD sigue siendo una línea separada en el presupuesto federal del Estado. El CEPD entiende que la ANPD ya tenía independencia sobre su presupuesto y financiación, pero, al convertirse en una agencia reguladora, su proceso administrativo se simplifica.

(49) El CEPD también acoge con satisfacción la nueva competencia de la ANPD, que recientemente ha sido designada como autoridad responsable de la protección de los menores en línea[39]. El CEPD toma nota de que, de conformidad con el capítulo IX de la LGPD, la ANPD cuenta con los poderes y las misiones necesarios y disponibles para garantizar el cumplimiento de los derechos de protección de datos y promover la sensibilización, como los poderes de investigación y sanción (artículo 55-J de la LGPD).

(50) En relación con el personal y el presupuesto de la ANPD, que desempeña un papel en su independencia, el CEPD toma nota positivamente de la reciente decisión de aumentar el personal con más de doscientos nuevos puestos[40].

(51) El CEPD observa, de conformidad con el artículo 55-C de la LGPD, que (actualmente) la ANPD está compuesta por una serie de organismos[41], entre ellos el Consejo Nacional para la Protección de los Datos Personales y de la Privacidad (en lo sucesivo, «Consejo»). El CEPD toma nota de su composición, que también incluye representantes del poder ejecutivo federal, del poder legislativo y del poder judicial[42]. El CEPD también señala que, de conformidad con el artículo 58-B de la LGPD, el Consejo es responsable, entre otras cosas, de: i) «proponer directrices estratégicas y proporcionar información de referencia para la elaboración de la política nacional para la protección de los datos personales y la privacidad y para las actividades de la ANPD»; y ii) «recomendar acciones que debe llevar a cabo la ANPD».

(52) Con especial atención a estas tareas, el CEPD considera importante comprender mejor cómo se aplican y en qué medida las propuestas y recomendaciones del Consejo influyen en el trabajo de la ANPD. Por consiguiente, invita a la Comisión Europea a que siga profundizando en estas tareas y en la interacción entre el Consejo y la ANPD, a fin de evaluar mejor la influencia del Consejo en las actividades de la ANPD.

2.6.2 Reparación

(53) El CEPD acoge con satisfacción el mecanismo de reparación previsto por la LGPD, que también otorga a los interesados el derecho a presentar una reclamación ante la ANPD y a impugnar su decisión presentando un recurso ante su Consejo de Administración. A continuación, los interesados pueden recurrir las decisiones del Consejo ante los órganos

[38] Medida provisional n.º 1.317/2025, disponible en https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.
[39] Ley n.º 15.211/2025 relativa a la protección de niños y menores en el entorno digital, disponible en https://www.in.gov.br/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619.
[40] https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.
[41] Según el artículo 55-C de la LGPD, la ANPD está compuesta por: el Consejo de Administración, el máximo órgano de gobierno; el Consejo Nacional para la Protección de los Datos Personales y de la Privacidad; la Oficina del Consejo de Disciplina; IV — la Oficina del Defensor del Pueblo; VI — la Oficina de Asuntos Jurídicos, y VI — las Unidades administrativas y unidades especializadas necesarias para la aplicación de las disposiciones de la LGDP. Véanse igualmente los considerandos 126 a 130 del proyecto de Decisión.
[42] Véase igualmente el considerando 132 del proyecto de Decisión y el artículo 55-C de la LGPD.

jurisdiccionales, así como presentar cualquier recurso contra la ANPD por incumplimiento de sus obligaciones en virtud de la LGPD. La diferencia entre el instrumento de apelación y el instrumento de recurso no se desprende claramente del proyecto de Decisión. El CEPD invita a la Comisión a que aclare en mayor medida el funcionamiento de estas dos vías, en particular si el recurso se limita únicamente a la negativa a tramitar una reclamación o a la desestimación en cuanto al fondo de una reclamación.

(54) Del mismo modo, el CEPD acoge con satisfacción la disposición del derecho a una indemnización por daños y perjuicios materiales y morales, así como del recurso colectivo (artículo 22 de la LGPD).

2.6.3 Sanciones

(55) El CEPD recuerda que la existencia de sanciones efectivas y disuasorias puede desempeñar un papel importante a la hora de garantizar el respeto de las normas de protección de datos, ya que es una señal del alto grado de rendición de cuentas y de concienciación que garantiza el sistema. El CEPD acoge con satisfacción los poderes correctivos que se le otorgan a la ANPD, que se han ejercido en varias ocasiones[43] e incluyen una serie de medidas, como la advertencia, multas de hasta el dos por ciento (2 %) de los ingresos brutos de la entidad jurídica privada implicada, multas diarias, el bloqueo de los datos personales relacionados con la infracción hasta su regularización, la suspensión temporal de las actividades de tratamiento de datos pertinentes y la supresión de los datos personales en cuestión (artículo 52 de la LGPD)[44]. El CEPD invita a la Comisión a supervisar su aplicación coherente, con especial atención a las sanciones.

(56) El CEPD acoge con satisfacción que la ANPD haya emitido un Reglamento sobre sanciones (vinculante). Este Reglamento clasifica las sanciones en diferentes niveles utilizando factores objetivos, como el tipo y el volumen de los datos tratados o la repercusión de los derechos de los interesados, y establece una metodología para el cálculo de las multas, que está en consonancia con los requisitos del artículo 83 del RGPD.

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

(57) De conformidad con el artículo 45, apartado 2, del RGPD, la evaluación de las limitaciones y garantías previstas en la legislación brasileña en lo que respecta al acceso y posterior uso por parte de las autoridades públicas brasileñas de los datos personales transferidos a los responsables y encargados del tratamiento en Brasil con fines de control de la aplicación del

[43] Véase la ANPD, Registro de Sanciones: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/decisoes-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.
[44] «Estas sanciones pueden imponerse a entidades públicas o privadas, con la excepción de multas y multas diarias, que no pueden imponerse a entidades públicas» (considerando 135 del proyecto de Decisión).

Derecho penal y de seguridad nacional (acceso gubernamental) es un elemento importante del criterio de la «equivalencia sustancial», tal como lo interpreta el TJUE.

(58) El CEPD valora positivamente la atención específica y la información fáctica facilitada por la Comisión sobre este aspecto en el proyecto de Decisión[45]. Por consiguiente, el CEPD se abstiene de reproducir en el presente Dictamen la mayor parte de las apreciaciones y análisis de los hechos. En su lugar, evalúa la interferencia del sistema brasileño para el acceso gubernamental con fines de control de la aplicación del Derecho penal y de seguridad nacional sobre la base de los cuatro elementos determinados por el CEPD en las garantías esenciales europeas para medidas de vigilancia, adoptadas el 10 de noviembre de 2020[46]:

- Garantía A: normas jurídicas claras, precisas y accesibles;
- Garantía B: necesidad y proporcionalidad con respecto a los objetivos legítimos perseguidos;
- Garantía C: mecanismo de supervisión independiente;
- Garantía D: vías de recurso eficaces y mecanismos de reparación a disposición del individuo.

3.1 Acceso y uso por parte de las autoridades públicas brasileñas a efectos de la aplicación del Derecho penal

3.1.1 Marco jurídico en el ámbito de la aplicación del Derecho penal

(59) El CEPD señala que el acceso a los datos personales y su posterior uso por parte de las autoridades brasileñas encargadas de garantizar el cumplimiento de la ley[47] están regulados por un sistema de actos jurídicos de distinta naturaleza jurídica. La protección de datos y la privacidad, incluido el secreto de la correspondencia y las comunicaciones, están consagradas en el artículo 5 de la Constitución como derechos fundamentales. El CEPD acoge con especial satisfacción que el alcance de la protección de estos derechos, al igual que en la UE, no se limite únicamente a los ciudadanos brasileños, sino que abarque también a los extranjeros que residen o no en Brasil[48].

(60) A continuación, existen varias leyes sectoriales especializadas que regulan el posible acceso a los datos personales a efectos de aplicación de la ley. Por lo que se refiere a este acceso a los datos transferidos a Brasil desde la UE, son especialmente pertinentes el Código Penal, la Ley relativa a la intercepción telefónica, el Marco civil para internet, la Ley relativa a la confidencialidad de las instituciones financieras, la Ley relativa a las organizaciones delictivas y las investigaciones penales, y otros. El CEPD señala que estos actos jurídicos son de acceso público y podrían considerarse suficientemente claros para dar a los interesados una indicación sobre las circunstancias y las condiciones en las que las autoridades públicas están facultadas para acceder a sus datos[49].

(61) Otra fuente importante de Derecho en Brasil es la jurisprudencia del Tribunal Supremo Federal de Brasil, que parece aplicar una interpretación amplia del alcance de los derechos

[45] Véanse los considerandos 152 a 217 del proyecto de Decisión.
[46] Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia.
[47] Véase la lista de autoridades en el considerando 165 del proyecto de Decisión.
[48] Véanse los considerandos 8 y 9 del proyecto de Decisión.
[49] Véase la sentencia del TEDH en el asunto Zakharov, apartado 229.

a la privacidad y a la protección de datos[50], así como la jurisprudencia de la Corte Interamericana de Derechos Humanos responsable de la interpretación y aplicación de la Convención Americana sobre Derechos Humanos, ratificada por Brasil en 1992[51].

(62) El CEPD observa que el ámbito de aplicación de la LGPD en caso de tratamiento de datos personales a efectos de la aplicación del Derecho penal es parcial, lo que puede dar lugar a inseguridad jurídica.

(63) Como reconoce la Comisión en el proyecto de Decisión, la LGPD no se aplica al tratamiento de datos realizado *exclusivamente* con fines de seguridad pública, defensa nacional, seguridad del Estado o investigación y enjuiciamiento de delitos[52]. De conformidad con el artículo 4, puntos I y III, de la LGPD, el tratamiento de datos en estos ámbitos se regirá por una legislación específica, que deberá incluir los principios y los derechos de los interesados descritos en la LGPD. Según el conocimiento del CEPD, confirmado por la Comisión, Brasil aún no ha adoptado legislación específica sobre el tratamiento de datos personales en el ámbito de la justicia penal y la aplicación de la ley (por ejemplo, similar a la Directiva sobre protección de datos en el ámbito penal[53]).

(64) Al mismo tiempo, el CEPD observa positivamente que el Tribunal Supremo Federal de Brasil, en su jurisprudencia[54], ha interpretado la LGPD de una manera que amplía su aplicabilidad parcial al tratamiento de datos personales para las investigaciones penales y el mantenimiento del orden público.

(65) El CEPD acoge con satisfacción que la autoridad de control de Brasil, la ANPD, apoye plenamente esta interpretación y sostiene que «la ausencia de legislación específica no concede una autorización amplia y sin restricciones a las agencias de seguridad para tratar datos personales de los ciudadanos con fines exclusivos de seguridad pública y de investigación y enjuiciamiento de delitos sin límites»[55]. Al mismo tiempo, el CEPD señala que, de conformidad con el artículo 4, punto III y apartado 3, de la LGPD, para algunos tratamientos específicos de datos realizados exclusivamente a efectos de aplicación de la ley, la ANPD parece tener en la actualidad principalmente una función consultiva con respecto a las autoridades encargadas de garantizar el cumplimiento de la ley.

(66) El CEPD invita a la Comisión a que siga evaluando y aclarando en el proyecto de Decisión la aplicabilidad de la LGPD en caso de tratamiento de datos personales a efectos de la aplicación del Derecho penal, incluidos los poderes de la ANPD, y a que tenga muy en cuenta cualquier desarrollo pertinente a este respecto como parte de su supervisión futura (véase igualmente la sección sobre supervisión y reparación).

3.1.2 Necesidad y proporcionalidad

(67) El CEPD observa con satisfacción que, por regla general, el acceso a los datos de comunicación, tanto el contenido como los metadatos, así como a otras categorías de

[50] Véase la Decisión del Tribunal Supremo Federal sobre la ADI 6649, de septiembre de 2022.
[51] Véase el considerando 10 del proyecto de Decisión.
[52] Véanse los considerandos 30 y 31 del proyecto de Decisión.
[53] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).
[54] Véase la Decisión del Tribunal Supremo Federal sobre la ADI 6649, de septiembre de 2022.
[55] Véase la nota técnica ANPD n.º 29/2024/FIS/CGF/ANPD, dirigida al Ministerio de Justicia y Seguridad Pública, punto 5.4.1.29, disponible en SEI/ANPD - 0132350 - Nota Técnica.

información confidencial protegida, como los datos bancarios y fiscales, requiere autorización judicial previa.

(68) Por lo que se refiere al acceso a los datos de comunicación, el CEPD acoge con satisfacción que, de conformidad con la Ley relativa a la interceptación telefónica y la jurisprudencia del Tribunal Supremo Federal, dicha medida se considere excepcional y esté sujeta a condiciones estrictas destinadas a garantizar su necesidad y proporcionalidad[56]. Además, como medida preventiva contra posibles abusos, el Derecho brasileño establece que la interceptación de comunicaciones sin autorización judicial o con fines no autorizados por la ley constituye un delito punible con hasta cuatro años de prisión[57].

(69) La estricta aplicación de las garantías para el acceso a los datos de comunicación es especialmente pertinente dada la existencia en Brasil de una obligación general de conservación de datos para los prestadores de servicios de conexión a internet y aplicaciones en línea mediante la cual se deben conservar los registros de conexión durante un año[58]. Aunque el CEPD observa positivamente que el acceso a los datos conservados solo es posible previa autorización judicial[59], recuerda el enfoque estricto y las restricciones a la conservación generalizada e indiscriminada de metadatos de comunicación en la UE[60] y toma nota positivamente de la información adicional facilitada por la Comisión en relación con la ausencia de conservación masiva de datos en el país. Por consiguiente, el CEPD anima a la Comisión a que preste especial atención al régimen jurídico y la práctica en Brasil en relación con el acceso a los datos de comunicación durante el seguimiento y la revisión del proyecto de Decisión.

(70) El CEPD observa positivamente que también se aplican garantías similares en lo que respecta al acceso por parte de las autoridades encargadas de garantizar el cumplimiento de la ley a los datos fiscales y bancarios, es decir, el requisito de autorización judicial previa, permitido únicamente para delitos graves, la existencia de sanciones penales en caso de abuso, etc.

(71) Según el proyecto de Decisión, existe una excepción al requisito general de autorización judicial previa para el acceso de las autoridades encargadas de garantizar el cumplimiento de la ley a determinadas categorías de datos personales[61]. De conformidad con los artículos 15 y 16 de la Ley relativa a las organizaciones delictivas y las investigaciones penales, un jefe de policía y la Fiscalía pueden acceder sin autorización judicial a los datos de registro de una persona investigada con respecto a lo siguiente: «cualificación personal, afiliación y dirección mantenida por el Tribunal Electoral, las empresas telefónicas, las entidades financieras, los proveedores de internet y los administradores de tarjetas de crédito»[62]. En la misma línea, las empresas de transporte permitirán, durante un período de cinco años, el acceso directo y permanente de un juez, de la Fiscalía o de un jefe de policía a las bases de datos de reservas y registros de viajes[63].

[56] Véanse los considerandos 169 y 170 del proyecto de Decisión.
[57] *Ibid*.
[58] Véase el considerando 173 del proyecto de Decisión.
[59] *Ibid*.
[60] Para más información sobre la conservación de datos, véase el documento *Statement 5/2024 on the Recommendations of the High Level Group on Access to Data for Effective Law Enforcement* [«Declaración 5/2024 del CEPD sobre las recomendaciones del Grupo de Alto Nivel sobre el acceso a los datos para una aplicación eficaz de la ley», documento en inglés], disponible en https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf.
[61] Véase el considerando 164 del proyecto de Decisión.
[62] Véase el artículo 15 de la Ley relativa a las organizaciones delictivas y las investigaciones penales.
[63] Véase el artículo 16 de la Ley relativa a las organizaciones delictivas y las investigaciones penales.

(72) El CEPD señala que el ámbito de aplicación de la Ley relativa a las organizaciones delictivas y las investigaciones penales se limita a la investigación y sanción de organizaciones delictivas organizadas y organizaciones terroristas, que plantean un riesgo significativo para los ciudadanos y la sociedad y, por tanto, pueden justificar una injerencia más grave en los derechos fundamentales a la privacidad y a la protección de datos[64]. Al mismo tiempo, el CEPD considera que la información sobre estas excepciones facilitada en el considerando 164 del proyecto de Decisión es muy general y no completa. En particular, de la información contenida en el proyecto de Decisión no se desprende claramente si, en tal caso, el acceso a los datos personales está sujeto a un control judicial *ex post* de la necesidad y la proporcionalidad.

(73) En vista de ello, el CEPD invita a la Comisión a que aclare y explique en mayor medida en el proyecto de Decisión el ámbito de aplicación y la naturaleza de los casos en los que el acceso a los datos por parte de las autoridades encargadas de garantizar el cumplimiento de la ley no requiere autorización judicial, así como las garantías aplicables en la legislación brasileña. El CEPD también considera que la Comisión debe prestar especial atención a la aplicación de estas excepciones en virtud de la legislación brasileña durante su seguimiento del proyecto de Decisión.

3.1.3 Uso posterior de los datos y transferencias ulteriores

(74) El CEPD recuerda que el nivel de protección ofrecido a los datos personales transferidos desde la UE o el EEE a Brasil no debe verse menoscabado por el uso o el intercambio ulterior de los datos con destinatarios en Brasil o en un tercer país, es decir, que las transferencias ulteriores solo deben permitirse cuando se garantice un nivel de protección continuado esencialmente equivalente al previsto en el Derecho de la Unión.

(75) A este respecto, el CEPD observa positivamente que el Tribunal Supremo Federal de Brasil ha dictaminado que el intercambio de datos personales entre organismos públicos (también cuando se comparten entre los organismos encargados de la aplicación de la ley y los servicios de inteligencia) 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»[65].

(76) A pesar de esta importante sentencia del tribunal supremo de Brasil, dada la complejidad ya mencionada, el alcance exacto y las modalidades de aplicación de la LGPD a las autoridades encargadas de garantizar el cumplimiento de la ley, el CEPD invita a la Comisión a seguir de cerca la evolución y la práctica en este ámbito.

(77) En lo que respecta a la transferencia ulterior de datos personales a las autoridades encargadas de garantizar el cumplimiento de la ley en materia penal en terceros países, el proyecto de Decisión a que se refiere el artículo 33, punto 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,

[64] Véase la sentencia del TJUE, de 6 de octubre de 2020, en los asuntos acumulados La Quadrature du Net y otros, C-511/18 y C-512/18, ECLI:EU:C:2020:791, apartados 95 a 98, y la sentencia, de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, apartados 54, 57 y 60 [sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas)], C-746/18, ECLI:EU:C:2021:152, apartado 35.
[65] Véase el considerando 187 del proyecto de Decisión.

investigación y enjuiciamiento, con arreglo a instrumentos del Derecho internacional»[66]. El CEPD considera que esta explicación es demasiado general e invita a la Comisión a seguir profundizando en el proyecto de Decisión sobre las condiciones y garantías que rigen las transferencias ulteriores.

3.1.4 Supervisión y reparación

(78) El CEPD recuerda que cualquier injerencia en el derecho a la privacidad y la protección de datos debe estar sujeta a un sistema de supervisión eficaz, independiente e imparcial que debe brindar un juez u otro organismo independiente (por ejemplo, una autoridad administrativa o una instancia parlamentaria)[67].

(79) También señala que, en el marco brasileño, tal como describe la Comisión, las actividades de las autoridades encargadas de garantizar el cumplimiento de la ley en materia penal son supervisadas por diferentes organismos: i) el poder judicial; ii) la ANPD; y iii) el Ministerio Fiscal.

(80) El control judicial, como se ha explicado anteriormente en la sección sobre necesidad y proporcionalidad[68], se aplica en relación con la recogida y el acceso a los datos personales, en particular en forma de revisión *ex ante* y autorización.

(81) Por lo que se refiere al papel de la ANPD, como ya se ha explicado en la sección 3.1.1 del presente Dictamen, el proyecto de decisión de adecuación recuerda que, de conformidad con el artículo 4, punto III, de la LGPD, esta Ley no se aplica al tratamiento de datos personales realizado *exclusivamente* con fines de: i) seguridad pública; ii) defensa nacional; iii) seguridad del Estado; y iv) investigación y enjuiciamiento de delitos. Además, el artículo 4, punto I, establece que dicho tratamiento se regirá por una legislación específica que, entre otras cosas, debe incluir los principios generales de protección y los derechos de los interesados, tal como se describen en la LGPD. El apartado 3 del mismo artículo reconoce una función consultiva a la ANPD en relación con las excepciones previstas en el punto III cuando se lleva a cabo exclusivamente para estos fines, en particular las competencias de la ANPD para emitir dictámenes técnicos y recomendaciones, así como para solicitar EIPD a los responsables del tratamiento pertinentes.

(82) En su proyecto de Decisión[69], la Comisión hace referencia a una importante Decisión, de 15 de septiembre de 2022, del Tribunal Supremo Federal, que indica la aplicabilidad de los principios generales de protección de datos y los derechos de los interesados al tratamiento de datos personales por parte del Estado para la prestación de servicios públicos. Esta Decisión se centra en el «intercambio de datos personales» entre los organismos y entidades de la Administración Pública y en las actividades de inteligencia, y en el «acceso de las agencias y entidades gubernamentales» al Registro Base de Ciudadanos. En relación con la función de ejecución de la ANPD, el CEPD entiende, a partir de la información adicional facilitada por la Comisión, que la ANPD ya ha ejercido dicha función sobre la policía, así como sobre el Ministerio de Justicia y Seguridad Pública. Esto se hizo sobre la base de la jurisprudencia que, al ampliar la aplicabilidad parcial de los principios generales y los

[66] *Ibid*.
[67] Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, adoptadas el 10 de noviembre de 2020, véase la página 12 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_es.pdf.
[68] Véase la sección 3.1.2 anterior.
[69] Véase el considerando 187 del proyecto de Decisión.

derechos de los interesados al tratamiento realizado a efectos de aplicación de la ley, también hace que la ANPD sea responsable de supervisar y hacer cumplir la legislación en este ámbito.

(83) En vista de lo anterior, el CEPD invita a la Comisión a seguir profundizando en la función de ejecución de la ANPD, en particular en lo que respecta a las bases jurídicas pertinentes y sus poderes de investigación y correctivos frente a las autoridades encargadas de garantizar el cumplimiento de la ley, y a seguir de cerca la evolución de la situación en este ámbito.

(84) Por último, el CEPD observa que el Ministerio Fiscal tiene una competencia más amplia que la supervisión de las normas de protección de datos y privacidad y la imposición de sanciones por violaciones de los derechos fundamentales. Por ejemplo, como ya se ha explicado en la sección 3.1 del presente Dictamen, en virtud de la Ley relativa a las organizaciones delictivas y a las investigaciones penales, el Ministerio Fiscal es una de las autoridades que pueden acceder sin autorización judicial a los datos de registro de una persona investigada. Por consiguiente, el CEPD invita a la Comisión a seguir desarrollando y explicando en el proyecto de Decisión el papel y los poderes del Ministerio Fiscal en relación con la supervisión del tratamiento de datos personales por parte de las autoridades brasileñas encargadas de garantizar el cumplimiento de la ley.

(85) Por lo que se refiere a la reparación, el CEPD observa positivamente que los mecanismos jurídicos descritos en la primera parte del presente Dictamen y, en particular, los recursos judiciales a disposición de los interesados para hacer valer sus derechos a la protección de datos y a la privacidad, también se aplican en relación con las actividades de los organismos encargados de garantizar el cumplimiento de la ley en materia penal.

3.2 Acceso y uso por parte de las autoridades públicas brasileñas con fines de seguridad nacional

3.2.1 Ámbito de aplicación de la exención del artículo 4, punto III, de la LGPD y su aplicabilidad a los delitos contra la seguridad del Estado

(86) Tal como ha introducido la Comisión, el artículo 4, punto III, de la LGDP exime a la «seguridad del Estado» de la aplicación de la LGDP en el tratamiento de datos personales, junto con la seguridad pública, la defensa nacional y las actividades de investigación y enjuiciamiento de delitos.

(87) El CEPD señala que la legislación brasileña en materia de «Seguridad Nacional», tal como se establece en la Ley n.º 14.197, de 1 de septiembre de 2021, por la que se modifica el Código Penal y se revoca la Ley de seguridad nacional de 1983[70], expresa el concepto brasileño de seguridad nacional sobre la base de una lista exhaustiva de delitos[71], que abordan diferentes amenazas a la integridad del Estado brasileño como institución [soberanía nacional, espionaje (artículo 350-K), delitos contra las instituciones democráticas (artículo 359-L) y otros]. Las normas de la Ley n.º 14.197 se han establecido como parte integrante del Código Penal brasileño.

[70] Ley n.º 14.197, de 1 de septiembre de 2021, disponible en https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm (2.10.2026).
[71] Véase el considerando 200 del proyecto de Decisión.

(88) Dicho esto, el CEPD espera que el tratamiento de datos de las autoridades brasileñas para el enjuiciamiento de los delitos establecidos en la Ley n.º 14.197 se rija por el régimen aplicable al acceso y uso de las autoridades brasileñas a efectos de la aplicación del Derecho penal, tal como se describe en el capítulo 3.2 del proyecto de Decisión, por lo que se enfrenta a las mismas consideraciones en materia de protección de datos que se recogen en el capítulo 3.1 del presente Dictamen. Por consiguiente, el CEPD pide a la Comisión que aclare en el proyecto de Decisión si el tratamiento de datos relacionado con el enjuiciamiento de los delitos que figuran en la Ley n.º 14.197 se rige efectivamente por el régimen de protección de datos aplicable a las actividades de aplicación de la ley o por otro régimen. En este último caso, el CEPD invita a la Comisión a que explique con más detalle las normas de protección de datos aplicables al enjuiciamiento penal de estos delitos a efectos de la seguridad nacional.

3.2.2 Marco jurídico para la seguridad nacional

(89) El marco jurídico codificado en el que el proyecto de Decisión basa sus conclusiones en su capítulo sobre el acceso gubernamental «con fines de seguridad nacional» consiste en la Ley n.º 14.197 de 2021, la Ley n.º 9.883, de 7 de diciembre de 1999, por la que se establece el Sistema Brasileño de Inteligencia, y el Decreto n.º 4.376 de 2002 relacionado. Los dos últimos actos legislativos mencionados crearon el Sistema Brasileño de Inteligencia (SISBIN) y definieron su funcionamiento. Les sigue el Decreto presidencial n.º 8.793 [72] de 2016 vinculante, que define la política nacional de inteligencia —la denominada Política Nacional de Inteligencia (en lo sucesivo, «PNI»)—, así como la LGPD en 2018.

(90) El Decreto presidencial n.º 8.793 de 2016 describe el objeto, los objetivos y los límites de la PNI. Las actividades previstas en el presente Decreto tienen por objeto generar y difundir a las autoridades competentes conocimientos sobre hechos y situaciones que se producen dentro o fuera del territorio nacional, con influencia inmediata o potencial en el proceso de toma de decisiones, la acción gubernamental y la seguridad de la sociedad y la inteligencia del Estado. En estas circunstancias, la inteligencia se refiere al conjunto de la información, así como los datos, necesaria y tratada para apoyar el proceso de toma de decisiones del poder ejecutivo en este ámbito.

(91) Con arreglo a la base jurídica del SISBIN presentada por la Comisión, el SISBIN y sus entidades se han establecido como el mecanismo central para la aplicación de la PNI y, como tales, se encargan de llevar a cabo actividades relacionadas con el ámbito de la seguridad nacional, así como con la seguridad pública y la protección de las instituciones democráticas. A tal fin, el SISBIN prevé el intercambio de conocimientos y la planificación integrada de las actividades[73]. En consecuencia, el concepto de seguridad nacional en Brasil a la luz de las actividades del SISBIN no parece limitarse únicamente a los delitos codificados en la Ley n.º 14.197, sino que podría considerarse parte integrante de un concepto más amplio de inteligencia nacional.

(92) El SISBIN se creó inicialmente, compuesto por dieciocho entidades federales, entre ellas trece ministerios, y posteriormente se amplió a cuarenta y ocho de las denominadas agencias en virtud del Decreto n.º 11.693, de 6 de septiembre de 2023, relativo a la organización y el funcionamiento de SISBIN[74]. El CEPD señala que la cooperación dentro del SISBIN integra

[72] Véase el considerando 199 del proyecto de Decisión.
[73] Decreto presidencial n.º 8.793, sección 5, designa al SISBIN y los órganos integrados en él, el intercambio de conocimientos dentro del SISBIN y la planificación integrada de la cooperación entre los miembros del SISBIN como instrumentos para llevar a cabo la PNI.
[74] Véase el considerando 202 del proyecto de Decisión.

entidades más allá de las instituciones de seguridad clásicas, como el Ministerio de Ciencia (artículo 4, punto IV), la agricultura (artículo 4, punto XV) y la energía (artículo 4, punto XVIII) y el Fiscal General federal (artículo 4, punto XIX).

(93) Mientras que el Decreto n.º 4.376 de 2002 exigió al Consejo Consultivo del Sistema Brasileño de Inteligencia que propusiera normas y procedimientos generales para el intercambio de «conocimientos y comunicación» dentro del SISBIN[75], el Decreto n.º 11.693 de 2023 encomienda al órgano central del SISBIN la elaboración de herramientas técnicas[76] para el intercambio de datos y conocimientos de información y describe el intercambio y la utilización de los datos obtenidos por las entidades del SISBIN. Sin embargo, el proyecto de Decisión de la Comisión no proporciona más información sobre tales reglas o normas jurídicas emitidas por el órgano central, por ejemplo, cuando las entidades del SISBIN comparten datos personales entre ellas.

(94) Además, parece haber diferencias en los conceptos de sensibilidad de la información, dado que, en virtud de la legislación pertinente que rige las actividades del SISBIN, la sensibilidad está relacionada con el grado de confidencialidad otorgado a una información[77] y con la limitación de la finalidad en comparación con los principios generales del RGPD[78].

(95) Como ya se ha explicado anteriormente, el artículo 4, punto III, letras a) a c), de la LGPD, que se codificó tras el establecimiento del SISBIN y el establecimiento de una política nacional de inteligencia, exime de la aplicación de la LGPD a las actividades de tratamiento de datos realizadas exclusivamente con fines de seguridad pública, defensa nacional y seguridad del Estado, con excepción de los principios generales establecidos en materia de protección de datos.

(96) Como subraya la Comisión en el proyecto de Decisión, el marco general de la Constitución brasileña, así como la participación de Brasil en la Corte Interamericana de Derechos Humanos, se refieren al marco jurídico para el acceso gubernamental a efectos de inteligencia nacional. El CEPD reconoce asimismo que las sentencias del Tribunal Supremo Federal de Brasil también han desempeñado un papel importante en la definición del panorama jurídico[79]. Hasta la fecha, las sentencias del Tribunal Supremo han sido un apoyo conciso y pertinente para seguir desarrollando la protección de los datos personales de conformidad con la Constitución brasileña. Al mismo tiempo, cabe señalar que las sentencias del Tribunal Supremo no precisan ni establecen normas generales abstractas de protección de datos para el tratamiento de datos personales, sino que interpretan las disposiciones y los principios de la Constitución y de la LGPD.

(97) El CEPD es consciente del hecho de que se concede a los Estados un amplio margen de apreciación a la hora de definir las cuestiones de seguridad nacional, lo que permite entonces exenciones de seguridad nacional en el tratamiento de datos personales. En este contexto, recuerda la definición dada por el Tribunal Europeo de Derechos Humanos, según la cual las amenazas a la seguridad nacional deben distinguirse por su naturaleza, gravedad y

[75] Véase el artículo 7, punto II, del Decreto n.º 4.376.
[76] Véase el artículo 10, punto XI, disponible en https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm (26.9.2025).
[77] Véanse el Decreto n.º 8.793 de 2016, el Decreto n.º 11.693 y el considerando 204 del proyecto de Decisión.
[78] Véase el artículo 6, punto I, de la LGPD, que se refiere a fines legítimos y específicos, mientras que el RGPD exige fines lícitos y específicos.
[79] Véase el considerando 203 del proyecto de Decisión.

circunstancias específicas de los riesgos generales para la seguridad pública o de los delitos graves[80].

(98) El CEPD entiende que los datos tratados por las entidades del SISBIN solo se benefician de la exención prevista en el artículo 4, punto III, de la LGPD cuando el tratamiento se lleva a cabo *exclusivamente* con fines de seguridad pública, defensa nacional y seguridad del Estado. Esto parece aplicarse específicamente a las actividades del órgano central del SISBIN, la Agencia Brasileña de Inteligencia (en lo sucesivo, «ABIN»). Por consiguiente, a menos que una entidad del SISBIN actúe en nombre de la ABIN para uno de estos fines, la LGPD es plenamente aplicable.

(99) El CEPD pide a la Comisión que confirme esta interpretación y que describa y explique con mayor precisión en el proyecto de Decisión el esbozo del concepto de seguridad nacional con arreglo a la legislación brasileña, en particular en relación con la recogida y el intercambio de datos entre entidades y por entidades en nombre de las actividades del SISBIN, y con respecto a la aplicación de la PNI. En relación con esto, el CEPD invita a la Comisión a que aclare también cómo las exenciones de la LGPD a efectos de seguridad nacional se refieren a la exención para la seguridad nacional en virtud del RGPD.

3.2.3 Transferencias ulteriores y acuerdos internacionales

(100) El artículo 33 de la LGPD define las condiciones previas para la transferencia internacional de datos. El artículo 33, puntos I y II, de la LGPD establece requisitos similares a una decisión de adecuación o los requisitos de garantías adicionales en virtud del RGPD. Estos requisitos quedan exentos en el artículo 33, puntos III, VI y VII, de la LGPD, que abordan los casos de «cooperación jurídica entre inteligencia», transferencias que responden a «un compromiso contraído en acuerdos de cooperación internacional» y transferencias «necesarias para la aplicación de un orden público o una atribución legal al servicio público», es decir, la seguridad nacional y la inteligencia nacional. Esta decisión parece estar en consonancia con el concepto del artículo 4, punto III, de la LGPD, que limita la aplicación de la LGPD únicamente a sus principios en materia de seguridad pública, defensa nacional y seguridad del Estado. Así pues, podría considerarse que las transferencias ulteriores con fines de inteligencia nacional deben llevarse a cabo de conformidad con los principios generales de protección de datos de la LGPD, al tiempo que están sujetas a las disposiciones sobre cooperación internacional previstas en los actos jurídicos por los que se establecen la PNI y el SISBIN.

(101) Dicho esto, el CEPD reconoce que Brasil puede necesitar datos personales y los transmite a los servicios de inteligencia extranjeros con fines de cooperación o con el objetivo de aplicar la PNI con arreglo al objetivo de prevenir y detectar amenazas sobre la base del concepto integrado de seguridad mencionado.

(102) Como se ha señalado anteriormente, la Comisión señala la aplicabilidad del marco general de la Constitución brasileña y la garantía de los datos *habeas data* para la protección de los datos personales en el seno del SISBIN, que también se aplican a las transferencias ulteriores con fines de seguridad nacional. El CEPD invita a la Comisión a que aclare en mayor medida la base jurídica y las garantías y condiciones en materia de protección de datos que la ABIN y los demás miembros del SISBIN están obligados a considerar antes de revelar datos personales con fines de inteligencia nacional a socios extranjeros.

[80] TEDH, Big Brother Watch y otros c. Reino Unido, 25 de mayo de 2021, artículo 350.

(103) El CEPD también señala que la Comisión no integró consideraciones sobre la existencia de acuerdos internacionales celebrados entre Brasil y terceros países u organizaciones internacionales en su evaluación de la adecuación. Dado que en la LGPD no se establece legislación vinculante más allá de los principios generales de protección de datos, estos acuerdos podrían contener disposiciones específicas para la transferencia internacional de datos personales en poder de la ABIN o de los demás miembros del SISBIN a terceros países. El CEPD considera que es probable que la celebración de acuerdos bilaterales y multilaterales con terceros países a efectos de inteligencia nacional afecten al marco jurídico de protección de datos aplicable.

(104) Por consiguiente, el CEPD invita a la Comisión a aclarar si existen tales acuerdos internacionales con fines de inteligencia nacional y a evaluar su posible repercusión en el nivel de protección otorgado a los datos personales transferidos desde el EEE a Brasil en relación con el marco jurídico evaluado principalmente para el tratamiento de datos con fines de inteligencia nacional.

3.2.4 Supervisión y reparación

(105) El proyecto de decisión de adecuación presenta diferentes órganos para supervisar las actividades de las autoridades nacionales de seguridad brasileñas, en particular: i) el poder ejecutivo, ii) el poder legislativo; iii) la ANPD; y iv) el poder judicial. En relación con la ANPD, el CEPD recuerda la consideración y las conclusiones formuladas en la sección 3.1.4 del presente Dictamen, que también siguen siendo válidas en este caso.

(106) Según el proyecto de Decisión, la Cámara de Relaciones Exteriores y Defensa Nacional del Consejo de Gobierno es responsable de supervisar la ejecución de la Policía Nacional de Inteligencia, y la Oficina de Seguridad Institucional se encarga de coordinar las actividades de inteligencia a escala federal. El CEPD señala que este control solo se refiere a garantizar los objetivos que debe alcanzar el Sistema de Inteligencia y a su aplicación, pero no incluye ningún poder de investigación o sanción, y no abarca el tratamiento real de datos personales.

(107) De hecho, corresponde a la Comisión Mixta para el Control de las Actividades de Inteligencia (en lo sucesivo, «CCAI») (poder legislativo) ejercer un control en relación con las actividades de inteligencia, incluyendo su legitimidad y eficacia. El CEPD acoge con satisfacción que se hayan reforzado la estructura y las competencias de la CCAI, aumentando la transparencia de sus actividades y permitiendo al organismo ejercer un control adecuado, como la realización de revisiones, auditorías y controles posteriores a las operaciones en curso. El CEPD también observa con satisfacción que la CCAI pueda tramitar las reclamaciones de los interesados como parte de su competencia para investigar las reclamaciones sobre violaciones de los derechos y garantías fundamentales.

(108) La competencia del poder judicial para conocer de los asuntos presentados por los ciudadanos contra las autoridades públicas es un aspecto positivo, en particular porque permite la supervisión judicial de las actividades realizadas en nombre de la seguridad nacional, garantizando el cumplimiento, entre otros, de los derechos constitucionales (incluido el derecho a la protección de datos) y de la LGPD. El CEPD observa positivamente que la posibilidad de apelación está prevista a través del Tribunal Supremo Federal y, en última instancia, a través de la Corte Interamericana de Derechos Humanos.

(109) El CEPD entiende que, en el contexto de las actividades nacionales de inteligencia, se conceden a los interesados: i) los derechos consagrados en la LGPD (como consecuencia de la Decisión del Tribunal Supremo Federal de 15 de septiembre de 2022); ii) el derecho de

acceso y rectificación de los datos personales a través de la vía de reparación constitucional de los datos *habeas data*; y iii) el derecho a la indemnización de los daños y perjuicios materiales y morales.

(110) El CEPD acoge con satisfacción la existencia de tales derechos y el hecho de que puedan invocarse a través de mecanismos judiciales y administrativos, en particular la CCAI, así como el hecho de que estas vías de reparación sean accesibles para todas las personas, independientemente de su nacionalidad.

4. APLICACIÓN Y SUPERVISIÓN DEL PROYECTO DE DECISIÓN

(111) En cuanto al seguimiento y la revisión del proyecto de Decisión, el CEPD señala que, de conformidad con la jurisprudencia del TJUE, «dado que el nivel de protección garantizado por un tercer país puede evolucionar, incumbe a la Comisión, tras adoptar una decisión [de adecuación] en virtud del [artículo 45 del RGPD], comprobar periódicamente si sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión. En cualquier caso esa comprobación es obligada cuando hay indicios que generan una duda en ese sentido»[81].

(112) El CEPD señala que la revisión de la constatación de la adecuación tendrá lugar al menos cada cuatro años, de conformidad con el artículo 45, apartado 3, del RGPD[82].

(113) El CEPD acoge con satisfacción que el proyecto de Decisión en su considerando 230 prevea la participación del CEPD en la reunión organizada entre la Comisión y las autoridades brasileñas y dedicada a llevar a cabo la revisión del funcionamiento de la decisión de adecuación. Por lo que respecta a la participación práctica del CEPD y sus representantes en la preparación y el desarrollo de las revisiones periódicas futuras, el CEPD reitera que toda documentación pertinente, incluso la correspondencia, debe compartirse por escrito con el CEPD con antelación suficiente a la fecha de las revisiones.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Anu Talus)

[81] Sentencia del TJUE Schrems I, apartado 76. Véase igualmente el artículo 3, apartado 4, del proyecto de Decisión.
[82] Véanse el considerando 229 y el artículo 3, apartado 4, del proyecto de Decisión.