II

(Actos no legislativos)

DECISIONES

DECISIÓN DE EJECUCIÓN (UE) 2019/419 DE LA COMISIÓN

de 23 de enero de 2019

con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal

[notificada con el número C(2019) 304]

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

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

Previa consulta al Supervisor Europeo de Protección de Datos,

1. INTRODUCCIÓN

- (1) El Reglamento (UE) 2016/679 establece las normas que regulan la transferencia de datos personales desde los responsables o encargados del tratamiento en la Unión Europea a terceros países y organizaciones internacionales, en la medida en que tales transferencias se encuentren comprendidas dentro de su ámbito de aplicación. Las normas sobre transferencias internacionales de datos personales se establecen en el capítulo V de dicho Reglamento, más concretamente en los artículos 44 a 50. El flujo de datos personales hacia y desde países no pertenecientes a la Unión Europea es necesario para la expansión de la cooperación y el comercio internacionales, y garantiza al mismo tiempo que el nivel de protección de los datos personales en la Unión Europea no se vea menoscabado.
- (2) De conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, la Comisión puede decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado. En tal caso, la transferencia de datos personales a dicho tercer país, territorio, sector u organización internacional puede realizarse sin necesidad de obtener ninguna otra autorización, de conformidad con lo dispuesto en el artículo 45, apartado 1, y en el considerando 103 del Reglamento.
- (3) Tal como se especifica en el artículo 45, apartado 2, del Reglamento (UE) 2016/679, la adopción de una decisión de adecuación ha de basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país, por lo que se refiere tanto a las normas aplicables a los importadores de datos como a las limitaciones y salvaguardas en lo que respecta al acceso a los datos personales por parte de las autoridades públicas. La evaluación debe determinar si el tercer país en cuestión garantiza un nivel de protección «equivalente en lo esencial» al ofrecido en la Unión Europea [considerando 104 del Reglamento (UE) 2016/679]. Tal como ha precisado el Tribunal de Justicia de la Unión Europea, no se exige un nivel de protección idéntico ⁽²⁾. En particular, los medios de que se sirve el tercer país en cuestión pueden ser diferentes de los aplicados en la Unión Europea, siempre que, en la práctica, sean eficaces para garantizar un nivel de protección adecuado ⁽³⁾. Por consiguiente, el nivel de adecuación no exige que

⁽¹⁾ DO L 119 de 4.5.2016, p. 1.

⁽²⁾ Asunto C-362/14, Maximilian Schrem/Data Protection Commissioner (en lo sucesivo, «Schrems»), ECLI:EU:C:2015:650, apartado 73.

⁽³⁾ Schrems, apartado 74.

se reproduzcan al pie de la letra las normas de la Unión. Se trata más bien de determinar si el sistema extranjero ofrece, en su conjunto y por la esencia de los derechos de privacidad y su aplicación, fuerza ejecutiva y supervisión efectivas, el nivel de protección exigido ⁽⁴⁾.

- (4) La Comisión ha analizado detenidamente la legislación y las prácticas japonesas. Sobre la base de las constataciones expuestas en los considerandos 6 a 175, la Comisión concluye que Japón garantiza un nivel adecuado de protección de los datos personales transferidos a las organizaciones que entran dentro del ámbito de aplicación de la Ley sobre la protección de la información personal ⁽⁵⁾ y siempre que se cumplan las condiciones adicionales contempladas en la presente Decisión. Estas condiciones se establecen en las Reglas complementarias (anexo I) adoptadas por la Comisión de Protección de la Información Personal (CPIP) ⁽⁶⁾ y en las declaraciones, garantías y compromisos oficiales del Gobierno japonés a la Comisión Europea (anexo II).
- (5) La presente Decisión tiene por efecto que las transferencias desde un responsable o encargado del tratamiento en el Espacio Económico Europeo (EEE) ⁽⁷⁾ hacia dichas organizaciones en Japón pueden realizarse sin necesidad de obtener ninguna otra autorización. No tiene ninguna incidencia en la aplicación directa del Reglamento (UE) 2016/679 a dichas organizaciones cuando se cumplan las condiciones enunciadas en su artículo 3.

2. NORMATIVA APLICABLE AL TRATAMIENTO DE DATOS POR PARTE DE LOS OPERADORES ECONÓMICOS

2.1. El marco de protección de datos japonés

- (6) El régimen jurídico que rige la privacidad y la protección de datos en Japón tiene sus raíces en la Constitución de 1946.
- (7) El artículo 13 de la Constitución dispone:

«Todos los ciudadanos serán respetados como personas individuales. Su derecho a la vida, la libertad y al logro de la felicidad, será, en tanto que no interfiera con el bienestar público, el objetivo supremo de la legislación y de los demás actos de Gobierno.»

- (8) Sobre la base de dicho artículo, el Tribunal Supremo japonés ha precisado los derechos de las particulares en lo que respecta a la protección de la información personal. En una resolución de 1969, reconoció el derecho a la vida privada y a la protección de datos como un derecho constitucional ⁽⁸⁾. Entre otras cosas, el Tribunal sostuvo que «cada particular es libre de proteger su propia información personal de modo que no sea comunicada a terceros ni hecha pública sin un motivo justificado». Por otra parte, en una resolución de 6 de marzo de 2008 («Juki-Net») ⁽⁹⁾, el Tribunal Supremo mantuvo que «la libertad de los ciudadanos en su vida privada estará protegida contra el ejercicio de la autoridad pública y puede considerarse que, como una de las libertades de las personas en su vida privada, cada particular es libre de proteger su propia información personal de modo que no sea comunicada a terceros ni hecha pública sin un motivo justificado.» ⁽¹⁰⁾.
- (9) El 30 de mayo de 2003, Japón promulgó una serie de leyes en el ámbito de la protección de datos:
- la Ley sobre la protección de la información personal (LPIP),
 - la Ley sobre la protección de la información personal en poder de órganos administrativos (LPIPPOA),
 - la Ley sobre la protección de la información personal en poder de agencias administrativas incorporadas (LPIPPAAI).

⁽⁴⁾ Véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo, «Intercambio y protección de los datos personales en un mundo globalizado», COM(2017) 7 de 10.1.2017, sección 3.1, pp. 7-8.

⁽⁵⁾ Ley sobre la protección de la información personal (Ley n.º 57, 2003).

⁽⁶⁾ Puede encontrarse más información sobre la CPIP en el enlace siguiente: <https://www.ppc.go.jp/en/> (incluidos los datos de contacto para consultas y reclamaciones: <https://www.ppc.go.jp/en/contactus/access/>).

⁽⁷⁾ La presente Decisión es pertinente a efectos del EEE. El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») prevé la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La Decisión del Comité Mixto (DCM) por la que se incorpora el Reglamento (UE) 2016/679 al anexo XI del Acuerdo EEE fue adoptada por el Comité Mixto del EEE el 6 de julio de 2018 y entró en vigor el 20 de julio de 2018. El Reglamento está cubierto pues por dicho Acuerdo.

⁽⁸⁾ Tribunal Supremo, sentencia de la Gran Sala de 24 de diciembre de 1969, Keishu, vol. 23, n.º 12, p. 1625.

⁽⁹⁾ Tribunal Supremo, sentencia de 6 de marzo de 2008, Minshu, vol. 62, n.º 3, p. 665.

⁽¹⁰⁾ Tribunal Supremo, sentencia de 6 de marzo de 2008, Minshu, vol. 62, n.º 3, p. 665.

- (10) Las dos últimas Leyes (modificadas en 2016) contienen disposiciones aplicables a la protección de la información personal por parte de las entidades del sector público. El tratamiento de datos comprendido en el ámbito de aplicación de dichas Leyes no es objeto de la constatación de adecuación contenida en la presente Decisión, que se limita a la protección de la información personal por parte de los «operadores económicos que manejan información personal» (OEMIP) en el sentido de la LPIP.
- (11) La LPIP ha sido reformada en los últimos años. La LPIP modificada fue promulgada el 9 de septiembre de 2015 y entró en vigor el 30 de mayo de 2017. La modificación introdujo una serie de nuevas salvaguardas y reforzó las ya existentes, acercando así el sistema de protección de datos japonés al europeo. Se incluyen, por ejemplo, una serie de derechos individuales exigibles o el establecimiento de una autoridad de control independiente (CPIP) encargada de la supervisión y del control de la aplicación de la LPIP.
- (12) Además de la LPIP, el tratamiento de la información personal comprendida en el ámbito de aplicación de la presente Decisión está sujeto a normas de ejecución adoptadas sobre la base de la LPIP. Se trata sobre todo de la modificación de la Orden del Gabinete para asegurar el cumplimiento de la Ley sobre la protección de la información personal, de 5 de octubre de 2016, y las llamadas normas de ejecución de la Ley sobre la protección de la información personal adoptadas por la CPIP⁽¹¹⁾. Ambos conjuntos de normas son legalmente vinculantes y tienen carácter ejecutivo y entraron en vigor al mismo tiempo que la LPIP modificada.
- (13) Por otra parte, el 28 de octubre de 2016, el Gabinete de Japón (compuesto por el primer ministro y los ministros que forman su Gobierno) adoptó una «política de base» con el fin de «promover de manera global e integrada medidas tendentes a la protección de la información personal». De conformidad con el artículo 7 de la LPIP, la «política de base» se adoptó en forma de Decisión del Gabinete e incluye orientaciones estratégicas relativas a la ejecución de la LPIP, dirigidas tanto a la Administración central como a las autoridades locales.
- (14) Recientemente, mediante Decisión del Gabinete de 12 de junio de 2018, el Gobierno japonés ha modificado la «política de base». Con el fin de facilitar las transferencias internacionales de datos, dicha Decisión del Gabinete delega en la CPIP, como autoridad competente para la gestión y aplicación de la LPIP, «la facultad de adoptar las medidas necesarias para salvar las diferencias entre los sistemas y las operaciones de Japón y los del país extranjero de que se trate sobre la base del artículo 6 de la Ley, con el fin de garantizar el manejo apropiado de la información personal recibida de dicho país». La Decisión del Gabinete dispone que esta facultad incluye la competencia para asegurar protecciones reforzadas mediante la adopción por parte de la CPIP de normas más estrictas, que complementen y vayan allá de las establecidas en la LPIP y en la Orden del Gabinete. Con arreglo a dicha Decisión, estas normas más estrictas serán vinculantes y tendrán carácter ejecutivo para los operadores económicos japoneses.
- (15) Sobre la base del artículo 6 de la LPIP y de la referida Decisión del Gabinete, la CPIP adoptó el 15 de junio de 2018 unas «Reglas complementarias en virtud de la Ley sobre la protección de información personal para el manejo de datos personales transferidos desde la UE sobre la base de una decisión de adecuación» (en lo sucesivo, las «Reglas complementarias»), con miras a reforzar la protección de la información personal transferida desde la Unión Europea a Japón sobre la base de la presente decisión de adecuación. Estas Reglas complementarias son jurídicamente vinculantes para los operadores económicos japoneses y pueden ser invocadas tanto por la CPIP como por los órganos jurisdiccionales, del mismo modo que las disposiciones de la LPIP a las que las Reglas complementan con normas más estrictas o detalladas⁽¹²⁾. Como los operadores económicos japoneses que reciben o tratan ulteriormente datos personales procedentes de la Unión Europea están obligados legalmente a cumplir con las Reglas complementarias, tendrán que garantizar [p. ej. por medios técnicos («etiquetado») o de logística (almacenamiento en una base de datos específica)] que pueden identificar tales datos personales a lo largo de todo su «ciclo de vida»⁽¹³⁾. En las secciones siguientes, el contenido de cada Regla complementaria se analiza en el marco de la evaluación de los artículos de la LPIP a los que complementa.
- (16) A diferencia de lo que sucedía antes de la modificación de 2015, cuando esta cuestión era competencia de diferentes ministerios japoneses en sectores específicos, la LPIP faculta a la CPIP a adoptar «Directrices» para «garantizar la ejecución apropiada y efectiva de las medidas que deben tomar los operadores económicos» en virtud de la normativa de protección de datos. A través de sus Directrices, la CPIP ofrece una interpretación autorizada de esas normas, en particular la LPIP. Según la información recibida de la CPIP, estas Directrices forman

⁽¹¹⁾ Disponibles en la dirección siguiente: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

⁽¹²⁾ Véanse las Reglas complementarias (sección introductoria).

⁽¹³⁾ Esta exigencia no es puesta en entredicho por la obligación general de mantener registros (solo) durante un determinado período de tiempo. Aun cuando el origen de los datos se encuentre en la información que el OEMIP adquirente ha de confirmar con arreglo al artículo 26, apartado 1, de la LPIP, el requisito de conformidad con el artículo 26, apartado 4, de la LPIP, leído en relación con el artículo 18 de las Normas de la CPIP, solo afecta a una forma particular de registro (véase el artículo 16 de las Normas de la CPIP) y no impide que un OEMIP asegure la identificación de los datos durante períodos más largos. Este extremo ha sido confirmado por la CPIP, que ha declarado que «[l]a información sobre el origen de los datos de la UE deberá ser conservada por el OEMIP durante el tiempo que sea necesario para poder cumplir con las Reglas complementarias».

parte integrante del marco jurídico, y deben leerse conjuntamente con el texto de la LPIP, la Orden del Gabinete, las normas de la CPIP y un conjunto de preguntas y respuestas⁽¹⁴⁾ elaboradas por la CPIP. Son por tanto «vinculantes para los operadores económicos». Cuando las Directrices establecen que un operador económico «debe» o «no debe» actuar de una determinada manera, la CPIP considerará que el incumplimiento de las disposiciones pertinentes constituye una vulneración de la ley⁽¹⁵⁾.

2.2. **Ámbito de aplicación material y personal**

- (17) El ámbito de aplicación de la LPIP viene determinado por los conceptos definidos de «información personal», «datos personales» y «operador económico que maneja información personal». Al mismo tiempo, la LPIP prevé una serie de excepciones importantes a su ámbito de aplicación, sobre todo en relación con los datos personales tratados de forma anónima y con determinados tipos de tratamiento por parte de ciertos operadores. Aunque la LPIP no utiliza el término «tratamiento», se basa en el concepto equivalente de «manejo», que, con arreglo a la información recibida de la CPIP, comprende «cualquier actuación que tenga relación con datos personales», incluida la adquisición, entrada, acumulación, organización, almacenamiento, edición/tratamiento, renovación, cancelación, salida, utilización, o suministro de información personal.

2.2.1. *Definición de «información personal»*

- (18) En primer lugar, por lo que se refiere a su ámbito de aplicación material, la LPIP establece una distinción entre la información personal y los datos personales, siendo aplicables a la primera categoría solo ciertas disposiciones de la Ley. De conformidad con el artículo 2, apartado 1, de la LPIP, el concepto de «información personal» comprende toda información relativa a una persona viva que permite su identificación. La definición distingue dos categorías de información personal: i) los códigos de identificación individuales y ii) otra información personal que permita la identificación de una persona concreta. La última categoría incluye asimismo la información que, por sí sola, no permite la identificación de una persona concreta, pero que sí la hace posible mediante un «simple cotejo» con otras informaciones. Con arreglo a las Directrices de la CPIP⁽¹⁶⁾, la posibilidad de que un «simple cotejo» de la información permita la identificación se evaluará caso por caso, teniendo en cuenta la situación real («condición») del operador económico. Este extremo se dará por supuesto si dicho cotejo es (o puede ser) llevado a cabo por un operador económico medio («normal»), sirviéndose de los medios a su disposición. Por ejemplo, la información no permite «un simple cotejo» con otras informaciones si el operador económico debe hacer esfuerzos inusuales o cometer actos ilícitos para obtener las informaciones que deben cotejarse de uno o varios operadores económicos.

2.2.2. *Definición de «datos personales»*

- (19) En virtud de la LPIP, solo determinadas modalidades de información personal entran dentro del concepto de «datos personales». De hecho, los «datos personales» se definen como «la información personal que constituye una base de datos de información personal», es decir, un «corpus colectivo de información» que incluye información personal «organizada de forma sistemática con el fin de permitir la búsqueda de información personal concreta utilizando un ordenador»⁽¹⁷⁾ o «definida por orden del Gabinete como información que ha sido organizada de forma sistemática para permitir buscar fácilmente información personal concreta», pero «con exclusión de la información definida por orden del Gabinete como poco susceptible de perjudicar los derechos e intereses de un particular, teniendo en cuenta su método de utilización»⁽¹⁸⁾.
- (20) Esta excepción se especifica con más detalle en el artículo 3, apartado 1, de la Orden del Gabinete, que dispone que se han de cumplir las tres condiciones acumulativas siguientes: i) el corpus colectivo de información debe haberse publicado con la finalidad de ser vendido a un gran número de personas indeterminadas y sin que en dicha publicación se violen las disposiciones de una ley u orden basada en ella; ii) debe poder ser «adquirida en cualquier momento por un gran número de personas indeterminadas» y iii) los datos personales que contenga deben ser

⁽¹⁴⁾ CPIP, Preguntas y respuestas, 16 de febrero de 2017 (modificadas el 30 de mayo de 2017), disponibles en la dirección siguiente: <https://www.ppc.go.jp/files/pdf/kojohouQA.pdf>. Las preguntas y respuestas versan sobre una serie de cuestiones abordadas en las Directrices y ofrecen ejemplos prácticos como, por ejemplo, qué constituye datos personales sensibles, la interpretación del consentimiento individual, las transferencias de terceros en el contexto de la computación en nube o la obligación de llevar un registro de las transferencias transfronterizas. La sección de preguntas y respuestas solo está disponible en japonés.

⁽¹⁵⁾ En respuesta a una pregunta específica, la CPIP ha informado al SEPD de que «los tribunales japoneses basan su interpretación en las Directrices cuando aplican la LPIP/las Normas de la CPIP en casos concretos de que conocen y, por tanto, remiten directamente al texto de la Directrices de la CPIP en sus sentencias. Por lo tanto, también desde este punto de vista las Directrices de la CPIP son vinculantes para los operadores económicos. La CPIP no tiene constancia de que el tribunal se haya apartado nunca de las Directrices». A este respecto, la CPIP ha remitido a la Comisión a una sentencia dictada en el ámbito de la protección de datos en la que el tribunal se basó explícitamente en las directrices para elaborar sus conclusiones (véase Tribunal de Distrito de Osaka, resolución de 19 de mayo de 2006, Hanrei Jiho, vol. 1948, p. 122, en la que el tribunal dictaminó que el operador económico estaba obligado a adoptar una medida de control de la seguridad sobre la base de las referidas Directrices).

⁽¹⁶⁾ Directrices de la CPIP (Edición de la norma general), p. 6.

⁽¹⁷⁾ Se aplica a cualquier sistema de archivo electrónico. Las Directrices de la CPIP (edición de la norma general, p. 17) ofrecen ejemplos concretos a este respecto, por ejemplo un listado de direcciones de correo electrónico almacenado en el programa cliente de correo electrónico.

⁽¹⁸⁾ Artículo 2, apartados 4 y 6, de la LPIP.

«facilitados para su finalidad original sin la adición de ninguna otra información que concierna a un particular vivo». según las explicaciones dadas por la CPIP, esta limitada excepción se introdujo con la finalidad de excluir las guías telefónicas u otros tipos de directorios similares.

- (21) En el caso de los datos recogidos en Japón, esta distinción entre «información personal» y «datos personales» es pertinente ya que dicha información no siempre forma parte de una «base de datos de información personal» (por ejemplo, un conjunto único de datos recogidos y tratados manualmente) y, por lo tanto, no serán de aplicación las disposiciones de la LPIP que solo se refieren a datos personales ⁽¹⁹⁾.
- (22) Por el contrario, esta distinción no será pertinentes para los datos personales importados de la Unión Europea a Japón sobre la base de una decisión de adecuación. Como estos datos se suelen transferir por medios electrónicos (pues en la era digital es esta la forma habitual de intercambio de datos, especialmente a gran distancia, como ocurre entre la UE y Japón), y, por lo tanto, pasan a formar parte del fichero electrónico del importador, tales datos de la UE entraran en la categoría de «datos personales» en virtud de la LPIP. En el caso excepcional de que los datos personales se transfirieran desde la UE por otros medios (p. ej. en formato papel), seguirán estando cubiertos por la LPIP si, tras la transferencia, pasan a formar parte de un «corpus colectivo de información» organizado sistemáticamente a fin de facilitar la búsqueda de información específica [artículo 2, apartado 4, inciso ii), de la LPIP]. Con arreglo al artículo 3, apartado 2, de la Orden del Gabinete, este será el caso cuando la información se organice «con arreglo a una cierta norma» y la base de datos incluya herramientas tales como, por ejemplo, una tabla de contenido o un índice para facilitar la búsqueda. Esto se corresponde con la definición de «fichero» en el sentido del artículo 2, apartado 1, del RGPD.

2.2.3. Definición de «datos personales conservados»

- (23) Determinadas disposiciones de la LPIP, en particular los artículos 27 a 30, relativos a los derechos individuales, solo se aplican a una categoría específica de datos personales, los «datos personales conservados». En el artículo 2, apartado 7, de la LPIP, estos datos se definen como los datos personales distintos de aquellos que i) «conforme a una orden del Gabinete, podrían perjudicar a los intereses públicos o a otros intereses si se llegara a conocer su presencia o ausencia» o ii) «deben ser suprimidos en un plazo no superior a un año que será definido por orden del Gabinete».
- (24) La primera de estas dos categorías se explica en el artículo 4 de la Orden del Gabinete y comprende cuatro tipos de exenciones ⁽²⁰⁾. Estas exenciones persiguen objetivos similares a los recogidos en el artículo 23, apartado 1, del Reglamento (UE) 2016/679, en particular la protección del interesado («interesado principal» en la terminología de la LPIP) y las libertades de otros, la seguridad nacional, la seguridad pública, la ejecución de sanciones penales u otros objetivos importantes de interés público general. Además, de la redacción del artículo 4, apartado 1, incisos i) a iv), de la Orden del Gabinete se desprende que su aplicación presupone siempre un riesgo específico para uno de los intereses importantes protegidos ⁽²¹⁾.
- (25) La segunda categoría se ha perfilado de forma más detallada en el artículo 5 de la Orden del Gabinete. Leído en relación con el artículo 2, apartado 7, de la LPIP, excluye del ámbito de aplicación del concepto de datos personales conservados, y, por ende, de los derechos individuales garantizados por la LPIP, los datos personales que «deben ser suprimidos» en un plazo de seis meses. La CPIP ha explicado que esta exención tiene por objeto incentivar a los operadores económicos a conservar y tratar los datos el tiempo más breve posible. Sin embargo, esto significaría que los interesados de la UE no podrían disfrutar de importantes derechos solo en razón de la duración de la conservación de sus datos por el operador económico de que se trate.
- (26) A fin de poner remedio a esta situación, la Regla complementaria n.º 2 dispone que los datos personales transferidos desde la Unión Europea «se considerarán datos personales conservados en el sentido del artículo 2, apartado 7, de la Ley, con independencia del plazo previsto para su supresión». Por lo tanto, el período de conservación no afectará a los derechos conferidos a los interesados de la UE.

⁽¹⁹⁾ Por ejemplo, el artículo 23 de la LPIP, relativo a las condiciones para el intercambio de datos personales con terceros.

⁽²⁰⁾ A saber, los datos personales i) «en relación con los cuales, si se llegara a conocer su presencia o su ausencia, existe el riesgo de que ello sea perjudicial para la vida, la integridad física o el patrimonio de un interesado principal o de un tercero»; ii) los datos «en relación con los cuales, si se llegara a conocer su presencia o su ausencia, existe el riesgo de que ello aliente o induzca a cometer un acto ilícito o injusto»; iii) los datos «en relación con los cuales, si se llegara a conocer su presencia o ausencia, existe el riesgo de que se vea comprometida la seguridad nacional, se destruya una relación de confianza con un país extranjero o una organización internacional, o suponga una situación de desventaja en las negociaciones con un país extranjero o una organización internacional»; y iv) los datos «en relación con los cuales, si se llegara a conocer su presencia o su ausencia, existe el riesgo de que ello obstaculice el mantenimiento del orden público y de la seguridad pública, por ejemplo en lo que respecta a la prevención, represión o investigación de un delito».

⁽²¹⁾ En estas condiciones, no se requiere la notificación del particular, lo que está en consonancia con el artículo 23, apartado 2, letra h), del RGPD, que dispone que los interesados no tienen que ser informados sobre la limitación si ello «puede ser perjudicial a los fines de esta».

2.2.4. Definición de «información personal tratada de forma anónima»

- (27) Los requisitos aplicables a la información personal tratada de forma anónima, tal como se define en el artículo 2, apartado 9, de la LPIP, se establecen en el capítulo IV, sección 2, de la Ley («Funciones de un operador económico que maneja información tratada de forma anónima»). Por el contrario, dicha información no se rige por las disposiciones del capítulo IV, sección 1, de la LPIP, que incluyen los artículos en los que se establecen las salvaguardas en materia de protección de datos y los derechos aplicables al tratamiento de los datos personales en virtud de dicha Ley. Por consiguiente, aunque la «información personal tratada de forma anónima» no está sujeta a las normas «estándar» en materia de protección de datos (especificadas en el capítulo IV, sección 1, y en el artículo 42 de la LPIP), sí que entra en el ámbito de aplicación de la LPIP, en particular de sus artículos 36 a 39.
- (28) De conformidad con el artículo 2, apartado 9, de la LPIP, se entiende por «información personal tratada de forma anónima» la información sobre un particular que ha sido «producida a partir del tratamiento de información personal» sirviéndose de las medidas dispuestas en la LPIP (artículo 36, apartado 1) y especificadas en las Normas de la CPIP (artículo 19), de manera que resulte imposible identificar a un particular concreto o restablecer la información personal.
- (29) De estas disposiciones se desprende, y así lo ha confirmado también la CPIP, que el proceso de «anonimización» de la información personal no debe ser técnicamente irreversible. Con arreglo al artículo 36, apartado 2, de la LPIP, simplemente se exige que los operadores económicos que manejan «información personal tratada de forma anónima» impidan la reidentificación adoptando medidas destinadas a garantizar la seguridad de las «descripciones [...]» y los códigos de identificación individuales suprimidos de la información personal utilizada para producir la información tratada de forma anónima, y la información relativa al método de tratamiento aplicado».
- (30) Dado que la «información personal tratada de forma anónima», tal como se define en la LPIP, incluye datos mediante los cuales aún es posible la reidentificación del particular, ello podría significar que los datos personales transferidos desde la Unión Europea podrían perder parte de las protecciones disponibles a través de un proceso que, de conformidad con el Reglamento (UE) 2016/679, sería considerado una forma de «seudonimización» más bien que de «anonimización» (por lo que no se alteraría su naturaleza como datos personales).
- (31) Para poner remedio a esta situación, las Reglas complementarias prevén requisitos adicionales aplicables únicamente a los datos personales transferidos desde la Unión Europea en virtud de la presente Decisión. De conformidad con la Regla n.º 5 de las Reglas complementarias, esta información personal solo se considera «información personal tratada de forma anónima» en el sentido de la LPIP «si el operador económico que maneja la información personal adopta medidas para hacer irreversible la anonimización del particular para otros, en particular suprimiendo la información relativa, entre otras cosas, al método de tratamiento». Esta disposición se desarrolla en las Reglas complementarias, que especifican que se trata de la información relativa a las descripciones y los códigos de identificación individuales que hayan sido suprimidos de la información personal utilizada para producir «información personal tratada de forma anónima», así como la información relativa a la aplicación de un método de tratamiento al suprimir estas descripciones y códigos de identificación individuales. En otros términos, las Reglas complementarias exigen que el operador económico que produce «información personal tratada de forma anónima» destruya la «clave» que permite la reidentificación de los datos. Esto significa que los datos personales originarios de la Unión Europea solo estarán sujetos a las disposiciones de la LPIP relativas a la «información personal tratada de forma anónima» en los casos en que también se consideren información anónima en virtud del Reglamento (UE) 2016/679 ⁽²²⁾.

2.2.5. Definición de «operador económico que maneja información personal» (OEMIP)

- (32) En lo que respecta a su ámbito de aplicación personal, la LPIP solo se aplica a los OEMIP. El concepto de OEMIP se define en el artículo 2, apartado 5, de la LPIP como «una persona que facilita una base de datos de información personal para su uso en el marco de una actividad económica», con exclusión del Gobierno y de las agencias administrativas, tanto a nivel central como local.
- (33) Con arreglo a las Directrices de la CPIP, se entiende por «actividad económica» cualquier «práctica destinada a la explotación reiterada y continua de una empresa reconocida socialmente con miras a la consecución de un determinado objetivo, con independencia de que tenga o no ánimo de lucro». Las organizaciones sin personalidad jurídica (como las asociaciones de hecho) o los particulares se consideran OEMIP si facilitan (utilizan) una base de datos personales para sus actividades económicas ⁽²³⁾. El concepto de «actividad económica» en la LPIP es por tanto muy amplio, pues incluye no solo las actividades lucrativas, sino también las que no tienen ánimo de lucro, llevadas a cabo por todo tipo de organizaciones y particulares. Por otra parte, el «uso en el marco de una actividad económica» abarca asimismo la información personal que no es utilizada en las relaciones comerciales (externas) del operador, sino a nivel interno, por ejemplo el tratamiento de los datos de los trabajadores.

⁽²²⁾ Véase el Reglamento (UE) 2016/679, considerando 26.

⁽²³⁾ Directrices de la CPIP (Edición de la norma general), p. 18.

- (34) Por lo que se refiere a los beneficiarios de las protecciones previstas en la LPIP, la Ley no establece ninguna distinción en función de la nacionalidad, la residencia o la localización. Lo mismo ocurre respecto de las posibilidades para obtener reparación, ya sea ante la CPIP o ante los tribunales.

2.2.6. Los conceptos de «responsable del tratamiento» y «encargado del tratamiento»

- (35) En virtud de la LPIP no se establece una distinción específica de las obligaciones impuestas a los responsables y a los encargados del tratamiento. El hecho de que no se reconozca esta distinción no afecta al nivel de protección, porque todos los OEMIP están sujetos al conjunto de las disposiciones de la Ley. Un OEMIP que confíe el manejo de datos personales a un mandatario (el equivalente de un encargado en el RGPD) está sujeto a las obligaciones que imponen la LPIP y las Reglas complementarias con respecto a los datos confiados. Además, en virtud del artículo 22 de la LPIP, está obligado a «ejercer una supervisión necesaria y apropiada» del mandatario. A su vez, como ha confirmado la CPIP, el mandatario está vinculado por todas las obligaciones previstas en la APPI y las Reglas complementarias.

2.2.7. Exclusiones sectoriales

- (36) El artículo 76 de la LPIP excluye ciertas categorías de tratamiento de datos del ámbito de aplicación del capítulo IV de la Ley, que contiene las principales disposiciones en materia de protección de datos (principios de base, obligaciones de los operadores económicos, derechos individuales, control por parte de la CPIP). El tratamiento cubierto por la exclusión sectorial prevista en el artículo 76 también está exento de las competencias de ejecución forzosa de la CPIP, con arreglo a lo dispuesto en el artículo 43, apartado 2, de la LPIP ⁽²⁴⁾.
- (37) Las categorías pertinentes para la exclusión sectorial prevista en el artículo 76 de la CPIP se definen utilizando un doble criterio basado en el tipo de OEMIP que trata la información personal y la finalidad del tratamiento. Más concretamente, la exclusión se aplica a: i) los organismos de radiodifusión, los editores de periódicos, las agencias de comunicación u otras organizaciones de prensa (incluidos los particulares que ejercen actividades de prensa), en la medida en que traten información personal para la prensa; ii) los escritores profesionales, en la medida en que manejen información personal; iii) las universidades y otras organizaciones o grupos relacionados con los estudios académicos, o cualquier persona adscrita a una organización de este tipo, en la medida en que traten información personal con fines académicos; iv) las instituciones religiosas en la medida en que traten información personal con fines religiosos (incluidas todas las actividades afines); y v) los organismos políticos en la medida en que traten información personal con fines políticos (incluidas todas las actividades afines). El tratamiento de información personal con uno de los fines enumerados en el artículo 76 por otros tipos de OEMIP, así como el tratamiento de información personal por uno de los OEMIP enumerados con otros fines, por ejemplo en el marco del empleo, siguen estando cubiertos por las disposiciones del capítulo IV.
- (38) Con el fin de garantizar un nivel de protección adecuado de los datos personales transferidos desde la Unión Europea a operadores económicos en Japón, solo debe estar cubierto por la presente Decisión el tratamiento de información personal que entre en el ámbito de aplicación del capítulo IV de la LPIP (es decir, el tratamiento realizado por un OEMIP en la medida en que no corresponda a ninguna de las exclusiones sectoriales). Por consiguiente, su ámbito de aplicación debe adaptarse al de la LPIP. Según la información recibida de la CPIP, cuando un OEMIP cubierto por la presente Decisión modifique ulteriormente la finalidad de la utilización (en la medida en que esté permitido), pasando así a estar cubierto por una de las exclusiones sectoriales previstas en el artículo 76 de la LPIP, se consideraría que se trata de una transferencia internacional (dado que, en tales casos, el tratamiento de la información personal dejaría de estar cubierto por el capítulo IV de la LPIP y quedaría por tanto fuera de su ámbito de aplicación). Lo mismo se aplicaría en caso de que un OEMIP facilitara información personal a una entidad cubierta por el artículo 76 de la LPIP para su utilización a efectos de una de las finalidades de tratamiento indicadas en dicha disposición. Por lo que respecta a los datos personales transferidos desde la Unión Europea, se trataría por tanto de una transferencia ulterior sujeta a las salvaguardas pertinentes (en particular, las especificadas en el artículo 24 de la LPIP y la Regla complementaria n.º 4). Cuando el OEMIP se base en el consentimiento del interesado ⁽²⁵⁾, tendría que facilitarle toda la información necesaria, en particular que la información personal dejaría de estar protegida por la LPIP.

⁽²⁴⁾ En lo que respecta a los demás operadores, la CPIP no debe obstaculizar, en el ejercicio de sus competencias, su derecho a la libertad de expresión, la libertad de cátedra, la libertad religiosa y la libertad de actividad política (artículo 43, apartado 1, de la LPIP).

⁽²⁵⁾ Como ha explicado la CPIP, el consentimiento se interpreta en las Directrices de la CPIP como «expresión de una voluntad del interesado principal en el sentido de que acepta que la información personal que le concierne pueda ser manejada utilizando un método indicado por una empresa encargada del manejo de información personal». Las Directrices de la CPIP (Edición de la norma general, p. 24) recogen la lista de formas de consentimiento que se consideran «prácticas empresariales habituales en Japón», es decir, alcanzar un acuerdo verbal, devolver formularios u otros documentos, manifestar un acuerdo por correo electrónico, marcar una casilla en una página web, hacer clic en una página de Internet, utilizar un botón de consentimiento, pulsar un panel táctil, etc. Todos estos métodos constituyen una forma de consentimiento expreso.

2.3. Salvaguardas, derechos y obligaciones

2.3.1. Limitación de la finalidad

- (39) Los datos personales deben tratarse con una finalidad específica y, posteriormente, solo deben utilizarse en la medida en que ello no sea incompatible con la finalidad del tratamiento. Este principio de protección de datos está garantizado por los artículos 15 y 16 de la LPIP.
- (40) La LPIP se sustenta en el principio de que un operador económico tiene que especificar la finalidad de la utilización «de la forma más explícita posible» (artículo 15, apartado 1) y, por tanto, está vinculado por dicha finalidad al tratar los datos.
- (41) A este respecto, el artículo 15, apartado 2, de la LPIP dispone que el OEMIP no puede modificar la finalidad inicial «más allá de lo que sea razonablemente pertinente para la finalidad de la utilización con anterioridad a la modificación», lo que las Directrices de la CPIP interpretan como lo que puede ser objetivamente anticipado por el interesado sobre la base de «convenciones sociales normales» ⁽²⁶⁾.
- (42) Por otra parte, el artículo 16, apartado 1, de la LPIP prohíbe a los OEMIP manejar información personal más allá de «lo que sea necesario para lograr una finalidad de utilización» especificada en el artículo 15 sin obtener previamente el consentimiento del interesado, salvo que se aplique una de las excepciones previstas en el artículo 16, apartado 3 ⁽²⁷⁾.
- (43) Cuando se trata de información personal adquirida de otro operador económico, el OEMIP es, en principio, libre de fijar una nueva finalidad de utilización ⁽²⁸⁾. Con el fin de garantizar que, en el caso de transferencia desde la Unión Europea, tal destinatario esté vinculado por la finalidad para la que se transfirieron los datos, la Regla complementaria n.º 3 exige que, «en aquellos casos en que un [OEMIP] reciba datos personales desde la UE sobre la base de una decisión de adecuación» o tal operador «reciba de otro [OEMIP] datos personales transferidos previamente desde la UE sobre la base de una decisión de adecuación (comunicación ulterior), el destinatario debe «especificar que dichos datos personales se utilizarán en la medida en que sea necesario para la finalidad de utilización para la cual los datos fueron recibidos inicialmente o posteriormente». Esta Regla garantiza pues que, en el contexto de una transferencia, la finalidad especificada con arreglo al Reglamento (UE) 2016/679 sigue determinando el tratamiento y que una modificación de dicha finalidad en cualquiera de las fases de la cadena de tratamiento en Japón requeriría el consentimiento del interesado de la UE. Aunque la obtención de dicho consentimiento requiere que el OEMIP se ponga en contacto con el interesado, cuando ello sea imposible, la única consecuencia es que debe mantenerse la finalidad original.

2.3.2. Legalidad y equidad del tratamiento

- (44) La protección adicional a que se hace referencia en el considerando 43 es tanto más pertinente cuanto que es gracias al principio de limitación de la finalidad que el sistema japonés garantiza igualmente un tratamiento lícito y equitativo de los datos personales.
- (45) En virtud de la LPIP, cuando un OEMIP recoge información personal, ha de especificar de manera detallada la finalidad de la utilización de la información personal ⁽²⁹⁾ e informar rápidamente al interesado de esta finalidad (o hacerla pública) ⁽³⁰⁾. Además, el artículo 17 de la LPIP dispone que un OEMIP no puede adquirir información personal de forma engañosa o por otros medios inapropiados. Por lo que se refiere a ciertas categorías de datos como la información personal que exige especial atención, su adquisición requiere el consentimiento del interesado (artículo 17, apartado 2, de la LPIP).

⁽²⁶⁾ La sección de preguntas y respuestas de la CPIP contiene una serie de ejemplos que ilustran este concepto. Entre los ejemplos de situaciones en las que la modificación no va más allá de lo razonablemente pertinente, cabe destacar la utilización de información personal adquirida de los compradores de bienes o servicios en el marco de una operación comercial, con el fin de informarles de la disponibilidad de otros bienes o servicios pertinentes (p. ej. el operador de un gimnasio que registra las direcciones de correo electrónico de los miembros para informarles de los cursos y programas impartidos). Al mismo tiempo, la sección de preguntas y respuestas incluye igualmente un ejemplo de una situación en la que la modificación de la finalidad de utilización no está permitida (el de una empresa que envía información sobre sus bienes y servicios a direcciones de correo electrónico que ha recopilado con el fin de advertir contra la utilización fraudulenta o el robo de una tarjeta de miembro).

⁽²⁷⁾ Estas exenciones pueden resultar de otras disposiciones legales y reglamentarias o estar relacionadas con situaciones en las que el manejo de información personal sea necesario i) para la «protección de la vida humana, la integridad física o el patrimonio»; ii) para «la mejora de la higiene pública o la promoción del crecimiento de niños sanos»; o iii) para a «la cooperación con las agencias u organismos gubernamentales o con sus representantes» en el ejercicio de sus misiones estatutarias. Por otra parte, las categorías i) y ii) solo se aplican si resulta difícil obtener el consentimiento del interesado, y la categoría iii), si existe un riesgo de que la obtención del consentimiento del interesado interfiera con el desempeño de dichas tareas.

⁽²⁸⁾ Dicho esto, del artículo 23, apartado 1, de la LPIP se desprende que la comunicación de datos a un tercero requiere, en principio, el consentimiento del particular de que se trate. De esta forma, el particular puede ejercer un cierto control sobre la utilización de sus datos por parte de otro operador económico.

⁽²⁹⁾ De conformidad con el artículo 15, apartado 1, de la LPIP, tal especificación debe ser «lo más explícita posible».

⁽³⁰⁾ Artículo 18, apartado 1, de la LPIP.

- (46) Posteriormente, como se ha explicado en los considerandos 41 y 42, el OEMIP no puede tratar la información personal para otras finalidades, a no ser que el interesado haya dado su consentimiento a dicho tratamiento o que se aplique una de las excepciones previstas en el artículo 16, apartado 3, de la LPIP.
- (47) Por último, en lo que respecta a la puesta a disposición ulterior de información personal a un tercero⁽³¹⁾, el artículo 23, apartado 1, de la LPIP limita dicha comunicación a ciertos casos específicos, en general previo consentimiento del interesado⁽³²⁾. El artículo 23, apartados 2, 3 y 4, de la LPIP prevé una serie de excepciones al requisito de obtener el consentimiento. Sin embargo, estas excepciones solo son aplicables a los datos no sensibles y requieren que el operador económico informe de antemano a los particulares afectados de su intención de comunicar la información personal que le concierne a un tercero y de la posibilidad de oponerse a toda comunicación ulterior⁽³³⁾.
- (48) Por lo que respecta a las transferencias desde la Unión Europea, los datos personales tendrán que haber sido recogidos y tratados primero en la UE de conformidad con el Reglamento (UE) 2016/679. Esto implicará siempre, por una parte, la recogida y el tratamiento, en particular para la transferencia desde la Unión Europea a Japón, sobre la base de una de las condiciones que se mencionan en el artículo 6, apartado 1, del Reglamento y, por otra, la recogida con una finalidad específica, explícita y legítima, así como la prohibición de tratamiento ulterior, incluso por medio de una transferencia, en una forma que sea incompatible con dicha finalidad, tal como se establece en el artículo 5, apartado 1, letra b), y en el artículo 6, apartado 4, del Reglamento.
- (49) Con arreglo a la Regla complementaria n.º 3, tras la transferencia, el OEMIP que vaya a recibir los datos deberá «confirmar» la finalidad o finalidades específicas subyacentes a la transferencia [es decir, la finalidad especificada de conformidad con el Reglamento (UE) 2016/679] y tratar ulteriormente estos datos en consonancia con tal finalidad o finalidades⁽³⁴⁾. Esto significa que no solo el primer adquirente de tales datos personales en Japón, sino también cualquier futuro destinatario de los datos (incluido un mandatario), está vinculado por la finalidad o finalidades especificadas en virtud del Reglamento.
- (50) Por otra parte, en caso de que el OEMIP desee modificar la finalidad especificada previamente en virtud del Reglamento (UE) 2016/679, el artículo 16, apartado 1, de la LPIP dispone que tiene que obtener, en principio, el consentimiento del interesado. Sin tal consentimiento, cualquier tratamiento de datos que vaya más allá de lo necesario para alcanzar esa finalidad de utilización constituiría una infracción del artículo 16, apartado 1, que podría ser invocada por la CPIP y por los órganos jurisdiccionales competentes.
- (51) Por ende, puesto que, en virtud del Reglamento (UE) 2016/679, una transferencia requiere una base jurídica válida y una finalidad específica, que se reflejan en la finalidad de utilización «confirmada» en virtud de la LPIP, la combinación de las disposiciones aplicables de la LPIP y de la Regla complementaria n.º 3 garantiza que el tratamiento de los datos de la UE en Japón seguirá siendo lícito.

2.3.3. Exactitud y minimización de los datos

- (52) Los datos deben ser exactos y, en caso necesario, se han de mantener actualizados. También deben ser adecuados, pertinentes y no excesivos con respecto a las finalidades para las que se traten.
- (53) Estos principios están consagrados en la legislación japonesa en el artículo 16, apartado 1, de la LPIP, que prohíbe el manejo de información personal más allá de «lo necesario para alcanzar una finalidad de utilización». Como ha explicado la CPIP, esta prohibición no solo excluye una utilización de los datos que no sea adecuada y el uso excesivo de datos (más allá de lo que sea necesario para alcanzar la finalidad de utilización), sino que implica asimismo la prohibición de manejar datos no pertinentes para alcanzar la finalidad de utilización.

⁽³¹⁾ Aunque los mandatarios están excluidos de la noción de «terceros» a los efectos de la aplicación del artículo 23 (véase el apartado 5), esta exclusión solo se aplica en la medida en que el mandatario maneje datos personales dentro de los límites del mandato («en la medida necesaria para alcanzar una finalidad de utilización»), es decir, actúe como encargado.

⁽³²⁾ Los otros motivos (excepcionales) son los siguientes: i) la puesta a disposición de información personal «sobre la base de disposiciones legales y reglamentarias»; ii) los casos «en que sea necesario proteger una vida humana, la integridad física o el patrimonio, y resulte difícil obtener el consentimiento del interesado principal»; iii) en los casos «en que sea especialmente necesario mejorar la higiene pública o promover la buena salud de los niños, y resulte difícil obtener el consentimiento del interesado principal»; y iv) en los casos «en que sea necesario cooperar con un organismo de la Administración central o de una Administración local o con una persona a la que estas hayan encomendado la realización de tareas preceptuadas por disposiciones legales o reglamentarias, y cuando exista la posibilidad de que la obtención del consentimiento del principal interfiera con el desempeño de dichas tareas».

⁽³³⁾ La información que ha de facilitarse incluye, en particular, las categorías de datos personales que vayan a compartirse con un tercero y el método de transmisión. Por otra parte, el OEMIP debe informar al interesado de la posibilidad de oponerse a la transmisión y de la forma de presentar dicha demanda.

⁽³⁴⁾ Con arreglo al artículo 26, apartado 1, inciso ii), de la LPIP, un OEMIP está obligado, cuando recibe datos personales procedentes de un tercero, a «confirmar» (verificar) los «detalles relativos a la adquisición de los datos personales por el tercero», en particular la finalidad de dicha adquisición. Aunque el artículo 26 no exige expresamente que el OEMIP tenga que respetar esta finalidad, sí lo hace de manera explícita la Regla complementario n.º 3.

- (54) Por lo que se refiere a la obligación de mantener los datos exactos y actualizados, el artículo 19 de la LPIP exige que el OEMIP «vele por mantener los datos personales exactos y actualizados en la medida necesaria para alcanzar la finalidad de utilización». Esta disposición debe leerse en relación con el artículo 16, apartado 1, de la LPIP: según las explicaciones dadas por la CPIP, si un OEMIP no cumple los estándares de exactitud prescritos, no se considerará que el tratamiento de la información personal persigue la finalidad de utilización, por lo que su manejo será ilícito en virtud del artículo 16, apartado 1.

2.3.4. Limitación de la conservación

- (55) En principio, los datos no deben conservarse más tiempo del que sea necesario para las finalidades para las que se traten.
- (56) De conformidad con el artículo 19 de la LPIP, los OEMIP deben «velar [...] por suprimir los datos personales sin demora cuando su utilización haya dejado de ser necesaria». Esta disposición debe leerse en relación con el artículo 16, apartado 1, de la LPIP, que prohíbe el manejo de información personal más allá de «lo necesario para alcanzar una finalidad de utilización». Una vez alcanzada la finalidad de utilización, el tratamiento de la información personal no puede considerarse necesario y, por tanto, no puede continuar (a menos que el OEMIP obtenga el consentimiento del interesado a tal fin).

2.3.5. Seguridad de los datos

- (57) Los datos personales deben ser tratados de modo que se garantice su seguridad, incluida la protección contra todo tratamiento no autorizado o ilícito y contra su pérdida, destrucción o deterioro de origen accidental. A tal fin, los operadores económicos deben adoptar las medidas técnicas u organizativas apropiadas para proteger los datos personales frente a posibles amenazas. Estas medidas deben evaluarse teniendo en cuenta los últimos avances y los costes conexos.
- (58) En el ordenamiento jurídico japonés, este principio está consagrado en el artículo 20 de la LPIP, que dispone que un OEMIP «deberá adoptar las medidas necesarias apropiadas para garantizar el control de la seguridad de los datos personales, en particular a fin de prevenir la fuga, la pérdida o el deterioro de los datos personales que maneje». Las Directrices de la CPIP explican las medidas que deben adoptarse, incluidos los métodos que se han de seguir para establecer las políticas de base, las normas relativas al manejo de los datos y una serie de «acciones de control» (relativas tanto a la seguridad organizativa como a la seguridad humana, física y tecnológica) ⁽³⁵⁾. Además, las Directrices de la CPIP y una nota específica (apéndice 8 relativo al «Contenido de las medidas de gestión de la seguridad que han de tomarse») publicada por la CPIP ofrecen más detalles sobre las medidas relativas a los incidentes de seguridad que impliquen, por ejemplo, la fuga de información personal, en el marco de las medidas de gestión de la seguridad que debe adoptar el OEMIP ⁽³⁶⁾.
- (59) Por otra parte, cada vez que manejen datos personales los empleados o subcontratistas, los artículos 20 y 21 de la LPIP disponen que debe garantizarse una «supervisión necesaria y apropiada» a efectos de control de la seguridad. Por último, el artículo 83 de la LPIP impone una pena de hasta un año de prisión en caso de fuga intencional o robo de información personal.

2.3.6. Transparencia

- (60) Los interesados deben ser informados de las principales características del tratamiento de sus datos personales.
- (61) El artículo 18, apartado 1, de la LPIP exige que el OEMIP ponga la información sobre la finalidad de la utilización de la información personal adquirida a disposición del interesado, excepto en «los casos en que una finalidad de utilización ya haya sido hecha pública previamente». La misma obligación se aplica en el caso de modificación lícita de la finalidad (artículo 18, apartado 3). Así se garantiza también que el interesado sea informado del hecho de que sus datos han sido recogidos. Aunque la LPIP no exige en general que el OEMIP informe al interesado sobre los destinatarios previstos de la información personal en la fase de recogida, tal información es una condición necesaria para cualquier comunicación ulterior de información a un tercero (destinatario) sobre la base del artículo 23, apartado 2, es decir, cuando esta transmisión se hace sin el consentimiento previo del interesado.

⁽³⁵⁾ Directrices de la CPIP (Edición de la norma general), p. 41 y pp. 86 a 98.

⁽³⁶⁾ Con arreglo a la sección 3-3-2 de las Directrices de la CPIP, en caso de fuga, deterioro o pérdida, el OEMIP está obligado a realizar las investigaciones necesarias y, en particular, a evaluar la magnitud de la vulneración de los derechos e intereses del particular, así como la naturaleza y el volumen de la información personal afectada.

- (62) En lo que respecta a los «datos personales conservados», el artículo 27 de la LPIP establece que el OEMIP debe informar al interesado de su identidad (datos de contacto), de la finalidad de la utilización y de los procedimientos previstos para responder a cualquier solicitud relativa a los derechos individuales del interesado formulada en virtud de los artículos 28, 29 y 30 de la LPIP.
- (63) Habida cuenta de que, en virtud de las Reglas complementarias, los datos personales transferidos desde la Unión Europea se consideran (a menos que estén cubiertos por una exención) «datos personales conservados», con independencia de su período de conservación, siempre estarán sometidos a los requisitos de transparencia en virtud de las disposiciones antes mencionadas.
- (64) Tanto los requisitos del artículo 18 como la obligación de informar sobre la finalidad de la utilización prevista en el artículo 27 de la LPIP están sujetos al mismo conjunto de excepciones, en su mayoría basadas en consideraciones de interés público y la protección de los derechos e intereses del interesado, de los terceros y del responsable del tratamiento ⁽³⁷⁾. Según la interpretación desarrollada en las Directrices de la CPIP, esas excepciones se aplican en situaciones muy específicas, por ejemplo cuando la información sobre la finalidad de la utilización pueda socavar las medidas legítimas adoptadas por el operador económico para proteger ciertos intereses (p. ej. la lucha contra el fraude, el espionaje industrial o el sabotaje).

2.3.7. Categorías especiales de datos

- (65) Deben preverse salvaguardas específicas cuando se estén tratando «categorías especiales» de datos.
- (66) El concepto de «información personal que requiere especial atención» se define en el artículo 2, apartado 3, de la LPIP. Esta disposición hace referencia a la «información personal que revele la raza, el credo, el estatus social, el historial médico, los antecedentes penales, el hecho de haber sufrido daños resultantes de un delito, u otras descripciones prescritas por la Orden del Gabinete, por ejemplo aquellas cuyo manejo requiera especial atención a fin de evitar que el interesado principal sufra discriminación injusta, prejuicio o cualquier otro daño». Estas categorías se corresponden en gran medida con la lista de datos sensibles recogida en los artículos 9 y 10 del Reglamento (UE) 2016/679. En concreto, «historial médico» corresponde a los datos relativos a la salud, mientras que «los antecedentes penales y el hecho de haber sufrido daños resultantes de un delito» son sustancialmente idénticos a las categorías a que se refiere el artículo 10 del Reglamento (UE) 2016/679. Las categorías contempladas en el artículo 2, apartado 3, de la LPIP se explican en más detalle en la Orden del Gabinete y en las Directrices de la CPIP. Con arreglo a la sección 2.3, punto 8, de las Directrices de la CPIP, las subcategorías de «historial médico» que se detallan en el artículo 2, incisos ii) y iii), de la Orden del Gabinete se interpretan en el sentido de que incluyen los datos genéticos y biométricos. Además, aunque la lista no incluye expresamente los términos «origen étnico» y «opiniones políticas», sí incorpora referencias a la «raza» y el «credo». Como se explica en la sección 2.3, puntos 1 y 2, de las Directrices de la CPIP, la referencia a la «raza» abarca «los vínculos étnicos o los vínculos con una determinada parte del mundo», mientras que por «credo» se entiende tanto las convicciones religiosas como las opiniones políticas.
- (67) Como se desprende claramente del tenor de la disposición, no se trata de una lista cerrada, ya que podrían añadirse otras categorías de datos en la medida en que su tratamiento entrañe un riesgo de «discriminación injusta, prejuicio o cualquier otro daño para el interesado principal».
- (68) Aunque el concepto de datos «sensibles» es, por su propia naturaleza, un constructo social en la medida en que se sustenta en tradiciones culturales y jurídicas, consideraciones de orden moral, opciones políticas, etc. de una sociedad dada, habida cuenta de la importancia de garantizar salvaguardas adecuadas para los datos sensibles cuando se transfieren a operadores económicos en Japón, la Comisión ha obtenido que las protecciones especiales previstas para la «información que requiere especial atención» en virtud del Derecho japonés se hagan extensivas a todas las categorías reconocidas como «datos sensibles» en el Reglamento (UE) 2016/679. A tal fin, la Regla complementaria n.º 1 establece que los datos transferidos desde la Unión Europea relativos a la vida sexual, la orientación sexual o la afiliación sindical serán tratados por los OEMIP «de la misma manera que la información personal que requiere especial atención en el sentido del artículo 2, apartado 3, de la LPIP».

⁽³⁷⁾ Se trata de: i) los casos en que exista la posibilidad de que el hecho de informar al interesado de la finalidad de la utilización, o de hacerla pública, pudiera «perjudicar la vida humana, la integridad física, el patrimonio u otros derechos e intereses del interesado principal o de un tercero» o «los derechos o intereses legítimos del [...] OEMIP»; ii) los casos en que «sea necesario cooperar con un organismo de la Administración central o de una Administración local» en el ejercicio de sus funciones estatutarias y si tal información o comunicación pudiera interferir con tales «funciones»; iii) los casos en que esté clara la finalidad de la utilización sobre la base de la situación en que se hayan adquirido los datos.

- (69) En lo que respecta a las salvaguardas sustantivas adicionales aplicables a la información personal que requiere especial atención, el artículo 17, apartado 2, de la LPIP, prohíbe a los OEMIP adquirir este tipo de datos sin el consentimiento previo del particular de que se trate, con la única salvedad de algunas excepciones limitadas⁽³⁸⁾. Además, esta categoría de información personal está excluida de la posibilidad de una comunicación a terceros sobre la base del procedimiento previsto en el artículo 23, apartado 2, de la LPIP (que permite la transmisión de datos a terceros sin el consentimiento previo del particular de que se trate).

2.3.8. Responsabilidad

- (70) De conformidad con el principio de responsabilidad, las entidades que traten datos están obligadas a adoptar las medidas técnicas y organizativas apropiadas para cumplir efectivamente sus obligaciones en materia de protección de datos y deben demostrar el respeto de estas obligaciones, en particular ante la autoridad de control competente.
- (71) Como se indica en la nota 34 (considerando 49), los OEMIP están obligados, en virtud del artículo 26, apartado 1, de la LPIP, a verificar la identidad de un tercero que les facilita datos personales y las «circunstancias» en las que adquirió dichos datos (si se trata de datos personales cubiertos por la presente Decisión, de conformidad con la LPIP y la Regla complementaria n.º 3, esas circunstancias incluirán el hecho de que los datos proceden de la Unión Europea, así como la finalidad para la cual los datos fueron transferidos inicialmente). Entre otras cosas, esta medida tiene por objeto garantizar la legalidad del tratamiento de datos a lo largo de la cadena de manejo de datos personales por los OEMIP. Además, en virtud del artículo 26, apartado 3, de la LPIP, los OEMIP están obligados a llevar un registro de la fecha de recepción y de la información (obligatoria) facilitada por el tercero con arreglo al apartado 1, así como del nombre del particular (interesado) de que se trate, de las categorías de datos tratados y, en la medida en que sea pertinente, del hecho de que el interesado haya dado su consentimiento para intercambiar sus datos personales. Como se indica en el artículo 18 de las Normas de la CPIP, esos registros deben conservarse durante un período de al menos uno a tres años, en función de las circunstancias. En el ejercicio de sus funciones, la CPIP puede exigir la presentación de dichos registros⁽³⁹⁾.
- (72) Los OEMIP deben dar curso rápidamente y de forma adecuada a las reclamaciones de los particulares de que se trate relativas al tratamiento de la información personal que les concierna. A fin de facilitar la tramitación de las reclamaciones, deben establecer un «sistema necesario para alcanzar [esta] finalidad», lo que implica que deben poner en marcha los procedimientos apropiados en su organización (por ejemplo, asignar responsabilidades o establecer un punto de contacto).
- (73) Por último, la LPIP crea un marco para la participación de las organizaciones sectoriales en los esfuerzos desplegados al objeto de asegurar un alto nivel de conformidad (véase el capítulo IV, sección 4). El papel de tales organizaciones homologadas en el ámbito de la protección de la información personal⁽⁴⁰⁾ consiste en promover la protección de la información personal aportando a las empresas su pericia, pero también en contribuir a la implementación de las salvaguardas, en particular tramitando las reclamaciones de los particulares y ayudando a solucionar los conflictos relacionados. A tal fin, pueden instar a los OEMIP participantes a que adopten, si procede, las medidas que sean necesarias⁽⁴¹⁾. Por otra parte, en caso de violación de datos o de otros incidentes de seguridad, los OEMIP deben, en principio, informar a la CPIP, así como al interesado (o el público) y emprender las acciones necesarias, incluidas medidas para reducir al mínimo los daños y evitar que se repitan incidentes similares⁽⁴²⁾. Aunque estos regímenes se establecen sobre una base voluntaria, el 10 de agosto de 2017 la CPIP tenía registradas 44 organizaciones, la más importante de las cuales, el Centro Japonés de Desarrollo y Tratamiento

⁽³⁸⁾ Las exenciones son las siguientes: i) «los casos basados en disposiciones legales y reglamentarias». ii) «los casos en que sea necesario proteger la vida humana, la integridad física o el patrimonio y resulte difícil obtener el consentimiento del interesado principal»; iii) «los casos en que sea especialmente necesario mejorar la higiene pública o promover la salud de los niños, y resulte difícil obtener el consentimiento del interesado principal»; iv) «los casos en que sea necesario cooperar con un organismo de la Administración central o una Administración local o una persona a la que estas hayan encargado desempeñar tareas prescritas por disposiciones legales y reglamentarias, y exista la posibilidad de que la obtención del consentimiento del interesado principal interfiera con el desempeño de dichas tareas»; y v) los casos en que la referida información personal que requiere especial atención sea comunicada al público por un interesado, una organismo gubernamental, una Administración local, una persona perteneciente a una de las categorías contempladas en el artículo 76, apartado 1, u otras personas contempladas en las normas de la CPIP. Otra categoría comprende «otros casos contemplados en la Orden del Gabinete como equivalentes a los casos recogidos en cada punto anterior» y, en virtud de la Orden del Gabinete actual, engloba, en particular, características manifiestas de una persona (como un problema de salud visible) si los datos sensibles han sido adquiridos (de manera no intencional) observando, filmando o fotografiando al interesado, por ejemplo mediante cámaras de circuito cerrado de televisión.

⁽³⁹⁾ De conformidad con el artículo 40, apartado 1, de la LPIP, la CPIP puede, en la medida en que sea necesario para la implementación de las disposiciones pertinentes de la LPIP, exigir a un OEMIP que facilite la información o el material necesarios relacionados con el manejo de información personal.

⁽⁴⁰⁾ La LPIP prevé, entre otras cosas, normas para la homologación de dichas organizaciones; véanse los artículos 47 a 50 de la LPIP.

⁽⁴¹⁾ Artículo 52 de la LPIP.

⁽⁴²⁾ Nota n.º 1/2017 de la CPIP «Medidas que han de adoptarse en caso de violación de datos personales u otros incidentes».

de Información (CJDTI), contaba con 15 436 operadores económicos ⁽⁴³⁾. Entre estas organizaciones homologadas figuran asociaciones sectoriales como la Asociación Japonesa de Corredores de Valores, la Asociación Japonesa de Autoescuelas o la Asociación de Agencias Matrimoniales ⁽⁴⁴⁾.

- (74) Las organizaciones de protección de información personal homologadas presentan informes anuales sobre sus actividades. Según el «Balance del estado de ejecución de la LPIP en el ejercicio financiero 2015», publicado por la CPIP, las organizaciones de protección de información personal homologadas han recibido un total de 442 reclamaciones, han dirigido a los operadores económicos bajo su jurisdicción 123 solicitudes de explicaciones, han solicitado a estos operadores documentación en 41 casos, han formulado 181 instrucciones y han emitido dos recomendaciones ⁽⁴⁵⁾

2.3.9. Limitaciones en materia de transferencias ulteriores

- (75) El nivel de protección de los datos personales transferidos desde la Unión Europea a operadores económicos en Japón no debe verse comprometido por la transferencia ulterior de dichos datos a destinatarios que se encuentran en un tercer país que no sea Japón. Estas «transferencias ulteriores», que constituyen, desde el punto de vista del operador económico japonés, transferencias internacionales desde Japón, solo deberían estar permitidas cuando el destinatario ulterior fuera de Japón, por su parte, esté sujeto a normas que aseguren un nivel de protección similar al garantizado en el ordenamiento jurídico japonés.
- (76) Una primera protección está consagrada en el artículo 24 de la LPIP, que prohíbe, de manera general, la transferencia de datos personales a un tercero fuera del territorio japonés sin el previo consentimiento del particular de que se trate. La Regla complementaria n.º 4 garantiza que, en el caso de transferencias de datos desde la Unión Europea, dicho consentimiento se dé con pleno conocimiento de causa, ya que exige que al particular de que se trate «se le facilite información sobre las circunstancias que rodean la transferencia necesaria para que el interesado principal tome una decisión en cuanto a su consentimiento». Sobre esta base, el interesado debe ser informado del hecho de que los datos van a transferirse al extranjero (fuera del ámbito de aplicación de la LPIP) y del país de destino específico, lo que le permitirá evaluar el riesgo para la vida privada que entraña la transferencia. Asimismo, como puede deducirse del artículo 23 de la LPIP (véase el considerando 47), la información facilitada al interesado principal debe comprender los elementos obligatorios en virtud de su apartado 2, a saber, las categorías de datos de carácter personal puestos a disposición de un tercero y el método de comunicación.
- (77) El artículo 24 de la LPIP, aplicado junto con el artículo 11-2 de las Normas de la CPIP, prevé una serie de excepciones a esta regla fundada en el consentimiento. Además, de conformidad con el artículo 24, las mismas excepciones aplicables en virtud del artículo 23, apartado 1, de la LPIP se aplican igualmente a las transferencias internacionales de datos ⁽⁴⁶⁾.
- (78) A fin de garantizar la continuidad de la protección de los datos personales transferidos desde la Unión Europea a Japón en virtud de la presente Decisión, la Regla complementaria n.º 4 refuerza el nivel de protección aplicable a las transferencias ulteriores de tales datos efectuadas por el OEMIP hacia un destinatario de un tercer país. Para ello, fija limitaciones y establece un marco para las transferencias internacionales que el OEMIP puede utilizar como alternativa al consentimiento. Más en concreto, y sin perjuicio de las excepciones previstas en el artículo 23, apartado 1, de la LPIP, los datos personales transferidos en virtud de la presente Decisión solo pueden ser objeto de transferencias (ulteriores) sin consentimiento en dos casos: i) cuando los datos sean transferidos a un tercer país que haya sido reconocido por la CPIP, en virtud del artículo 24 de la LPIP, como uno de los países que garantizan un nivel de protección equivalente al garantizado en Japón ⁽⁴⁷⁾; o ii) cuando el OEMIP y el tercero destinatario hayan adoptado conjuntamente medidas que garanticen un nivel de protección equivalente al de la LPIP, leída en relación con las Reglas complementarias, por medio de un contrato, de otros tipos de acuerdos vinculantes o de arreglos vinculantes dentro de un grupo empresarial. La segunda categoría corresponde a los instrumentos utilizados en virtud del Reglamento (UE) 2016/679 para asegurar salvaguardas apropiadas (en particular cláusulas contractuales y normas corporativas vinculantes). Además, como ha confirmado la CPIP, incluso en esos casos, la transferencia sigue estando sometida a las reglas generales aplicables a cualquier facilitación de datos personales en virtud de la LPIP (es decir, la obligación de obtener el consentimiento prevista en el artículo 23, apartado 1, o, alternativamente, la obligación de información con posibilidad de exclusión prevista en el artículo 23, apartado 2,

⁽⁴³⁾ Según las cifras publicadas en el sitio web PrivacyMark del CJDTI, con fecha de 2 de octubre de 2017.

⁽⁴⁴⁾ CPIP, Lista de organizaciones de protección de datos personales homologadas, disponible en la siguiente dirección: <https://www.ppc.go.jp/personal/nintei/list/> o https://www.ppc.go.jp/files/pdf/nintei_list.pdf

⁽⁴⁵⁾ CPIP, Balance del estado de ejecución de la LPIP en el ejercicio financiero 2015 (octubre de 2016), disponible (únicamente en japonés) en la siguiente dirección: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

⁽⁴⁶⁾ Véase la nota 32.

⁽⁴⁷⁾ Con arreglo al artículo 11 de las Normas de la CPIP, esto exige no solo estándares sustantivos equivalentes a los de la LPIP controlados efectivamente por una autoridad independiente encargada de hacerlos respetar, sino también la garantía de la implementación de las normas pertinentes en el tercer país.

de la LPIP). En caso de que no se pueda hacer llegar al interesado una solicitud de consentimiento o a fin de facilitar la información previa necesaria en virtud del artículo 23, apartado 2, de la LPIP, no se podrá proceder a la transferencia.

- (79) Por lo tanto, salvo en los casos en que la CPIP haya constatado que el tercer país en cuestión asegura un nivel de protección equivalente al garantizado por la LPIP⁽⁴⁸⁾, los requisitos contemplados en la Regla complementaria n.º 4 excluyen el recurso a instrumentos de transferencia que no conduzcan a la creación de una relación vinculante entre el exportador de datos japonés y el importador de datos del tercer país y que no garanticen el nivel de protección requerido. Este será el caso, por ejemplo, del Sistema de Normas de Privacidad Transfronteriza (NPT) de la APEC, de la que Japón es una economía participante⁽⁴⁹⁾, ya que en dicho sistema las protecciones no son el resultado de un arreglo vinculante entre el exportador y el importador en el contexto de su relación bilateral y su nivel es claramente inferior al garantizado por la combinación de la LPIP y las Reglas complementarias⁽⁵⁰⁾.
- (80) Por último, los artículos 20 y 22 de la LPIP ofrecen una salvaguarda adicional en caso de transferencias (ulteriores). Con arreglo a estas disposiciones, cuando un operador de un tercer país (importador de datos) actúe por cuenta del OEMIP (exportador de datos), es decir, como un (sub)encargado del tratamiento, este último ha de garantizar el control del primero en lo que respecta a la seguridad del tratamiento de datos.

2.3.10. Derechos individuales

- (81) Al igual que la legislación de protección de datos de la UE, la LPIP confiere a los particulares una serie de derechos exigibles, entre ellos el derecho de acceso («comunicación»), el derecho de rectificación y el derecho de supresión, así como el derecho de objeción («cese de la utilización»).
- (82) En primer lugar, de conformidad con el artículo 28, apartados 1 y 2, de la LPIP, un interesado tiene derecho a solicitar a un OEMIP «que le comunique los datos personales conservados que puedan identificarle» y, tras la recepción de dicha solicitud, el OEMIP «[...] comunicará los datos personales conservados» al interesado. El artículo 29 (derecho de rectificación) y el artículo 30 (derecho al cese de la utilización) tienen la misma estructura que el artículo 28.
- (83) El artículo 9 de la Orden del Gabinete precisa que la comunicación de información personal tal como se contempla en el artículo 28, apartado 2, de la LPIP, debe realizarse por escrito, a menos que el OEMIP y el interesado hayan acordado otra cosa.
- (84) Estos derechos están sujetos a tres tipos de limitaciones, relativas a los derechos e intereses del propio particular o de terceros⁽⁵¹⁾, a una interferencia grave en el ejercicio de las actividades económicas del OEMIP⁽⁵²⁾, y a los casos en que la comunicación vulneraría otras disposiciones legales o reglamentarias⁽⁵³⁾. Las situaciones en las que se aplicarían estas limitaciones son similares a algunas de las excepciones aplicables en virtud del artículo 23, apartado 1, del Reglamento (UE) 2016/679, que permite limitaciones de los derechos de las personas por motivos relacionados con la «protección del interesado o de los derechos y libertades de otros» u «otros objetivos importantes de

⁽⁴⁸⁾ A día de hoy, la CPIP no ha adoptado ninguna decisión en virtud del artículo 24 de la LPIP por la que se reconozca que un tercer país ofrece un nivel de protección equivalente al garantizado en Japón. La única decisión que actualmente está considerando adoptar atañe al EEE. Por lo que respecta a otras posibles decisiones en el futuro, la Comisión seguirá de cerca la situación y, en caso necesario, adoptará las medidas apropiadas para hacer frente a los posibles efectos adversos para la continuidad de la protección (véanse *infra* los considerandos 176, 177 y 184 y el artículo 3, apartado 1).

⁽⁴⁹⁾ Aunque solo hay dos empresas japonesas homologadas de conformidad con el Sistema NPT de la APEC (véase https://english.jpipdec.or.jp/sp/protection_org/cbpr/list.html). Fuera de Japón, los únicos otros operadores económicos homologados con arreglo a este sistema son unas pocas (23) empresas estadounidenses (véase <https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list>).

⁽⁵⁰⁾ Por ejemplo, no contiene una definición ni protecciones específicas para los datos sensibles, como tampoco una obligación de conservación de datos durante un período limitado. Véase asimismo el Dictamen 02/2014 del Grupo de Trabajo del artículo 29, relativo a los criterios de referencia para los requisitos aplicables a las normas corporativas vinculantes presentadas a las autoridades nacionales de protección de datos en la UE y a las normas de privacidad transfronteriza presentadas a los agentes de rendición de cuentas del sistema NPT de la APEC, 6 de marzo de 2014.

⁽⁵¹⁾ Con arreglo a la CPIP, solo esos intereses pueden justificar una restricción «digna de protección legal». Esta evaluación ha de llevarse a cabo caso por caso «tomando en consideración la interferencia con los derechos fundamentales a la vida privada, incluida la protección de los datos tal como reconocen la Constitución y la jurisprudencia». Los intereses protegidos pueden incluir, por ejemplo, los intercambios comerciales u otros secretos comerciales.

⁽⁵²⁾ El concepto de «interferencia grave en el ejercicio de las actividades económicas del operador» se ilustra en las Directrices de la CPIP con diferentes ejemplos, por ejemplo tal es el caso de una persona que presenta solicitudes complejas, reiteradas e idénticas cuando tales solicitudes impliquen una carga significativa para un operador económico que pondría en peligro su capacidad de responder a otras solicitudes (Directrices de la CPIP [Edición de la norma general], p. 62). De manera más general, la CPIP ha confirmado que esta categoría se limita a casos excepcionales que vayan más allá de meros inconvenientes. En concreto, un OEMIP no puede denegar la comunicación por el mero hecho de que se ha solicitado una gran cantidad de datos.

⁽⁵³⁾ Como ha confirmado la CPIP, tales disposiciones legales han de respetar el derecho a la vida privada consagrado por la Constitución y, por tanto, «reflejar una restricción necesaria y razonable».

interés público general». Aunque la categoría de casos en que la comunicación vulneraría «otras disposiciones legales o reglamentarias» puede parecer amplia, las disposiciones legales y reglamentarias que prevean limitaciones en este sentido deben respetar el derecho constitucional a la vida privada y solo pueden imponer limitaciones en la medida en que el ejercicio de este derecho «interfiera con el bienestar público»⁽⁵⁴⁾. A tal fin, conviene a encontrar un equilibrio entre los diferentes intereses en juego.

- (85) De conformidad con el artículo 28, apartado 3, de la LPIP, si los datos solicitados no existen, o si el OEMIP de que se trate decide no conceder el acceso a los datos conservados, este ha de informar sin demora al particular.
- (86) En segundo lugar, de conformidad con el artículo 29, apartados 1 y 2, de la LPIP, un interesado tiene derecho a solicitar la rectificación, adición o supresión de los datos personales conservados que le conciernan cuando estos datos sean inexactos. Cuando reciba una solicitud de este tipo, el OEMIP «[...] llevará a cabo una investigación necesaria» y, en función de los resultados de esta investigación «procederá a una rectificación [...] del contenido de los datos conservados».
- (87) En tercer lugar, de conformidad con el artículo 30, apartados 1 y 2, de la LPIP, un interesado tiene derecho a solicitar a un OEMIP que deje de utilizar información personal o que suprima esta información, cuando esta sea manejada de forma contraria al artículo 16 (que trata de la limitación de la finalidad) o haya sido indebidamente adquirida en violación del artículo 17 de la LPIP (que trata de la adquisición de forma engañosa o por otros medios impropios o, en el caso de datos sensibles, sin consentimiento). Asimismo, de conformidad con el artículo 30, apartados 3 y 4, de la LPIP, el particular tiene derecho a solicitar del OEMIP que ponga fin a la puesta a disposición de la información a un tercero, cuando ello suponga una violación de las disposiciones del artículo 23, apartado 1, o del artículo 24 de la LPIP (en relación con la puesta a disposición de terceros, incluidas las transferencias internacionales).
- (88) Cuando la solicitud sea fundada, el OEMIP pondrá fin sin demora a la utilización de los datos o a la puesta a disposición de un tercero, en la medida en que sea necesario para poner remedio a la infracción o, en caso de que un asunto esté cubierto por una excepción (en particular si el cese de la utilización pudiera ocasionar unos gastos particularmente elevados)⁽⁵⁵⁾, adoptará las medidas alternativas necesarias para proteger los derechos e intereses del particular de que se trate.
- (89) Contrariamente al Derecho de la UE, la LPIP y las normas de menor rango pertinentes no contienen disposiciones legales que aborden específicamente la posibilidad de oponerse a un tratamiento con fines de mercadotecnia directa. Sin embargo, en virtud de la presente Decisión, dicho tratamiento se inscribirá en el marco de una transferencia de datos personales recogidos previamente en la Unión Europea. En virtud del artículo 21, apartado 2, del Reglamento (UE) 2016/679, el interesado tendrá siempre la posibilidad de oponerse a una transferencia de datos cuando el tratamiento tenga por finalidad la mercadotecnia directa. Además, tal como se explica en el considerando 43, en virtud de la Regla complementaria n.º 3, un OEMIP está obligado a tratar los datos recibidos sobre la base de la Decisión con la misma finalidad para la que hayan sido transferidos desde la Unión Europea, a menos que el interesado dé su consentimiento para modificar la finalidad de la utilización. Por consiguiente, si la transferencia se ha hecho con fines que no sean la mercadotecnia directa, un OEMIP en Japón no podrá proceder al tratamiento de los datos con fines de mercadotecnia directa sin el consentimiento del interesado de la UE.
- (90) En todos los casos mencionados en los artículos 28 y 29 de la LPIP, el OEMIP está obligado a comunicar sin demora al particular el curso dado a su solicitud y debe explicar además la eventual denegación (parcial) sobre la base de las excepciones previstas en los artículos 27 a 30 (artículo 31 de la LPIP).

⁽⁵⁴⁾ El artículo 13 de la Constitución ha sido interpretado por el Tribunal Supremo en el sentido de que confiere un derecho a la protección de la vida privada (véanse más arriba los considerandos 7 y 8). Si bien este derecho puede limitarse en los casos en que «interfiera con el bienestar de los ciudadanos», en su sentencia de 6 de marzo de 2008 (véase el considerando 8), el Tribunal Supremo dejó claro que cualquier limitación (que permita, en el caso que nos ocupa, a una autoridad pública recoger y procesar datos personales) debe ponderarse con el derecho al respeto de la vida privada, teniendo en cuenta factores tales como la naturaleza de los datos en cuestión, los riesgos que el tratamiento de estos datos crea para los particulares, las salvaguardas aplicables y los beneficios de interés público resultantes del tratamiento. Esta ponderación es muy similar a la que requiere el Derecho de la UE, sobre la base de los principios de necesidad y proporcionalidad, para autorizar cualquier limitación a los derechos de protección de datos y salvaguardas.

⁽⁵⁵⁾ Para más precisiones sobre estas excepciones, véase Profesor Katsuya Uga, Comentario artículo por artículo de la Ley sobre la protección de la información personal revisada, 2015, p. 217. A título de ejemplo de solicitud que provoca «gastos elevados», cabe citar una situación en la que solo algunos nombres incluidos en una larga lista (por ejemplo, una guía telefónica) son tratados en violación del principio de limitación de la finalidad, cuando la guía ya está a la venta, por lo que la retirada de estos ejemplares y su sustitución por otros nuevos resultaría muy costosa. En el mismo ejemplo, en caso de que ya se hayan vendido numerosos ejemplares y sea imposible retirarlos todos, también sería «difícil hacer efectivo el cese de la utilización». En estos supuestos, una «acción alternativa necesaria» podría consistir, por ejemplo, en la publicación y distribución de una nota rectificativa. Tal acción no excluye otras vías de reparación (judicial), ya sea por violación de la vida privada, daño a la imagen (difamación) causada por la publicación o violación de otros intereses.

- (91) Por lo que se refiere a las condiciones para presentar una solicitud, el artículo 32 de la LPIP (junto con la Orden del Gabinete) permite al OEMIP definir procedimientos razonables, en particular en lo que respecta a la información necesaria para identificar los datos personales conservados. Sin embargo, con arreglo al apartado 4 del presente artículo, los OEMIP no deben imponer una «carga excesiva al interesado principal». En determinados casos, el OEMIP puede imponer igualmente tasas, siempre que su importe sea «razonable teniendo en cuenta los costes efectivos» (artículo 33 de la LPIP).
- (92) Por último, el interesado puede formular objeciones a la puesta a disposición de un tercero de datos personales que le conciernan en virtud del artículo 23, apartado 2, de la LPIP, o denegar su consentimiento en virtud del artículo 23, apartado 1 (evitando así la comunicación de la información en caso de que no exista otra base legal disponible). Del mismo modo, el particular puede poner fin al tratamiento de datos efectuado para una finalidad diferente, negándose a prestar su consentimiento de conformidad con el artículo 16, apartado 1, de la LPIP.
- (93) Contrariamente al Derecho de la UE, la LPIP y las normas de menor rango pertinentes no contienen disposiciones generales que aborden la cuestión de las decisiones que afectan al interesado basadas únicamente en el tratamiento automatizado de datos personales. Sin embargo, esta cuestión se aborda en ciertas normas sectoriales aplicables en Japón que son particularmente pertinentes para este tipo de tratamiento. Se trata, entre otros, de los sectores en los que las empresas tienen más propensión a recurrir al tratamiento automatizado de datos personales para adoptar decisiones que afectan a los particulares (p. ej. el sector financiero). Así, por ejemplo, las «Directrices generales relativas a la supervisión de las grandes entidades bancarias», revisadas en junio de 2017, prevén que se debe dar al particular de que se trate explicaciones específicas sobre los motivos de la denegación de una solicitud de celebración de un contrato de préstamo. Estas normas ofrecen pues protecciones en el número probablemente limitado de casos en que las decisiones automatizadas serían adoptadas por el operador económico japonés «importador» (y no por los responsables del tratamiento de datos de la UE «exportadores»).
- (94) En cualquier caso, en lo que respecta a los datos personales que hayan sido recogidos en la Unión Europea, toda decisión basada en un tratamiento automatizado será adoptada normalmente por el responsable del tratamiento de los datos en la Unión (que tiene una relación directa con el interesado de que se trate) y está por tanto sujeta al Reglamento (UE) 2016/679 ⁽⁵⁶⁾. Se trata, por ejemplo, de escenarios de transferencias en los que el tratamiento lo lleva a cabo un operador económico extranjero (p.ej. japonés) que actúa como agente (encargado) por cuenta del responsable de la UE (o como subencargado que actúa por cuenta del encargado de la UE, que haya recibido los datos del responsable de la UE que los recogió) que sobre esta base toma entonces la decisión. Por lo tanto, es poco probable que la ausencia en la LPIP de normas específicas sobre la toma de decisiones automatizadas incida en el nivel de protección de los datos personales transferidos en virtud de la presente Decisión.

2.4. Supervisión y control de la aplicación de la normativa

2.4.1. Supervisión independiente

- (95) Con el fin de garantizar un nivel adecuado de protección de los datos también en la práctica, debe existir una autoridad de control independiente encargada de supervisar las normas en materia de protección de datos y de hacerlas cumplir. Esta autoridad debe actuar con total independencia e imparcialidad en el desempeño de sus funciones y en el ejercicio de sus competencias.
- (96) En Japón, la autoridad encargada de supervisar la LPIP y de hacerla cumplir es la CPIP. Esta está compuesta por un presidente y ocho comisarios nombrados por el primer ministro con el acuerdo de las dos cámaras de la Dieta. La duración del mandato del presidente y de cada uno de los comisarios es de cinco años, con la posibilidad de renovación (artículo 64 de la LPIP). Los comisarios solo pueden ser destituidos por una causa justificada, en un conjunto limitado de circunstancias excepcionales ⁽⁵⁷⁾, y no pueden ejercer activamente actividades políticas. Por otra parte, en virtud de la LPIP, los comisarios a tiempo completo deben abstenerse de ejercer cualesquiera otras actividades remuneradas, o actividades empresariales. Todos los comisarios están sujetos asimismo a normas internas que les impide participar en las deliberaciones en caso de un posible conflicto de intereses. La CPIP está asistida por una Secretaría, dirigida por un secretario general y creada con el fin de llevar a cabo las tareas asignadas a la CPIP (artículo 70 de la LPIP). Tanto los comisarios como el conjunto de los funcionarios de la Secretaría están sujetos a normas estrictas en materia de confidencialidad (artículos 72 y 82 de la LPIP).

⁽⁵⁶⁾ Por el contrario, puede existir excepcionalmente una relación directa entre el operador japonés y el interesado de la UE, lo que normalmente es consecuencia de que este operador se dirija específicamente al particular en la Unión Europea ofreciéndole bienes o servicios o haciendo un seguimiento de su comportamiento. En tal supuesto, el propio operador japonés entrará dentro del ámbito de aplicación del Reglamento (UE) 2016/679 (artículo 3, apartado 2) y, por lo tanto, ha de cumplir directamente la legislación de la UE en materia de protección de datos.

⁽⁵⁷⁾ De conformidad con el artículo 65 de la LPIP, la destitución de los comisarios en contra de su voluntad solo es posible por uno de los motivos siguientes: i) la apertura de un procedimiento de quiebra; ii) una condena por violación de la LPIP o de la Ley relativa a la utilización de números de identificación; iii) una condena a una pena de prisión no acompañada de trabajos o incluso a una pena aún más severa; iv) la incapacidad para ejercer sus funciones debido a trastornos mentales o físicos o a un comportamiento indebido.

- (97) Las competencias de la CPIP, que esta ejerce con total independencia⁽⁵⁸⁾, se prevén principalmente en los artículos 40, 41 y 42 de la LPIP. En virtud del artículo 40, la CPIP puede pedir a los OEMIP que informen o que presenten documentación sobre las operaciones de tratamiento y puede proceder a inspecciones *in situ* o a controles de libros u otros documentos. En la medida en que sea necesario para hacer cumplir la LPIP, la CPIP también puede prestar a los OEMIP orientación o asesoramiento sobre el manejo de información personal. La CPIP ya ha hecho uso de esta facultad en virtud del artículo 41 de la LPIP cuando prestó orientación a Facebook a raíz de las revelaciones en el caso Facebook/Cambridge Analytica.
- (98) Lo que es más importante, la CPIP tiene competencia —previa reclamación o por propia iniciativa— para formular recomendaciones y dictar órdenes con el fin de hacer cumplir la LPIP y otras normas vinculantes (incluidas las Reglas complementarias) en casos concretos. Estas competencias se establecen en el artículo 42 de la LPIP. Aunque sus apartados 1 y 2 prevén un mecanismo en dos fases por el que la CPIP puede dictar una orden (únicamente) a raíz de una recomendación previa, el apartado 3 permite la adopción directa de una orden en casos de urgencia.
- (99) Todas las disposiciones del capítulo IV, sección 1, de la LPIP no se recogen en el artículo 42, apartado 1, que delimita asimismo el ámbito de aplicación del artículo 42, apartado 2, lo que puede explicarse por el hecho de que algunas de estas disposiciones no atañen a las obligaciones del OEMIP⁽⁵⁹⁾ y de que todas las protecciones esenciales ya están garantizadas por otras disposiciones que figuran en esa lista. Por ejemplo, aunque no se menciona el artículo 15 (que exige al OEMIP que determine la finalidad de la utilización y trate la información personal pertinente exclusivamente dentro de su ámbito de aplicación), el incumplimiento de este requisito puede dar lugar a una recomendación basada en una infracción del artículo 16, apartado 1 (que prohíbe al OEMIP tratar información personal más allá de lo necesario para alcanzar la finalidad de la utilización, salvo que obtenga el consentimiento del interesado)⁽⁶⁰⁾. Otra disposición que no se recoge en el artículo 42, apartado 1, es el artículo 19 de la LPIP, relativo a la exactitud de los datos y a su conservación. El incumplimiento de esta disposición puede ejecutarse como infracción del artículo 16, apartado 1, o del artículo 29, apartado 2, si el particular de que se trate solicita la rectificación o la supresión de datos erróneos o excesivos y el OEMIP se niega a atender esta solicitud. Por lo que se refiere a los derechos del interesado con arreglo al artículo 28, apartado 1, el artículo 29, apartado 1, y el artículo 30, apartado 1, la supervisión por parte de la CPIP está garantizada por las competencias de ejecución conferidas a esta en lo que respecta a las obligaciones correspondientes del OEMIP enunciadas en dichos artículos.
- (100) De conformidad con el artículo 42, apartado 1, de la LPIP, la CPIP puede, si reconoce que es «necesario proteger los derechos e intereses de un particular en caso de que un [OEMIP] haya infringido» disposiciones específicas de la LPIP, emitir una recomendación con miras a la «suspensión del acto de infracción o a la adopción de otras medidas necesarias para poner remedio a la infracción». Tal recomendación no es vinculante, pero allana el camino a la adopción de una orden vinculante con arreglo al artículo 42, apartado 2, de la LPIP. Sobre la base de esta disposición, si no se sigue la recomendación «sin motivos legítimos» y la CPIP «reconoce el carácter inminente una violación grave de los derechos e intereses de un particular», puede ordenar al OEMIP que adopte medidas en consonancia con la recomendación.
- (101) La Reglas complementarias precisan y refuerzan las competencias de ejecución de la CPIP. Más en concreto, en caso de que se trate de datos importados desde la Unión Europea, la CPIP considerará siempre que el hecho de que un OEMIP no haya adoptado, sin motivo legítimo, medidas en consonancia con una recomendación emitida por la LPIP con arreglo al artículo 42, apartado 1, constituye una violación grave de carácter inminente de los derechos e intereses de un particular en el sentido del artículo 42, apartado 2, y, por lo tanto, una infracción que justifica la emisión de una orden vinculante. Por otra parte, la CPIP solo aceptará como «motivo legítimo» para no seguir una recomendación un «hecho de carácter excepcional [que impida el cumplimiento] que escape al control del [OEMIP] y que no pueda preverse razonablemente (por ejemplo, catástrofes naturales)» o los casos en que la necesidad de adoptar medidas en relación con una recomendación «haya desaparecido por haber adoptado el [OEMIP] medidas alternativas que remedien plenamente la violación».

⁽⁵⁸⁾ Véase el artículo 62 de la LPIP.

⁽⁵⁹⁾ Por ejemplo, ciertas disposiciones se refieren a las acciones facultativas de la OEMIP (artículos 32 y 33 de la LPIP) o a las obligaciones de actuar «con la debida diligencia», que son, por su propia naturaleza, no ejecutables (artículos 31 y 35, artículo 36, apartado 6, y artículo 39 de la LPIP). Ciertas disposiciones no se dirigen al OEMIP sino a otros actores. Este es el caso, por ejemplo, del artículo 23, apartado 4, del artículo 26, apartado 2, y del artículo 34 de la LPIP [sin embargo, el cumplimiento del artículo 26, apartado 2, de la LPIP queda garantizado gracias a la posibilidad de imponer penas de conformidad con el artículo 88, letra i), de la LPIP].

⁽⁶⁰⁾ Además, como se explica en el considerando (48), en el caso de una transferencia, «la finalidad de la utilización» será especificada por la persona que exporta los datos desde la UE, que a este respecto está obligada a ello por la obligación enunciada en el artículo 5, apartado 1, letra b), del Reglamento (UE) 2016/679. Esta obligación es ejecutable por la autoridad de protección de datos (APD) competente en la Unión Europea.

- (102) El incumplimiento de una orden de la CPIP es considerado una infracción penal en virtud del artículo 84 de la LPIP, y un OEMIP declarado culpable puede ser condenado a una pena de prisión acompañada de trabajos de hasta seis meses o una multa máxima de 300 000 yenes japoneses (JPY). Por otra parte, con arreglo al artículo 85, letra i), de la LPIP, la falta de cooperación con la CPIP o una obstrucción a la investigación está castigada con una multa máxima de 300 000 JPY. Estas sanciones penales vienen a sumarse a las que pueden imponerse por infracciones sustantivas de la LPIP (véase el considerando 108).

2.4.2. Reparación judicial

- (103) A fin de garantizar una protección adecuada y, en particular, el respeto de los derechos individuales, el interesado debe disponer de la posibilidad de incoar recursos administrativos y acciones judiciales efectivos, incluida la indemnización por daños y perjuicios.
- (104) Antes o en lugar de interponer un recurso administrativo o una acción judicial, un particular puede decidir presentar una reclamación en relación con el tratamiento de sus datos personales ante el propio responsable del tratamiento. Sobre la base del artículo 35 de la LPIP, los OEMIP procurarán dar curso a dichas reclamaciones «rápidamente y de manera apropiada» e implantar sistemas internos de tramitación de las reclamaciones para alcanzar este objetivo. Además, en virtud del artículo 61, inciso ii), de la LPIP, la CPIP es responsable de la «mediación necesaria en relación con una reclamación presentada y la cooperación ofrecida a un operador económico que se ocupa de la reclamación», lo que incluye, en ambos casos, las reclamaciones presentadas por extranjeros. A tal efecto, el legislador japonés también ha confiado a la Administración central la misión de adoptar las «medidas necesarias» para permitir y facilitar la resolución de las reclamaciones por los OEMIP (artículo 9), mientras que los entes locales deben, en tales casos, asegurar la mediación (artículo 13). A este respecto, los particulares pueden presentar una reclamación ante uno de los más de 1 700 centros de consumidores creados por los entes locales sobre la base de la Ley de seguridad de los consumidores⁽⁶¹⁾, además de la posibilidad de que disponen de presentar una reclamación ante el Centro Nacional de Consumidores de Japón. Tales reclamaciones también pueden interponerse con respecto a una infracción de la LPIP. En virtud del artículo 19 de la Ley fundamental de protección de los consumidores⁽⁶²⁾, los entes locales deben esforzarse por recurrir a la mediación con respecto a las reclamaciones y aportar a las partes la pericia necesaria. Estos mecanismos de resolución de litigios parecen bastante eficaces, con un índice de resolución del 91,2 %, es decir, más de 75 000 reclamaciones en 2015.
- (105) Las violaciones de las disposiciones de la LPIP por un OEMIP puede dar lugar a acciones civiles y a procedimientos y sanciones penales. En primer lugar, si un particular considera que se han vulnerado los derechos que le asisten en virtud de los artículos 28, 29 y 30 de la LPIP, puede solicitar medidas cautelares solicitando al órgano jurisdiccional que ordene a un OEMIP atender su solicitud en virtud de alguna de estas disposiciones, es decir, comunicando los datos personales conservados (artículo 28), rectificando los datos personales conservados que sean incorrectos (artículo 29) o poniendo fin al tratamiento ilícito o la puesta a disposición de los datos a un tercero (artículo 30). Tales acciones pueden emprenderse sin necesidad de invocar el artículo 709 del Código Civil⁽⁶³⁾ o, de otra forma, el Derecho de responsabilidad civil⁽⁶⁴⁾. En concreto, esto significa que el particular no tiene que demostrar la existencia de un perjuicio.
- (106) En segundo lugar, en caso de que la supuesta infracción no afecte a los derechos individuales conferidos por los artículos 28, 29 y 30, sino a principios u obligaciones generales en materia de protección de datos aplicables al OEMIP, el particular de que se trate puede interponer una acción civil contra el operador económico sobre la base de las disposiciones del Código Civil japonés en materia de responsabilidad extracontractual, en particular su artículo 709. Aunque una acción en justicia interpuesta en virtud del artículo 709 requiere, además de la existencia de culpa (intencional o por negligencia), la demostración de un perjuicio, tal perjuicio puede ser, de conformidad con el artículo 710 del Código Civil, tanto material como inmaterial. No se prevé ninguna limitación en cuanto a la cuantía de la indemnización.
- (107) Por lo que se refiere a las reparaciones disponibles, el artículo 709 del Código Civil japonés prevé una indemnización pecuniaria. Sin embargo, según la interpretación de la jurisprudencia japonesa este artículo confiere igualmente el derecho a obtener un requerimiento⁽⁶⁵⁾. Por lo tanto, si el interesado intenta una acción en virtud del artículo 709 del Código Civil y alega que sus derechos o intereses se han visto perjudicados por una infracción de una disposición de la LPIP por parte de la parte demandada, la demanda puede incluir, además de una indemnización por daños y perjuicios, una solicitud de medidas cautelares, tendente sobre todo al cese del tratamiento ilícito.

⁽⁶¹⁾ Ley n.º 50, de 5 de junio de 2009.

⁽⁶²⁾ Ley n.º 60, de 22 de agosto de 2012.

⁽⁶³⁾ El artículo 709 del Código Civil constituye la principal base de los procedimientos civiles por daños y perjuicios. Según esta disposición, «el que dolosa o culposamente lesione derechos o bienes ajenos jurídicamente protegidos quedará obligado a la indemnización de los daños y perjuicios ocasionados».

⁽⁶⁴⁾ Alto Tribunal de Tokio, sentencia de 20 de mayo de 2015 (no publicada). Tribunal de Distrito de Tokio, sentencia de 8 de septiembre de 2014, Westlaw Japón 2014WLJPCA09088002. Véase asimismo el artículo 34, apartados 1 y 3, de la LPIP.

⁽⁶⁵⁾ Véase Tribunal Supremo, sentencia de 24 de septiembre de 2002 (Hanrei Times, vol. 1106, p. 72).

- (108) En tercer lugar, además de las acciones por responsabilidad civil, un interesado puede presentar una reclamación ante un fiscal o un agente de la policía judicial por las infracciones de la LPIP que pudieran dar lugar a sanciones penales. El capítulo VII de la LPIP contiene una serie de disposiciones penales. La más importante (artículo 84) se refiere al incumplimiento por parte del OEMIP de las órdenes dictadas por la CPIP de conformidad con el artículo 42, apartados 2 y 3. Si un operador económico no cumple una orden dictada por la CPIP, el presidente de esta (o cualquier otro funcionario gubernamental) ⁽⁶⁶⁾ puede remitir el asunto al Ministerio Fiscal o a un agente de la policía judicial y, de este modo, desencadenar la apertura de un procedimiento penal. La sanción por el incumplimiento de una orden de la CPIP es pena de prisión acompañada de trabajos de una duración máxima de seis meses o una multa de hasta 300 000 JPY. Otras disposiciones de la LPIP prevén sanciones en caso de infracciones de la LPIP que afecten a los derechos e intereses de los interesados, entre ellas el artículo 83 de la LPIP (que trata de la «puesta a disposición o la utilización encubiertas» de una base de datos personales «con el fin de obtener [...] beneficios ilícitos») y el artículo 88, letra i), de la LPIP (que se refiere al incumplimiento por parte de un tercero de la obligación de informar correctamente al OEMIP cuando este último reciba datos personales de conformidad con el artículo 26, apartado 1, de la LPIP, en particular sobre los datos del propio tercero, antes de su adquisición). Las sanciones aplicables a tales infracciones de la LPIP son, respectivamente, una pena de prisión acompañada de trabajos de una duración máxima de un año o una multa de hasta 500 000 JPY (en el caso del artículo 83) o una multa administrativa de hasta 100 000 JPY (en el caso del artículo 88, letra i). Aunque la amenaza de una sanción penal ya puede tener un importante efecto disuasorio sobre los directivos que dirigen las operaciones de tratamiento del OEMIP, así como sobre los particulares que manejan los datos, el artículo 87 de la LPIP aclara que cuando un representante, empleado u otro trabajador de una entidad corporativa ha cometido una infracción de conformidad con los artículos 83 a 85 de la LPIP, «el autor será castigado y se impondrá a dicha entidad corporativa una multa establecida en los artículos correspondientes». En este caso, se pueden imponer tanto al trabajador como a la empresa multas por la cuantía máxima prevista.
- (109) Por último, los particulares también pueden buscar reparación por las acciones u omisiones de la CPIP. A este respecto, la legislación japonesa prevé varias vías de recurso administrativo y judicial.
- (110) Cuando un particular no esté satisfecho con una línea de actuación seguida por la CPIP, puede interponer un recurso administrativo en virtud de la Ley de revisión de las reclamaciones administrativas ⁽⁶⁷⁾. A la inversa, cuando un particular considera que la CPIP no ha actuado cuando debería haberlo hecho, puede solicitar a esta autoridad, con arreglo al artículo 36-3 de dicha Ley, que adopte una disposición o dé orientaciones administrativas si estima que «no se han adoptado disposiciones o directrices administrativas necesarias para la corrección de la infracción».
- (111) Por lo que se refiere a las vías de recurso judicial, con arreglo a la Ley de lo contencioso administrativo un particular que no esté satisfecho con una disposición administrativa adoptada por la CPIP puede solicitar un mandamiento judicial ⁽⁶⁸⁾ por el que el órgano jurisdiccional conmine a la CPIP a tomar otras medidas ⁽⁶⁹⁾. En ciertos casos, el órgano jurisdiccional puede dictar también un mandamiento judicial provisional a fin de evitar daños irreparables ⁽⁷⁰⁾. Además, en virtud de la referida Ley, un particular puede solicitar la revocación de una decisión de la CPIP ⁽⁷¹⁾.
- (112) Por último, un particular también puede presentar ante el Estado una demanda de indemnización contra la CPIP en virtud del artículo 1, apartado 1, de la Ley de reparaciones a cargo del Estado si ha sufrido daños porque una orden dictada por la CPIP y dirigida a un operador económico era ilícita o porque la CPIP no ha ejercido sus competencias.

3. ACCESO Y UTILIZACIÓN POR LAS AUTORIDADES PÚBLICAS JAPONESAS DE DATOS PERSONALES TRANSFERIDOS DESDE LA UNIÓN EUROPEA

- (113) La Comisión ha evaluado asimismo las limitaciones y salvaguardas previstas, incluidos los mecanismos de supervisión y de recurso disponibles en el Derecho japonés en lo que respecta a la recogida y utilización ulterior de los datos personales transferidos a operadores económicos en Japón por las autoridades públicas en aras del interés público, en particular a efectos coercitivos y de seguridad nacional («acceso de los poderes públicos»). A este respecto, el Gobierno japonés ha facilitado a la Comisión declaraciones, garantías y compromisos oficiales firmados al más alto nivel ministerial y de servicios, que figuran en el anexo II de la presente Decisión.

⁽⁶⁶⁾ Artículo 239, apartado 2, del Código de Enjuiciamiento Criminal.

⁽⁶⁷⁾ Ley n.º 160 de 2014.

⁽⁶⁸⁾ Artículo 37-2 de la Ley de lo contencioso administrativo.

⁽⁶⁹⁾ De conformidad con el artículo 3, apartado 6, de la Ley de lo contencioso administrativo, el término «procedimiento de mandamiento judicial» designa una acción tendente a obtener una orden judicial contra una agencia administrativa a fin de que esta adopte una disposición administrativa original que no adoptó pese a que «debería» haberlo hecho.

⁽⁷⁰⁾ Artículo 37-5 de la Ley de lo contencioso administrativo.

⁽⁷¹⁾ Capítulo II, sección 1, de la Ley de lo contencioso administrativo.

3.1. Marco jurídico general

- (114) En tanto que ejercicio de la autoridad pública, en Japón el acceso de los poderes públicos a los datos ha de hacerse en el pleno respeto de la ley (principio de legalidad). A este respecto, la Constitución japonesa contiene una serie de disposiciones que limitan y estructuran la recogida de datos personales por parte de las autoridades públicas. Como ya se ha indicado en relación con el tratamiento de los datos por los operadores económicos, sobre la base del artículo 13 de la Constitución, que consagra, entre otros, el derecho a la libertad, el Tribunal Supremo de Japón ha reconocido el derecho a la vida privada y a la protección de datos ⁽⁷²⁾. Un aspecto importante de este derecho es que los particulares son libres de impedir la comunicación de su información personal a terceros sin autorización ⁽⁷³⁾, lo que implica un derecho a la protección efectiva de los datos personales contra los abusos y, en particular, el acceso no autorizado. Una protección complementaria es asegurada por el artículo 35 de la Constitución, relativo al derecho a que no se viole la seguridad de domicilio ni se registren ni secuestren papeles y efectos personales, que exige a los poderes públicos que obtengan una orden judicial dictada con «causa suficiente» ⁽⁷⁴⁾ siempre que se proceda a «registros e incautaciones». En su sentencia de 15 de marzo de 2017 (asunto GPS), el Tribunal Supremo ha precisado que esta exigencia de orden judicial se aplica siempre que el Gobierno invade (se inmiscuye en) la esfera privada de tal forma que anula la voluntad del particular por medio de una «investigación obligatoria». Un juez solo podrá expedir tal orden cuando exista una sospecha concreta de que se ha cometido un delito, es decir, cuando obren en su poder pruebas documentales que demuestren que la persona investigada ha cometido una infracción penal ⁽⁷⁵⁾. Por consiguiente, las autoridades japonesas no tienen competencias para recoger información personal por medios coercitivos cuando aún no se ha producido una violación de la ley ⁽⁷⁶⁾, por ejemplo a fin de prevenir un delito o cualquier otra amenaza para la seguridad (como es el caso de las investigaciones por motivos de seguridad nacional).
- (115) En virtud del principio de reserva de ley, toda recogida de datos llevada a cabo en el marco de una investigación coercitiva debe ser autorizada expresamente por la ley (como dispone, por ejemplo, el artículo 197, apartado 1, del Código de Enjuiciamiento Criminal [«CEC»] en lo que respecta a la recogida obligatoria de información a efectos de una investigación criminal). Esta exigencia se aplica igualmente al acceso a la información electrónica.
- (116) Cabe destacar que el artículo 21, apartado 2, de la Constitución garantiza el secreto de todos los medios de comunicación, únicamente con las limitaciones permitidas por la ley por razones de interés público. El artículo 4 de la Ley de telecomunicaciones, según el cual no se puede violar el secreto de las comunicaciones manejadas por una empresa de telecomunicaciones, implementa este requisito de confidencialidad a nivel de la ley. Se ha interpretado que esta norma prohíbe la comunicación de información a no ser que se cuente con el consentimiento de los usuarios o que la comunicación se base en una de las exenciones explícitas de responsabilidad penal recogidas en el Código Penal ⁽⁷⁷⁾.
- (117) Asimismo, la Constitución garantiza el derecho a la tutela judicial (artículo 32) y el derecho a demandar al Estado para obtener reparación en caso de que un particular haya sufrido daños motivados por actos ilícitos cometidos por un funcionario público (artículo 17).
- (118) En lo que respecta específicamente al derecho a la protección de los datos, el capítulo III, secciones 1, 2 y 3, de la LPIP establece una serie de principios generales comunes a todos los sectores, incluido el sector público. En concreto, el artículo 3 de la LPIP dispone que toda la información personal debe manejarse de conformidad con el principio de respeto de la personalidad de los particulares. Una vez que la información personal, incluida la que forma parte de ficheros electrónicos, haya sido recogida («obtenida») por las autoridades públicas ⁽⁷⁸⁾, su manejo se rige por la Ley de protección de la información personal en poder de órganos administrativos

⁽⁷²⁾ Véase, por ejemplo, la sentencia del Tribunal Supremo, de 12 de septiembre de 2003, en el asunto n.º 1656 [2002 (Ju)]. En particular, el Tribunal Supremo ha estimado que «todo particular es libre de proteger su propia información personal de manera que no se comunique a terceros ni se haga pública si no existe un buen motivo para ello.»

⁽⁷³⁾ Tribunal Supremo, sentencia de 6 de marzo de 2008 (Juki-net).

⁽⁷⁴⁾ Solo existe «causa suficiente» cuando se considera que el particular de que se trate (sospechoso o acusado) ha cometido una infracción y el registro e incautación son necesarios para la investigación criminal. Véase la sentencia del Tribunal Supremo, de 18 de marzo de 1969, en el asunto n.º 100 [1968 (Shi)].

⁽⁷⁵⁾ Artículo 156, apartado 1, de las Normas de enjuiciamiento criminal.

⁽⁷⁶⁾ Cabe señalar, no obstante, que la Ley de represión de la delincuencia organizada y de control del producto de la delincuencia, de 15 de junio de 2017, tipifica como nuevo delito la preparación de actos de terrorismo y otras formas de delincuencia organizada. Las investigaciones solo se iniciarán en caso de sospechas concretas, fundadas en pruebas, de que se dan las tres condiciones necesarias para que haya infracción (participación de un grupo delictivo organizado, «acto de planificación» y «acto de preparación para la comisión» del delito). Véanse asimismo, por ejemplo, los artículos 38 a 40 de la Ley de prevención de actividades subversivas (Ley n.º 240, de 21 de julio de 1952).

⁽⁷⁷⁾ Artículo 15, apartado 8, de las Directrices sobre la protección de la información personal en el sector de las telecomunicaciones.

⁽⁷⁸⁾ Los órganos administrativos tal como se definen en el artículo 2, apartado 1, de la LPIPOA. Según la información recibida del Gobierno japonés, todas las autoridades públicas, a excepción de la policía prefectural, entran dentro de la definición de «órganos administrativos». Al mismo tiempo, la policía prefectural opera dentro del marco jurídico establecido por las Ordenanzas prefecturales sobre la protección de la información personal (véase el artículo 11 de la LPIP y la política de base), que prevén disposiciones relativas a la protección de la información personal equivalentes a las recogidas en la LPIPOA. Véase el anexo II, sección I.B.. Como ha explicado la CPIP con arreglo a la «política de base» estas Ordenanzas han de aprobarse sobre la base del contenido de las notas de la LPIPOA y el MIC emite nota para dar a las autoridades locales las instrucciones necesarias a este respecto. Según ha subrayado la CPIP, «[d]entro de estos límites, la ordenanza de protección de la información personal en cada prefectura se establecerá [...] sobre la base de la política de base y el contenido de las notas.»

(«LPIPOA») ⁽⁷⁹⁾. En principio ⁽⁸⁰⁾, esta disposición se aplica igualmente al tratamiento de información personal con fines de control del cumplimiento del Derecho penal o de seguridad nacional. Entre otras cosas, la LPIPOA dispone que las autoridades públicas: i) solo pueden conservar información personal en la medida en que sea necesario para el ejercicio de sus funciones; ii) no pueden hacer uso de dicha información para alcanzar un objetivo «injusto» ni para comunicarla a un tercero sin justificación; iii) deben especificar la finalidad y no deben modificarla más allá de lo que pueda considerarse razonablemente pertinente para la finalidad original (limitación de la finalidad); iv) no pueden, en principio, utilizar ni poner a disposición de terceros la información personal conservada para otras finalidades y, si lo consideran necesario, deben imponer restricciones a la finalidad o al método de utilización por parte de terceros; v) deben tomar las medidas necesarias para asegurar la exactitud de la información (calidad de los datos); vi) deben adoptar las medidas necesarias para asegurar una gestión adecuada de la información y evitar fugas, pérdidas o daños (seguridad de los datos); y vii) deben velar por tramitar de manera adecuada y rápida cualquier reclamación relativa al tratamiento de la información ⁽⁸¹⁾.

3.2. Acceso a los datos y utilización de los mismos por parte de las autoridades públicas japonesas a efectos de control de la aplicación del Derecho penal

- (119) La legislación japonesa prevé una serie de limitaciones al acceso a los datos personales y a su utilización a efectos coercitivos, así como mecanismos de supervisión y reparación que ofrecen salvaguardas suficientes para proteger efectivamente dichos datos contra las interferencias ilícitas y el riesgo de abuso.

3.2.1. Base jurídica y limitaciones/salvaguardas aplicables

- (120) En el marco jurídico japonés, se permite la recogida de información electrónica a efectos coercitivos sobre la base de una orden judicial (recogida obligatoria) o de una solicitud de comunicación voluntaria.

3.2.1.1. Investigación obligatoria sobre la base de una orden judicial

- (121) Como se ha indicado en el considerando 115, toda recogida de datos en el marco de una investigación coercitiva ha de ser autorizada específicamente por la ley y solo puede llevarse a cabo sobre la base de una orden judicial dictada con «causa suficiente» (artículo 35 de la Constitución). Por lo que se refiere a la investigación de infracciones penales, esta exigencia se recoge en las disposiciones del Código de Enjuiciamiento Criminal («CEC»). De conformidad con el artículo 197, apartado 1, del CEC, no se aplicarán medidas obligatorias «a menos que existan disposiciones especiales previstas en el presente Código». Por lo que se refiere a la recogida de información electrónica, las únicas bases jurídicas pertinentes ⁽⁸²⁾ a este respecto son los artículos 218 (registro e incautación) y 222-2 del CEC, en virtud de los cuales las medidas obligatorias de interceptación de comunicaciones electrónicas sin el consentimiento de las partes han de ejecutarse sobre la base de otros actos legislativos, a saber, la Ley de escuchas telefónicas a efectos de investigación criminal («Ley de escuchas telefónicas»). En ambos casos, se aplica el requisito de mandato.
- (122) Más en concreto, con arreglo al artículo 218, apartado 1, del CEC, un fiscal, un fiscal adjunto o un agente de la policía judicial puede, si es necesario para la investigación de un delito, proceder a un registro o incautación (incluso con levantamiento de acta) sobre la base de un mandato dictado previamente por un juez ⁽⁸³⁾. Entre otras cosas, dicho mandato debe incluir el nombre del sospechoso o acusado, el delito que se le imputa ⁽⁸⁴⁾, los archivos electromagnéticos que han de incautarse y «el lugar o los artículos» que se han de inspeccionar (artículo 219, apartado 1, del CEC).

⁽⁷⁹⁾ La información personal obtenida por los funcionarios de un órgano administrativo en el ejercicio de sus funciones y conservada por este para un uso organizativo entra dentro del ámbito de la definición de «información personal conservada» en el sentido del artículo 2, apartado 3, de la LPIPOA, en tanto en cuanto esté registrada como «documentos administrativos». Se incluye aquí la información electrónica recogida y posteriormente tratada por dichos órganos, habida cuenta de que la definición de «documentos administrativos» que figura en el artículo 2, apartado 2, de la Ley sobre el acceso a la información en poder de los órganos administrativos (Ley n.º 42 de 1999) incluye los archivos electromagnéticos.

⁽⁸⁰⁾ Sin embargo, según el artículo 53-2 del Código de Enjuiciamiento Criminal, el capítulo IV de la LPIPOA no es aplicable a la «documentación judicial», que, según la información recibida, incluye la información electrónica obtenida sobre la base de una orden judicial o de una solicitud de cooperación voluntaria en el marco de una investigación criminal. Del mismo modo, por lo que se refiere a la información recogida en el ámbito de la seguridad nacional, los particulares no pueden invocar los derechos que les asisten en virtud de la LPIPOA si el director de la autoridad pública tiene «motivos fundados» para considerar que la comunicación «puede poner en peligro la seguridad nacional» [véase el artículo 14, inciso iv)]. Dicho esto, las autoridades públicas están obligadas a conceder una comunicación al menos parcial siempre que sea posible (artículo 15).

⁽⁸¹⁾ Véanse las referencias específicas a la LPIPOA en el anexo II, sección II.A.1, letra b), número 2).

⁽⁸²⁾ Aunque el artículo 220 del CEC autoriza el registro e incautación «sobre el terreno» sin mandato cuando un fiscal, un fiscal adjunto o un agente de la policía judicial ordene la detención de un sospechoso/infractor sorprendido *in flagranti*, esta circunstancia no es pertinente en un contexto de transferencia y, por consiguiente, tampoco lo es a efectos de la presente Decisión.

⁽⁸³⁾ De conformidad con el artículo 222, apartado 1, leído en relación con el artículo 110 del CEC, la orden de registro o incautación de archivos debe presentarse a la persona que va a sufrir la medida.

⁽⁸⁴⁾ Véase asimismo el artículo 189, apartado 2, del CEC, en virtud del cual un agente de la policía judicial debe investigar al acusado y las pruebas que le incriminan «cuando estime que se ha cometido un delito». Del mismo modo, el artículo 155, apartado 1, de las Normas de enjuiciamiento criminal exige que una solicitud escrita de orden judicial contenga, entre otras cosas, el «delito imputado» y un «resumen de los hechos constitutivos de delito».

- (123) Por lo que se refiere a la interceptación de las comunicaciones, el artículo 3 de la Ley de escuchas telefónicas solo autoriza tales medidas si se cumplen exigencias estrictas. En particular, las autoridades públicas tienen que obtener previamente una orden judicial, que solo puede dictarse para las investigaciones relativas a determinados delitos graves (enumerados en el anexo de la Ley) ⁽⁸⁵⁾ y cuando sea «extremadamente difícil identificar al autor o aclarar las circunstancias y pormenores del delito cometido por cualquier otro medio» ⁽⁸⁶⁾. En virtud del artículo 5 de la Ley de escuchas telefónicas, la orden se expide para un período limitado de tiempo y el juez puede imponer condiciones adicionales. Por otra parte, la Ley de escuchas telefónicas prevé otras garantías como, por ejemplo, la comparecencia obligatoria de testigos (artículos 12 y 20), la prohibición de escuchar las comunicaciones de determinados grupos privilegiados (por ejemplo, médicos o abogados) (artículo 15), la obligación de poner fin a las escuchas si estas dejan de estar justificadas aun cuando no haya concluido el período de validez de la orden (artículo 18), o la exigencia general de notificar al particular de que se trate y permitir el acceso a los registros durante los 30 días siguientes al cese de las escuchas (artículos 23 y 24).
- (124) En relación con todas las medidas obligatorias basadas en una orden, solo puede llevarse a cabo tal examen «cuando sea necesario para alcanzar su objetivo», es decir, cuando los objetivos perseguidos por la investigación no puedan alcanzarse de otro modo (artículo 197, apartado 1, del CEC). Aunque los criterios para determinar esta necesidad no se especifican en la ley, el Tribunal Supremo de Japón ha dictaminado que el órgano jurisdiccional que dicte una orden debe proceder a una apreciación global teniendo en cuenta, en particular, i) la gravedad de la infracción y la forma en que se cometió; ii) el valor y la importancia de los materiales que se van a incautar como pruebas; iii) la probabilidad (el riesgo) de que las pruebas puedan ocultarse o destruirse, y iv) la medida en que la incautación pueda causar un perjuicio al particular de que se trate ⁽⁸⁷⁾.

3.2.1.2. Solicitud de comunicación voluntaria sobre la base de una «ficha de consulta»

- (125) Dentro de los límites de sus competencias, las autoridades públicas también pueden recoger información electrónica sobre la base de solicitudes de comunicación voluntaria. Se trata de una forma de cooperación no obligatoria en la que no se puede obligar al destinatario de la solicitud a atenderla ⁽⁸⁸⁾, dispensando así a las autoridades públicas de la obligación de obtener una orden judicial.
- (126) En la medida en que dicha solicitud se dirija a un operador económico y se refiera a información personal, el operador debe ajustarse a las exigencias de la LPIP. De conformidad con el artículo 23, apartado 1, de la LPIP, los operadores económicos solo pueden comunicar información personal a terceros sin el consentimiento del particular afectado en ciertos casos, por ejemplo cuando la comunicación «se base en disposiciones legales y reglamentarias» ⁽⁸⁹⁾. En el ámbito del control del cumplimiento del Derecho penal, la base jurídica para tales solicitudes es el artículo 197, apartado 2, del CEC, según el cual «se podrá pedir a las organizaciones privadas que informen sobre cuestiones necesarias relacionadas con la investigación.» Habida cuenta de que las «fichas de consulta» solo se autorizan en el marco de investigación criminal, presuponen siempre una sospecha concreta de un delito ya cometido ⁽⁹⁰⁾. Por otra parte, dado que tales investigaciones son llevadas a cabo generalmente por la policía prefectural, son aplicables las limitaciones previstas en el artículo 2, apartado 2, de la Ley de Policía ⁽⁹¹⁾. Con arreglo a dicha disposición, las actividades de la Policía están «estrictamente limitadas» al ejercicio de sus responsabilidades y funciones (es decir, la prevención, represión e investigación de los delitos). Por otra parte, en el ejercicio de sus funciones, la Policía ha de actuar de manera imparcial, libre de perjuicio y equitativa y no debe abusar nunca de sus poderes «de modo que interfiera con los derechos y libertades de un particular garantizados por la Constitución de Japón» (lo que incluye, como se ha indicado más arriba, el derecho a la vida privada y a la protección de datos) ⁽⁹²⁾.
- (127) Concretamente en lo que respecta al artículo 197, apartado 2, del CEC, la Agencia Nacional de Policía («ANP»), en su calidad de autoridad federal encargada, entre otras cosas, de todas las cuestiones relativas a la policía judicial, ha

⁽⁸⁵⁾ El anexo hace referencia a nueve tipos de delitos, entre ellos los relacionados con las drogas y las armas de fuego, la trata de seres humanos y el asesinato organizado. Cabe destacar que el recién introducido delito de «preparación de actos de terrorismo y otras formas de delincuencia organizada» (véase la nota 76) no figura en esta lista restrictiva.

⁽⁸⁶⁾ Por otra parte, con arreglo al artículo 23 de la Ley de escuchas telefónicas, la autoridad encargada de la investigación ha de notificar por escrito al particular de que sus comunicaciones han sido interceptadas (y, por lo tanto, incluidas en el acta de interceptación).

⁽⁸⁷⁾ Véase el anexo II, sección II.A.1, letra b), número 1).

⁽⁸⁸⁾ Según la información recibida, los operadores económicos que no se presten a cooperar no sufren consecuencias negativas (por ejemplo sanciones) en virtud de ninguna ley. Véase el anexo II, sección II.A.2, letra a).

⁽⁸⁹⁾ Con arreglo a la Directrices de la CPIP (Edición de la norma general), el artículo 23, apartado 1, inciso i), constituye la base para la comunicación de información personal en respuesta a una orden judicial (artículo 218 del CEC) y a una «ficha de consulta» (artículo 197, apartado 2, del CEC).

⁽⁹⁰⁾ Esto significa que la «ficha de consulta» solo puede utilizarse para recoger información en casos individuales y no para recopilar, a gran escala, datos personales. Véase el anexo II, sección I.A.2, letra b), número 1).

⁽⁹¹⁾ Así como los reglamentos de la Comisión Prefectural de Seguridad Pública, véase el artículo 189, apartado 1, del CEC.

⁽⁹²⁾ Véase igualmente el artículo 3 de la Ley de Policía, según el cual todos los agentes de policía prestan juramento de «respetar la obligación de defender y respetar la Constitución y las leyes de Japón, y de desempeñar sus funciones de manera imparcial, equitativa, justa y libre de perjuicio.».

dado instrucciones a la policía prefectural⁽⁹³⁾ sobre el «buen uso de las consultas escritas en materia de investigación». Con arreglo a esta nota, las solicitudes deben presentarse utilizando un formulario preestablecido (el «formulario n.º 49»⁽⁹⁴⁾, también conocido como «ficha de consulta»), han de referirse a los archivos «relativos a una investigación específica» y la información solicitada debe ser «necesaria para [dicha] investigación». En cada caso, el responsable de la investigación ha de «examinar detenidamente la necesidad, el contenido [...] de la consulta en cuestión» y debe recabar la aprobación interna de un funcionario de alto rango.

- (128) Por otra parte, en dos sentencias de 1969 y 2008⁽⁹⁵⁾, el Tribunal Supremo de Japón estableció una serie de limitaciones con respecto a las medidas no obligatorias que interfieren con el derecho a la vida privada⁽⁹⁶⁾. En concreto, el Tribunal consideró que tales medidas deben ser «razonables» y no ir más allá de los «límites generalmente admisibles», es decir han de ser necesarias para la investigación de un sospechoso (recogida de pruebas) y han de ponerse en práctica «mediante métodos apropiados para alcanzar el objetivo de la investigación⁽⁹⁷⁾». En virtud de ambas sentencias, esto implica un control de la proporcionalidad que tenga en cuenta todas las circunstancias del asunto (p. ej. el nivel de interferencia con el derecho a la vida privada, incluida la expectativa de privacidad, la gravedad del delito, la probabilidad de obtener pruebas útiles, la importancia de estas pruebas, los posibles medios alternativos de investigación, etc.)⁽⁹⁸⁾.
- (129) Además de estas limitaciones al ejercicio de la autoridad pública, se espera de los operadores económicos que verifiquen («confirмен») la necesidad y la «racionalidad» de la puesta a disposición de un tercero⁽⁹⁹⁾. Se trata sobre todo de saber si la ley les impide cooperar. Estas obligaciones jurídicas contradictorias pueden derivar, en particular, de obligaciones de confidencialidad como las previstas en el artículo 134 del Código Penal (sobre la relación entre un médico y su paciente, un abogado y su cliente, un sacerdote y su feligrés, etc.). Asimismo, «toda persona que ejerza una actividad de telecomunicaciones deberá guardar, mientras permanezca en el cargo, los secretos de otras personas que hayan llegado a su conocimiento en lo que respecta a las comunicaciones manejadas por la empresa de telecomunicaciones» (artículo 4, apartado 2, de la Ley del sector de las telecomunicaciones). Esta obligación está respaldada por la sanción prevista en el artículo 179 de la Ley del sector de las telecomunicaciones, en virtud del cual toda persona que haya violado el secreto de las comunicaciones manejadas por una empresa de telecomunicaciones será culpable de una infracción penal y castigada con una pena de prisión acompañada de trabajos de hasta dos años o una multa de hasta un millón JPY⁽¹⁰⁰⁾. Aunque esta exigencia no es absoluta y permite, en particular, las medidas conculcadoras del secreto de las comunicaciones que constituyan «actos justificables» en el sentido del artículo 35 del Código Penal⁽¹⁰¹⁾, esta excepción no cubre la respuesta a las solicitudes no obligatorias presentadas por las autoridades públicas relativas a la comunicación de información electrónica formuladas con arreglo a lo dispuesto en el artículo 197, apartado 2, del CEC.

3.2.1.3. Utilización ulterior de la información recogida

- (130) En el momento en que es recogida por las autoridades públicas japonesas, la información personal pasa a entrar en el ámbito de aplicación de la LPIPHAO. Esta Ley regula el manejo (tratamiento) de la «información personal

⁽⁹³⁾ De conformidad con el artículo 30, apartado 1, y el artículo 31, apartado 2, de la Ley de Policía, el Director General de las Oficinas de la Policía Regional (delegaciones locales de la APE), «dirigirá y supervisará» la policía prefectural.

⁽⁹⁴⁾ La ficha de consulta debe especificar asimismo los datos de contacto del «gestor» («nombre de la sección [cargo], nombre del gestor, número de teléfono de la oficina, extensión, etc.»).

⁽⁹⁵⁾ Tribunal Supremo, sentencia de 24 de diciembre de 1969 [1965(A) 1187]; sentencia de 15 de abril de 2008 [2007(A) 839].

⁽⁹⁶⁾ Aunque estas sentencias no se refieren a la recogida de información electrónica, el Gobierno japonés ha precisado que la aplicación de los criterios establecidos por el Tribunal Supremo se hace extensiva a cualquier interferencia de las autoridades públicas con el derecho a la privacidad, inclusive todas las «investigaciones voluntarias» y, por tanto, los criterios también vinculan a las autoridades japonesas a la hora de formular solicitudes de comunicación voluntaria de información. Véase el anexo II, sección II.A.2, letra b), número 1).

⁽⁹⁷⁾ Según la información recibida, estos factores han de considerarse «razonables con arreglo a convenciones socialmente aceptadas». Véase el anexo II, sección II.A.2, letra b), número 1).

⁽⁹⁸⁾ Para consideraciones similares en el contexto de investigaciones obligatorias (escuchas telefónicas), véase también la sentencia del Tribunal Supremo de 16 de diciembre de 1999, 1997(A) 636.

⁽⁹⁹⁾ A este respecto, las autoridades japonesas han llamado la atención sobre las Directrices de la CPIP (Edición de la norma general) y el punto 5/14 de la sección de preguntas y respuestas preparada por la CPIP para la aplicación de la LPIP. Según las autoridades japonesas, «habida cuenta de la creciente sensibilización de los particulares sobre su derecho a la vida privada, así como de la carga de trabajo generada por estas solicitudes, los operadores económicos son cada vez más cautos a la hora de responder a dichas solicitudes». Véase el anexo II, sección II.A.2, también en relación con la Nota de la ANP de 1999. Según la información recibida, se han producido efectivamente casos en los que los operadores económicos se han negado a cooperar. Por ejemplo, en su informe sobre la transparencia de 2017, LINE (la aplicación de mensajería más popular de Japón) indica: «Cuando recibimos solicitudes de agencias de investigación, verificamos que son apropiadas desde el punto de vista de la legalidad, la protección de los usuarios, etc. En función de la verificación, rechazamos las solicitudes en ese momento si se detecta una deficiencia jurídica. Si el alcance de la solicitud es demasiado amplio a efectos de la investigación, pedimos a la agencia de investigación una explicación. Si esta es infundada, no respondemos a la solicitud.» Disponible en la siguiente dirección: <https://linecorp.com/en/security/transparency/top>

⁽¹⁰⁰⁾ Las sanciones previstas son una pena de prisión acompañada de trabajos de tres años o una multa no superior a 2 millones JPY para toda persona que «ejerza una actividad de telecomunicaciones».

⁽¹⁰¹⁾ En virtud del Código Penal, por «actos justificables» se entiende, en particular, aquellos actos de una empresa de telecomunicaciones por los cuales esta última cumple las medidas del Estado que tienen efecto jurídico (medidas obligatorias), por ejemplo cuando las autoridades de investigación adoptan medidas basadas en una orden dictada por un juez. Véase el anexo II, sección II.A.2, letra b), número 2), que remite a las Directrices sobre la protección de la información personal en el sector de las telecomunicaciones.

conservada» e impone al efecto una serie de limitaciones y salvaguardas (véase el considerando 118) ⁽¹⁰²⁾. Por otra parte, el hecho de que un órgano administrativo solo pueda conservar información personal «cuando la conservación sea necesaria para ejercer las actividades bajo su jurisdicción en virtud de disposiciones legales y reglamentarias» (artículo 3, apartado 1, de la LPIPHAO) impone igualmente restricciones, al menos indirectamente, a la recogida inicial.

3.2.2. Supervisión independiente

- (131) En Japón, la recogida de información electrónica en el ámbito del control del cumplimiento del Derecho penal ⁽¹⁰³⁾ es en principio competencia de la policía prefectural ⁽¹⁰⁴⁾, que está sujeta a este respecto a varios niveles de supervisión.
- (132) En primer lugar, en todos los casos en los que la información electrónica se recoge por medios obligatorios (registro e incautación), la policía tiene que obtener previamente una orden judicial (véase el considerando 121). Por consiguiente, la recogida en tales casos será controlada *ex ante* por un juez, sobre la base de un estándar estricto de «causa suficiente».
- (133) Aunque en el caso de las solicitudes de comunicación voluntaria no existe un control *ex ante* por parte de un juez, los operadores económicos a quienes se dirigen dichas solicitudes pueden oponerse a ellas sin exponerse a sufrir consecuencias negativas (y han de tener en cuenta el impacto en la vida privada de toda comunicación). Por otra parte, con arreglo al artículo 192, apartado 1, del CEC, los agentes de policía siempre deben cooperar y coordinar sus actuaciones con el Ministerio Fiscal (y la Comisión Prefectural de Seguridad Pública) ⁽¹⁰⁵⁾. A su vez, el fiscal puede dar las instrucciones generales necesarias para establecer estándares con vistas a una investigación justa o dictar órdenes específicas en relación con una investigación particular (artículo 193 del CEC). En caso de que no se atiendan tales instrucciones y/u órdenes, el Ministerio Fiscal puede presentar cargos con vistas a la adopción de medidas disciplinarias (artículo 194 del CEC). Por consiguiente, la policía prefectural está bajo la supervisión del Ministerio Fiscal.
- (134) En segundo lugar, con arreglo al artículo 62 de la Constitución, cualquiera de las cámaras del Parlamento japonés (la Dieta) puede abrir investigaciones en relación con el Gobierno, incluso en lo que respecta a la legalidad de la recogida de información por la Policía. A tal fin, puede exigir la presencia y la declaración de testigos, o la consulta de actas. Estas competencias de investigación se especifican en la Ley de la Dieta, en particular en su capítulo XII. En concreto, el artículo 104 de la Ley de la Dieta dispone que el Gabinete, las agencias públicas y otras instancias públicas «deben atender las solicitudes presentadas por una de las Cámaras o cualquiera de sus comisiones respecto de los informes y actas necesarios a efectos de investigación». La negativa a atender estas solicitudes solo está autorizada si los poderes públicos alegan un motivo plausible aceptable por la Dieta, o en caso de declaración oficial de que la presentación de informes y actas sería «gravemente perjudicial para el interés nacional» ⁽¹⁰⁶⁾. Además, los miembros de la Dieta pueden plantear preguntas escritas al Gabinete (artículos 74 y 75 de la Ley de la Dieta) y, en el pasado, algunas de estas «consultas escritas» han abordado asimismo el manejo de información personal por parte de la Administración ⁽¹⁰⁷⁾. El papel de la Dieta en la supervisión del ejecutivo se ve reforzado por las obligaciones impuestas en materia de presentación de informes, por ejemplo con arreglo al artículo 29 de la Ley de escuchas telefónicas.
- (135) En tercer lugar, también en el seno del poder ejecutivo, la policía prefectural está sujeta a una supervisión independiente. Esta supervisión es ejercida, en particular, por las comisiones prefecturales de seguridad pública, establecidas a nivel prefectural para garantizar una administración democrática y la neutralidad política de la policía ⁽¹⁰⁸⁾. Estas comisiones están compuestas por miembros nombrados por el gobernador prefectural con el consentimiento de la asamblea prefectural (de entre ciudadanos que no han ocupado un cargo de funcionario de la policía en los cinco años anteriores) y su mandato está garantizado (en particular, los despidos solo son posibles por un motivo justificado) ⁽¹⁰⁹⁾. Según la información recibida, no reciben instrucciones, por lo que pueden considerarse totalmente independientes ⁽¹¹⁰⁾. En lo que respecta a las funciones y competencias de las comisiones

⁽¹⁰²⁾ En lo que respecta a los derechos de las personas afectadas, véase la sección 3.1.

⁽¹⁰³⁾ En principio, un fiscal (o un fiscal adjunto a sus órdenes) puede, si lo estima necesario, investigar una infracción (artículo 191, apartado 1, del CEC).

⁽¹⁰⁴⁾ Según la información recibida, la Agencia de Policía Nacional no lleva a cabo investigaciones criminales específicas. Véase el anexo II, sección II.A.1, letra a).

⁽¹⁰⁵⁾ Véase igualmente el artículo 246 del CEC, en virtud del cual la policía judicial tiene la obligación de remitir el expediente al fiscal, una vez haya llevado a cabo la investigación de una infracción penal («principio de remisión en todos los casos»).

⁽¹⁰⁶⁾ La Dieta también puede solicitar que la Junta de supervisión y revisión de los secretos específicamente diseñados investigue la negativa a responder. Véase el artículo 104-II de la Ley de la Dieta.

⁽¹⁰⁷⁾ Véase el anexo II, sección II.B.4.

⁽¹⁰⁸⁾ Además, con arreglo a lo dispuesto en el artículo 100 de la Ley de autonomía local, la asamblea local tiene autoridad para investigar las actividades de las autoridades que ejercen funciones coercitivas establecidas a nivel prefectural, incluida la policía prefectural.

⁽¹⁰⁹⁾ Véanse los artículos 39 a 41 de la Ley de Policía. Por lo que se refiere a la neutralidad política, véase igualmente el artículo 42 de la Ley de Policía.

⁽¹¹⁰⁾ Véase el anexo II, sección II.B.3 («sistema de consejo independiente»).

prefecturales de seguridad pública son responsables, con arreglo al artículo 38, apartado 3, leído en relación con el artículo 2 y el artículo 36, apartado 2, de la Ley de Policía, de «la protección de los derechos y libertades de un particular». A tal efecto, están facultadas para «supervisar»⁽¹¹¹⁾ todas las actividades de investigación de la policía prefectural, incluida la recogida de datos personales. En concreto, las comisiones «pueden, en caso necesario, instruir a esta en detalle o en un caso particular de inspección de una falta cometida por el personal de la policía»⁽¹¹²⁾. Cuando el jefe de la policía prefectural⁽¹¹³⁾ reciba tales instrucciones o descubra por sí mismo un posible caso de falta (incluida la violación de la normativa u otro tipo de comportamientos negligentes), debe proceder sin demora a la inspección del caso e informar del resultado de la inspección a la comisión prefectural de seguridad pública (artículo 56, apartado 3, de la Ley de Policía). Si esta lo considera necesario, también puede designar a uno de sus miembros para revisar el estado de implementación. Este proceso continúa hasta que la comisión prefectural de seguridad pública estima que el incidente se ha resuelto satisfactoriamente.

- (136) Además, en lo que respecta a la correcta aplicación de la LPIPHAO, el ministro o director de agencia competente (a saber, el comisario general de la ANP) tiene autoridad de ejecución, bajo la supervisión del ministerio del Interior y de Comunicaciones (MIC). Con arreglo al artículo 49 de la LPIPHAO, el MIC «podrá recabar informes sobre el estado de aplicación de la presente Ley» ante los jefes de los órganos administrativos (ministro). Esta función de supervisión está igualmente respaldada por los 51 «centros de información integrada» (uno en cada prefectura de Japón) adscritos al MIC, que tramitan cada año miles de consultas de particulares⁽¹¹⁴⁾ (que pueden, a su vez, sacar a la luz posibles violaciones de la ley). Cuando lo considere necesario para garantizar el respeto de la ley, el MIC puede pedir que se le presenten explicaciones y materiales, y emitir dictámenes sobre el manejo de información personal por parte del órgano administrativo de que se trate (artículos 50 y 51 de la LPIPHAO).

3.2.3. Reparación individual

- (137) Además de la supervisión de oficio, los particulares disponen asimismo de distintas posibilidades para obtener reparación a título individual, tanto a través de autoridades independientes (como las comisiones prefecturales de seguridad pública o la CPIP) como de los órganos jurisdiccionales japoneses
- (138) En primer lugar, en lo que respecta a la información personal recogida por órganos administrativos, estos tienen la obligación de «procurar tramitar las reclamaciones de manera apropiada y sin demora» teniendo en cuenta su tratamiento ulterior (artículo 48 de la LPIPHAO). Aunque el capítulo IV de la LPIPHAO, relativo a los derechos individuales, no es aplicable a la información personal que figure en «documentos relativos a los procesos y a los bienes incautados» (artículo 53-2, apartado 2, del CEC), que incluye la información personal recogida en el marco de investigaciones criminales, los particulares pueden presentar una reclamación invocando los principios generales de protección de datos como, por ejemplo, la obligación de conservar únicamente información personal «cuando ello sea necesario para el ejercicio de funciones coercitivas» (artículo 3, apartado 1, de la LPIPHAO).
- (139) Además, el artículo 79 de la Ley de Policía reconoce a los particulares que tengan dudas en cuanto al «desempeño de sus funciones» por parte del personal de policía, el derecho a presentar una reclamación ante la comisión prefectural de seguridad pública, que es un órgano independiente. La comisión tramitará tales reclamaciones «atentamente», de conformidad con las disposiciones legales y las ordenanzas locales, y comunicará por escrito los resultados al denunciante. Habida cuenta de la autoridad que detenta para supervisar a la policía prefectural y «darle instrucciones» en lo que respecta a las «faltas cometidas por el personal» (artículo 38, apartado 3, y artículo 43-2, apartado 1, de la Ley de policía), puede solicitar a la policía prefectural que investigue los hechos, adopte las medidas apropiadas sobre la base de las conclusiones de la investigación e informe sobre los resultados. Si estima que la investigación llevada a cabo por la policía no es satisfactoria, la comisión también puede dar instrucciones sobre la tramitación de la reclamación.
- (140) A fin de facilitar la tramitación de las reclamaciones, la ANP ha publicado una nota, dirigida a las comisiones de seguridad pública de la Policía y de las Prefecturas, sobre la forma de tramitar las reclamaciones relativas al desempeño de sus funciones por los agentes de policía. En dicho documento, la ANP establece estándares para

⁽¹¹¹⁾ Véanse el artículo 5, apartado 3, y el artículo 38, apartado 3, de la Ley de Policía.

⁽¹¹²⁾ Véanse el artículo 38, apartado 3, y el artículo 43-2, apartado 1, de la Ley de Policía. En caso de que «dé una instrucción» en el sentido del artículo 43-2, apartado 1, la comisión prefectural de seguridad pública puede ordenar a un comité designado por la comisión que asegure el seguimiento de su implementación (apartado 2). Además, la comisión puede recomendar medidas disciplinarias o la destitución del jefe de la policía prefectural (artículo 50, apartado 2), así como de otros agentes de policía (artículo 55, apartado 4, de la Ley de Policía).

⁽¹¹³⁾ Lo mismo se aplica al superintendente general en el caso de la Policía Metropolitana de Tokio (véase el artículo 48, apartado 1, de la Ley de Policía).

⁽¹¹⁴⁾ Según la información recibida, en el ejercicio financiero 2017 (de abril de 2017 a marzo de 2018), los «centros de información integrada» atendieron un total de 5 186 consultas de particulares.

la interpretación e implementación del artículo 79 de la Ley de Policía. Entre otras cosas, insta a la policía prefectural a que implante «un sistema de tramitación de reclamaciones» y a que tramite todas las reclamaciones e informe «de inmediato» a la comisión prefectural de seguridad pública competente. La nota define las reclamaciones como alegaciones en favor de la corrección de «cualquier desventaja específica ocasionada por un comportamiento ilícito o inadecuado»⁽¹¹⁵⁾ o como «la inacción por parte de un agente de policía en el desempeño de sus cometidos»⁽¹¹⁶⁾, así como «cualquier agravio o insatisfacción manifestado respecto de un modo inadecuado de ejecutar sus funciones por parte de un agente de policía». El ámbito de aplicación material de una reclamación se define así en sentido lato, comprendiendo cualquier solicitud ilícita de recogida de datos, y el denunciante no tendrá que demostrar la existencia de un daño sufrido como consecuencia de las actuaciones de un agente de policía. Cabe destacar que la nota establece que los extranjeros (entre otros) recibirán asistencia sobre cómo formular una reclamación. A raíz de una queja, las comisiones prefecturales de seguridad pública deben velar por que la policía prefectural examine los hechos, ponga en práctica medidas «en función de los resultados del examen» e informe sobre los resultados. Cuando la comisión considera que el examen es insuficiente, emite una instrucción sobre la tramitación de la reclamación que la policía prefectural está obligada a seguir. Sobre la base de los informes recibidos y de las medidas adoptadas, la comisión informa al particular, indicándole, entre otras cosas, las medidas adoptadas para atender la reclamación. La nota de la ANP subraya que las reclamaciones deben tramitarse «atentamente» y que el resultado debe comunicarse «en un plazo [...] apropiado acorde a las normas sociales y al sentido común».

- (141) En segundo lugar, dado que normalmente la reparación ha de buscarse en un sistema y una lengua extranjeros, el Gobierno japonés ha hecho uso de sus competencias para crear un mecanismo específico, gestionado y supervisado por la CPIP, encargado de la tramitación y resolución de las reclamaciones en este ámbito, con el fin de facilitar vías de reparación a los particulares de la UE cuyos datos personales se transfieran a operadores económicos en Japón y a los que, posteriormente, tengan acceso las autoridades públicas. Este mecanismo se basa en la obligación de cooperación impuesta a las autoridades públicas japonesas por la LPIIP y en el papel especial que desempeña la CPIP en lo que respecta a las transferencias internacionales de datos desde terceros países en virtud del artículo 6 de la LPIIP y de la política de base (tal como fue establecida por orden del gabinete del Gobierno japonés). Este mecanismo se presenta en detalle en las declaraciones, garantías y compromisos recibidos del Gobierno japonés que se adjuntan a la presente Decisión como anexo II. El mecanismo no está sujeto a ningún requisito de legitimación y está abierto a cualquier particular, con independencia de si es sospechoso o está acusado de una infracción penal
- (142) En el marco de este mecanismo, un particular que sospeche que datos que le conciernan transferidos desde la Unión Europea han sido recogidos o utilizados por las autoridades públicas japonesas (incluidos los responsables de hacer cumplir el Derecho penal) en violación de las normas aplicables puede presentar una reclamación a la CPIP (a título individual o a través de la autoridad de protección de datos de su país en el sentido del artículo 51 del RGPD). La CPIP está obligada a tramitar la reclamación y, en una primera fase, debe informar a las autoridades públicas competentes, incluidos los órganos de supervisión pertinentes, del curso dado a la misma. Estas autoridades están obligadas a cooperar con la CPIP, «en particular facilitando la información necesaria y el material pertinente para permitir a la CPIP evaluar si la recogida o la utilización ulterior de la información personal ha tenido lugar de conformidad con las normas aplicables»⁽¹¹⁷⁾. Esta obligación, derivada del artículo 80 de la APIP (que obliga a las autoridades públicas japonesas a cooperar con la CPIP), es de aplicación general y, por lo tanto, comprende la revisión de cualquier medida de investigación adoptada por dichas autoridades, que además se han comprometido a esta cooperación mediante garantías ofrecidas por escrito por los ministros y jefes de agencias competentes, como se indica en el anexo II.
- (143) Si de la evaluación se desprende que se ha infringido la normativa aplicable, «la cooperación entre las autoridades públicas afectadas y la CPIP incluye la obligación de subsanar la infracción», lo que, en caso de recogida ilícita de información personal, requiere la supresión de tales datos. Cabe destacar que el cumplimiento de esta obligación se hace bajo la supervisión de la CPIP que «confirmará, antes de concluir la evaluación, que la infracción ha sido totalmente subsanada.»
- (144) Una vez concluida la evaluación, la CPIP debe informar al particular, en un plazo razonable, de los resultados de la evaluación, incluidas, en su caso, las medidas correctoras adoptadas. Al mismo tiempo, la CPIP también debe informar al particular de la posibilidad de solicitar a la autoridad pública competente la confirmación de los resultados y la identidad de la autoridad a la que debe dirigir tal solicitud. La posibilidad de recibir dicha

⁽¹¹⁵⁾ La condición de que exista una «desventaja específica» significa simplemente que el reclamante ha de verse afectado a título individual por la conducta (o la inacción) de la policía, no que tenga que demostrar la existencia de perjuicio.

⁽¹¹⁶⁾ El cumplimiento de la ley, incluidos los requisitos legales para la recogida y utilización de datos personales, forma parte de esos cometidos. Véanse el artículo 2, apartado 2, y el artículo 3 de la Ley de Policía.

⁽¹¹⁷⁾ Al llevar a cabo su evaluación, la CPIP cooperará con el MIC, que, como se explica en el considerando 136, puede pedir que se le den explicaciones y se le faciliten materiales, y emitir un dictamen, sobre el manejo de la información personal por el órgano administrativo correspondiente (artículos 50 y 51 de la LPIPHAO).

confirmación, incluidos los motivos en que se basa la decisión de la autoridad competente, podrá ser de utilidad al particular a la hora de adoptar nuevas medidas, en particular la incoación de una acción judicial. El acceso a la información detallada acerca de los resultados de la evaluación puede limitarse si existen motivos razonables para considerar que la comunicación de dicha información puede entrañar un riesgo para la investigación en curso.

- (145) En tercer lugar, una persona que no esté de acuerdo con una decisión (orden) de incautación⁽¹¹⁸⁾ relativa a sus datos personales dictada por un juez, o con las medidas de ejecución de dicha decisión por parte de la Policía o el Ministerio Fiscal, puede solicitar la anulación o la modificación de dicha decisión o de dichas medidas (artículo 429, apartado 1, y artículo 430, apartados 1 y 2, del CEC y artículo 26 de la Ley de escuchas telefónicas)⁽¹¹⁹⁾. En caso de que el tribunal que está reexaminando el asunto considere que la propia orden judicial o su ejecución («procedimiento de incautación») son ilegales, aceptará la solicitud y ordenará la restitución de los artículos incautados⁽¹²⁰⁾.
- (146) En cuarto lugar, todo particular que considere que la recogida de información personal que le concierna en el marco de una investigación criminal es ilícita puede optar por una forma más indirecta de control judicial e invocar este carácter ilícito en el proceso penal. Si el tribunal acepta esta alegación, las pruebas serán excluidas por inadmisibilidad.
- (147) Por último, en virtud del artículo 1, apartado 1, de la Ley de reparaciones a cargo del Estado a las víctimas de la actuación ilegítima del Estado, un tribunal puede conceder una indemnización cuando un funcionario que ejerza la autoridad pública del Estado, haya ocasionado daños, en el ejercicio sus funciones, de forma ilícita y culposa (con intencionalidad o por negligencia) al particular de que se trate. De conformidad con el artículo 4 de la Ley de reparaciones a cargo del Estado, la responsabilidad del Estado por daños y perjuicios se basa en las disposiciones del Código Civil. A este respecto, el artículo 710 del Código Civil dispone que esta responsabilidad cubre no solo los daños ocasionados a la propiedad, sino también los daños morales (por ejemplo, en forma de «sufrimiento psicológico»). Se incluyen aquí los casos en que se haya violado la privacidad de un particular mediante actividades de vigilancia ilícita o recogida de información personal que le concierna (p. ej. la ejecución ilegal de una orden judicial)⁽¹²¹⁾.
- (148) Además de la indemnización pecuniaria, los particulares también pueden, en ciertas condiciones, beneficiarse de medidas cautelares (por ejemplo, la supresión de los datos personales recogidos por las autoridades públicas) invocando su derecho a la vida privada consagrado en el artículo 13 de la Constitución⁽¹²²⁾.
- (149) Con respecto a todas esas vías de reparación, el mecanismo de resolución de litigios creado por el Gobierno japonés permite a un particular que sigue insatisfecho con el resultado del procedimiento dirigirse a la CPIP, «la cual informará al particular de las distintas posibilidades y procedimientos detallados para obtener una reparación en virtud de las disposiciones legales y reglamentarias japonesas». Además, la CPIP «prestará apoyo al particular, en particular asesoramiento y asistencia para emprender nuevas acciones ante el órgano administrativo o judicial pertinente».
- (150) Esto incluye el uso de los derechos procedimentales previstos en el Código de Enjuiciamiento Criminal. Por ejemplo, «[c]uando de la evaluación se desprenda que un particular es sospechoso de haber cometido un delito, la CPIP le informará al respecto»⁽¹²³⁾, así como de la posibilidad, de conformidad con el artículo 259 del CEC, de solicitar al Ministerio Fiscal que le haga saber cuando este haya decidido no incoar un procedimiento penal. Además, si la evaluación pone de manifiesto que se ha utilizado información personal que concierne al particular en el marco de un asunto que ya ha sido cerrado, la CPIP informará al particular de que puede consultar el expediente con arreglo al artículo 53 del CEC (y el artículo 4 de la Ley sobre los expedientes de los asuntos penales cerrados). Es importante que un particular tenga acceso a su expediente porque ello le ayudará a comprender mejor

⁽¹¹⁸⁾ Esto incluye una orden de escuchas telefónicas, para las cuales la Ley de escuchas telefónicas prevé una obligación de notificación específica (artículo 23). Con arreglo a esta disposición, la autoridad encargada de la investigación debe informar por escrito a los particulares afectados de que sus comunicaciones han sido interceptadas (y figuran, por tanto, en el acta de interceptación). Otro ejemplo: de conformidad con el artículo 100, apartado 3, del CEC, cuando un órgano jurisdiccional se haya incautado de envíos postales o de telegramas enviados al acusado o recibidos por él, debe informar al remitente o al destinatario, a menos que exista el riesgo de que dicha notificación pudiera obstaculizar los procedimientos judiciales. El artículo 222, apartado 1, del CEC remite a esta disposición para los registros e incautaciones llevados a cabo por la autoridad encargada de la investigación.

⁽¹¹⁹⁾ Aunque dicha solicitud no tiene como efecto automático la suspensión de la ejecución de la decisión de incautación, el tribunal que esté reexaminando el asunto puede ordenar la suspensión hasta que se haya dictado una resolución sobre el fondo. Véanse el artículo 429, apartado 2, y el artículo 432, leídos en relación con el artículo 424, del CEC.

⁽¹²⁰⁾ Véase el anexo II, sección II.C.1.

⁽¹²¹⁾ Véase el anexo II, sección II.C.2.

⁽¹²²⁾ Véase, por ejemplo, la sentencia (n.º 2925), dictada el 24 de marzo de 1988 por el tribunal de distrito de Tokio y la sentencia (n.º 2925), dictada el 26 de abril de 2007 por el tribunal de distrito de Osaka. Según el tribunal de distrito de Osaka, se ha de encontrar un equilibrio entre una serie de factores como, por ejemplo: i) la naturaleza y el contenido de la información personal en cuestión; ii) la forma en que ha sido recogida; iii) los inconvenientes para el particular en caso de que no se suprima la información; y iv) el interés público, incluidos los inconvenientes para la autoridad pública en caso de que se suprima la información.

⁽¹²³⁾ En cualquier caso, una vez iniciado el procedimiento criminal, el Ministerio Fiscal brindará al acusado la oportunidad de examinar dichas pruebas (véanse los artículos 298 y 299 del CEC). Por lo que respecta a las víctimas de delitos, véanse los artículos 316 a 333 del CEC.

la investigación de la que es objeto y, por tanto, a preparar una posible acción judicial (por ejemplo, una indemnización por daños y perjuicios) si estima que los datos que le conciernen han sido recogidos o utilizados de forma ilícita.

3.3. Acceso a los datos y utilización de los mismos por parte de las autoridades públicas japonesas a efectos de seguridad nacional

- (151) Según las autoridades japonesas, ninguna ley en Japón permite las solicitudes obligatorias de información o las «escuchas administrativas» fuera de las investigaciones criminales. Por consiguiente, por razones de seguridad nacional, la información solo puede obtenerse de una fuente a la que pueda acceder libremente cualquier persona o por comunicación voluntaria. Los operadores económicos que reciban una solicitud de cooperación voluntaria (en forma de comunicación de información electrónica) no tienen ninguna obligación legal de facilitar esta información ⁽¹²⁴⁾.
- (152) Además, según la información recibida, solo cuatro entidades públicas están facultadas para recoger la información electrónica que obre en poder de los operadores económicos japoneses por motivos de seguridad nacional, a saber: i) la Oficina de Inteligencia e Investigación del Gabinete (OIIG); ii) el Ministerio de Defensa (MdD); iii) la Policía [la Agencia Nacional de Policía (ANP) ⁽¹²⁵⁾ y la policía prefectural]; y iv) la Agencia de Inteligencia en materia de Seguridad Pública («AISP»). Sin embargo, la OIIG nunca recoge información directamente de los operadores económicos, ni siquiera mediante la interceptación de comunicaciones. Cuando reciba información de otras autoridades públicas a efecto de análisis dirigido al Gabinete, estas otras autoridades tienen que cumplir, a su vez, la legislación, incluidas la limitaciones y salvaguardas que se analizan en la presente Decisión. Sus actividades no son pertinentes pues en un contexto de transferencia.

3.3.1. Base jurídica y limitaciones/salvaguardas aplicables

- (153) Según la información recibida, el MdD recoge información (electrónica) sobre la base de la Ley por la que se crea el MdD. Conforme a su artículo 3, el MdD tiene por misión administrar y dirigir las fuerzas armadas y «realizar las acciones necesarias para asegurar la paz y la independencia nacional, y la seguridad de la nación». El artículo 4, apartado 4, dispone que es competencia del MdD «la defensa y la protección», las medidas que vayan a adoptar las fuerzas de autodefensa y el despliegue de las fuerzas armadas, incluida la recogida de la información necesaria a tales efectos. El MdD solo tiene autoridad para recoger información (electrónica) de los operadores económicos en el marco de una cooperación voluntaria.
- (154) La policía prefectural, por su parte, es la encargada de velar por «el mantenimiento del orden y la seguridad pública» (artículo 35, apartado 2, leído en relación con el artículo 2, apartado 1, de la Ley de Policía). En el marco de estas competencias, la policía puede recoger información, pero solo sobre una base voluntaria, sin valor jurídico. Por otra parte, las actividades de la policía deben «limitarse a lo estrictamente necesario» para el desempeño de sus funciones. Además, la policía debe actuar de manera «imparcial, neutral, libre de prejuicios y justa» y nunca podrá abusar de sus poderes «de modo que pueda violar los derechos y libertades de un particular garantizados en la Constitución japonesa» (artículo 2 de la Ley de Policía).
- (155) Por último, la AISP puede realizar investigaciones en virtud de la Ley de prevención de actividades subversivas (LPAS) y la Ley sobre el control de las organizaciones que han cometido masacres indiscriminadas (LCO) cuando tales investigaciones sean necesarias para preparar la adopción de medidas de control contra determinadas organizaciones ⁽¹²⁶⁾. En virtud de ambas leyes, a solicitud del director general de la AISP la comisión de examen de la seguridad pública puede adoptar ciertas «disposiciones» (vigilancia y prohibiciones en el caso de la LCO ⁽¹²⁷⁾, disolución y prohibiciones en el caso de la LPAS ⁽¹²⁸⁾), y, en este contexto, la AISP puede llevar a cabo investigaciones ⁽¹²⁹⁾. Con arreglo a la información recibida, estas investigaciones se realizan siempre sobre una base

⁽¹²⁴⁾ Por lo tanto, los operadores económicos pueden elegir libremente no cooperar, sin que ello entrañe riesgo de sanciones u otras consecuencias negativas. Véase el anexo II, sección III.A.1.

⁽¹²⁵⁾ No obstante, según la información recibida, el principal papel de la ANP consiste en coordinar las investigaciones llevadas a cabo por los distintos departamentos de la policía prefectural e intercambiar información con las autoridades extranjeras. Incluso en este papel, la ANP está sujeta a supervisión por parte de la Comisión Nacional de Seguridad Pública, responsable, entre otras cosas, de la protección de los derechos y libertades de los particulares (artículo 5, apartado 1, de la Ley de Policía).

⁽¹²⁶⁾ Véase el anexo II, sección III.A.1, número 3). Los ámbitos de aplicación de estas dos Leyes están limitados: la LPAS se refiere a las «actividades subversivas de terrorismo» y la LCO, a los «actos indiscriminados de masacres» (es decir, una «actividad subversiva de terrorismo» en virtud de la LPAS «en el que un gran número de personas son asesinadas indiscriminadamente»).

⁽¹²⁷⁾ Véanse los artículos 5 y 8 de la LCO. Una disposición de vigilancia implica igualmente una obligación de información para la organización afectada por la medida. Para las salvaguardas procedimentales, en particular los requisitos de transparencia y la autorización previa de la comisión de examen de la seguridad pública, véanse los artículos 12, 13, y 15 a 27 de la LCO.

⁽¹²⁸⁾ Véanse los artículos 5 y 7 de la LPAS. Para las salvaguardas procedimentales, en particular los requisitos de transparencia y la autorización previa de la comisión de examen de la seguridad pública, véanse los artículos 11 a 25 de la LPAS.

⁽¹²⁹⁾ Véanse el artículo 27 de la LPAS y los artículos 29 y 30 de la LCO.

voluntaria, en decir, la AISP no puede obligar a un propietario de información personal a facilitar dicha información⁽¹³⁰⁾. En cada caso, los controles y las investigaciones deben limitarse a lo estrictamente necesario para alcanzar el objetivo de control y en ningún caso pueden llevarse a cabo para restringir «irrazonablemente» los derechos y libertades garantizados en la Constitución japonesa (artículo 3, apartado 1, de la LPAS/LCO). Por otra parte, con arreglo al artículo 3, apartado 2, de la LPAS/LCO, la AISP no debe abusar en ningún caso de tales controles ni de las investigaciones preparatorias. Si un agente de la AISP abusa de la autoridad que le confiere la ley y obliga a una persona a hacer algo a lo que no está obligada o interfiere en el ejercicio de los derechos de una persona, pueden imponérsele sanciones penales de conformidad con el artículo 45 de la LPAS o el artículo 42 de la LCO. Por último, ambas leyes establecen expresamente que sus disposiciones, incluidas las competencias que confieren, no deben «en ningún caso ser objeto de una interpretación amplia» (artículo 2 de la LPAS/LCO).

- (156) En todos los casos de acceso a los datos de las autoridades públicas por motivos de seguridad nacional que se describen en la presente sección, son aplicables las limitaciones previstas por el Tribunal Supremo japonés para las investigaciones de carácter voluntario, lo que significa que la recogida de información (electrónica) debe atenerse a los principios de necesidad y proporcionalidad («método apropiado»)⁽¹³¹⁾. Como han confirmado explícitamente las autoridades japonesas, «la recogida y el tratamiento de información tiene lugar únicamente en la medida necesaria para el desempeño de las funciones específicas de la autoridad pública competente, así como sobre la base de amenazas específicas». Por lo tanto, «quedan excluidas la recogida o el acceso masivos e indiscriminados de información personal por motivos de seguridad nacional»⁽¹³²⁾.
- (157) Asimismo, una vez recogida, toda información personal conservada por las autoridades públicas por motivos de seguridad nacional estará sujeta y, por lo tanto, se beneficiarán de las medidas de protección previstas en la LPIPHAO que se aplicarán a su almacenamiento, utilización y comunicación ulteriores (véase el considerando 118).

3.3.2. Supervisión independiente

- (158) La recogida de información personal por motivos de seguridad nacional está sujeta a varios niveles de supervisión por parte de los tres poderes del Estado.
- (159) En primer lugar, la Dieta japonesa, a través de sus comisiones especializadas, puede examinar la legalidad de las investigaciones basándose en sus competencias de control parlamentario (artículo 62 de la Constitución y artículo 104 de la Ley de la Dieta; véase el considerando 134). Esta función de supervisión está respaldada por la obligación específica de informar sobre las actividades realizadas en virtud de algunas de las bases jurídicas mencionadas⁽¹³³⁾.
- (160) En segundo lugar, en el seno del poder ejecutivo existen varios mecanismos de supervisión.
- (161) Por lo que se refiere al MdD, la supervisión es ejercida por la Oficina del Inspector General (OIG) encargado de la conformidad con la legislación⁽¹³⁴⁾, creada en virtud del artículo 29 de la Ley por la que se crea el MdD como oficina adscrita al Ministerio de Defensa (del cual depende) y bajo su supervisión, pero independiente de los departamentos operativos de este. La OIG es la encargada de asegurar la conformidad con las disposiciones legales y reglamentarias, así como la buena ejecución de las funciones que incumben a los funcionarios del MdD. Entre sus competencias, la autoridad lleva a cabo «inspecciones en el ámbito de la defensa», tanto a intervalos regulares («inspecciones de defensa regulares») como en circunstancias puntuales («inspecciones de defensa especiales»), que, en el pasado, han abordado igualmente el manejo adecuado de información personal⁽¹³⁵⁾. En el marco de dichas

⁽¹³⁰⁾ Véase el anexo II, sección III.A.1, número 3).

⁽¹³¹⁾ Véase el anexo II, sección III.A.2, letra b). «De la jurisprudencia del Tribunal Supremo se desprende que las solicitudes de cooperación voluntaria dirigidas a un operador económico han de ser necesarias para la investigación de un presunto delito y debe ser razonable para alcanzar la finalidad de la investigación. Aunque las investigaciones efectuadas por los servicios de investigación en materia de seguridad nacional y las realizadas por los servicios de investigación en el ámbito del control del cumplimiento de ley difieren en lo que respecta tanto a su base jurídica como a su finalidad, los principios fundamentales relativos a la “necesidad de la investigación” y “adecuación del método” se aplican de manera similar en el ámbito de la seguridad nacional y han de respetarse teniendo debidamente en cuenta las circunstancias específicas de cada caso».

⁽¹³²⁾ Véase el anexo II, sección III.A.2, letra b).

⁽¹³³⁾ Véanse, por ejemplo, el artículo 36 de la LPAS y el artículo 31 de la LCO (para la AISP).

⁽¹³⁴⁾ El jefe de la OIG es un antiguo fiscal. Véase el anexo II, sección III.B.3.

⁽¹³⁵⁾ Véase el anexo II, sección III.B.3. Según el ejemplo citado, la inspección de defensa regular llevada a cabo en 2016 sobre el tema «Concienciación y preparación en materia de conformidad legal» versaba, entre otras cosas, sobre «la situación en materia de protección de la información personal» (gestión, almacenamiento, etc.). El informe elaborado a raíz de esta inspección constató casos de gestión de datos inapropiada e instó a que se introdujeran mejoras en este sentido. El MdD ha publicado el informe en su sitio web.

inspecciones, la OIG puede tener acceso a sitios (oficinas) y solicitar que se le presenten documentos o información, inclusive explicaciones del viceministro adjunto del MdD. Al término de la inspección, se remite al Ministro de Defensa un informe, en el que figuran las conclusiones y las medidas propuestas para mejorar la situación (cuya puesta en práctica puede ser objeto asimismo de nuevas inspecciones). Sobre la base de este informe, el ministro de Defensa formula instrucciones sobre la puesta en práctica de las medidas necesarias para poner remedio a la situación; el viceministro adjunto es el encargado de llevar a cabo estas medidas y debe informar sobre su seguimiento.

- (162) En lo que respecta a la policía prefectural, la supervisión está garantizada por las comisiones prefecturales de seguridad pública, que son órganos independientes, tal como se ha explicado en el considerando 135, con respecto al control del cumplimiento del Derecho penal.
- (163) Por último, como se ha indicado, la AISP solo puede llevar a cabo investigaciones en la medida en que sea necesario para la adopción de una prohibición, una disolución o una medida de vigilancia en virtud de la LAPS/LCO, y para estas disposiciones la comisión independiente de examen de la seguridad pública⁽¹³⁶⁾ ejerce una supervisión *ex ante*. Además, se organizan inspecciones regulares/periódicas (que en términos generales se ocupan de las operaciones de la AISP)⁽¹³⁷⁾ e inspecciones internas⁽¹³⁸⁾ sobre las actividades de los distintos servicios/oficinas, etc., llevadas a cabo por inspectores designados específicamente y que pueden ir aparejadas de instrucciones, entre otros, a los jefes de los departamentos afectados, encaminadas a la adopción de medidas correctoras o a la introducción de mejoras.
- (164) Estos mecanismos de supervisión, que se han visto reforzados al reconocerse la posibilidad de que los particulares soliciten la intervención de la CPIP como autoridad de control independiente (véase más adelante el considerando 168), ofrecen garantías adecuadas contra el riesgo de abuso por parte de las autoridades japonesas de sus competencias en el ámbito de la seguridad nacional, y contra cualquier recogida ilícita de información electrónica.

3.3.3. Reparación individual

- (165) Si se trata de una reparación individual, en relación con la información personal recogida y, por tanto, «conservada» por los órganos administrativos, estos últimos tienen la obligación de «procurar tramitar las reclamaciones de manera apropiada y sin demora» en relación con dicho tratamiento (artículo 48 de la LPIPHAO).
- (166) Por otra parte, a diferencia de lo que ocurre con las investigaciones criminales, los particulares (incluidos los nacionales extranjeros que viven fuera de su país) tienen, en principio, derecho a comunicar⁽¹³⁹⁾, rectificar (inclusive suprimir) y suspender la utilización/puesta a disposición en virtud de la LPIPHAO. Sin embargo, el jefe del órgano administrativo puede denegar la comunicación de la información «respecto de la cual existan motivos razonables [...] para considerar que su comunicación puede causar un perjuicio a la seguridad nacional» [artículo 14, inciso iv), de la LPIPHAO], incluso sin revelar la existencia de tal información (artículo 17 de la LPIPHAO). Del mismo modo, aunque un particular puede solicitar la suspensión de su utilización o la supresión con arreglo al artículo 36, apartado 1, letra i), de la LPIPHAO en caso de que el órgano administrativo haya obtenido la información de forma ilícita o la conserve/utilice más allá de lo que es necesario para alcanzar la finalidad especificada, la autoridad puede rechazar la solicitud si considera que la suspensión del uso «puede obstaculizar la buena ejecución de los asuntos relativos a las finalidades de utilización de la información personal conservada debido a la naturaleza de dichos asuntos» (artículo 38 de la LPIPHAO). Es más, cuando sea posible separar y excluir fácilmente porciones que estén sujetas a una excepción, los órganos administrativos están obligados a conceder al menos una comunicación parcial (véase, por ejemplo, el artículo 15, apartado 1, de la LPIPHAO)⁽¹⁴⁰⁾.

⁽¹³⁶⁾ Con arreglo a la Ley por la que se crea la comisión de examen de la seguridad pública, el presidente y los miembros de la comisión «ejercerán su autoridad con independencia» (artículo 3). Son nombrados por el primer ministro con el consentimiento de ambas cámaras de la Dieta y solo pueden ser destituidos «con motivo» (p. ej. prisión, falta grave, trastorno mental o físico, apertura de un procedimiento de quiebra).

⁽¹³⁷⁾ Reglamento relativo a las inspecciones periódicas de la Agencia de Inteligencia en materia de Seguridad Pública (Director General de la AISP, instrucción n.º 4, 1986).

⁽¹³⁸⁾ Reglamento relativo a las inspecciones especiales de la Agencia de Inteligencia en materia de Seguridad Pública (Director General de la AISP, instrucción n.º 11, 2008). Se llevarán a cabo inspecciones especiales cuando el Director General de la AISP lo considere necesario.

⁽¹³⁹⁾ Este derecho corresponde al derecho a recibir una copia de la «información personal conservada».

⁽¹⁴⁰⁾ Véase igualmente la posibilidad de una «comunicación discrecional» incluso cuando se incluya «información no comunicable» en la «información personal conservada» cuya comunicación se solicita (artículo 16 de la LPIPHAO).

- (167) En cualquier caso, el órgano administrativo tiene que adoptar una decisión por escrito en un plazo determinado (30 días, que, en ciertas condiciones, puede prorrogarse por otros 30 días). Si la solicitud es rechazada, aceptada solo en parte, o si el particular considera que el comportamiento del órgano administrativo es «ilícito o injusto» por otros motivos, puede solicitar una revisión administrativa basada en la Ley de revisión de las reclamaciones administrativas⁽¹⁴¹⁾. En tal caso, el jefe del órgano administrativo encargado de tomar una decisión sobre el recurso consultará al consejo de revisión en materia de protección de la información personal y de la comunicación de información (artículos 42 y 43 de la LPIPHAO), un consejo especializado e independiente, cuyos miembros son nombrados por el primer ministro con el consentimiento de las dos cámaras de la Dieta. Según la información recibida, el consejo de revisión puede proceder a un examen⁽¹⁴²⁾ y, en este sentido, solicitar al órgano administrativo que facilite la información personal conservada, incluido cualquier contenido clasificado, así como otra información y documentación. Aunque el informe final remitido al reclamante, así como al órgano administrativo, y hecho público no es jurídicamente vinculante, sus recomendaciones son seguidas en casi todos los casos⁽¹⁴³⁾. El particular tiene además la posibilidad de impugnar la decisión de apelación ante los tribunales sobre la base de la Ley de lo contencioso administrativo. Se abre así la vía al control judicial de la utilización de la excepción o excepciones de seguridad nacional, a fin de determinar, en particular, si esta excepción ha sido utilizada de manera abusiva o si sigue estando justificada.
- (168) A fin de facilitar el ejercicio de los derechos antes mencionados en virtud de la LPIPHAO, el MIC ha creado 51 «centros de información general» que facilitan información consolidada sobre estos derechos, los procedimientos aplicables para presentar una solicitud y las posibles vías de recurso⁽¹⁴⁴⁾. Los órganos administrativos, por su parte, están obligados a facilitar «la información que contribuya a especificar la información personal conservada»⁽¹⁴⁵⁾ y a adoptar «otras medidas adecuadas teniendo en cuenta la conveniencia de la persona que tiene la intención de presentar la solicitud» (artículo 47, apartado 1, de la LPIPHAO).
- (169) Como ocurre en el caso de las investigaciones en el ámbito del control del cumplimiento del Derecho penal, los particulares también pueden obtener reparación a título individual en el ámbito de la seguridad nacional poniéndose directamente en contacto con la CPIP. Así se pone en marcha el procedimiento específico de resolución de litigios creado por el Gobierno japonés para los ciudadanos de la Unión cuyos datos personales se transfieren en virtud de la presente Decisión (véanse las explicaciones detalladas en los considerandos 141 a 144 y en el considerando 149).
- (170) Además, los particulares pueden interponer un recurso en forma de acción de daños en virtud de la Ley de reparaciones a cargo del Estado, que cubre también los daños morales y, en ciertas condiciones, la supresión de los datos recogidos (véase el considerando 147).

4. CONCLUSIÓN: NIVEL DE PROTECCIÓN ADECUADO DE LOS DATOS PERSONALES TRANSFERIDOS DESDE LA UNIÓN EUROPEA A LOS OPERADORES ECONÓMICOS EN JAPÓN

- (171) La Comisión considera que la LPIP, complementada por las Reglas complementarias recogidas en el anexo I, junto con las declaraciones, las garantías y los compromisos oficiales que figuran en el anexo II, garantiza un nivel de protección de los datos personales transferidos desde la Unión Europea sustancialmente equivalente al que garantiza el Reglamento (UE) 2016/679.
- (172) Por otra parte, la Comisión estima que, en su conjunto, los mecanismos de supervisión y las vías de reparación previstos en el Derecho japonés permiten identificar y sancionar en la práctica las infracciones cometidas por los OEMIP destinatarios y ofrecen al interesado remedios legales para obtener acceso a los datos personales que le conciernen y, en su caso, su rectificación o supresión.

⁽¹⁴¹⁾ Ley de revisión de las reclamaciones administrativas (Ley n.º 160 de 2014), en particular su artículo 1, apartado 1.

⁽¹⁴²⁾ Véase el artículo 9 de la Ley por la que se crea el consejo de revisión en materia de protección de la información personal y de la comunicación de información (Ley n.º 60 de 2003).

⁽¹⁴³⁾ Según la información recibida, en los trece años transcurridos desde 2005 (año en que entró en vigor la LPIPHAO), el órgano administrativo no ha seguido el informe en solo dos casos de más de 2000, aunque las decisiones administrativas han sido contradichas por el consejo de revisión en varias ocasiones. Por otra parte, cuando el órgano administrativo adopta una decisión que se aparta de las conclusiones del informe, debe indicar claramente los motivos. Véase el anexo II, sección III.C, con referencia al artículo 50, apartado 1, inciso iv), de la Ley de revisión de las reclamaciones administrativas.

⁽¹⁴⁴⁾ Los centros de información integrada —uno en cada prefectura— ofrecen a los ciudadanos explicaciones sobre la información personal recogida por las autoridades públicas (por ejemplo, bases de datos existentes) y las normas de protección de datos aplicables (LPIPHAO), incluido el modo de ejercer los derechos de comunicación, rectificación o suspensión de uso. Al mismo tiempo, los centros trabajan como punto de contacto para las preguntas o reclamaciones presentadas por los ciudadanos. Véase el anexo II, sección II.C.4, letra a).

⁽¹⁴⁵⁾ Véanse asimismo los artículos 10 y 11 de la LPIPAHO relativos al «registro de los expedientes de información personal», que contienen sin embargo amplias excepciones cuando se trata de «expedientes de información personal» preparados u obtenidos a efectos de investigaciones criminales o que contienen elementos relativos a la seguridad y otros intereses esenciales del Estado [véase el artículo 10, apartado 2, incisos i) y ii), de la LPIPHAO].

- (173) Por último, sobre la base de la información disponible acerca del ordenamiento jurídico de Japón, incluidas las declaraciones, garantías y compromisos del Gobierno japonés que figuran en el anexo II, la Comisión considera que toda vulneración de los derechos fundamentales de los particulares cuyos datos personales sean transferidos desde la Unión Europea a Japón por las autoridades públicas japonesas por motivos de interés público, en particular a efectos de control del cumplimiento del Derecho penal y de seguridad nacional, se limitará a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido, y que existe una tutela judicial efectiva contra tales vulneraciones.
- (174) Por consiguiente, a la luz de las constataciones contenidas en la presente Decisión, la Comisión considera que Japón garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a OEMIP en Japón que estén sujetos a la LPIP, excepto en los casos en que el destinatario pertenezca a una de las categorías enumeradas en el artículo 76, apartado 1, de la LPIP y que las finalidades del tratamiento corresponden en todo o en parte a uno de las finalidades definidas en esa disposición.
- (175) Habida cuenta de todo lo hasta aquí expuesto, la Comisión concluye que se cumple la norma en materia de adecuación prevista en el artículo 45 del Reglamento (UE) 2016/679, interpretada a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, en particular en la sentencia Schrems ⁽¹⁴⁶⁾.

5. ACTUACIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS E INFORMACIÓN DESTINADA A LA COMISIÓN

- (176) De conformidad con la jurisprudencia del Tribunal de Justicia ⁽¹⁴⁷⁾, y tal y como se reconoce en el artículo 45, apartado 4, del Reglamento (UE) 2016/679, la Comisión debe supervisar de manera continuada los acontecimientos en el tercer país después de la adopción de una decisión de adecuación, para evaluar si Japón todavía garantiza un nivel de protección equivalente en lo esencial. Debe procederse obligatoriamente a tal control, en cualquier caso, cuando la Comisión sea informada de algún indicio que genere una duda razonable al respecto.
- (177) Por consiguiente, la Comisión debe supervisar de manera continuada la situación en lo que respecta al marco jurídico y la práctica real del tratamiento de los datos personales tal y como se evalúan en la presente Decisión, en particular el cumplimiento por las autoridades japonesas de las declaraciones, garantías y compromisos recogidos en el anexo II. Para facilitar este proceso, se espera de las autoridades japonesas que informen a la Comisión de toda novedad pertinente para la presente Decisión, tanto en lo que respecta al tratamiento de datos personales por parte de los operadores económicos como a las limitaciones y salvaguardas aplicables al acceso de las autoridades públicas a los datos personales. Esto debería incluir todas las decisiones adoptadas por la CPIP en virtud del artículo 24 de la LPIP por las que se reconozca que un tercer país ofrece un nivel de protección equivalente al garantizado en Japón.
- (178) Además, a fin de que la Comisión pueda desempeñar eficazmente su función de seguimiento, los Estados miembros deben informarle de cualquier medida relevante adoptada por las autoridades de protección de datos («APD») nacionales, en particular en lo que respecta a las consultas o las reclamaciones de los interesados de la UE en relación con la transferencia de datos personales desde la Unión Europea a los operadores económicos en Japón. La Comisión también debe ser informada de todo indicio de que las acciones de las autoridades públicas japonesas responsables de la prevención, la investigación, la detección o la persecución de infracciones penales, o de la seguridad nacional, incluidos los órganos de supervisión, no garantizan el nivel de protección necesario.
- (179) Los Estados miembros y sus órganos están obligados a adoptar las medidas necesarias para dar cumplimiento a los actos de las instituciones de la Unión, ya que estos disfrutan de una presunción de legalidad, y producen por consiguiente efectos jurídicos en tanto no hayan sido revocados, anulados en el marco de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad. Por lo tanto, toda decisión de adecuación adoptada por la Comisión en virtud del artículo 45, apartado 3, del Reglamento (UE) 2016/679 vincula a todos los órganos de los Estados miembros destinatarios, incluidas las autoridades de control independientes. Al mismo tiempo, tal como explica el Tribunal de Justicia en la sentencia Schrems ⁽¹⁴⁸⁾ y se reconoce en el artículo 58, apartado 5, del Reglamento, en el supuesto de que una APD cuestione, incluso a raíz de una reclamación, la compatibilidad de una decisión de adecuación adoptada por la Comisión con los derechos fundamentales del particular a la vida privada y a la protección de datos, el Derecho nacional debe ofrecer a dicha autoridad una vía de recurso que le permita exponer tales objeciones ante los órganos jurisdiccionales, los cuales, en caso de duda, están obligados a suspender el procedimiento y plantear una cuestión prejudicial al Tribunal de Justicia ⁽¹⁴⁹⁾.

⁽¹⁴⁶⁾ Véase más arriba la nota 3.

⁽¹⁴⁷⁾ Schrems, apartado 76.

⁽¹⁴⁸⁾ Schrems, apartado 65.

⁽¹⁴⁹⁾ Schrems, apartado 65: «A ese efecto, corresponde al legislador nacional prever las vías de recurso que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de esta.».

6. REVISIÓN PERIÓDICA DE LA CONSTATACIÓN DE ADECUACIÓN

- (180) En aplicación del artículo 45, apartado 3, del Reglamento (UE) 2016/679 ⁽¹⁵⁰⁾, y teniendo en cuenta el hecho de que el nivel de protección que ofrece el ordenamiento jurídico japonés puede ser objeto de modificación, la Comisión, tras la adopción de la presente Decisión, debe comprobar periódicamente si las constataciones relativas a la adecuación del nivel de protección garantizado por Japón siguen estando justificadas desde el punto de vista factual y legal.
- (181) A tal fin, la presente Decisión debe someterse a una primera revisión en un plazo de dos años después de su entrada en vigor. Tras la primera revisión y en función de sus resultados, la Comisión decidirá, en estrecha consulta con el comité establecido en virtud del artículo 93, apartado 1, de RGPD, si debe mantenerse el ciclo de dos años. En cualquier caso, las revisiones posteriores deben realizarse al menos cada cuatro años ⁽¹⁵¹⁾. La revisión debe comprender todos los aspectos relativos al funcionamiento de la presente Decisión, y en particular la aplicación de las Reglas complementarias (prestando especial atención a las protecciones ofrecidas en caso de transferencias ulteriores), la aplicación de las normas sobre consentimiento, en particular en caso de retirada, la eficacia del ejercicio de los derechos individuales, así como las limitaciones y salvaguardas con respecto al acceso de las autoridades públicas, incluido el mecanismo de reparación que se establece en el anexo II de la presente Decisión. También debe comprender la eficacia de la supervisión y la ejecución forzosa, con respecto a las normas aplicables tanto a los OEMIP como en el ámbito de la ejecución forzosa del Derecho penal y de la seguridad nacional.
- (182) Al proceder a la revisión, la Comisión debe reunirse con la CPIP, acompañada, en su caso, de otras autoridades japonesas responsables del acceso de las autoridades públicas, incluidos los correspondientes órganos de supervisión. La participación en esta reunión debe estar abierta a los representantes de los miembros del Comité Europeo de Protección de Datos (SEPD). En el marco de la revisión conjunta, la Comisión debe solicitar a la CPIP que facilite información completa sobre todos los aspectos pertinentes a efectos de la constatación de adecuación, en particular sobre las limitaciones y salvaguardas relativas al acceso por parte de las autoridades públicas ⁽¹⁵²⁾. La Comisión también debe pedir explicaciones sobre cualquier información pertinente para la presente Decisión que haya recibido, incluidos los informes públicos elaborados por las autoridades japonesas u otras partes interesadas en Japón, el SEPD, las distintas APD, los grupos de la sociedad civil, los informes de los medios de comunicación o cualquier otra fuente de información disponible.
- (183) Sobre la base de la revisión conjunta, la Comisión debe elaborar un informe público que presentará al Parlamento Europeo y al Consejo.

7. SUSPENSIÓN DE LA DECISIÓN DE ADECUACIÓN

- (184) Cuando, sobre la base de las comprobaciones periódicas y *ad hoc* o de cualquier otra información disponible, la Comisión llegue a la conclusión de que el nivel de protección que ofrece el ordenamiento jurídico de Japón ya no puede considerarse equivalente en lo esencial al de la Unión Europea, debe informar de ello a las autoridades japonesas competentes y pedir que se tomen las medidas pertinentes dentro de un plazo determinado razonable. Se incluyen aquí las normas aplicables tanto a los operadores económicos como a las autoridades públicas japonesas responsables de la ejecución forzosa del Derecho penal o de la seguridad nacional. Por ejemplo, se activaría un procedimiento de este tipo en los casos en que dejaran de realizarse transferencias ulteriores, en particular sobre la base de decisiones adoptadas por la CPIP en virtud del artículo 24 de la LPIP por las que se reconozca que un tercer país ofrece un nivel de protección equivalente al garantizado en Japón, en virtud de las salvaguardas para asegurar la continuidad de la protección a tenor del artículo 44 del RGPD.
- (185) Si, transcurrido el plazo especificado, las autoridades japonesas competentes no logran demostrar satisfactoriamente que la presente Decisión sigue basándose en un nivel de protección adecuado, la Comisión debe, en aplicación del artículo 45, apartado 5, del Reglamento (UE) 2016/679, iniciar el procedimiento conducente a la suspensión parcial o total o a la derogación de la presente Decisión. Alternativamente, la Comisión debe iniciar el procedimiento tendente a la modificación de la presente Decisión, en particular sometiendo las transferencias de datos a condiciones adicionales o limitando el alcance de la constatación de adecuación únicamente a las transferencias de datos para los cuales esté asegurada la continuidad de la protección a tenor del artículo 44 del RGPD.

⁽¹⁵⁰⁾ De conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, «[e]l acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional».

⁽¹⁵¹⁾ El artículo 45, apartado 3, del Reglamento (UE) 2016/679 establece que debe procederse a una revisión periódica al menos cada cuatro años. Véase también CEPD, *Adequacy Referential*, WP 254 rev. 01.

⁽¹⁵²⁾ Véase también el anexo II, sección IV: «En el marco de la revisión periódica de la decisión de adecuación, la CPIP y la Comisión Europea intercambiarán información sobre el tratamiento de los datos con arreglo a las condiciones de la constatación de adecuación, incluidas las establecidas en la presente Declaración.».

- (186) En particular, la Comisión debe iniciar el procedimiento de suspensión o derogación en caso de que existan indicios de que las Reglas complementarias que figuran en el anexo I no son cumplidas por los operadores económicos que reciban datos personales en el marco de la presente Decisión y/o no son ejecutadas efectivamente, o de que las autoridades japonesas no cumplan las declaraciones, garantías y compromisos recogidos en el anexo II de la presente Decisión.
- (187) La Comisión ha de considerar asimismo la posibilidad de iniciar el procedimiento conducente a la modificación, suspensión o derogación de la presente Decisión si, en el contexto de la revisión conjunta o de otra forma, las autoridades japonesas competentes no facilitan la información o las aclaraciones necesarias para la evaluación del nivel de protección de los datos personales transferidos desde la Unión Europea a Japón o el cumplimiento de la presente Decisión. A este respecto, la Comisión debe tener en cuenta en qué medida puede obtenerse la información pertinente de otras fuentes.
- (188) Por razones de urgencia debidamente justificadas, tales como el riesgo de vulneración grave de los derechos de los interesados, la Comisión debe considerar adoptar una decisión para suspender o derogar la presente Decisión, que debe aplicarse de forma inmediata, con arreglo al artículo 93, apartado 3, del Reglamento (UE) 2016/679, leído en relación con el artículo 8 del Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ⁽¹⁵³⁾.

8. CONSIDERACIONES FINALES

- (189) El Comité Europeo de Protección de Datos publicó su dictamen ⁽¹⁵⁴⁾, que se ha tomado en consideración en la elaboración de la presente Decisión.
- (190) El Parlamento Europeo ha adoptado una Resolución sobre una estrategia de comercio digital que insta a la Comisión a priorizar y acelerar la adopción de decisiones de adecuación con socios comerciales importantes con arreglo a las condiciones establecidas en el Reglamento (UE) 2016/679 como un importante mecanismo de salvaguarda de la transferencia de datos personales desde la Unión Europea ⁽¹⁵⁵⁾. El Parlamento Europeo ha adoptado asimismo una resolución sobre la adecuación de la protección de los datos personales conferida por Japón ⁽¹⁵⁶⁾.
- (191) Las medidas previstas en la presente Decisión se ajustan al dictamen del comité establecido en virtud del artículo 93, apartado 1, del RGPD.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

1. A efectos de la aplicación del artículo 45 del Reglamento (UE) 2016/679, Japón garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a operadores económicos que manejen información personal en Japón sujeta a la Ley sobre la protección de la información personal, complementada por las Reglas complementarias que figuran en el anexo I, junto con las declaraciones, garantías y compromisos oficiales recogidos en el anexo II.

⁽¹⁵³⁾ Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

⁽¹⁵⁴⁾ Dictamen 28/2018 sobre el proyecto de Decisión de Ejecución de la Comisión Europea relativa a la adecuación de la protección de los datos personales por parte de Japón, adoptado el 5 de diciembre de 2018.

⁽¹⁵⁵⁾ Resolución del Parlamento Europeo, de 12 de diciembre de 2017, «Hacia una estrategia de comercio digital» [2017/2065 (INI)]. Véase en particular el punto 8 («[...] recuerda asimismo que los datos personales pueden ser transferidos a terceros países sin recurrir a las disciplinas generales de los acuerdos de comercio cuando se cumplan los requisitos, tanto en la actualidad como en el futuro — consagrados en [...] el capítulo V del Reglamento (UE) 2016/679; reconoce que las decisiones de adecuación, incluidas las parciales y las sectoriales, constituyen un mecanismo fundamental en materia de salvaguarda de la transferencia de datos personales desde la Unión a un tercer país; señala que la Unión solo ha adoptado decisiones de adecuación con cuatro de sus veinte socios comerciales principales [...]») y el punto 9 («Pide a la Comisión que priorice y acelere la adopción de decisiones de adecuación, siempre y cuando los terceros países garanticen, mediante su legislación nacional o sus compromisos internacionales, un nivel de protección “equivalente en lo esencial” al garantizado en la Unión [...]»).

⁽¹⁵⁶⁾ Resolución del Parlamento Europeo, de 13 de diciembre de 2018, sobre la adecuación de la protección de los datos personales conferida por Japón [2018/2979 (RSP)]

2. La presente Decisión no concierne a los datos personales transferidos a los destinatarios que entren dentro de una de las categorías siguientes, en la medida en que la finalidad del tratamiento de los datos personales corresponda, en todo o en parte, a una de las finalidades enumeradas, a saber:

- a) los organismos de radiodifusión, los editores de periódicos, las agencias de comunicación u otras organizaciones de prensa (incluidos los particulares que ejercen actividades de prensa), en la medida en que traten datos personales para la prensa;
- b) los escritores profesionales, en la medida en que manejen datos personales;
- c) las universidades y otras organizaciones o grupos relacionados con los estudios académicos, o cualquier persona adscrita a una organización de este tipo, en la medida en que traten datos personales con fines académicos;
- d) las instituciones religiosas en la medida en que traten datos personales con fines religiosos (incluidas todas las actividades afines), y
- e) los organismos políticos en la medida en que traten datos personales con fines políticos (incluidas todas las actividades afines).

Artículo 2

Cuando las autoridades competentes de los Estados miembros, a fin de proteger a los particulares en lo que respecta al tratamiento de sus datos personales, ejerzan sus poderes en virtud del artículo 58 del Reglamento (UE) 2016/679 y ello conduzca a la suspensión o la prohibición definitiva de los flujos de datos hacia un operador económico concreto de Japón en el ámbito de aplicación establecido en el artículo 1, el Estado miembro en cuestión informará sin demora a la Comisión.

Artículo 3

1. La Comisión procederá a un seguimiento continuo de la aplicación del marco jurídico en que se basa la presente Decisión, incluidas las condiciones en que se realizan las transferencias ulteriores, al objeto de evaluar si Japón sigue garantizando un nivel adecuado de protección en el sentido de lo dispuesto en el artículo 1.

2. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que la Comisión de Protección de la Información Personal, o cualquier otra autoridad competente japonesa, no garantice el cumplimiento del marco jurídico en el que se sustenta la presente Decisión.

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

4. En el plazo de dos años a partir de la fecha de notificación de la presente Decisión a los Estados miembros y posteriormente al menos cada cuatro años, la Comisión evaluará la constatación formulada en el artículo 1, apartado 1, sobre la base de toda la información disponible, incluida la información recibida como parte de la revisión conjunta realizada junto con las autoridades japonesas pertinentes.

5. En caso de que la Comisión tenga indicios de que ya no está garantizado un nivel adecuado de protección, la Comisión informará de ello a las autoridades japonesas competentes. Si es necesario, podrá decidir suspender, modificar o derogar la presente Decisión, o limitar su ámbito de aplicación, en particular si existen indicios de que:

- a) los operadores económicos en Japón que hayan recibido datos personales de la Unión Europea en virtud de la presente Decisión no cumplen las salvaguardas adicionales recogidas en las Reglas complementarias que figuran en el anexo I de la presente Decisión, o de que son insuficientes la supervisión y el control del cumplimiento de la legislación en este sentido;
- b) las autoridades públicas japonesas no cumplen las declaraciones, garantías y compromisos recogidos en el anexo II de la presente Decisión, en particular en lo que respecta a las condiciones y limitaciones para la recogida y el acceso a los datos personales transferidos en virtud de la presente Decisión por las autoridades públicas japonesas a efectos de control del cumplimiento del Derecho penal o de seguridad nacional.

La Comisión podrá asimismo presentar dichos proyectos de medidas cuando la falta de cooperación del Gobierno japonés le impida determinar si se ha producido algún cambio que afecte a la constatación formulada en el artículo 1, apartado 1, de la presente Decisión.

Artículo 4

Los destinatarios de la presente Decisión son los Estados miembros.

Hecho en Bruselas, el 23 de enero de 2019.

Por la Comisión
Věra JOUROVÁ
Miembro de la Comisión

ANEXO I

REGLAS COMPLEMENTARIAS EN VIRTUD DE LA LEY SOBRE LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL RELATIVAS AL MANEJO DE LOS DATOS PERSONALES TRANSFERIDOS DESDE LA UE SOBRE LA BASE DE UNA DECISIÓN DE ADECUACIÓN

Índice

1) Información personal que requiere especial atención (artículo 2, apartado 3, de la Ley)	38
2) Datos personales conservados (artículo 2, apartado 7, de la Ley)	39
3) Especificación de una finalidad de utilización, restricción debida a una finalidad de utilización (artículo 15, apartado 1, artículo 16, apartado 1, y artículo 26, apartados 1 y 3, de la Ley).	40
4) Restricción de la puesta a disposición de un tercero en un país extranjero (artículo 24 de la Ley; Artículo 11-2 de las Reglas)	41
5) Reparación individual frente a investigaciones ilegales o inadecuadas de las autoridades públicas: reclamación a la CPIP	41

[Términos]

«Ley»	Ley sobre la protección de la información personal (Ley n.º 57, 2003)
«Orden del Gabinete»	Orden del Gabinete para asegurar el cumplimiento de la Ley sobre la protección de la información personal (Orden del Gabinete n.º 507, 2003)
«Reglas»	Reglas de ejecución la Ley sobre la protección de la información personal (Reglas de la Comisión de Protección de la Información Personal n.º 3, 2016)
«Directrices sobre las Reglas generales»	Directrices relativas a la Ley sobre la protección de la información personal (volumen sobre las reglas generales) (Nota de la Comisión de Protección de la Información Personal n.º 65, 2015)
«UE»	Unión Europea, incluidos sus Estados miembros, y, a la luz del Acuerdo EEE, Islandia, Liechtenstein y Noruega
«RGPD»	Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
«Decisión de adecuación»	Decisión de la Comisión Europea por la que se reconoce que un tercer país o un territorio situado en ese tercer país, etc., garantiza un nivel adecuado de protección de los datos personales de conformidad con el artículo 45 del RGPD

La Comisión de Protección de la Información Personal, a efectos de la transferencia mutua y fluida de datos personales entre Japón y la UE, designó a la UE como país extranjero que aplica un sistema de protección de la información personal que incluye normas equivalentes a las de Japón en relación con la protección de los derechos e intereses de los particulares con arreglo al artículo 24 de la Ley, y la Comisión Europea decidió al mismo tiempo que Japón garantiza un nivel adecuado de protección de los datos personales de conformidad con el artículo 45 del RGPD.

Queda así asegurada una transferencia mutua y fluida de datos personales entre Japón y la UE, de tal manera que se garantice un elevado nivel de protección de los derechos e intereses de los particulares. Con el fin de garantizar ese elevado nivel de protección en relación con la información personal recibida de la UE sobre la base de una decisión de adecuación y teniendo en cuenta el hecho de que, pese al alto grado de convergencia entre los dos sistemas, existen algunas diferencias importantes, la Comisión de Protección de la Información Personal ha adoptado las presentes Reglas complementarias, basadas en las disposiciones de la Ley relativas a la aplicación, etc., de la cooperación con los Gobiernos de otros países y con el fin de garantizar un manejo apropiado de la información personal recibida de la UE sobre la base de una decisión de adecuación por un operador económico que maneja información personal y una aplicación adecuada y efectiva de las obligaciones establecidas en dichas reglas ⁽¹⁾.

⁽¹⁾ Artículos 4, 6, 8, 24, 60 y 78 de la Ley y artículo 11 de las Reglas.

En particular, el artículo 6 de la Ley prevé la facultad de adoptar las medidas legislativas y de otro tipo necesarias para garantizar una mayor protección de la información personal y construir un sistema homologable internacionalmente en materia de información personal dotado con normas más estrictas que completen y vayan más allá de las establecidas en la Ley y en la Orden del Gabinete. Por consiguiente, la Comisión de Protección de la Información Personal, como autoridad encargada de la gestión general de la Ley, está facultada para establecer, de conformidad con el artículo 6 de la Ley, una regulación más estricta, mediante la formulación de las presentes Reglas complementarias, que ofrecen un nivel más elevado de protección de los derechos e intereses de los particulares en relación con el manejo de los datos personales recibidos de la UE sobre la base de una decisión de adecuación, en particular en lo que se refiere a la definición de la información personal que requiere especial atención, con arreglo al artículo 2, apartado 3, de la Ley, y a los datos personales conservados, de conformidad con el artículo 2, apartado 7, de la Ley (incluido el período de conservación pertinente).

Partiendo de esta base, las Reglas complementarias son vinculantes para los operadores económicos que manejan información personal que reciban datos personales transferidos desde la UE sobre la base de una decisión de adecuación y que están, por tanto, obligados a cumplirlas. Como normas jurídicamente vinculantes, los derechos y obligaciones son ejecutables por la Comisión de Protección de la Información Personal de la misma manera que las disposiciones de la Ley a la que complementan con normas más estrictas o detalladas. En caso de vulneración de los derechos y obligaciones derivados de las Reglas complementarias, los particulares también pueden obtener reparación de los tribunales, de la misma manera que con respecto a las disposiciones de la Ley a la que dichas Reglas complementan con normas más estrictas o detalladas.

Por lo que se refiere a la ejecución por parte de la Comisión de Protección de la Información Personal, en caso de que un operador económico que maneja información personal no cumpla una o varias de las obligaciones en virtud de las Reglas complementarias, dicha Comisión está facultada para adoptar medidas de conformidad con el artículo 42 de la Ley. En lo que respecta, en general, a la información personal recibida de la UE sobre la base de una decisión de adecuación, el hecho de que un operador económico que maneja información personal no adopte medidas acordes con una recomendación recibida de conformidad con el artículo 42, apartado 1, de la Ley, sin motivo legítimo⁽²⁾ (*2), se considera una vulneración grave de carácter inminente de los derechos e intereses de un particular a tenor del artículo 42, apartado 2, de la Ley.

1) Información personal que requiere especial atención (artículo 2, apartado 3, de la Ley)

Artículo 2, apartado 3, de la Ley

3) A efectos de la presente Ley se entenderá por «información personal que requiere especial atención» la información personal que revele la raza, el credo, el estatus social, el historial médico, los antecedentes penales, el hecho de haber sufrido daños resultantes de un delito, u otras descripciones, etc., prescritas por la Orden del Gabinete, por ejemplo aquellas cuyo manejo requiera especial atención a fin de evitar que el interesado principal sufra discriminación injusta, prejuicio o cualquier otro daño.

Artículo 2 de la Orden del Gabinete

Dichas descripciones, etc., prescritas por la Orden del Gabinete en virtud del artículo 2, apartado 3, de la Ley serán aquellas que contengan alguno de los elementos que se indican a continuación (excluidas las que figuran en el historial médico o los antecedentes penales del interesado principal):

- i) el hecho de sufrir una discapacidad física, intelectual, mental (incluidas las discapacidades de desarrollo) u otras discapacidades funcionales físicas o mentales contempladas en las Reglas de la Comisión de Protección de la Información Personal;
- ii) los resultados de un reconocimiento médico u otro tipo de examen (en lo sucesivo, «reconocimiento médico, etc.») para la prevención y detección precoz de una enfermedad realizado a un interesado principal por un médico u otra persona que desempeñe funciones relacionadas con la medicina (en lo sucesivo, «médico, etc.»);
- iii) el hecho de que un médico, etc., haya dado orientaciones para la mejora de las condiciones físicas y mentales, o prestado atención médica o prescripción, sobre la base de los resultados de un reconocimiento médico, etc., o por enfermedad, lesiones u otras alteraciones mentales y físicas;
- iv) el hecho de que se haya procedido a una detención, registro, incautación, retención, persecución u otros procedimientos relacionados con un proceso penal contra un interesado principal como sospechoso o demandado;

⁽²⁾ Se entenderá por «motivo legítimo» cualquier hecho de carácter excepcional que escape al control del operador económico que maneja información personal y que no pueda preverse razonablemente (por ejemplo, catástrofes naturales) o los casos en que haya desaparecido la necesidad de adoptar medidas en relación con una recomendación de la Comisión de Protección de la Información Personal, de conformidad con el artículo 42, apartado 1, de la Ley, porque el operador económico que maneja información personal haya adoptado medidas alternativas que remedien plenamente la violación.

- v) el hecho de que se haya llevado a cabo una investigación, medida de observación y protección, audiencia y decisión, medida de protección u otros procedimientos relacionados con un caso de protección de menores contra un interesado principal como delincuente juvenil o sospechoso de ello con arreglo al artículo 3, apartado 1, de la Ley de la juventud.

Artículo 5 de las Reglas

Las discapacidades físicas y mentales funcionales previstas en las Reglas de la Comisión de Protección de la Información Personal de conformidad con el artículo 2, inciso i), de la Orden, serán las siguientes:

- i) discapacidades físicas establecidas en un cuadro adjunto de la Ley n.º 283 de 1949 sobre el bienestar de las personas con discapacidades físicas;
- ii) discapacidades intelectuales contempladas en la Ley n.º 37 de 1960 sobre el bienestar de las personas con discapacidades intelectuales;
- iii) discapacidades mentales contempladas en la Ley n.º 123 de 1950 sobre la salud mental y el bienestar de las personas con discapacidades mentales (incluidas las discapacidades para el desarrollo previstas en el artículo 2, apartado 1, de la Ley sobre el apoyo a las personas con discapacidades de desarrollo, y excluidas las discapacidades intelectuales que entran dentro del ámbito de aplicación de la Ley sobre el bienestar de las personas con discapacidades intelectuales);
- iv) una enfermedad para la que no existan métodos de cura establecidos u otras enfermedades raras cuya gravedad, establecida por los profesionales indicados en el artículo 4, apartado 1, de la Ley n.º 123 de 2005 sobre el apoyo global a la vida diaria y social de las personas con discapacidad, sea equivalente a la establecida por el Ministerio de Salud, Trabajo y Bienestar de conformidad con dicho apartado.

Si los datos personales recibidos de la UE sobre la base de una decisión de adecuación contienen datos relativos a la vida sexual o la orientación sexual de una persona física o a la afiliación a un sindicato, que se definen como categorías especiales de datos personales en virtud del RGPD, los operadores económicos que manejan información personal deben manejar dichos datos personales de la misma forma que la información personal que requiere especial atención a tenor del artículo 2, apartado 3, de la Ley.

2) Datos personales conservados (artículo 2, apartado 7, de la Ley)

Artículo 2, apartado 7, de la Ley

- 7) A efectos de la presente Ley se entenderá por «datos personales conservados» los datos personales que un operador económico que maneja información personal está facultado para comunicar, rectificar, añadir contenido o eliminarlo, poner fin a su utilización, suprimir y poner fin a su puesta a disposición de terceros, que no sean ni los previstos por la Orden del Gabinete como susceptibles de perjudicar al interés público o a otros intereses si se llegara a conocer su presencia o su ausencia, ni los establecidos para ser suprimidos en un plazo no superior a un año establecido por la Orden del Gabinete.

Artículo 4 de la Orden del Gabinete

Los datos establecidos por la Orden del Gabinete en virtud del artículo 2, apartado 7, serán los siguientes:

- i) los datos personales que, si se llegara a conocer su presencia o su ausencia, podrían ser perjudiciales para la vida, la integridad física o el patrimonio de un interesado principal o de un tercero;
- ii) los datos personales que, si se llegara a conocer su presencia o su ausencia, podrían alentar o inducir a la comisión de un acto ilícito o injusto;
- iii) los datos personales que, si se llegara a conocer su presencia o su ausencia, podrían poner en peligro la seguridad nacional, destruir una relación de confianza con un país extranjero o una organización internacional, o crear una situación de desventaja en las negociaciones con un país extranjero o una organización internacional;
- iv) los datos personales que, si se llegara a conocer su presencia o su ausencia, podrían entorpecer el mantenimiento del orden público y de la seguridad pública, por ejemplo en lo que respecta a la prevención, represión o investigación de un delito.»

Artículo 5 de la Orden del Gabinete

«El plazo establecido por la Orden del Gabinete en virtud del artículo 2, apartado 7, de la Ley será de seis meses.»

Los datos personales transferidos desde la Unión Europea sobre la base de una decisión de adecuación deben ser manejados como datos personales conservados a tenor o del artículo 2, apartado 7, de la Ley, con independencia del plazo previsto para su supresión.

Si los datos personales transferidos desde la Unión Europea sobre la base de una decisión de adecuación corresponden a los datos personales establecidos por la Orden del Gabinete como «susceptibles de perjudicar al interés público o a otros intereses en caso de que llegara a conocerse su presencia o ausencia», no será necesario manejar tales datos como datos personales conservados (véase el artículo 4 de la Orden del Gabinete; Directrices de las Reglas Generales «2-7. Datos personales conservados»).

- 3) Especificación de una finalidad de utilización, restricción debida a una finalidad de utilización (artículo 15, apartado 1, artículo 16, apartado 1, y artículo 26, apartados 1 y 3, de la Ley).

Artículo 15, apartado 1, de la Ley

- 1) Un operador económico que maneja información personal deberá especificar la finalidad de la utilización de la información personal (en lo sucesivo, la «finalidad de utilización») de la forma más explícita posible.

Artículo 16, apartado 1, de la Ley

- 1) Un operador económico que maneja información personal deberá obtener previamente el consentimiento del interesado principal para manejar información más allá de lo que sea necesario para conseguir una finalidad de utilización especificada de conformidad con lo dispuesto en el artículo anterior.

Artículo 26, apartados 1 y 3, de la Ley

- 1) Un operador económico que maneja información personal deberá confirmar, al recibir datos personales de un tercero, las cuestiones que se exponen a continuación con arreglo a las Reglas de la Comisión de Protección de la Información Personal. (omitido)

i) (omitido);

ii) las circunstancias en que dichos datos personales hayan sido adquiridos por el tercero.

- 3) Cuando haya realizado la confirmación prevista en el apartado 1, el operador económico que maneja información personal llevará un registro, con arreglo a las Reglas de la Comisión de Protección de la Información Personal, de la fecha en que se pusieron a su disposición datos personales, de los detalles de dicha confirmación, así como de otros detalles indicados en las Reglas de la Comisión de Protección de la Información Personal.

Si los operadores económicos que manejan información personal lo hacen más allá de lo que es necesario para conseguir una finalidad de utilización especificada en virtud del artículo 15, apartado 1, de la Ley, deberán obtener previamente el consentimiento del interesado principal (artículo 16, apartado 1, de la Ley). Al recibir datos personales de un tercero, los operadores económicos que manejan información personal, deberán, de conformidad con las Reglas, confirmar extremos tales como las circunstancias en las que dicho tercero ha adquirido dichos datos personales, y registrarán estos extremos (artículo 26, apartados 1 y 3, de la Ley).

En caso de que un operador económico que maneja información personal reciba datos personales desde la UE sobre la base de una decisión de adecuación, las circunstancias relativas a la adquisición de dichos datos personales, que se confirmarán y registrarán conforme a lo dispuesto en el artículo 26, apartados 1 y 3, incluirán la finalidad de utilización para la que fueron recibidos desde la UE.

Del mismo modo, en el caso de que un operador económico que maneja información personal reciba de otro operador económico que maneja información personal datos personales transferidos previamente desde la UE sobre la base de una decisión de adecuación, las circunstancias relativas a la adquisición de dichos datos personales, que se confirmarán y registrarán conforme a lo dispuesto en el artículo 26, apartados 1 y 3, incluirán la finalidad para la que fueron recibidos.

En los casos antes mencionados, el operador económico que maneja información personal deberá especificar la finalidad de la utilización de dichos datos personales con arreglo a la finalidad de utilización para la que fueron recibidos inicialmente o posteriormente los datos, tal como hayan sido confirmada y registrada con arreglo al artículo 26, apartados 1 y 3, y deberá utilizar dichos datos con arreglo a esa finalidad (según lo dispuesto en el artículo 15, apartado 1, y en el artículo 16, apartado 1, de la Ley).

4) Restricción de la puesta a disposición de un tercero en un país extranjero (artículo 24 de la Ley; Artículo 11-2 de las Reglas)

Artículo 24 de la Ley

Un operador económico que maneja información personal, salvo en los casos previstos en cada uno de los incisos del artículo anterior, apartado 1, en caso de que facilite datos personales a un tercero (con exclusión de una persona que aplique un sistema conforme a las normas establecidas por las Reglas de la Comisión de Protección de la Información Personal necesario para tomar de forma continuada medidas equivalentes a las que un operador económico que maneja información personal deberá adoptar en relación con el manejo de datos personales con arreglo a lo dispuesto en la presente sección; en lo sucesivo, lo mismo dispuesto en el presente artículo) en un país extranjero (es decir, un país o región situados fuera del territorio de Japón; en lo sucesivo, lo mismo) (excepto los previstos por las Reglas de la Comisión de Protección de la Información Personal como países extranjeros que aplican un sistema de protección de la información personal que se haya reconocido cuenta con normas equivalentes a las de Japón respecto de la protección de los derechos e intereses de un particular; en lo sucesivo, lo mismo dispuesto en el presente artículo), deberá obtener previamente el consentimiento del interesado principal en el sentido de que aprueba la puesta a disposición de un tercero en un país extranjero. En tal caso, no se aplicará lo dispuesto en el artículo anterior.

Artículo 11-2, de las Reglas

Las normas establecidas por las Reglas de la Comisión de Protección de la Información Personal en virtud del artículo 24 de la Ley corresponderán a cada uno de los incisos que figuran a continuación.

- i) un operador económico que maneja información personal y una persona que recibe datos personales han garantizado, en relación con el manejo de datos personales por la persona que recibe los datos, la aplicación de medidas acordes con lo dispuesto en el capítulo IV, sección 1, de la Ley, utilizando un método adecuado y razonable;
- ii) una persona que recibe datos personales ha obtenido un reconocimiento basado en un marco internacional relativo al manejo de información personal.

Un operador económico que maneja información personal, en casos de puesta a disposición de un tercero en un país extranjero de datos personales que haya recibido de la UE sobre la base de una decisión de adecuación, deberá obtener previamente el consentimiento del interesado principal de forma que autorice la puesta a disposición de un tercero en un país extranjero de conformidad con el artículo 24 de la Ley, tras haber recibido información sobre las circunstancias que rodean la transferencia necesaria para que el interesado principal tome una decisión sobre su consentimiento, con exclusión de los casos que correspondan a alguno de los incisos i) a iii) siguientes:

- i) cuando el tercero se halle en un país que según las Reglas es un país extranjero que aplica un sistema de protección de la información personal reconocido como un sistema con estándares equivalentes a los de Japón con respecto a la protección de los derechos e intereses de un particular;
- ii) cuando un operador económico que maneja información personal y un tercero a cuya disposición se ponen los datos personales, en relación con el manejo de datos personales por el tercero, hayan aplicado conjuntamente medidas que ofrezcan un nivel equivalente de protección al de la Ley, leída en relación con las presentes Reglas, utilizando un método adecuado y razonable (es decir, un contrato, otras formas de acuerdos vinculantes o arreglos vinculantes en el seno de un grupo corporativo);
- iii) en los casos previstos en los diferentes incisos del artículo 23, apartado 1, de la Ley.

5) Información tratada de forma anónima (artículo 2, apartado 9, y artículo 36, apartados 1 y 2, de la Ley)

Artículo 2, apartado 9, de la Ley

- 9) A efectos de la presente Ley se entenderá por «información tratada de forma anónima» la información relativa a un particular que pueda ser producida a partir del tratamiento de información personal de manera que resulte imposible identificar a un particular concreto mediante la adopción de las medidas contempladas en cada uno de los incisos siguientes, de conformidad con las categorías de información personales establecidas en cada uno de los incisos siguientes, ni restablecer la información personal.

- i) la información personal contemplada en el apartado 1, inciso i);

Supresión de una parte de las descripciones, etc., que figuran en dicha información personal (incluida la sustitución de dicha parte de las descripciones, etc. por otras descripciones, etc., mediante un método sin regularidad que pueda restablecer dicha parte de las descripciones, etc.);

- ii) la información personal contemplada en el apartado 1, inciso ii);

Supresión de todos los códigos de identificación individuales que figuran en dicha información personal (incluida la sustitución de dichos códigos de identificación individuales por otras descripciones, etc., mediante un método sin regularidad que pueda restablecer dichos códigos de identificación personal).

Artículo 36, apartado 1, de la Ley

- 1) Un operador económico que maneja información personal, cuando produzca información tratada de forma anónima (limitada a la que constituya una base de datos de información tratada de forma anónima, etc.; en lo sucesivo, lo mismo), deberá tratar la información personal con arreglo a las normas prescritas por las Reglas de la Comisión de Protección de la Información Personal como necesarias para hacer imposible la identificación de un particular concreto y el restablecimiento de la información personal utilizada para la producción.

Artículo 19 de las Reglas

Las normas establecidas por las Reglas de la Comisión de Protección de la Información Personal en virtud del artículo 36, apartado 1, de la Ley serán las siguientes:

- i) supresión de la totalidad o parte de las descripciones, etc., que pueden identificar a un particular concreto contenidas en la información personal (incluida la sustitución de dichas descripciones, etc. por otras descripciones, etc., mediante un método sin regularidad que pueda restablecer la totalidad o parte de las descripciones, etc.);
- ii) supresión de todos los códigos de identificación individuales que figuran en la información personal (incluida la sustitución de dichos códigos por otras descripciones, etc., mediante un método sin regularidad que pueda restablecer los códigos de identificación individuales);
- iii) supresión de los códigos (limitada a los códigos que vinculan mutuamente la información plural que esté siendo efectivamente manejada por un operador económico que maneja información personal) que vinculan la información personal y la información obtenida mediante la adopción de medidas contra la información personal (incluida la sustitución de dichos códigos por otros códigos que no puedan vincular la información personal mencionada y la obtenida mediante la adopción de medidas contra dicha información personal mediante un método sin regularidad que pueda restablecer dichos códigos);
- iv) supresión de las descripciones idiosincrásicas, etc. (incluida la sustitución de dichas descripciones, etc., por otras descripciones, etc., mediante un método sin regularidad que pueda restablecer las descripciones idiosincrásicas, etc.);
- v) además de las medidas previstas en cada uno de los incisos anteriores, adopción de las medidas oportunas sobre la base de los resultados del examen del atributo, etc., de la base de datos de información personal, etc., tales como una diferencia entre las descripciones, etc., que figuran en la información personal y las descripciones, etc., incluidas en otra información personal que constituya la base de datos de información personal, etc., que incluyan dicha información personal.

Artículo 36, apartado 2, de la Ley

- 2) Un operador económico que maneja información personal, cuando haya producido información tratada de forma anónima, de conformidad con las normas prescritas por las Reglas de la Comisión de Protección de la Información Personal como necesarias para evitar la fuga de información relativa a dichas descripciones, etc., y los códigos de identificación individuales suprimidos de la información personal utilizada para producir la información tratada de forma anónima, así como la información relativa a un método de tratamiento llevado a cabo de conformidad con lo dispuesto en el apartado anterior, deberá tomar medidas para el control de la seguridad de dicha información.

Artículo 20 de las Reglas

Las normas prescritas por las Reglas de la Comisión de Protección de la Información Personal en virtud del artículo 36, apartado 2, de la Ley serán las siguientes:

- i) definir claramente la autoridad y la responsabilidad de una persona que maneja información relativa a dichas descripciones, etc., y códigos de identificación individuales que se hayan suprimido de la información personal utilizada para producir información tratada de forma anónima e información relativa a un método de tratamiento aplicado de conformidad con lo dispuesto en el artículo 36, apartado 1, (limitado a los que puedan restablecer la información personal utilizando dicha información relacionada) (en lo sucesivo denominada «información relacionada con el método de transformación, etc.» del presente artículo);
- ii) establecer normas y procedimientos sobre el manejo de la información relacionada con el método de tratamiento, etc., la manipulación de información relacionada con el método de procesamiento adecuado, etc., de conformidad con las reglas y procedimientos, evaluar la situación de manejo, y sobre la base de dichos resultados de la evaluación, adoptar las medidas necesarias para buscar mejoras;
- iii) adoptar las medidas necesarias y apropiadas para impedir que una persona sin autoridad legítima maneje información relacionada con el método de tratamiento, etc..

La información personal recibida de la UE sobre la base de una decisión de adecuación solo se considerará información tratada de forma anónima a tenor del artículo 2, apartado 9, de la Ley, si el operador económico que maneja información personal adopta medidas que hagan irreversibles la anonimización del particular para cualquiera, incluso suprimiendo la información relacionada con el método de procesamiento, etc. (es decir, la información relativa a dichas descripciones, etc. y los códigos de identificación individuales que se hayan eliminado de la información personal utilizados para producir la información tratada de forma anónima y la información relativa a un método de tratamiento aplicado de conformidad con lo dispuesto en el artículo 36, apartado 1, de la Ley (limitada a los que pueden restablecer la información personal utilizando dicha información relacionada).

ANEXO 2

Excelentísima señora Věra Jourová, comisaria de Justicia, Consumidores e Igualdad de Género de la Comisión Europea

Excelencia:

Celebro los debates constructivos entablados entre Japón y la Comisión Europea con miras a la creación del marco para la transferencia mutua de datos personales entre Japón y la UE.

En respuesta a la petición cursada por la Comisión Europea al Gobierno de Japón, le envío el documento adjunto, en el que se ofrece una visión general del marco jurídico relativo al acceso a la información por parte de las autoridades públicas japonesas.

El presente documento atañe a numerosos ministerios y agencias del Gobierno de Japón, y en relación con el contenido del documento, los ministerios y agencias competentes (Secretaría del Gabinete, Agencia Nacional de Policía, Comisión de Protección de la Información Personal, Ministerio del Interior y de Comunicaciones, Ministerio de Justicia, Agencia de Inteligencia de la Seguridad Pública, Ministerio de Defensa) son responsables de los pasajes correspondientes a sus respectivas competencias. A continuación figuran los ministerios y agencias pertinentes, así como las firmas correspondientes.

La Comisión de Protección de la Información Personal responderá a todas las consultas relativas al presente documento y coordinará las respuestas necesarias entre los ministerios y las agencias pertinentes.

Espero que este documento le resulte útil para tomar las decisiones que sean oportunas en la Comisión Europea.

Le agradezco la gran contribución que ha realizado hasta la fecha en este asunto.

Atentamente,

Yoko Kamikawa

Ministra de Justicia

El presente documento ha sido elaborado por el Ministerio de Justicia y los siguientes ministerios y agencias.

Koichi Hamano

Consejero, Secretaría del Gabinete

Schunichi Kuryu

Comisario General de la Agencia Nacional de Policía

Mari Sonoda

Secretaria General de la Comisión de Protección de la Información Personal

Mitsuru Yasuda

Viceministro, Ministerio del Interior y de Comunicaciones

Seimei Nakagawa

Agencia de Inteligencia de la Seguridad Pública

Kenichi Takahashi

Viceministro administrativo de Defensa

14 de septiembre de 2018

Recogida y utilización de información personal por parte de las autoridades públicas japonesas con fines coercitivos y de seguridad nacional

El presente documento ofrece una visión general del marco jurídico para la recogida y utilización de información personal (electrónica) por parte de las autoridades públicas japonesas con fines coercitivos y de seguridad nacional (en lo sucesivo, «acceso por parte de las autoridades públicas»), en particular en lo que respecta a las bases jurídicas disponibles, las condiciones aplicables (limitaciones) y las salvaguardas, incluidas la supervisión independiente y las posibilidades de reparación individual. La presente declaración va dirigida a la Comisión Europea con vistas a expresar el compromiso y ofrecer garantías de que el acceso de las autoridades públicas a la información personal transferida desde la UE a Japón se limitará a lo que sea necesario y proporcionado y estará sujeta a una supervisión independiente y de que los particulares afectados podrán obtener reparación en caso de cualquier posible vulneración de su derecho fundamental a la vida privada y a la protección de datos. La presente declaración prevé asimismo la creación de un nuevo mecanismo de reparación, gestionado por la Comisión de Protección de la Información Personal (CPIP), para tramitar las reclamaciones de los particulares de la UE relativas al acceso de las autoridades públicas a sus datos personales transferidos desde la UE a Japón.

I. Principios jurídicos generales pertinentes para el acceso por parte de las autoridades públicas

En tanto que ejercicio de autoridad pública, el acceso de las autoridades públicas a los datos ha de hacerse en el pleno respeto de la ley (principio de legalidad). En Japón, la información personal está protegida tanto en el sector privado como en el sector público por medio de un mecanismo de varios niveles.

A. Marco constitucional y principio de reserva de ley

El artículo 13 de la Constitución y la jurisprudencia reconocen el derecho a la vida privada como un derecho constitucional. A este respecto, el Tribunal Supremo ha estimado que es natural que los particulares no deseen que otros conozcan su información personal sin que exista una buena razón para ello, y que esta expectativa debe protegerse⁽¹⁾. Protecciones adicionales están consagradas en el artículo 21, apartado 2, de la Constitución, que garantiza el respeto del secreto de las comunicaciones, y el artículo 35 de la Constitución, que garantiza el derecho a no ser objeto de un registro e incautación sin orden judicial, lo que significa que la recogida de información personal, incluido el acceso, por medios obligatorios debe basarse siempre en una orden judicial. Solo se podrá expedir una orden para la investigación de un delito ya cometido. Por consiguiente, en el marco jurídico japonés no se permite la recogida de información por medios obligatorios a efectos de seguridad nacional que no se base en una investigación criminal.

Por otra parte, de conformidad con el principio de reserva de ley, la recogida obligatoria de información debe ser autorizada específicamente por ley. En caso de recogida voluntaria o no obligatoria, la información se obtiene de una fuente a la que puede accederse libremente o sobre la base de una solicitud de comunicación voluntaria, es decir, una solicitud que no puede ejecutarse contra la entidad física o jurídica que posee la información. Sin embargo, esto solo es admisible en la medida en que la autoridad pública sea competente para llevar a cabo la investigación, dado que cada autoridad pública solo puede actuar en el ámbito de su competencia administrativa prescrita por la ley (independientemente de que sus actividades interfieran o no con los derechos y libertades de los particulares). Este principio se aplica a la capacidad de la autoridad para recoger información personal.

B. Reglas específicas relativas a la protección de la información personal

La Ley sobre la protección de la información personal (LPIP) y la Ley sobre la protección de la información personal en poder de órganos administrativos (LPIPPOA), que se basan en disposiciones constitucionales y las precisan, garantizan el derecho a la información personal tanto en el sector privado como en el público.

El artículo 7 de la LPIP dispone que la CPIP formulará la «política de base en materia de protección de la información personal» (política de base). La política de base, que se adopta mediante decisión del Gabinete de Japón en su calidad de órgano central del Gobierno japonés (primer ministro y ministros de Estado), fija la dirección en materia de protección de la información personal en Japón. De este modo, la CPIP, en su calidad de autoridad de control independiente, sirve de «centro de mando» del sistema japonés de protección de la información personal.

Cuando los órganos administrativos recogen información personal, y con independencia de que lo hagan por medios obligatorios o no, deben cumplir en principio⁽²⁾ los requisitos de la LPIPPOA. La LPIPPOA es una ley general aplicable al tratamiento de la «información personal conservada»⁽³⁾ por «órganos administrativos» (tal como se definen en el artículo 2, apartado 1, de la LPIPPOA). También regula el tratamiento de datos en el ámbito de la ejecución forzosa de la legislación penal y de la seguridad nacional. Entre las autoridades públicas autorizadas a aplicar el acceso gubernamental, todas las autoridades, excepto la policía prefectural, son autoridades gubernamentales nacionales que entran dentro de la

⁽¹⁾ Sentencia del Tribunal Supremo, de 12 de septiembre de 2003, en el asunto n.º 1656 [2002 (Ju)].

⁽²⁾ Por lo que se refiere a las excepciones relativas al capítulo 4 de la LPIPPOA, véase más adelante la página 16.

⁽³⁾ Según el artículo 2, apartado 5, de la LPIPPOA, se entiende por «información personal conservada» la información personal elaborada u obtenida por un empleado de un órgano administrativo en el ejercicio de sus funciones que obre en poder de dicho órgano para su uso organizativo por parte de sus empleados.

definición de «órganos administrativos». El manejo de información personal por parte de la policía prefectural se rige por ordenanzas prefecturales ⁽⁴⁾ que establecen principios para la protección de la información personal, derechos y obligaciones equivalentes a los de la LPIPOA.

II. Acceso de las autoridades públicas a fines de la ejecución forzosa del Derecho penal

A) Bases jurídicas y limitaciones

1) Recogida de información personal por medios obligatorios

a) Bases jurídicas

De conformidad con el artículo 35 de la Constitución, no se violará la seguridad de domicilio ni se registrarán ni secuestrarán papeles y efectos personales, excepto con el debido mandamiento expedido con «causa suficiente» y en el que se especifique en particular el lugar que se registrará y los objetos que se deben secuestrar. Por consiguiente, la recogida obligatoria de información electrónica por parte de las autoridades públicas en el marco de una investigación criminal solo puede tener lugar sobre la base de una orden judicial. Esta norma se aplica tanto a la recogida de registros electrónicos que contienen información (personal) como a la interceptación en tiempo real de las comunicaciones (las llamadas escuchas telefónicas). La única excepción a esta norma (que, sin embargo, no es pertinente en el contexto de una transferencia electrónica de datos personales desde el extranjero) es el artículo 220, apartado 1, del Código de Enjuiciamiento Criminal ⁽⁵⁾, según el cual un fiscal, un fiscal adjunto o un agente de la policía judicial pueden, al proceder a la detención de un sospechoso o infractor sorprendido *in flagranti*, llevar a cabo, en su caso, un registro e incautación *in situ* en el momento de la detención».

De conformidad con el artículo 197, apartado 1, del Código de Enjuiciamiento Criminal, no se aplicarán medidas obligatorias «a menos que el presente Código prevea disposiciones especiales». En lo que respecta a la recogida obligatoria de información electrónica, las bases jurídicas pertinentes son el artículo 218, apartado 1, del Código de Enjuiciamiento Criminal (según el cual un fiscal, un fiscal adjunto o un agente de la policía judicial puede, si es necesario para la investigación de un delito, proceder a un registro, incautación o inspección sobre la base de un mandato expedido por un juez) y el artículo 222-2 del Código de Enjuiciamiento Criminal (según el cual las medidas obligatorias de interceptación de comunicaciones electrónicas sin el consentimiento de una de las partes se ejecutarán sobre la base de otros actos legislativos). Esta última disposición se refiere a la Ley de escuchas telefónicas a efectos de investigación criminal, que, en su artículo 3, apartado 1, establece las condiciones en las que están autorizadas las escuchas de comunicaciones relativas a determinados delitos graves sobre la base de una orden de escuchas telefónicas dictada por un juez ⁽⁶⁾.

En cuanto a la policía, la autoridad de investigación corresponde en todos los casos a la policía prefectural, mientras que la Agencia Nacional de Policía (ANP) no realiza investigaciones criminales sobre la base del Código de Enjuiciamiento Criminal.

b) Limitaciones

La recogida obligatoria de información electrónica está limitada por la Constitución y por los estatutos de atribución de competencias, según la interpretación de la jurisprudencia, que establecen, en particular, los criterios que deben aplicar los órganos jurisdiccionales al dictar una orden judicial. Además, la LPIPOA impone una serie de limitaciones aplicables tanto a la recogida como al manejo de información (mientras que las ordenanzas locales reproducen esencialmente los mismos criterios para la policía prefectural).

1) Limitaciones derivadas de la Constitución y del estatuto de atribución de competencias

De conformidad con el artículo 197, apartado 1, del Código de Enjuiciamiento Criminal, no se aplicarán disposiciones obligatorias «a menos que el presente Código prevea disposiciones especiales». El artículo 218, apartado 1, de Código de Enjuiciamiento Criminal establece que la incautación, etc., puede llevarse a cabo sobre la base de una orden dictada por

⁽⁴⁾ Todas las prefecturas cuentan con su propia «ordenanza prefectural» aplicable a la protección de la información personal por parte de la policía prefectural. No existen traducciones al inglés de estas ordenanzas prefecturales.

⁽⁵⁾ El artículo 220, apartado 1, del Código de Enjuiciamiento Criminal dispone que cuando un fiscal, un fiscal adjunto o un agente de la policía judicial proceda a la detención de un sospechoso, podrá adoptar, en su caso, las siguientes medidas: a) entrar en la residencia de otra persona, etc., para buscar al sospechoso; b) proceder a registros, incautaciones o inspecciones *in situ* en el momento de la detención.

⁽⁶⁾ Más en concreto, esta disposición dispone que «la fiscalía o la policía judicial, en los casos atinentes a alguno de los incisos siguientes, cuando existan indicios suficientes para sospechar que van a tener lugar comunicaciones sobre compromisos, preparativos, conspiraciones sobre acciones de seguimiento como la eliminación de pruebas, etc., instrucciones y otras intercomunicaciones relativas al acto delictivo contempladas en cada una de dichos incisos (en lo sucesivo, una «serie de delitos» en los incisos segundo y tercero), así como comunicaciones que contengan elementos relativos a dicho delito (en lo sucesivo, «comunicaciones relativas al delito») y en los casos en que resulte extremadamente difícil identificar al delincuente o aclarar las situaciones o los detalles de la comisión del delito por cualquier otra vía, podrán escuchar las comunicaciones relacionada con el delito, sobre la base de la orden de escucha dictada por un juez, en relación con un medio de comunicación especificado por un número de teléfono y otros números/códigos con el fin de identificar la fuente o el destino de la comunicación telefónica que sean utilizados por el sospechoso sobre la base del contrato con compañías de telecomunicaciones, etc. (excepto aquellas que puedan considerarse no sospechosas de ser utilizadas como «comunicaciones relacionadas con el delito»), o aquellas para las que existan motivos para sospechar que se están utilizando como «comunicaciones relacionadas con el delito», y podrán realizarse escuchas telefónicas de las comunicaciones relacionadas con el delito por este medio de comunicaciones.»

un juez solo «cuando sea necesaria para la investigación de un delito». Aunque los criterios para juzgar esta necesidad no se especifican con más detalle en la legislación, el Tribunal Supremo ⁽⁷⁾ ha dictaminado que, al evaluar la necesidad de las disposiciones, el juez debe realizar una evaluación global, teniendo en cuenta, en particular, los siguientes elementos:

- a) la gravedad del delito y la forma en que se cometió;
- b) el valor e importancia de los materiales incautados como elementos de prueba;
- c) la probabilidad de que se oculte o destruya el material incautado;
- d) el alcance de las desventajas ocasionadas por la incautación;
- e) otras circunstancias conexas.

También del requisito establecido en el artículo 35 de la Constitución relativo a una «causa suficiente» se derivan una serie de limitaciones. En virtud del requisito de «causa suficiente», puede dictarse una orden judicial si: 1) es necesaria una investigación criminal [véase la sentencia del Tribunal Supremo, de 18 de marzo de 1969, en el asunto n.º 100 [1968 (Shi)] antes mencionada, 2) existe una situación en la que se considera que el sospechoso (el acusado) ha cometido un delito (artículo 156, apartado 1, de las Normas de Enjuiciamiento Criminal) ⁽⁸⁾, 3) la orden de investigación corporal, de artículos, de residencia o de cualquier otro lugar relacionado con una persona distinta del acusado solo debe dictarse cuando quepa suponer razonablemente que existen artículos que deben ser incautados (artículo 102, apartado 2, del Código de Enjuiciamiento Criminal). Cuando un juez considere que las pruebas documentales presentadas por las autoridades de investigación son insuficientes para sospechar que se ha cometido un delito, desestimará la solicitud de orden judicial. A este respecto, cabe señalar que, con arreglo a la Ley sobre las sanciones aplicables a la delincuencia organizada y al control del producto de la delincuencia, los «preparativos con vistas a la comisión» de un delito planeado (por ejemplo, la preparación de fondos para cometer un acto terrorista) constituyen en sí mismos un acto delictivo y, por tanto, pueden ser objeto de una investigación obligatoria sobre la base de una orden judicial.

Por último, cuando la orden se refiera a la investigación corporal, de artículos, de la residencia o cualquier otro lugar relacionado con una persona distinta del sospechoso o acusado, solo podrá dictarse una orden judicial cuando quepa suponer razonablemente la existencia de los artículos que han de ser incautados (artículo 102, apartado 2, y artículo 222, apartado 1, del Código de Enjuiciamiento Criminal).

Por lo que se refiere específicamente a la interceptación de comunicaciones a efectos de investigaciones criminales basadas en la Ley de escuchas telefónicas, solo podrá realizarse cuando se cumplan los estrictos requisitos establecidos en su artículo 3, apartado 1. Según esta disposición, la interceptación siempre requiere una orden judicial por adelantado, que solo puede dictarse en un número limitado de casos ⁽⁹⁾.

2) Limitaciones impuestas por la LPIPOA

Por lo que se refiere a la recogida ⁽¹⁰⁾ y ulterior manejo (en particular la conservación, gestión y utilización) de información personal por parte de los órganos administrativos, la LPIPOA establece, en particular, las siguientes limitaciones:

- a) De conformidad con el artículo 3, apartado 1, de la LPIPOA, los órganos administrativos solo pueden conservar información personal en la medida en que sea necesario para el ejercicio de las funciones que les encomienden disposiciones legales y reglamentarias. En el momento de la conservación, también están obligados a especificar (en la medida de lo posible) la finalidad de la utilización de la información personal. De conformidad con el artículo 3, apartados 2 y 3, de la LPIPOA, los órganos administrativos no deben conservar la información personal más allá de lo que sea necesario para la consecución del objetivo de utilización especificado y no pueden modificar la finalidad de utilización más allá de lo que pueda considerarse razonablemente pertinente para la finalidad original.
- b) El artículo 5 de la LPIPOA establece que el responsable de un órgano administrativo debe velar por mantener la información personal conservada exacta y actualizada, en la medida necesaria para alcanzar la finalidad de utilización.
- c) El artículo 6, apartado 1, de la LPIPOA establece que el responsable de un órgano de administración debe adoptar las medidas necesarias para evitar fugas, pérdidas o daños, así como para asegurar la correcta gestión de la información personal conservada.
- d) De conformidad con el artículo 7 de la LPIPOA, ningún empleado (incluidos los antiguos empleados) puede comunicar la información personal adquirida a otra persona sin un motivo justificado ni utilizar dicha información para una finalidad injusta.

⁽⁷⁾ Sentencia de 18 de marzo de 1969 en el asunto n.º 100 [1968 (Shi)].

⁽⁸⁾ El artículo 156, apartado 1, de las Normas de Enjuiciamiento Criminal dispone lo siguiente: «Al presentar la solicitud referida en el apartado 1 del artículo anterior, el solicitante deberá facilitar el material en base al cual debe considerarse que el sospechoso o el acusado han cometido un delito.»

⁽⁹⁾ Véase la nota a pie de página n.º 6.

⁽¹⁰⁾ El artículo 3, apartados 1 y 2, de la LPIPOA restringe el alcance de la conservación y, por tanto, también la recogida de información personal.

- e) Por otra parte, el artículo 8, apartado 1, de la LPIPOA establece que el responsable de un órgano administrativo no puede, salvo disposición en contrario prevista en disposiciones legislativas y reglamentarias, utilizar ni poner a disposición de terceros la información personal conservada para finalidades distintas de las especificadas. Aunque el artículo 8, apartado 2, contiene excepciones a esta norma en situaciones específicas, estas solo son aplicables si tal comunicación excepcional no puede causar un perjuicio «injusto» a los derechos e intereses del interesado o de un tercero.
- f) De conformidad con el artículo 9 de la LPIPOA, en caso de que la información personal conservada se facilite a otra persona, el responsable de un órgano administrativo debe imponer, en su caso, restricciones sobre la finalidad o el método de utilización, o cualquier otra restricción necesaria; también puede pedir al destinatario que adopte las medidas necesarias para prevenir las fugas y gestionar adecuadamente la información.
- g) El artículo 48 de la LPIPOA dispone que el responsable de un órgano administrativo procurará tramitar las reclamaciones relacionadas con el manejo de información personal de manera apropiada y diligente.

2) Recogida de información personal mediante solicitudes de cooperación voluntaria (investigación voluntaria)

a) Base jurídica

Aparte del uso de medios obligatorios, la información personal se obtiene bien de una fuente a la que puede accederse libremente, bien sobre la base de una comunicación voluntaria, incluso por parte de los operadores económicos que posean dicha información.

En este último caso, el artículo 197, apartado 2, del Código de Enjuiciamiento Criminal faculta a la fiscalía y a la policía judicial para formular «consultas escritas sobre cuestiones de la investigación» (las denominadas «fichas de consulta»). En virtud del Código de Enjuiciamiento Criminal, las personas consultadas deben informar a las autoridades de investigación. Sin embargo, no se prevén formas de obligar a informar a las oficinas públicas o las organizaciones públicas o privadas destinatarias de las consultas en caso de que se nieguen a hacerlo. Si no informan de las consultas, no pueden imponerse sanciones penales ni de otro tipo. Si las autoridades de investigación consideran que la información solicitada es indispensable, deberán obtenerla mediante un registro e incautación sobre la base de una orden judicial.

Habida cuenta de la creciente sensibilización de los particulares sobre su derecho a la vida privada, así como de la carga de trabajo que generan estas solicitudes, los operadores económicos son cada más cautos a la hora de responder a dichas solicitudes⁽¹¹⁾. A la hora de decidir si desean cooperar, tienen en cuenta, en particular, la naturaleza de la información solicitada, su relación con la persona a quien concierne la información, los riesgos para su reputación, los riesgos de litigio, etc.

b) Limitaciones

Por lo que se refiere a la recogida obligatoria de información electrónica, la investigación voluntaria está limitada por la Constitución, tal como interpreta la jurisprudencia, y el estatuto de atribución de competencias. Además, los operadores económicos no están autorizados legalmente a comunicar información en determinadas situaciones. Por último, la LPIPOA prevé una serie de limitaciones aplicables tanto a la recogida como al manejo de la información (mientras que las ordenanzas locales reproducen esencialmente los mismos criterios para la policía prefectural).

1) Limitaciones derivadas de la Constitución y del estatuto de atribución de competencias

Teniendo en cuenta el propósito del artículo 13 de la Constitución, el Tribunal Supremo, en sendas decisiones de 24 de diciembre de 1969 [1965 (A) n.º 1187] y de 15 de abril de 2008 [2007 (A) n.º 839], ha fijado una serie de límites a las investigaciones voluntarias llevadas a cabo por las autoridades de investigación. Aunque estas decisiones se referían a casos en los que la información personal (en forma de imágenes) fue recogida mediante fotografía o filmación, las conclusiones son pertinentes para las investigaciones voluntarias (no obligatorias) que interfieren con la vida privada de un particular en general. Por consiguiente, son aplicables y deben cumplirse, en lo que respecta a la recogida de información personal a través de una investigación voluntaria, teniendo en cuenta las circunstancias específicas de cada caso.

Con arreglo a estas decisiones, la legalidad de la investigación voluntaria depende del cumplimiento de tres criterios, a saber:

- «sospecha de un delito» (es decir, debe evaluarse si se ha cometido un delito);
- «necesidad de la investigación» (es decir, debe evaluarse si la solicitud se mantiene dentro de lo necesario para los fines de la investigación); e

⁽¹¹⁾ Véase también la notificación emitida por la Agencia Nacional de Policía el 7 de diciembre de 1999 (página 9), que coincide en este punto.

— «idoneidad de los métodos» (es decir, debe evaluarse si la investigación voluntaria es «apropiada» o razonable para lograr la finalidad de la investigación) ⁽¹²⁾.

En general, teniendo en cuenta los tres criterios mencionados, la legalidad de la investigación voluntaria se estima tomando en consideración si puede considerarse razonable con arreglo a los convenciones socialmente aceptables.

El requisito de que la investigación sea «necesaria» también se deriva directamente del artículo 197 del Código de Enjuiciamiento Criminal y ha sido confirmado en las instrucciones formuladas por la Agencia Nacional de Policía (ANP) a la policía prefectural en lo que respecta a la utilización de las «fichas de consulta». La notificación de la ANP de 7 de diciembre de 1999 establece una serie de limitaciones procedimentales, incluida la obligación de utilizar las «fichas de consulta» solo en caso de que sea necesario para los fines de la investigación. Además, el artículo 197, apartado 1, del Código de Enjuiciamiento Criminal se limita a las investigaciones criminales y solo puede aplicarse, por tanto, cuando exista una sospecha concreta de un delito ya cometido. Por el contrario, esta base jurídica no es aplicable a la recogida y utilización de información personal cuando aún no se ha violado la ley.

2) Limitaciones con respecto a ciertos operadores económicos

En determinados ámbitos, se aplican limitaciones adicionales basadas en las protecciones previstas en otras leyes.

En primer lugar, las autoridades de investigación y las empresas de telecomunicaciones que poseen información personal tienen el deber de respetar el secreto de las comunicaciones garantizado por el artículo 21, apartado 2, de la Constitución ⁽¹³⁾. Además, en lo que respecta a las empresas de telecomunicaciones, esta obligación se recoge igualmente en el artículo 4 de la Ley del sector de las telecomunicaciones ⁽¹⁴⁾. Según las «Directrices sobre la protección de la información personal en el sector de las telecomunicaciones», publicadas por el Ministerio del Interior y de Comunicaciones (MIC) sobre la base de la Constitución y la Ley del sector de las telecomunicaciones, en aquellos casos en que esté en peligro el secreto de las comunicaciones, las empresas de telecomunicaciones se abstendrán de comunicar a terceros información personal relativa al secreto de la comunicación, a no ser que hayan obtenido el consentimiento del particular o que puedan invocar una de las «causas justificables» para incumplir el Código Penal. Este último se refieren a «actos justificables» (artículo 35), «autodefensa» (artículo 36) y «neutralización de un peligro existente» (artículo 37). En virtud del Código Penal, solo se consideran «actos justificables» aquellos actos de una empresa de telecomunicaciones por los cuales cumple con las medidas obligatorias del Estado, lo que excluye la investigación voluntaria. Por consiguiente, si las autoridades de investigación solicitan información personal sobre la base de una «ficha de consulta» (artículo 197, apartado 2, del Código de Enjuiciamiento Criminal), las empresas de telecomunicaciones no pueden comunicar los datos.

En segundo lugar, los operadores económicos están obligados a rechazar las solicitudes de cooperación voluntaria cuando la ley les prohíba comunicar información personal. Se incluyen aquí, por ejemplo, los casos en que el operador esté obligado a respetar la confidencialidad de la información, por ejemplo de conformidad con el artículo 134 del Código Penal ⁽¹⁵⁾.

3) Limitaciones basadas en la LPIPPOA

En lo que respecta a la recogida y posterior manejo de la información personal por los órganos administrativos, la LPIPPOA establece las limitaciones que se mencionan en la sección II.A.1, letra b), número 2). Se derivan limitaciones equivalentes de las ordenanzas prefecturales aplicables a la policía prefectural.

B) Supervisión

1) Supervisión judicial

La recogida de información personal por medios obligatorios debe estar fundamentada en una orden ⁽¹⁶⁾ y estar supe-
ditada, por tanto, a un examen judicial *a priori*. En caso de que la investigación fuese ilegal, un juez podría excluir esa prueba del proceso penal posterior en el que se dirima el asunto. Un particular puede solicitar dicha exclusión en un proceso penal que le ataña alegando la ilegalidad de la investigación.

⁽¹²⁾ La gravedad del delito y la urgencia son factores pertinentes para evaluar la «idoneidad de los métodos».

⁽¹³⁾ El artículo 21, párrafo segundo, de la Constitución dispone: «No se mantendrá censura alguna ni se violará el secreto de ningún medio de comunicación».

⁽¹⁴⁾ El artículo 4 de la Ley del sector de las telecomunicaciones establece lo siguiente: «1) No se violará el secreto de las comunicaciones manejadas por una empresa de telecomunicaciones. 2) Toda persona que ejerza una actividad de telecomunicaciones no comunicará secretos que haya obtenido, mientras esté en ejercicio, en lo que respecta a las comunicaciones manejadas por una empresa de telecomunicaciones. Lo mismo se aplicará incluso después de haber cesado en sus funciones.»

⁽¹⁵⁾ Por último, el artículo 134 del Código Penal dispone lo siguiente: «1) Cuando un médico, farmacéutico, distribuidor de productos farmacéuticos, matrona, abogado, asesor de la defensa, notario o cualquier otra persona que haya ejercido anteriormente una de dichas profesiones comunique, sin motivos justificables, información confidencial de otra persona que haya conocido en el ejercicio de dicha profesión, se impondrá pena de prisión acompañada de trabajos de no más de 6 meses o una multa máxima de 100 000 yenes. 2) Lo mismo se aplicará cuando una persona que participe o haya participado en actividad religiosa comunique, sin motivos justificables, información confidencial de otra persona que haya conocido en el ejercicio de dichas actividades religiosas».

⁽¹⁶⁾ Véase la nota a pie de página n.º 5 para más información sobre la excepción a esta norma.

2) Supervisión basada en la LPIPOA

En Japón, el ministro o máximo responsable de cada ministerio o agencia es el titular de la autoridad de supervisión y ejecución sobre la base de la LPIPOA, mientras que el ministro del Interior y de Comunicaciones puede investigar la ejecución de la LPIPOA por todos los demás ministerios.

En caso de que el ministro del Interior y de Comunicaciones, basándose, por ejemplo, en la investigación sobre el estado de la ejecución de la LPIPOA ⁽¹⁷⁾, la tramitación de las denuncias o las consultas dirigidas a uno de sus centros de información integrada, lo considere necesario para alcanzar el objetivo de la LPIPOA, podrá solicitar al jefe de un órgano administrativo que presente materiales y explicaciones sobre el manejo de la información personal por parte de dicho órgano administrativo, sobre la base del artículo 50 de la LPIPOA. El ministro puede dirigir dictámenes al jefe del órgano administrativo en relación con el tratamiento de información personal en dicho órgano administrativo cuando lo considere necesario para alcanzar el objetivo de dicha Ley. Además, el ministro puede, por ejemplo, solicitar la revisión de las medidas mediante los actos para los que está facultado de conformidad con los artículos 50 y 51 de la Ley cuando se sospeche que se ha producido una infracción o una aplicación inadecuada de la Ley. Con ello se contribuye a garantizar la aplicación uniforme y el cumplimiento de la LPIPOA.

3) Supervisión por las comisiones de seguridad pública en lo que respecta a los cuerpos policiales

En lo que respecta a la administración policial, la ANP está sujeta a supervisión por parte de la Comisión Nacional de Seguridad Pública, mientras que la policía prefectural está sujeta a supervisión por una de las comisiones prefecturales de seguridad pública creadas en cada prefectura. Cada uno de esos organismos de supervisión garantiza la gestión democrática y la neutralidad política de la administración policial.

La Comisión Nacional de Seguridad Pública es responsable de los asuntos que dependen de su jurisdicción con arreglo a las leyes, en particular la Ley de Policía. Entre ellos están el nombramiento del comisario general de la ANP y de los altos cargos de la policía local, así como el establecimiento de políticas globales que recojan las orientaciones o medidas básicas en lo que respecta a la administración de la ANP.

Las comisiones prefecturales de seguridad pública están compuestas por miembros que representan a la población de sus respectivas prefecturas, sobre la base de la Ley de Policía, y gestionan la policía prefectural como un sistema de consejos independientes. Los miembros son nombrados por el gobernador de la prefectura previo consentimiento de la asamblea prefectural con arreglo al artículo 39 de la Ley de Policía. Su mandato dura tres años y solo pueden ser cesados contra su voluntad por las razones específicas que enumera la ley (como la incapacidad para el ejercicio de sus funciones, los actos contrarios a su cargo, la conducta inapropiada, etc.), lo cual garantiza su independencia (véanse los artículos 40 y 41 de la Ley de Policía). Además, con el fin de garantizar su neutralidad política, el artículo 42 de la Ley de Policía prohíbe a los miembros de la comisión que sirvan simultáneamente como miembros de un órgano legislativo, se conviertan en miembros de la ejecutiva de un partido político o cualquier otro organismo político o se comprometan activamente en movimientos políticos. Aunque cada comisión está sujeta a la jurisdicción del gobernador de la prefectura respectiva, este no tiene autoridad alguna para dar instrucciones en lo relativo al ejercicio de las funciones de la comisión.

Con arreglo al artículo 38, apartado 3, leído en relación con el artículo 2 y el artículo 36, apartado 2, de la Ley de Policía, las comisiones prefecturales de seguridad pública son responsables de «la protección de los derechos y libertades de un particular». Con ese fin, recibirán informes de los jefes de las policías prefecturales relativos a las actividades realizadas en sus respectivas jurisdicciones, en particular en el marco de reuniones periódicas que se celebrarán tres o cuatro veces al mes. Las comisiones ofrecen orientaciones sobre estas cuestiones a través del establecimiento de políticas globales.

Por otra parte, como parte de su función supervisora, las comisiones prefecturales de seguridad pública pueden emitir directrices a la policía prefectural para casos individuales concretos cuando lo consideren necesario en el contexto de una inspección de las actividades de la policía prefectural o de la conducta inapropiada de su personal. Además, las comisiones pueden encargar a un miembro designado que revise el estado de aplicación de las directrices emitidas, cuando lo consideren necesario (artículo 43, apartado 2, de la Ley de Policía).

⁽¹⁷⁾ Para garantizar la transparencia y facilitar la supervisión del Ministerio del Interior y de Comunicaciones (MIC), se exige que los jefes de los órganos administrativos, de conformidad con el artículo 11 de la LPIPOA, registren cada uno de los elementos mencionados en el artículo 10, apartado 1, de la LPIPOA, como el nombre del órgano administrativo encargado del expediente, la finalidad de uso del expediente, el método de recogida de la información personal, etc. (en lo que se denomina «Registro de expedientes de información personal»). No obstante, los expedientes de información personal contemplados en el artículo 10, apartado 2, de la LPIPOA, como por ejemplo los elaborados u obtenidos en el marco de una investigación penal o los relativos a cuestiones pertinentes para la seguridad nacional, son objeto de una exención de la obligación de notificarlos al MIC y de incluirlos en el registro público. Sin embargo, de conformidad con el artículo 7 de la Ley de registros públicos y gestión de archivos, siempre se exige al jefe de un órgano administrativo que registre la clasificación, el título, el período de conservación y la ubicación del almacenamiento, etc., de los documentos administrativos («Registro de gestión de expedientes administrativos»). La información indexada de ambos registros se publica en Internet y permite que los particulares comprueben el tipo de información personal contenida en los expedientes y el órgano administrativo que conserva esa información.

4) Supervisión de la Dieta

La Dieta puede llevar a cabo investigaciones en relación con las actividades de las autoridades públicas y solicitar, con ese fin, la elaboración de documentos y la declaración de testigos (artículo 62 de la Constitución). En este contexto, la comisión competente de la Dieta puede examinar la adecuación de las actividades de recogida de información llevadas a cabo por la policía.

Estos poderes se detallan en mayor medida en la Ley de la Dieta. Con arreglo a su artículo 104, la Dieta puede exigir al Gabinete y a las agencias públicas la elaboración de los documentos y registros necesarios para el desarrollo de su investigación. Además, los miembros de la Dieta pueden presentar «consultas escritas» de conformidad con el artículo 74 de la Ley de la Dieta. Estas consultas deben ser aprobadas por el presidente de la Cámara y, en principio, deben recibir una respuesta escrita del Gabinete en el plazo de siete días (cuando sea imposible responder en ese plazo, deberá motivarse la imposibilidad y fijarse un nuevo plazo, con arreglo al artículo 75 de la Ley de la Dieta). En ocasiones, las consultas escritas de la Dieta se han referido también al manejo de información personal por parte de la administración ⁽¹⁸⁾.

C) Reparación individual

Con arreglo al artículo 32 de la Constitución japonesa, no se negará a ninguna persona el derecho de recurrir a la justicia. Además, el artículo 17 de la Constitución garantiza a todas las personas el derecho a demandar al Estado o a una entidad pública para obtener reparación (de acuerdo con la ley) en caso de que haya sufrido daños motivados por actos ilegales de un funcionario público.

1) Reparación judicial contra la recogida obligatoria de información basada en una orden (artículo 430 del Código de Enjuiciamiento Criminal)

De conformidad con el artículo 430, apartado 2, del Código de Enjuiciamiento Criminal, un particular que no esté satisfecho con las medidas adoptadas por un agente de policía en relación con la incautación de artículos (incluidos los que contienen información personal) basada en una orden puede presentar una solicitud (la denominada «cuasi reclamación») ante el órgano jurisdiccional competente para que dichas medidas sean «rescindidas o modificadas».

Esta impugnación puede presentarse sin que el particular tenga que esperar a la conclusión del caso. Si el órgano jurisdiccional considera que la incautación no era necesaria o que existen otras razones para considerarla ilegal, podrá ordenar la rescisión o modificación de dichas medidas.

2) Reparación judicial en virtud del Código de Enjuiciamiento Civil y la Ley de reparaciones a cargo del Estado

Si los particulares consideran que se ha vulnerado su derecho a la vida privada solicite que la información personal recogida en el marco de una investigación penal sea suprimida.

Además, un particular puede interponer una acción de indemnización por daños y perjuicios basada en la Ley de reparaciones a cargo del Estado, en combinación con los artículos pertinentes del Código Civil, si considera que se ha vulnerado su derecho a la vida privada y ha sufrido un perjuicio debido a la recopilación de su información personal o su supervisión ⁽¹⁹⁾. Dado que el «daño» que está sujeto a una reclamación de indemnización no se limita a los daños a la propiedad (artículo 710 del Código Civil), esto puede cubrir también las «sufimientos psicológicos». El juez evaluará el importe de la indemnización por tales daños morales sobre la base de una «evaluación libre teniendo en cuenta diversos factores en cada caso» ⁽²⁰⁾.

El artículo 1, apartado 1, de la Ley de reparaciones a cargo del Estado concede el derecho a una indemnización cuando i) un funcionario que ejerza la autoridad pública del Estado (o de una entidad pública), ii) en el ejercicio de sus funciones, iii) con intencionalidad o por negligencia iv) y de forma ilícita y culposa, v) haya ocasionado daños al particular de que se trate.

El particular debe interponer la demanda ajustándose a lo dispuesto en el Código de Enjuiciamiento Civil. De acuerdo con las normas aplicables, debe hacerlo ante el órgano jurisdiccional competente en el lugar en que se ocasionó el daño.

⁽¹⁸⁾ Véase, por ejemplo, la consulta escrita n.º 92 de la Cámara de Consejeros, de 27 de marzo de 2009, relativa al manejo de información personal recogida en el contexto de investigaciones criminales, incluidas las relativas a infracciones de las obligaciones de confidencialidad por la policía y la fiscalía.

⁽¹⁹⁾ Un ejemplo de ese tipo de acción es «el asunto de la lista de la Agencia de Defensa» [Tribunal de Distrito de Niigata, sentencia de 11 de mayo de 2006 [2002(Wa) n.º 514]]. En dicho asunto, un funcionario de la Agencia de Defensa elaboró, mantuvo y distribuyó una lista de particulares que habían presentado solicitudes de comunicación de documentos administrativos a la Agencia de Defensa. La lista contenía descripciones de la información personal del demandante. El demandante insistía en que su vida privada, derecho a saber, etc., habían sido vulnerados y solicitó al demandado que le abonara una indemnización por daños y perjuicios en virtud del artículo 1, apartado 1, de la Ley de reparaciones a cargo del Estado. Esta solicitud fue parcialmente estimada por el Tribunal, que concedió al demandante una indemnización parcial.

⁽²⁰⁾ Tribunal Supremo, sentencia de 5 de abril de 1910 [1910(O) n.º 71].

3) Reparación individual contra investigaciones ilegales o inadecuadas de la policía: reclamación a la comisión prefectural de seguridad pública (artículo 79 de la Ley de Policía)

De conformidad con el artículo 79 de la Ley de Policía ⁽²¹⁾, y con arreglo a las aclaraciones incluidas en una instrucción del jefe de la ANP a las comisiones prefecturales de policía y de seguridad pública ⁽²²⁾, los particulares pueden presentar una denuncia por escrito ⁽²³⁾ ante la comisión prefectural de seguridad pública competente contra cualquier conducta ilegal o indebida por parte de un agente de policía en el ejercicio de sus funciones, lo que incluye los deberes en relación con la recogida y el uso de información personal. La comisión tramitará tales denuncias atentamente, de conformidad con las disposiciones legales y las ordenanzas locales, y comunicará por escrito los resultados de la investigación al denunciante.

Habida cuenta de su autoridad de supervisión de conformidad con el artículo 38, apartado 3, de la Ley de Policía, la comisión prefectural de seguridad pública dictará una instrucción a la policía prefectural para que investigue los hechos, adopte las medidas apropiadas sobre la base de los resultados del examen e informe a la comisión sobre los resultados. Cuando lo considere necesario, la comisión también puede dictar una instrucción sobre el tratamiento de la denuncia, por ejemplo si considera que la investigación llevada a cabo por la policía es insuficiente. Esta aplicación se describe en la nota enviada por la ANP a los jefes de las policías prefecturales.

La notificación del resultado de la investigación al denunciante se realiza también a la luz de los informes policiales relativos a la investigación y de las medidas adoptadas a petición de la Comisión.

4) Reparación individual en virtud de la LPIPOA y el Código de Enjuiciamiento Criminal

a) LPIPOA

En virtud del artículo 48 de la LPIPOA, los órganos administrativos deben tratar de tramitar de forma adecuada y diligente todas las denuncias sobre el manejo de la información personal. Como medio para facilitar información consolidada a los particulares (por ejemplo, sobre los derechos de comunicación, rectificación y suspensión de la utilización concedidos por la LPIPOA) y como punto de contacto para las consultas, el MIC ha establecido centros de información integrada sobre comunicación de información y protección de la información personal en cada una de las prefecturas, en virtud del artículo 47, apartado 2, de la LPIPOA. También son posibles las consultas realizadas por no residentes. Por ejemplo, en el ejercicio financiero 2017 (de abril de 2017 a marzo de 2018), el número total de casos en los que los centros de información integrada respondieron a las consultas, etc., fue de 5186.

Los artículos 12 y 27 de la LPIPOA otorgan a los particulares el derecho a solicitar la comunicación y la rectificación de la información personal conservada. Por otra parte, de conformidad con el artículo 36 de la LPIPOA, los particulares pueden solicitar la suspensión de la utilización o la supresión de su información personal conservada si el órgano administrativo no ha obtenido la información personal conservada de forma lícita, o bien conserva o utiliza dicha información de forma contraria a la ley.

Sin embargo, por lo que se refiere a la información personal recogida (ya sea mediante una orden o mediante una «ficha de consulta») y conservada a efectos de investigaciones criminales ⁽²⁴⁾, dicha información suele incluirse en la categoría de «información personal registrada en los documentos relacionados con procesos y artículos incautados». Por consiguiente, dicha información personal queda excluida del ámbito de aplicación de los derechos individuales del capítulo 4 de la LPIPOA, de conformidad con el artículo 53, apartado 2, del Código de Enjuiciamiento Criminal ⁽²⁵⁾. El tratamiento de esa información personal y los derechos del particular al acceso a esa información y a su rectificación están, en cambio, sujetos a normas especiales en virtud del Código de Enjuiciamiento Criminal y la Ley sobre los expedientes de

⁽²¹⁾ Artículo 79 de la Ley de Policía (extracto):

1. Quien tenga una reclamación contra la ejecución de funciones por parte del personal de la policía prefectural podrá presentar una denuncia por escrito ante la comisión prefectural de seguridad pública de la Prefectura a través del procedimiento prescrito en el Reglamento de la comisión prefectural de seguridad pública.
2. La comisión prefectural de seguridad pública que haya recibido la denuncia prevista en el apartado anterior la tramitará atentamente de conformidad con las leyes y ordenanzas locales, y notificará por escrito su resultado al denunciante, salvo en los casos siguientes:
 - 1) que la denuncia sea reconocida como interpuesta para obstaculizar la ejecución lícita de las funciones de la policía prefectural;
 - 2) que se desconozca la residencia actual del denunciante;
 - 3) que la denuncia pueda ser reconocida como interpuesta conjuntamente con otros denunciantes a los que ya se ha notificado el resultado de la denuncia conjunta.

⁽²²⁾ ANP, Comunicación relativa a la tramitación adecuada de las denuncias sobre la ejecución de las funciones de los agentes de policía, 13 de abril de 2001, con el apéndice 1 «Normas de interpretación/aplicación del artículo 79 de la Ley de Policía».

⁽²³⁾ De conformidad con la comunicación de la ANP (véase la nota a pie de página anterior), los particulares que tengan dificultades para formular una denuncia por escrito recibirán asistencia. Esto incluye expresamente el caso de los extranjeros.

⁽²⁴⁾ Por otra parte, habría documentos no clasificados como «documentos relacionados con procesos», ya que no constituyen información obtenida por una orden o consultas escritas sobre asuntos de investigación, sino que se han creado sobre la base de dichos documentos. Este sería el caso cuando la información privada no esté sujeta al artículo 45, apartado 1, de la LPIPOA y, por lo tanto, esa información no quedaría excluida de la aplicación del capítulo 4 de la LPIPOA.

⁽²⁵⁾ El artículo 53-2, apartado 2, del Código de Enjuiciamiento Criminal establece que las disposiciones del capítulo IV de la LPIPOA no se aplicarán a la información personal registrada en documentos relacionados con procesos y artículos incautados.

los asuntos penales cerrados (véase *infra*)⁽²⁶⁾. Esta exclusión se justifica por diversos factores, como la protección de la vida privada de las personas afectadas, el secreto de las investigaciones y el correcto desarrollo del proceso penal. Dicho esto, las disposiciones del capítulo 2 de la LPIPOA que rigen los principios del manejo de esa información siguen siendo aplicables.

b) *Código de Enjuiciamiento Criminal*

Con arreglo al Código de Enjuiciamiento Criminal, las posibilidades de acceder a información personal recogida a los efectos de una investigación criminal dependen tanto de la fase del procedimiento como del papel del particular en la investigación (sospechoso, acusado, víctima, etc.).

Como excepción a la norma contenida en el artículo 47 del Código de Enjuiciamiento Criminal, que establece que los documentos relacionados con el proceso no se harán públicos antes del inicio de este (ya que lo contrario podría vulnerar el derecho al honor y a la vida privada de las personas afectadas y dificultar la investigación o el proceso), se permite, en principio, que las víctimas de delitos inspeccionen dicha información, en la medida en que se considere razonable teniendo en cuenta el objetivo de la disposición del artículo 47 del Código de Enjuiciamiento Criminal⁽²⁷⁾.

En lo que respecta a los sospechosos, lo normal es que conozcan el hecho de ser objeto de una investigación criminal al ser interrogados por la policía judicial o el fiscal. Si, posteriormente, el fiscal decide no entablar acciones judiciales, lo notificará con celeridad al sospechoso a solicitud de este (artículo 259 del Código de Enjuiciamiento Criminal).

Además, a raíz de la interposición de acciones judiciales, el fiscal dará al acusado o a su abogado la oportunidad de examinar previamente las pruebas antes de solicitar su examen por el órgano jurisdiccional (artículo 299 del Código de Enjuiciamiento Criminal). Esto permite al acusado comprobar su información personal recogida mediante la investigación criminal.

Por último, la protección de la información personal recogida en el contexto de una investigación criminal, ya sea de un sospechoso, un acusado cualquier otra persona (por ejemplo, una víctima), queda garantizada mediante la obligación de confidencialidad (artículo 100 de la Ley de la función pública nacional) y la amenaza de una sanción en caso de filtración de información confidencial en el ejercicio de las funciones de servicio público (artículo 109, inciso xii), de la Ley de la función pública nacional).

5) Reparación individual frente a investigaciones ilegales o inadecuadas de las autoridades públicas: reclamación a la CPIP

De conformidad con el artículo 6 de la LPIP, el Gobierno debe adoptar las medidas necesarias, en colaboración con los gobiernos de terceros países, para construir un sistema de información personal que pueda adaptarse internacionalmente a través del fomento de la cooperación con organizaciones internacionales y otros marcos internacionales. Con base en esa disposición, la política básica para la protección de la información personal, adoptada por Decisión del Gobierno, delega en la CPIP, como autoridad competente para la administración global de la LPIP, la facultad de adoptar las medidas necesarias para salvar las diferencias entre los sistemas y las operaciones de Japón y los del país extranjero de que se trate con el fin de garantizar el manejo apropiado de la información personal recibida de dicho país.

Además, con arreglo a lo dispuesto en el artículo 61, incisos i) y ii), de la LPIP, se encomienda a la CPIP la tarea de formular y promover una política básica, así como la mediación en las denuncias presentadas contra los operadores comerciales. Por último, los órganos administrativos se informarán mutuamente y cooperarán estrechamente entre sí (artículo 80 de la LPIP).

Sobre la base de estas disposiciones, la LPIP tratará las denuncias presentadas por particulares de la siguiente manera:

- a) Una persona que sospeche que sus datos transferidos desde la UE han sido recogidos o utilizados por las autoridades públicas de Japón, incluidas las autoridades responsables de las actividades a las que se hace referencia en el capítulo II y el capítulo III de la presente «Declaración», en contravención de las normas aplicables, incluidas las que están sujetas a esta «Declaración», puede presentar una denuncia a la CPIP (por separado o a través de su APD).
- b) La CPIP tramita la denuncia, en particular haciendo uso de sus competencias en virtud del artículo 6, apartado 61, inciso ii), y el artículo 80 de la LPIP, e informa a las autoridades públicas competentes, incluidos los organismos de supervisión pertinentes, de la denuncia.

⁽²⁶⁾ En virtud del Código de Enjuiciamiento Criminal y de la Ley sobre los expedientes de los asuntos penales cerrados, el acceso a los artículos incautados y a los documentos e información personal relativos a procesos penales, así como la rectificación de los mismos, están sujetos a un sistema único y distintivo de normas que tiene por objeto proteger la vida privada de las personas afectadas, el secreto de las investigaciones y el buen desarrollo del proceso penal, etc.

⁽²⁷⁾ Más concretamente, se permite, en principio, que las víctimas de delitos inspeccionen la información relacionada con pruebas objetivas en relación con los registros no judiciales sobre los asuntos que implican participación de las víctimas estipulados en el artículo 316-33 y posteriores del Código de Enjuiciamiento Criminal, con el fin de que la protección de las víctimas de delitos sea más satisfactoria.

Estas autoridades están obligadas a cooperar con la CPIP en virtud del artículo 80 de la LPIP, en particular facilitando la información necesaria y el material pertinente para permitir a la CPIP evaluar si la recogida o la utilización ulterior de la información personal ha tenido lugar de conformidad con las normas aplicables. Al llevar a cabo su evaluación, la CPIP cooperará con el MIC.

- c) Si de la evaluación se desprende que se ha infringido la normativa aplicable, la cooperación entre las autoridades públicas afectadas y la CPIP incluye la obligación de subsanar la infracción.

En caso de recogida ilícita de información personal, esto requiere la supresión de tal información.

En caso de infracción de las normas aplicables, la CPIP confirmará, antes de concluir la evaluación, que la infracción ha sido totalmente subsanada.

- d) Una vez concluida la evaluación, la CPIP debe notificar al particular, en un plazo razonable, los resultados de la evaluación, incluidas, en su caso, las medidas correctoras adoptadas. Mediante esa notificación, la CPIP también debe informar al particular de la posibilidad de solicitar a la autoridad pública competente la confirmación de los resultados e indicarle quién es la autoridad a la que deberá dirigir tal solicitud.

El acceso a la información detallada acerca de los resultados de la evaluación puede limitarse si existen motivos razonables para considerar que la comunicación de dicha información puede entrañar un riesgo para la investigación en curso.

Cuando la denuncia atañe a la recogida o utilización de datos personales en el ámbito del enjuiciamiento criminal, y si la evaluación pone de manifiesto que se ha utilizado información personal que concierne al particular en el marco de un asunto que ya ha sido cerrado, la CPIP informará al particular de que puede consultar el expediente con arreglo al artículo 53 del CEC (y el artículo 4 de la Ley sobre los expedientes de los asuntos penales cerrados).

Cuando de la evaluación se desprenda que un particular es sospechoso de haber cometido un delito, la CPIP le informará al respecto, así como de la posibilidad de enviar una solicitud con arreglo al artículo 259 del CEC.

- e) Si un particular sigue insatisfecho con el resultado del procedimiento, puede dirigirse a la CPIP, la cual informará al particular de las distintas posibilidades y procedimientos detallados para obtener una reparación en virtud de las disposiciones legales y reglamentarias japonesas. La CPIP prestará apoyo al particular, en particular asesoramiento y asistencia para emprender nuevas acciones ante el órgano administrativo o judicial pertinente.

III. Acceso de las autoridades públicas a efectos de la seguridad nacional

A. Bases jurídicas y limitaciones para la recogida de información personal

- 1) Bases jurídicas para la recogida de información por el ministerio o la agencia correspondiente

Como se ha indicado anteriormente, la recogida de información personal a efectos de la seguridad nacional por parte de los órganos administrativos debe entrar en el ámbito de su jurisdicción administrativa.

En Japón no existe ninguna ley que permita la recogida de información por medios obligatorios únicamente a efectos de la seguridad nacional. De conformidad con el artículo 35 de la Constitución, es posible recoger información personal por la fuerza únicamente sobre la base de una orden emitida por un órgano jurisdiccional para la investigación de un delito. Solo podrá expedirse tal orden a los efectos de una investigación criminal. Esto supone que, en el sistema jurídico japonés, no se permite la recogida/el acceso a la información por medios obligatorios por razones de seguridad nacional. En cambio, en el ámbito de la seguridad nacional, los ministerios o agencias afectados solo pueden obtener información de fuentes de libre acceso o recibir información de los operadores económicos o de los particulares a través de la comunicación voluntaria. Los operadores económicos que reciban una solicitud de cooperación voluntaria no están obligados legalmente a facilitar dicha información y, por tanto, no tienen que afrontar ninguna consecuencia negativa si se niegan a cooperar.

Varios departamentos ministeriales y agencias tienen responsabilidades en el ámbito de la seguridad nacional.

1) Secretaría del Gabinete

La Secretaría del Gabinete lleva a cabo la recogida de información y la investigación sobre políticas importantes del Gabinete ⁽²⁸⁾ prescritas en el artículo 12-2, de la Ley del Gabinete ⁽²⁹⁾. Sin embargo, la Secretaría del Gabinete no está facultada para recoger información personal directamente de los operadores económicos. Recoge, incorpora, analiza y evalúa información de materiales de libre acceso, otras autoridades públicas, etc.

2) ANP/policía prefectural

En cada prefectura, la policía prefectural está facultada para recoger información dentro de su ámbito de competencia de conformidad con el artículo 2 de la Ley de Policía. Puede ocurrir que la ANP recoja directamente información en el ámbito de su competencia con arreglo a la Ley de Policía. Esto atañe, en particular, a las actividades de la Oficina de Seguridad y del Departamento de Asuntos Exteriores e Inteligencia de la ANP. De conformidad con el artículo 24 de la Ley de Policía, la Oficina de Seguridad se encarga de los asuntos relativos a la policía de seguridad ⁽³⁰⁾ y el Departamento de Asuntos Exteriores e Inteligencia se encarga de los asuntos relativos a los nacionales extranjeros, así como a los nacionales japoneses cuyas bases de actividad se encuentran en países extranjeros.

3) Agencia de Inteligencia en materia de Seguridad Pública (AISP).

La aplicación de la Ley de prevención de las actividades subversivas (LPAS) y la Ley sobre el control de las organizaciones que hayan cometido actos indiscriminados de asesinato masivo (LCO) son competencia principalmente de la Agencia de Inteligencia en materia de Seguridad Pública (AISP), adscrita al Ministerio de Justicia.

La LPAS y la LCO estipulan que pueden adoptarse disposiciones administrativas (es decir, medidas que ordenan la limitación de las actividades de dichas organizaciones, su disolución, etc.), en condiciones estrictas, contra las organizaciones que cometan determinados actos graves («actividades terroristas subversivas» o «actos indiscriminados de asesinato masivo») vulnerando la «seguridad pública» o el «sistema fundamental de la sociedad» en el marco de la Constitución. Las «actividades terroristas subversivas» están comprendidas en el ámbito de aplicación de la LPAS (véase el artículo 4, que abarca actividades como la insurrección, la instigación a la agresión extranjera, el homicidio con intención política, etc.), mientras que la LCO aborda los «actos indiscriminados de asesinato masivo» (véase el artículo 4 de la LCO). Solo las organizaciones identificadas con precisión que planteen amenazas específicas, internas o externas, para la seguridad pública pueden estar sujetas a las disposiciones de la LPAS o de la LCO.

Con este fin, la LPAS y la LCO confieren una autoridad jurídica de investigación. Los poderes de investigación fundamentales de los funcionarios de la AISP se establecen en el artículo 27 de la LPAS y en el artículo 29 de la LCO. Las investigaciones realizadas por la AISP en virtud de estas disposiciones se llevan a cabo en la medida en que sean necesarias con respecto a las disposiciones de control de las organizaciones a que se ha hecho referencia (por ejemplo, grupos radicales de izquierda, la secta *Aum Shinrikyo* y determinados grupos nacionales estrechamente vinculados a Corea del Norte han sido objeto de investigación en el pasado). Sin embargo, estas investigaciones no pueden sustentarse en medios obligatorios y, por lo tanto, una organización que posea información personal no puede verse obligada a facilitar dicha información.

La recogida y el uso de la información revelada a la AISP de forma voluntaria está sujeta a las salvaguardias y limitaciones pertinentes establecidas por la ley, como el secreto de las comunicaciones garantizado por la Constitución y las normas sobre el manejo de información personal con arreglo a la LPIPOA, entre otras.

4) Ministerio de Defensa (MdD);

En cuanto a la recogida de información por parte del Ministerio de Defensa (MdD), este recaba información sobre la base de los artículos 3 y 4 de la Ley para el establecimiento del Ministerio de Defensa en la medida necesaria para el ejercicio de sus competencias administrativas, incluidas las relativas a la defensa y la guardia, las medidas que deben tomar las Fuerzas de Autodefensa y el despliegue de las Fuerzas de Autodefensa terrestres, marítimas y aéreas. El MdD solo puede recoger información para estos fines a través de la cooperación voluntaria y de fuentes de libre acceso. No recoge información sobre el público en general.

2) Limitaciones y garantías

a) Limitaciones legales

1) Limitaciones generales basadas en la LPIPOA

La LPIPOA es una norma general aplicable a la recogida y el manejo de información personal por los órganos administrativos en cualquiera de sus ámbitos de actividad. Por lo tanto, las limitaciones y salvaguardas descritas en la sección II.A.1, letra b), número 2), se aplican también a la conservación, el almacenamiento, la utilización, etc., de la información personal en el ámbito de la seguridad nacional.

⁽²⁸⁾ Está dirigida por la Oficina de Inteligencia e Investigación del Gabinete, establecida con arreglo al artículo 4 de la Orden de organización de la Secretaría del Gabinete.

⁽²⁹⁾ Dichas funciones incluyen «la recogida y la investigación de información de inteligencia sobre políticas importantes del Gabinete».

⁽³⁰⁾ La policía de seguridad es responsable de las actividades de control de la delincuencia relacionadas con la seguridad pública y el interés de la nación. Esto incluye el control de la delincuencia y la recogida de información sobre actos ilegales relacionados con grupos de extrema izquierda, grupos derechistas y actividades perjudiciales contra Japón.

2) Limitaciones específicas aplicables a la policía (tanto a la ANP como a la policía prefectural)

Como se ha especificado anteriormente en la sección relativa a la recogida de información a efectos de aplicación de la ley, la policía solo puede recabar información en el ámbito de su competencia y, al hacerlo, podrá actuar, de conformidad con el artículo 2, apartado 2, de la Ley de Policía, en una medida «estrictamente limitada» al desempeño de sus funciones y de una manera «imparcial, no partidista, no prejuiciosa y equitativa». Por otra parte, sus poderes «nunca deberán ser objeto de abusos en modo alguno que pueda interferir con los derechos y libertades de una persona garantizados en la Constitución japonesa».

3) Limitaciones específicas aplicables a la AISP

Tanto el artículo 3 de la LPAS como el artículo 3 de la LCO disponen que las investigaciones realizadas en virtud de estos actos solo se llevarán a cabo en la medida mínima necesaria para alcanzar el objetivo perseguido y no se llevarán a cabo de forma que limite injustificadamente los derechos humanos fundamentales. Además, de conformidad con el artículo 45 de la LPAS y con el artículo 42 de la LCO, los abusos de autoridad por parte de un funcionario de la AISP constituyen un delito punible con sanciones penales más graves que los abusos de autoridad «generales» en otros ámbitos del sector público.

4) Limitaciones específicas aplicables al MdD

En cuanto a la recogida y la organización de información por el MdD, a las que hace referencia el artículo 4 de la Ley para el establecimiento del Ministerio de Defensa, la actividad de recogida de información del Ministerio se limita a la medida «necesaria» para el ejercicio de sus competencias relativas a 1) la defensa y la guardia, 2) las medidas que deben tomar las Fuerzas de Autodefensa y 3) las organizaciones, el número de efectivos, la estructura, el equipamiento y el despliegue de las Fuerzas de Autodefensa terrestres, marítimas y aéreas.

b) Otras limitaciones

Como se ha explicado anteriormente en la sección II.A.2, letra b), número 1), relativa a las investigaciones criminales, de la jurisprudencia del Tribunal Supremo se desprende que, para dirigir una solicitud de cooperación voluntaria a un operador económico, dicha solicitud debe ser necesaria para la investigación de un presunto delito y debe ser razonable para lograr el propósito de la investigación.

Aunque las investigaciones efectuadas por los servicios de investigación en materia de seguridad nacional y las realizadas por los servicios de investigación en el ámbito del control del cumplimiento de la ley difieren en lo que respecta tanto a su base jurídica como a su finalidad, los principios fundamentales relativos a la «necesidad de la investigación» y la «adecuación del método» se aplican de manera similar en el ámbito de la seguridad nacional y han de respetarse teniendo debidamente en cuenta las circunstancias específicas de cada caso.

La combinación de las limitaciones mencionadas garantiza que la recogida y el tratamiento de información tienen lugar únicamente en la medida necesaria para el desempeño de las funciones específicas de la autoridad pública competente, así como sobre la base de amenazas específicas. Quedan excluidas la recogida o el acceso masivos e indiscriminados de información personal por motivos de seguridad nacional.

B) Supervisión

1) Supervisión basada en la LPIPPOA

Como se ha explicado anteriormente en la sección II.B.2, en el sector público japonés, el ministro o el jefe de cada ministerio o agencia está investido del poder para supervisar y hacer cumplir la LPIPPOA en su ministerio o agencia. Además, el ministro del Interior y de Comunicaciones podrá investigar el estado de aplicación de la Ley, solicitar a cada ministro que presente materiales y explicaciones sobre la base de los artículos 49 y 50 de la Ley y enviar dictámenes a cada ministro sobre la base del artículo 51 de la Ley. Por ejemplo, puede solicitar la revisión de las medidas mediante los actos para los que está facultado en virtud de los artículos 50 y 51 de la Ley.

2) Supervisión de la policía por parte de las comisiones de seguridad pública

Como se ha explicado anteriormente en la sección «II. Recogida de información a efectos de la ejecución forzosa del Derecho penal», las comisiones prefecturales de seguridad pública, de naturaleza independiente, supervisan las actividades de la policía prefectural.

En lo que respecta a la Agencia Nacional de Policía (ANP), las funciones de supervisión son ejercidas por la Comisión Nacional de Seguridad Pública. De conformidad con el artículo 5 de la Ley de Policía, esta Comisión es responsable, en particular, de «la protección de los derechos y la libertad de los particulares». A tal fin, establecerá, en particular, políticas generales que regulen la gestión de los asuntos prescritos en cada inciso del artículo 5, apartado 4, de la Ley de Policía y otras orientaciones o medidas básicas que deben sustentar la realización de dichas actividades. La Comisión Nacional de Seguridad Pública (CNPS) tiene el mismo grado de independencia que las comisiones prefecturales de seguridad pública.

3) Supervisión del MdD por la Oficina de Cumplimiento Normativo de la Inspección General

La Oficina de Cumplimiento Normativo (OCN) de la Inspección General es una oficina independiente del Ministerio de Defensa, que está bajo la supervisión directa del ministro de conformidad con el artículo 29 de la Ley para el establecimiento del Ministerio de Defensa. La OCN puede llevar a cabo inspecciones relativas al cumplimiento de las leyes y reglamentos por parte de los funcionarios del MdD. Dichas inspecciones se denominan «inspecciones de Defensa».

La OCN realiza inspecciones desde el punto de vista de una oficina independiente con el fin de garantizar el cumplimiento normativo en todo el ministerio, incluidas las Fuerzas de Autodefensa (FA). Ejerce sus funciones con independencia de los departamentos operativos del MdD. Tras una inspección, la OCN informa sin demora de sus conclusiones, junto con las necesarias medidas de mejora, directamente al Ministerio de Defensa. Basándose en el informe de la OCN, el Ministerio de Defensa podrá dictar órdenes tendentes a la aplicación de las medidas necesarias para remediar la situación. El viceministro adjunto es responsable de la aplicación de estas medidas y debe informar al Ministerio de Defensa sobre el estado de dicha aplicación.

Como medida voluntaria de transparencia, las conclusiones de las inspecciones de Defensa se publican ahora en el sitio web del MdD (aunque la legislación no lo exija).

Existen tres categorías de inspecciones de Defensa:

- i) las inspecciones de Defensa ordinarias, que se realizan periódicamente ⁽³¹⁾;
- ii) las inspecciones de Defensa a efectos de control, que se llevan a cabo para comprobar si se han tomado efectivamente medidas correctoras; y
- iii) las inspecciones de Defensa especiales, que se centran en asuntos específicos por orden del ministro de Defensa.

En el contexto de estas inspecciones, el inspector general puede solicitar informes a la oficina en cuestión, solicitar la presentación de documentos, entrar en lugares para llevar a cabo la inspección, pedir explicaciones al viceministro adjunto, etc. Habida cuenta de la naturaleza de las tareas de inspección de la OCN, la oficina está presidida por expertos jurídicos de muy alto rango (antiguo fiscal superintendente).

4) Supervisión de la AISP

La AISP lleva a cabo inspecciones tanto periódicas como especiales sobre las operaciones de sus agencias y oficinas individuales (Agencia de Información de Seguridad Pública, Oficinas y Suboficinas de Información de Seguridad Pública, etc.). A efectos de la inspección periódica, se designa como inspector o inspectores a un director general adjunto o a un director. Las inspecciones también atañen a la gestión de la información personal.

5) Supervisión de la Dieta

En cuanto a la recogida de información a efectos de ejecución forzosa de la ley, la Dieta, a través de su comisión competente, puede examinar la legalidad de las actividades de recogida de información en el ámbito de la seguridad nacional. Los poderes de investigación de la Dieta se basan en el artículo 62 de la Constitución y en los artículos 74 y 104 de la Ley de la Dieta.

C. Reparación individual

La reparación individual puede obtenerse a través de las mismas vías que en el ámbito de la ejecución forzosa del Derecho penal. Esto incluye el nuevo mecanismo de reparación, administrado y supervisado por la CPIP para la tramitación y la resolución de las denuncias presentadas por particulares de la UE. A este respecto, véanse los pasajes pertinentes de la sección II.C.

Además, existen vías específicas de reparación individual en el ámbito de la seguridad nacional.

La información personal recogida por un órgano administrativo con fines de seguridad nacional está sujeta a las disposiciones del capítulo 4 de la LPIPOA. Esto incluye el derecho a solicitar la comunicación (artículo 12) y la rectificación (incluida la adición o la supresión) (artículo 27) de la información personal conservada de los particulares, así como el derecho a solicitar la suspensión de la utilización de la información personal en caso de que el órgano

⁽³¹⁾ Como ejemplo de una inspección pertinente respecto de las cuestiones cubiertas por esta Declaración, puede hacerse referencia a la inspección de Defensa ordinaria de 2016 con respecto a la «sensibilización/preparación para el cumplimiento normativo», ya que la protección de la información personal era uno de los puntos centrales de la inspección. Más concretamente, la inspección se refería a la situación de la gestión, el almacenamiento, etc. de la información personal. En su informe, la OCN señaló varios aspectos inadecuados en la gestión de la información personal que deben mejorarse, como la falta de protección de los datos a través de una contraseña. El informe puede consultarse en el sitio web del MdD.

administrativo haya obtenido de forma ilícita la información en cuestión (artículo 36). Dicho esto, en el ámbito de la seguridad nacional el ejercicio de esos derechos está sujeto a determinadas restricciones: las solicitudes de comunicación, rectificación o suspensión no se concederán cuando se refieran a «información sobre la cual existan motivos razonables para que el jefe de un órgano administrativo considere que la comunicación puede causar un perjuicio a la seguridad nacional, ocasionar daños a la relación de confianza mutua con otro país o una organización internacional, o causar una desventaja en las negociaciones con otro país u organización internacional» [artículo 14, inciso iv)]. Por lo tanto, no toda la recogida voluntaria de información relacionada con la seguridad nacional está afectada por la exención, ya que esta requiere siempre una evaluación concreta de los riesgos que conlleva su comunicación.

Por otra parte, si se rechaza la solicitud del particular alegando que la información en cuestión se considera no comunicable en el sentido del artículo 14, inciso iv), el particular puede interponer un recurso administrativo para la revisión de dicha decisión, alegando, por ejemplo, que en ese caso concreto no se cumplen las condiciones establecidas en el artículo 14, inciso iv). En tal caso, antes de tomar una decisión, el jefe del órgano administrativo correspondiente consulta al Consejo de revisión en materia de protección de la información personal y de la comunicación de información. El Consejo revisará el recurso desde un punto de vista independiente. El Consejo es un organismo muy especializado e independiente cuyos miembros son nombrados por el primer ministro, con el consentimiento de ambas Cámaras de la Dieta, de entre personas con un extraordinario conocimiento especializado ⁽³²⁾. El Consejo goza de fuertes facultades de investigación, entre ellas la posibilidad de solicitar documentos y la comunicación de la información personal en cuestión, de llevar a cabo deliberaciones internas y de aplicar el procedimiento del índice Vaughn ⁽³³⁾. A continuación, el Consejo elabora un informe escrito que se comunica al particular de que se trate ⁽³⁴⁾. Las conclusiones del informe se hacen públicas. Aunque el informe no es, en sentido estricto, jurídicamente vinculante, el órgano administrativo correspondiente cumple lo establecido en casi todos los informes ⁽³⁵⁾.

Por último, de conformidad con el artículo 3, apartado 3, de la Ley sobre resolución de litigios administrativos, el particular puede interponer una acción judicial para solicitar la revocación de la decisión tomada por el órgano administrativo de no comunicar la información personal.

IV. Revisión periódica

En el marco de la revisión periódica de la decisión de adecuación, la CPIP y la Comisión Europea intercambiarán información sobre el tratamiento de los datos con arreglo a las condiciones de la constatación de adecuación, incluidas las establecidas en la presente Declaración.

⁽³²⁾ Véase el artículo 4 de la Ley por la que se crea el consejo de revisión en materia de protección de la información personal y de la comunicación de información.

⁽³³⁾ Véase el artículo 9 de la Ley por la que se crea el consejo de revisión en materia de protección de la información personal y de la comunicación de información.

⁽³⁴⁾ Véase el artículo 16 de la Ley por la que se crea el consejo de revisión en materia de protección de la información personal y de la comunicación de información.

⁽³⁵⁾ En los últimos tres años no se ha producido ningún precedente en el que el órgano administrativo en cuestión haya tomado una decisión distinta de la contenida en las conclusiones del Consejo. Anteriormente, fueron muy pocos los casos en que esto ocurrió: solamente dos de un total de 2 000 casos en 2005 (año en el que entró en vigor la LPIPPOA). Cuando el órgano administrativo tome una determinación o decisión que difiera de las conclusiones del Consejo, de conformidad con el artículo 50, apartado 1, punto 4, de la Ley de revisión de las reclamaciones administrativas, tal como se ha aplicado con la sustitución del artículo 42, apartado 2, de la LPIPPOA, indicará claramente las razones de ello.